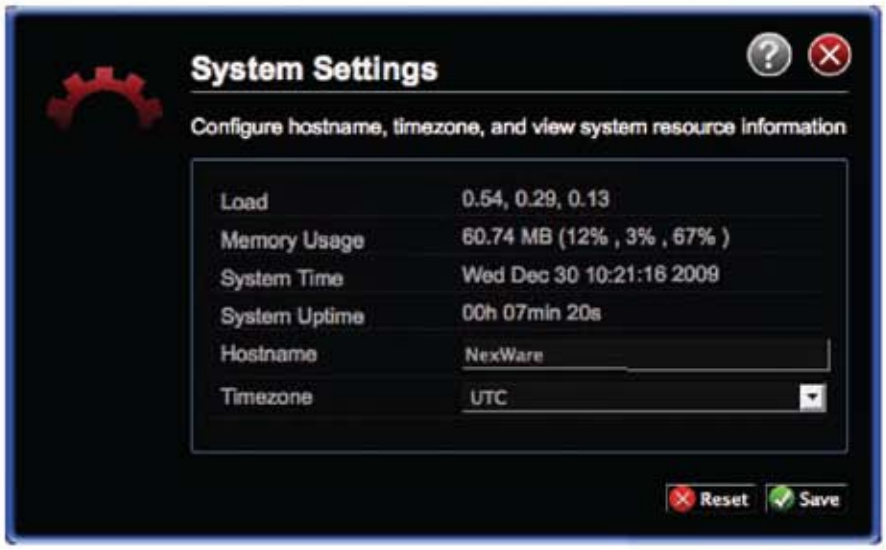
Tool Box

System Settings

- View system resource information such as load, memory usage, system time, and system up time.
- Configure the router Hostname and Timezone for logging timestamp.



Email Notifications

- Enable Email Notifications for certain router events.
- Choose to truncate system logs to the last 50 lines.
- Choose to be notified on:
  - Boot-up
  - Interface Failover
  - Interface Up/Down
- Input the name, Mail Domain, the To Address, the Mail Hub, Mail Port, Username, and Password
- Select Email Now to send the system log to the specified location now.

Glossary of Definitions

DHCP - Dynamic Host Configuration Protocol is a protocol used by networked devices (clients) to obtain the parameters necessary for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual configuration.

IP – Internet Protocol is a protocol used for communicating data across a packet switched Internetwork using the Internet Protocol Suite (TCP/IP).

LAN – Local Area Network is a computer network covering a small physical area, like a home, office, or small group of buildings, such as a school, or an airport. The defining characteristics of LANs, in contrast to wide-area networks (WANs), include their usually higher data-transfer rates, smaller geographic range, and lack of a need for leased telecommunication lines.

LAN IP – Local Area Network Internet Protocol varies depending on the hardware configuration. If the router is setup independently, not associated with other routers or other network hardware, the default settings are preferred. If the router is setup as part of a larger networking system, please refer to your system administrator for proper settings.

MAC - a Media Access Control address (MAC address) or Ethernet Hardware Address (EHA), hardware address, adapter address or physical address is a quasi-unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number.

Business Class II High Availability Router – Router which provides universal access to keep you connected anywhere on any network. Check Email, surf web, share music and photo files anytime. Integrated 802.11 b/g wireless data transfers with speeds up to 54 Mbps and wired data transfers up to 100 Mbps. Equipped with two Ethernet ports for LAN and WAN access, Type II PC card slot and USB port for 3G/4G network connections. For ExpressCards, a Universal adapter is available.

NexWare SM (The Nexaira in Communications Firmware and Software Management) – Provides a user with ease of use with its Industry defining Graphical User Interface (GUI). PoE - Power over Ethernet technology describes a system to transfer electrical power, along with data, to remote devices over standard twisted-pair cable in an Ethernet network. This technology is useful for powering IP telephones, wireless LAN access points, network cameras, remote network switches, embedded computers, and other appliances where it would be inconvenient, expensive (wiring must often be done by qualified and/or licensed electricians for legal or insurance reasons) or infeasible to supply power separately.

QoS – Quality of Service, High QoS of performance or achieved service quality for example high bit rate, low latency and low bit error probability.

Setup Wizard – Useful end user feature for advanced hardware configurations.

UPnP – Universal Plug and Play which allows the router to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and corporate environments. UPnP achieves this by defining and publishing UPnP device control protocols built upon open, Internet-based communication standards.

Technical Support

Nexaira provides free technical support for customers worldwide for the warranty period of one year on this product. For Nexaira Technical Support please visit our website: http://www.nexaira.com/

When contacting technical support, please provide the following information:
NOTE: All numbers referenced below can be found on the bottom of the router.

Model number or product name.
Serial number and MAC Address of the unit.
Firmware version
Defaulted IP

NOTE: The firmware version can be found by logging into the router and viewing the status page.

Technical Specifications

Access	1 ExpressCard Slot, 1 USB Port
Standards	IEEE 802.11 b/g/n IEEE 802.3u
Wireless Standard	IEEE 802.11 b/g/n
Wireless Data Rate	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Mbps, and 802.11n up to 300Mbps
Wireless Frequency	2.412 - 2.462 GHz CCK
Range Coverage	Tx/Rx power 27dbm indoors approx. 35-100 meters, outdoors up to 100-300 meters
# of Channels	1-11 for N. America (FCC); 1-11 for (DOC), 1-13 Europe (Except and ETSI), 1-14 (TELEC)
Security	64-bit and 128-bit WEP encryption, WPA encryption w/ WPA2 support, NAT (Networks Address Translation), VPN IPsec Pass Through, VPN IPsec Termination
Antenna	3.309 dbi
Supported WAN type	Static IP, Dynamic IP, PPPoE, PPTP, L2TP
Connection Scheme	Connect-on-demand, Auto-disconnect
NAT function	Class C; One-to-Many; Max 253 Users; Virtual Server; DMZ Host
VPN	PPTP, L2TP and IPSec Pass Through
Config. & Management	Web-Based IE, Nevigator browser and SNMP, DHCP Server and Client
Working Environment	Temperature: 0~40 C, Humidity 10%~90% non-condensing
OS Supported	Windows 95/98/ME/NT/2000/XP/VISTA/Windows 7, Linux, MAC
Adapter Power	Switching 12V 1.25A

2. Ensure that the settings on your NIC adapter are "Enabled" and set to accept an IP address from the DHCP. If settings appear to be correct, ensure that you are not using a crossover Ethernet cable. Although the Business Class II High Availability Router is MDI/MDIX compatible, not all NICs are. Therefore, it is recommended that you use a patch cable when possible.

3. The wireless connection keeps dropping.

1. Try different antenna orientations for the Business Class II High Availability Router.
2. Try to keep the antenna at least 6 inches away from the wall or other objects.
3. Try changing the channel on the Business Class II High Availability Router, your Access Point and Wireless interference.
4. Keep the Business Class II High Availability Router away (at least 3-6 feet) from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.
5. Move away from others.

4. I am unable to achieve a wireless connection.

NOTE: An Ethernet connection is required to troubleshoot the Business Class II Router. If you have enabled Encryption on the Business Class II Router, you must also enable encryption on all wireless clients in order to establish a wireless connection.

1. Ensure that the encryption level is the same for both the Business Class II High Availability Router and your Wireless Client. Ensure that the SSID (Service Set Identifier) on the Business Class II High Availability Router and the Wireless Client are exactly the same. If they are not, your wireless connection will not be established. Move the Business Class II High Availability Router and the wireless client into the same room, and then test the wireless connection.
2. Disable all security settings such as WEP, and MAC Address Control. Turn off the Business Class II High Availability Router and the client. Turn the Business Class II High Availability Router back on, and then turn on the client.
3. Ensure that the LED indicators are indicating normal activity. If not, ensure that the AC power and Ethernet cables are firmly connected.
4. Ensure that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network. If you are using 2.4GHz cordless phones, X-10 equipment, or other home security systems, ceiling fans, or lights, your wireless connection may degrade dramatically or drop altogether.
5. To avoid interference, change the Channel on the Business Class II High Availability Router and all devices in your network.
6. Keep your product at least 3-6 feet away from electrical devices that generate RF noise. Examples include: microwaves, monitors, electric motors, and so forth.

5. I do not remember my WiFi encryption key.

If you forgot your encryption key, you will not be unable to establish a proper connection. To reset the encryption key(s), login to the Router using a wired connection and modify the settings under Wi-Fi.

6. Reset the Business Class II High Availability Router to its factory default settings.

If other troubleshooting methods have failed, you may choose to Reset the Business Class II High Availability Router to its factory default settings. To reset the Business Class II High Availability Router to its factory default settings external to the router's GUI, follow the steps listed below:

1. Ensure the Business Class II High Availability Router is powered on.
2. Locate the Reset button on the back of the Wireless WAN Mobile Broadband Router.
3. Use a paper clip to press the Reset button.
4. Hold for 2 seconds and then release.
5. The Business Class II High Availability Router will re-boot with the factory default settings.

NOTE: Please note that this process will take a few minutes.

7. My Ethernet cable does not work properly.

1. Ensure that there is a solid cable connection between the Ethernet port on the Router and your NIC (Network Interface Card).

Troubleshooting

This section provides an overview of common issues, with solutions for the installation and operation of the Business Class II High Availability Router.

1. I am unable to access the Configuration Menu when I use my computer to configure the router.

It is recommended that you use an Ethernet connection to configure the Business Class II High Availability Router. Ensure that the LAN LED on the Business Class II High Availability Router is Blue. If the LAN is NOT blue, check to ensure if the cable for the Ethernet connection is securely inserted. Ensure that the IP Address assigned to the computer is in the same range and subnet as the Business Class II High Availability Router. NOTE: The default IP Address of the Business Class II High Availability Router is 192.168.1.1. All computers on the network must have a unique IP Address within the same range (e.g., 192.168.1.x). Any computer that has an identical IP Addresses will not be visible on the network. All computers must also have the same subnet mask (e.g.,255.255.255.0). Do a Ping test to 192.168.1.1 to make sure that the Business Class II High Availability Router is responding.

Go to **Start > Run** (Windows XP)

1: Type cmd

2: Select Enter

3: Type "ping 192.168.1.1" without the " " (A successful ping shows four replies). Note: If you have changed the default IP Address, ensure you ping the correct IP Address assigned to the Business Class II Router. Ensure that your Ethernet Adapter is working properly, and that all network drivers are installed properly. NOTE: Network adapter names will vary depending on your specific adapter. The installation steps listed below are applicable for all network adapters.

1. Go to Start > My Computer > Properties (Windows XP)
2. Select the Hardware Tab.
3. Click Device Manager.
4. Double-click on "Network Adapters".
5. Right-click on Wireless Cardbus Adapter, or your specific network adapter.
6. Select Properties to ensure that all drivers are installed properly.
7. Look under Device Status to see if the device is working properly.
8. Click "OK"

2. My wireless client can't access the Internet.

If you select either WEP, WPA-PSK, or WPA2-PSK encryption on Business Class II High Availability Router, ensure encryption settings match your WiFi settings on the computer. Please refer to your WiFi adapter documentation for additional information. Ensure that the wireless client is associated and joined with the correct Access Point. To check this connection, follow the steps below:

1. Right-click on the Wireless Network Connection icon in the Windows taskbar.
2. Select View Available Wireless Networks in Wireless Configure. The Connect to Wireless Network screen appears. Ensure you have selected the correct available network. Ensure the IP Address assigned to the wireless adapter is within the same subnet as the Access Point and gateway. The Business Class II High Availability Router has an IP Address of 192.168.1.1 Wireless adapters must have an IP Address in the same range (e.g., 192.168.1.x). The subnet mask must be the same for all the computers on the network, but two devices may have the same IP Address. Therefore, each device must have a unique IP Address.

Internet Failover

Internet Failover is a feature that provides failover from your primary internet connection, to your secondary internet connections when your primary connection fails.

- Choose to enable Internet Failover
- Choose Primary and Backup interfaces
- Choose to keep the backup connection alive
- Choose Failover and Switchback times
- Input Test IP names for connection testing
- Choose the number of seconds between each ping for connection testing.

Port Forwarding

Port forwarding allows a port or range of ports to be opened to inbound traffic. That traffic is then forwarded to a LAN host on a specified port or range of ports.

Adding an entry will insert fields requiring additional information to configure this feature.

- Insert Name (optional)
- Choose Protocol, TCP, UDP, or TCP+ UDP.
- Insert port number or range of ports (first-last) for external device.
- Select internal IP-address.
- Select internal port or range. (optional)

NOTE: After any changes, select "Save" to retain. System will refresh following, "Save".

VRRP

Virtual Router Redundancy Protocol (VRRP) is an open source router redundancy protocol as specified in RFC 3768. It is designed to provide gateway redundancy across multiple routers on the same subnet. It is important to note that this feature provides redundancy for routing functions only, and does not include other LAN functions such as DHCP.

NOTE: After configuring VRRP, the router must be rebooted before VRRP takes effect. The following configuration options are available:

- Enable Check Box: Enable or disable the VRRP feature.
- **ID:** The ID value of the router, a range of 1 through 254.
- **Priority:** This is the priority of the router in the VRRP chain; 254 is always master. The higher the value, the higher the priority of the device.
- **IP Address:** This is the virtual router IP address. By default it should match your primary gateway's LAN IP address. All VRRP routers on the subnet must utilize the same virtual router IP address.
- **Interval:** This is the interval by which VRRP registration messages are sent via broadcast and gratuitous ARP.

RIP

This feature allows use of RIP protocol over the selected RIP device. RIP Version 1 or Version 2 can be selected. Additional entries can also be added.

NOTE: After any changes, select "Save" to retain. System will refresh following, "Save".

DMZ Host

DMZ allows all traffic to be forwarded to one host on the LAN provided there are no other port forwarding rules that will effect that traffic.

- Check the enable box
- Type in the IP Address on LAN to be placed in DMZ.

NOTE: After any changes, select "Save" to retain. System will refresh following, "Save".

SSH Server

- Enable remote shell access
- Choose the port
- Select connection criteria:
  - Allow SSH access remotely
  - Choose to allow only listed IP addresses
  - Choose to allow authentication

SSH Keys

Insert Keys for public-key authentication.

Routing Settings

Routes

Active IPv4-Routes

- View current routes for the datacard, LAN

Static IPv4 Routes

- **Add entry:** Adding an entry inserts fields which require additional information.
- **Interface:** Set interface (LAN, datacard)
- **Target:** Select Target (Host-IP or Network).
- **IPv4-Netmask:** Select IPv4-Netmask (only if target is a network).
- **IPv4-Gateway:** Select IPv4-Gateway.

NOTE: After any changes, select "Save" to retain. System will refresh following, "Save".

Security Settings

Remote Admin

This feature allows you to enable administrative remote access to the router. You can choose the default port of 8080, or assign any other valid port.

NOTE: Many internet service providers block activity on certain ports, please consult with your ISP. After any changes, select "Save" to retain. System will refresh following, "Save".

IPsec

IP Security (IPSec) is a suite of protocols for transmitting encrypted IP data securely. This function is performed by authenticating and securing each packet from source to destination. The Business Class II router supports IPSec in tunnel mode, with multiple configuration options for authentication and encryption. Two concurrent IPSec tunnels utilizing AES encryption are supported in your router. The following configuration options are available:

- **Enable Check Box:** This checkbox will enable or disable the IPSec tunneling feature.
- **Initiate Tunnel:** Choose when tunnel is initiated.
- **Key Exchange Method:** Choose encryption key exchange method.
- **Local LAN Network:** Enter the Network and subnet in network prefix notation of your LAN.
- **Remote LAN IP:** Enter the LAN gateway IP address of the LAN you wish to connect to.
- **Remote LAN Network:** Enter the Network and subnet in network prefix notation of the LAN you wish to connect to
- **WAN IP Address:** Your router's public WAN IP address, either from Ethernet or should be entered here.
- **Integrity:** Choose integrity type.
- **Encryption Algorithm:** Choose encryption algorithm.
- **DH Group:** Choose DH group
- **Strict Negotiation**: Choose to use only above settings.
- **Pre-Shared Key**: Enter your chosen PSK value in this field.
- **Add Entry**: Choose to add an entry.

QoS

Quality of Service settings provide a mechanism to provide prioritization of certain types of traffic over other types of traffic. Disable by default, QoS can be enabled as necessary

- Downlink and Uplink speeds can be modified for WAN connection.
- Prioritization. This section allows for the following choices:
  - **Set Priority:** Low, normal, express, or priority
  - **Source address:** Select from detected sources.
  - **Target Address:** Select detected targets.
  - **Service:** Select Service option.
  - **Protocol:** Select internet protocol.
  - **Ports:** Enter ports.
  - **Bites sent**

NOTE: After any changes, select "Save" to retain. System will refresh following, "Save".

Dynamic DNS

The Dynamic DNS feature enables the router to interface directly with DDNS service providers to update your WAN IP address when it changes. Dynamic DNS maps the name of your DDNS host to your current WAN IP address. Before you enable Dynamic DNS, you need to register an account on one of the Dynamic DNS servers listed in the Service field. To enable Dynamic DNS click the check box next to Enable. Next enter the appropriate information about your Dynamic DNS Server.

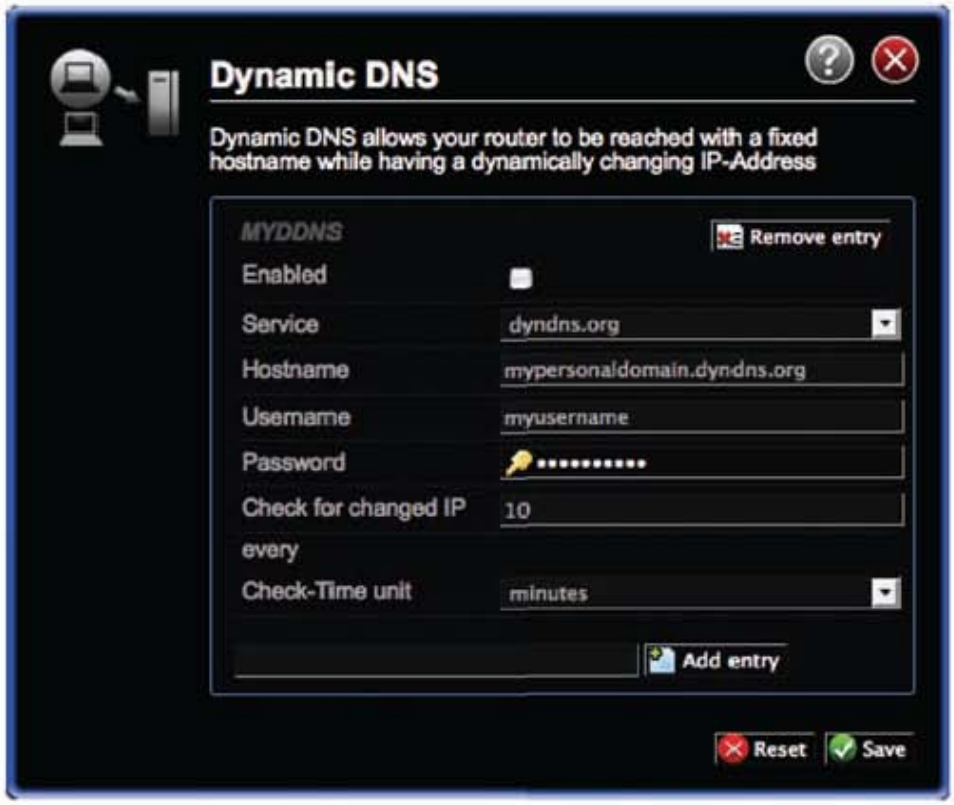
You have to define:

- Service
- Hostname
- Username
- Password

Additional controls of the Dynamic DNS server include:

- Check for changed IP every – Enter numeric value
- Check-Time unit – Select a unit of time from the list
- Add additional entry(ies).

NOTE: This information is established when you register an account on a Dynamic DNS server. After any changes, select "Save" to retain. System will refresh following, "Save".



Advanced Settings

DHCP Server

Here you can change whether the DHCP server is enabled, view current Active Leases, and assign Static DHCP Leases to other devices.

- Change first available lease number
- Change the total number of leases available
- Change the duration of an active lease (h = hours)
- Assign Static DHCP leases to other devices

NOTE: After any changes, select "Save" to retain. System will refresh following, "Save".

SNMP

Simple Network Management Protocol (SNMP) is used in conjunction with a network management system to monitor specified network devices for defined events and activities. Those activities are defined in a Management Information Base (MIB).

Your router supports a light implementation of SNMP with a defined MIB. The following configuration options are available:

- **Enable Check Box:** This box will enable or disable the SNMP feature.
- **Community Name:** Specify the community name for your SNMP neighborhood.
- **Device Description:** An optional field to give the device a description upon SNMP query.
- **Location Name:** An optional field to list the device's location.
- **Administrator Email:** An optional field to input the network administrator's email contact information.
- **LAN, WAN, and 3G/4G checkboxes:** Enable or disable reporting of these interfaces upon SNMP query.

System Log

View the System Log file.

Flash Firmware

- Browse and select the firmware upgrade file from a selected location.
- Choose to keep current or overwrite with new firmware configuration.
- Select Flash Firmware to flash selected firmware file.
    - Router will upload selected file, flash the new firmware, and reboot to the login screen upon completion.

Backup Interfaces

- Create a backup file of current settings to a selected location.
- Restore: Select a previously saved backup file by browsing to the file location and then clicking "Restore backup".

Reset to Defaults

- This feature will reset the router to factory defaults.

Reboot

- This feature will Reboot the router.

VPN – Virtual Private Network is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The linklayer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption.

WAN – Wide Area Network are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations.

WAN IP – Wide Area Network Internet Protocol can vary depending on hardware configuration. If the router is setup independently, not associated with other routers or other network hardware, the default settings are preferred. If the router is setup as part of a larger networking system, please refer to your system administrator for proper settings.

WAP – Wireless Application Protocol is an open international standard for application layer network communications in a wireless communication environment. Its main use is to enable access to the Internet (HTTP) from a mobile phone or PDA.

WEP – Wired Equivalent Privacy is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio and are thus more susceptible to eavesdropping than wired networks.