



Ubee DDW36C Advanced Wireless Gateway

Firmware Version: 8.22.2111

Subscriber User Guide Time Warner Cable



October 2015

www.ubeeinteractive.com
8085 S. Chester Street, Suite 200
Englewood, CO 80112
1.888.390.8233
Sales (email): amsales@ubeeinteractive.com
Support (email): amsupport@ubeeinteractive.com

Notices and Copyrights

Copyright 2015 Ubee Interactive. All rights reserved. This document contains proprietary information of Ubee and is not to be disclosed or used except in accordance with applicable agreements. This material is protected by the copyright laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Ubee), except in accordance with applicable agreements, contracts, or licensing, without the express written consent of Ubee and the business management owner of the material.

Ubee Interactive continuously improves its products and reserves the right to make changes to the product described in this document without notice. Ubee Interactive does not assume any liability that may occur due to the use of the product described in this document.

All trademarks mentioned in this document are the property of their respective owners.

This device is Wifi Alliance Certified:



Contents

1	Introduction	1
1.1	Understanding Safety and Regulatory Information	1
1.2	Understanding Connections and Applications	3
1.3	Requesting Support	3
1.4	Checking Device Package Components	4
1.5	Understanding the Device Panels, Connections and LEDs	5
1.6	Understanding Specifications, Standards, and Firmware	7
1.7	Understanding Default Values and Logins	9
1.8	Understanding the Device Label	10
2	Installing the DDW36C	12
2.1	Setting Up and Connecting the DDW36C	12
2.2	Connecting Devices to the Network	15
2.3	Troubleshooting the Installation	17
3	Using the Web User Interface	19
3.1	Accessing the Web User Interface Locally	19
3.2	Logging Out of the Web User Interface	21
4	Understanding the Status Menu	22
4.1	Using the Software Option	22
4.2	Using the Connection Option	23
4.3	Using the Account Option	26
4.4	Using the Diagnostics Option	26
4.5	Using the Client List Option	29
4.6	Using the User Default Option	31
5	Understanding the Basic Menu	32
5.1	Using the Setup Option	32
5.2	Using the DHCP Option	34
5.3	Using the DHCPv6 Option	36
5.4	Using the LAN IPv6 Option	38
5.5	Using the DDNS Option	39
5.6	Using the Static Lease Option	40
5.7	Using the Backup Option	41
5.8	Using the Time Option	45
6	Understanding the Advanced Menu	47
6.1	Using the Options Option	47
6.2	Using the IP Filtering Option	50
6.3	Using the MAC Filtering Option	51
6.4	Using the Port Filtering Option	52
6.5	Using the Forwarding Option	54
6.6	Using the Port Triggers Option	59
6.7	Using the Pass Through Option	60
6.8	Using the DMZ Host Option	61

7	Understanding the Firewall Menu	63
7.1	Using the Basic Option	63
7.2	Using the Local Log Option	64
7.3	Using the Remote Log Option	65
8	Understanding the Parental Control Menu	67
8.1	Using the Parental Control User Setup Option	67
8.2	Using the Basic Option	69
8.3	Using the ToD Filter Option	71
8.4	Using the Local Log Option	72
9	Understanding the Wireless Menu	74
9.1	Selecting the Wireless Radio Band	74
9.2	Using the Wireless Radio Option	75
9.3	Using the Primary Network Option	77
9.4	Using the Access Control Option	82
9.5	Using the Wi-Fi Multimedia Option	84
9.6	Using the Wireless Bridging Option	86
9.7	Deploying and Troubleshooting the Wireless Network	87
10	Understanding the MoCA Menu	93
10.1	Using the MoCA Software Option	93
11	Glossary	95

1 Introduction

Welcome to the Ubee family of data networking products. This guide is specific to the **DDW36C Advanced Wireless Gateway** for subscribers of **Time Warner Cable** and serves the following purposes:

- ❑ Provides instructions on how to install, connect and operate the DDW36C.
- ❑ Provides directions for accessing the Web user interface (UI) for configuration and management of the device.
- ❑ Defines all relevant device compliance standards and physical specifications.
- ❑ Provides a glossary to define technical terms and acronyms. Refer to the [Glossary on page 95](#).



Topics

See the following topics:

- ❑ [Understanding Safety and Regulatory Information on page 1](#)
- ❑ [Understanding Connections and Applications on page 3](#)
- ❑ [Requesting Support on page 3](#)
- ❑ [Checking Device Package Components on page 4](#)
- ❑ [Understanding the Device Panels, Connections and LEDs on page 5](#)
- ❑ [Understanding Specifications, Standards, and Firmware on page 7](#)
- ❑ [Understanding Default Values and Logins on page 9](#)
- ❑ [Understanding the Device Label on page 10](#)

1.1 Understanding Safety and Regulatory Information

Use the following information to better understand safety and regulatory standards to install, maintain, and use the DDW36C Advanced Wireless Gateway.

1.1.1 Understanding Safety

WARNING: The following information provides safety guidelines for anyone installing and maintaining the DDW36C. Read all safety instructions in this guide before attempting to unpack, install, operate, or connect power to this product. Follow all instruction labels on the device itself. Comply with the following safety guidelines for proper operation of the device.



Follow basic safety precautions to reduce the risk of fire, electrical shock, and injury. To prevent fire or shock hazard, do not expose the unit to rain and moisture or install this product near water. Never spill any form of liquid on or into this product. Do not use liquid cleaners or aerosol cleaners on or close to this product. Clean with a soft dry cloth.



Do not insert sharp objects into the product's module openings or empty slots. Doing so can accidentally damage its parts and/or cause electric shock.

Electrostatic discharge (ESD) can permanently damage semiconductor devices. Always follow ESD-prevention guidelines for equipment handling and storage.

Use only the power cable supplied with the device. Do not attach the power supply cable to building surfaces or floorings.

- ☐ Rest the power cable freely without any obstacles. Do not place heavy items on top of the power cable. Do not abuse, step, or walk on the cable.
- ☐ Do not place heavy objects on top of the device. Do not place the device on an unstable stand or table; the device can fall and become damaged.
- ☐ Place the device on a cool surface. Failure to do so may result in overheating which can cause damage to the unit or to furniture.
- ☐ Do not block the slots and openings in the module housing that provide ventilation to prevent overheating the device. Do not expose this device to direct sunlight. Do not place hot devices close to this device; it may degrade it or cause damage.

1.1.2 Understanding Eco-Environmental Statements

The following eco-environmental statements apply to the DDW36C.

Packaging Collection and Recovery Requirements:

Countries, states, localities, or other jurisdictions may require that systems be established for the return and/or collection of packaging waste from the consumer, or other end user, or from the waste stream. Additionally, reuse, recovery, and/or recycling targets for the return and/or collection of the packaging waste can be established. For more information regarding collection and recovery of packaging and packaging waste within specific jurisdictions, contact Ubee Interactive at www.ubeeinteractive.com.

1.1.3 Understanding Regulatory Statements

The following regulatory statements apply to the DDW36C.

Industry North America Statement:

This device complies with RSS-210 of the Industry North America Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.

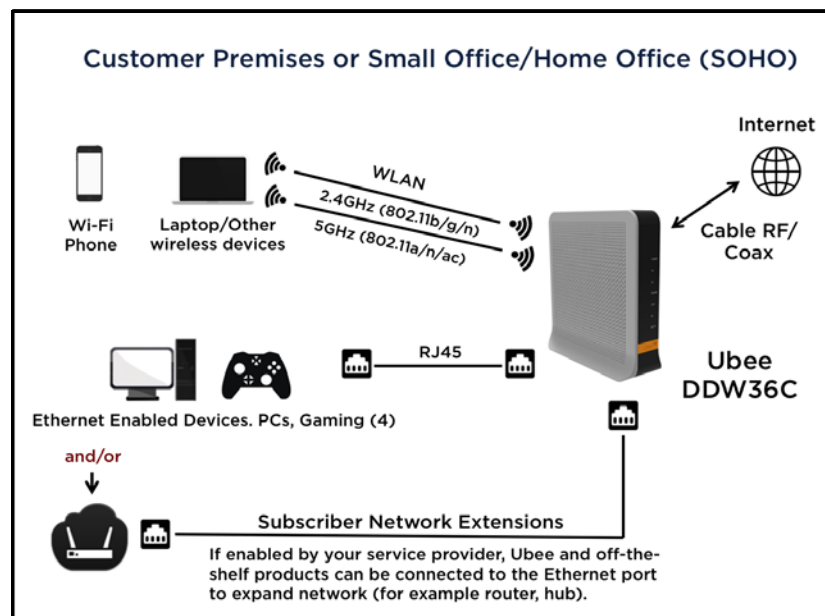
- (2) This device must accept any interference received, including interference that may cause undesired operation.

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between itself and your body. This device must not be co-located with or operating in conjunction with any other antenna or transmitter.

1.2 Understanding Connections and Applications

The following diagram illustrates the general connection topology and applications of the DDW36C.



1.3 Requesting Support

Contact your service provider (Time Warner Cable) for direct support. Device documentation support may be available at:

<http://www.ubeeinteractive.com>

1.4 Checking Device Package Components

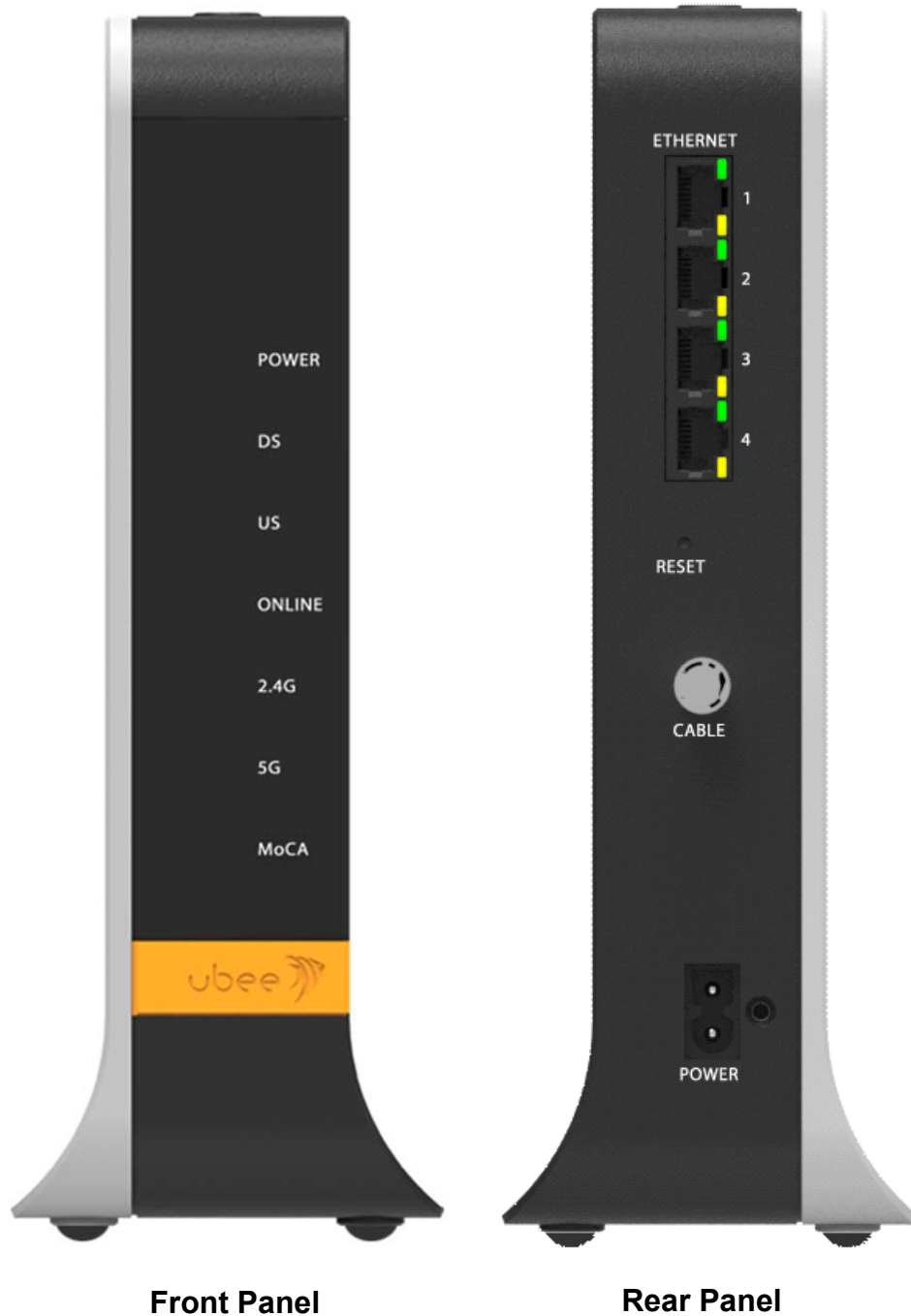
The package for the DDW36C contains the following items:

Item	Description
	1 - RJ45 Cable (Ethernet) Length ~ 5.0 ft RoHS & UL compliant <i>Sample image, actual appearance subject to change.</i>
	1 - Power Cable Input: 90-120VAC, 50-60Hz, 0.9A Max. CE and UL Certified <i>Sample image, actual appearance subject to change.</i>

1.5 Understanding the Device Panels, Connections and LEDs

1.5.1 Understanding the Device Front and Rear Panels

The following images represent the DDW36C front and rear panels. Connection descriptions are provided in section 1.5.3., and LED descriptions are provided in section 1.5.4.



1.5.2 Understanding the Device Connections

The following table describes the connections on the device.

Item	Description
ETHERNET 1 - 4	Connects to Ethernet devices such as computers, gaming consoles, and/or routers/hubs using an RJ45 cable. Each ETHERNET port on the back panel of the device has an LED to indicate its status when an Ethernet device is connected.
RESET	Restores the settings of the device including wireless and custom gateway settings. Use a pointed object to push down the reset button until the power LED turns off. After the power LED turns off, release the button.
CABLE	Connects to the cable outlet (with the cable provided by your service provider), or a cable splitter connected to the cable outlet.
POWER	Connects the power cable to the device. Use only the power cable provided with the DDW36C.
WPS	Located on top of the cable modem, this button is used for the WiFi Protected Setup (WPS) method to connect a PIN-protected WiFi device to the cable modem. Refer to Understanding the Wireless Menu on page 73 for more information.

1.5.3 Understanding LED Behavior

The following tables summarize the behavior of the LEDs on both the front and rear panels of the DDW36C.

FRONT PANEL		
LED	Color	Description
POWER	Blue	On – Internal power-on completed successfully. Flashes – Power-on failed. Note that the LED blinks briefly immediately after powering on the device.
DS (downstream)	Blue	Flashes – Once every second while scanning DS. Once locked on DS, flashes twice every second while registering the DS. On – Locked to DS channel and registered OK. Flashes – When a firmware upgrade is in progress, and POWER LED and ONLINE LEDs are ON solid.
US (upstream)	Blue	Flashes – Once every second while scanning US. Once locked on US, flashes twice every second while registering the US. On – Locked to US channel and registered OK. Flashes – When a firmware upgrade is in progress, and POWER LED and ONLINE LEDs are ON solid.
ONLINE	Blue	Flashes – Obtaining an IP address and configuration file. On – Configuration completed successfully, network connected. Off – Network connect failed.
2.4G	Blue	On – 2.4G WiFi is enabled. Off – 2.4G WiFi is disabled.

FRONT PANEL		
LED	Color	Description
5G	Blue	On – 5G WiFi is enabled. Off – 5G WiFi is disabled.
MoCA	Blue	On – The device is connected to a MoCA network. Off – The device is not connected to a MoCA network.
WPS BUTTON (top of device)	White	If not used, the LED is off. When a user pushes the WPS button or triggers WPS via the device's Web UI, an LED on the top-front of the device blinks for 4 minutes until a PIN is entered from the wireless client that wishes to connect (for example, a laptop computer). After a WiFi client attaches successfully, the LED remains On for 5 minutes, then turns Off.

REAR PANEL		
LED	Color	Description
ETHERNET 1-4	Green/ Orange	On Green – An Ethernet device is connected to the device at 1000 Mbps speeds (Gigabit Ethernet). On Orange – An Ethernet device is connected to the device at 10/100 Mbps speeds. Flashes (in Green or Orange) – When data is being passed between the cable modem and the connected device. The Ethernet ports are used to connect Ethernet devices such as computers, gaming consoles, and/or routers/hubs to the DDW36C using RJ-45 cables. Each Ethernet port on the back panel of the device has an LED to indicate its status when an Ethernet device is connected. 

1.6 Understanding Specifications, Standards, and Firmware

The following list provides the features and specifications of the DDW36C.

Interfaces and Standards

- ☐ Cable: F-Connector, female
- ☐ LAN: 4 10/100/1000 Mbps RJ45 ports
- ☐ DOCSIS 3.0 certified
- ☐ DOCSIS 1.0/1.1/2.0 certified
- ☐ CE/FCC Class B, ENERGY STAR® certified, WiFi Alliance certified

Downstream*

- ◆ Frequency Range: 88MHz ~ 1002MHz
- ◆ Modulation: 64 / 256 QAM
- ◆ Channel Bandwidth: 6 MHz
- ◆ Maximum Data Rate per Channel (up to 16 channels): DOCSIS = 30 Mbps (64 QAM), 42 Mbps (256 QAM),
- ◆ Total Max Bandwidth (16 Channels): DOCSIS = 686 Mbps
- ◆ Symbol Rate: 5361 Ksps
- ◆ RF (cable) Input Power: -15 to +15dBmV (64 QAM), -15 to +15dBmV (256 QAM)
- ◆ Input Impedance: 75 Ω

Upstream*

- ◆ Frequency Range: 5MHz ~ 42MHz
- ◆ Modulation A-TDMA: QPSK, 8, 16, 32, 64QAM, S-CMDA: QPSK, 8, 16, 32, 64, 128QAM
- ◆ Max Bandwidth of 4 Channels = 122.88 (108) Mbps, bandwidth per channel (up to 4 channels) = [QPSK 0.32 ~ 10.24 Mbps, 8 QAM 0.48 ~ 15.36 Mbps, 16 QAM 0.64 ~ 20.48 Mbps, 32 QAM 0.80 ~ 25.60 Mbps, 64 QAM 0.96 ~ 30.72 Mbps, 128 QAM/TCM 30.72 Mbps]
- ◆ Symbol Rate: 160, 320, 640, 1280, 2560, 5120 Ksps
- ◆ RF (cable) Output Power: TDMA/ATDMA: +8dBmV to +54dBmV (32/64 QAM). ATDMA Only: +8dBmV to +55dBmV (8/16 QAM), +8dBmV to +58dBmV (QPSK). S-CDMA: +8dBmV to +53dBmV (all modulations)

*Actual speeds vary based on factors including network configuration and speed.

Wireless, Security and Network

- ◆ Supports 8 SSIDs per radio, 802.11b/g/n/ac compliant with link speeds up to AC1900 WiFi (600Mbps @ 2.4GHz + 1300Mbps @ 5GHz), beam forming technology and high powered amplifiers to extend WiFi range, 3 Tx and 3 Rx antennas with dual-band concurrent, high power radios
- ◆ DHCP Client/Server, Static IP network assignment, RIPv1/ v2, Ethernet 10/100/1000 BaseT, full-duplex auto-negotiate functionality, IPv4 and IPv6 support
- ◆ NAT Firewall, MAC/IP/port filtering, parental control, stateful packet inspection (SPI), DoS attack protection, WPS/ WPA/ WPA2/ WPA-PSK & 64/128-bit WEP encryption
- ◆ VPN pass-through and VPN end-point support (IPSec/L2TP/PPTP), TACACS or RADIUS authentication

Device Management

- ◆ Supports IEEE 802.11e Wi-Fi Multimedia (WMM) and UAPSD (power savings)
- ◆ DOCSIS, Web-Based, and XML Configuration
- ◆ Telnet/SSH remote management
- ◆ Firmware upgrade via TFTP
- ◆ Configuration backup and restore
- ◆ SNMP support
- ◆ TR-069 capable

Physical and Environmental

- ◆ Dimensions: 1.77" (45mm) x 8.85" (225mm) x 9.45" (240mm)
- ◆ Weight: 800g (1 lb, 14 oz) (Contains internal PSU)
- ◆ Input: 90-120VAC, 50-60Hz
- ◆ Output: 12V 2.92A
- ◆ Operating Temperature: 0°C ~ 40°C (32°F ~ 104°F)
- ◆ Humidity: 5~90% (non-condensing)

1.7 Understanding Default Values and Logins

The DDW36C is pre-configured with the default parameters for Time Warner Cable.

Local Port Address: 192.168.100.1

Web Interface: <http://192.168.100.1>

Operation Mode: NAT Mode

Subnet Mask: 255.255.255.0

Wireless Defaults:

- ◆ Primary SSID (wireless network name) = "WIFI" plus the last 6 characters of the Cable Modem (CM) MAC address. "-5G" is added when the 5GHz band is being used.
 - ❖ Examples:
 1. 2.4G radio with CM MAC address 0071CC8E54C7
SSID: WIFI8E54C7
 2. 5G radio with CM MAC address 0071CC8E54C7
SSID: WIFI8E54C7-5G
 - ❖ If you change the SSID, the device does not revert to this default SSID when the device is power reset, except when a manual reset is performed through the Web UI.
 - ❖ The MAC address can be found on the device label or it can be found by opening an Internet browser window to the device. Refer to [Using the Software Option on page 19](#) for instructions.
- ◆ Security and Encryption Methods = WPA2-PSK with AES encryption
- ◆ WPA Pre-shared Key (PSK) = Unique key for each device. Also called the network key or the wireless password. The WPA pre-shared key is a randomly generated character string, 16 characters in length. It can be found on the device label and on the Wireless Primary Network screen. Refer to [Using the Primary Network Option on page 99](#).
 - ❖ Example WPA PSK: HP3WZ7IHXCT6D9QS
- ◆ WPS PIN = The WPS PIN is a randomly-generated number. It can be found on the device label and on the Wireless Primary Network screen. Refer to [Using the Primary Network Option on page 76](#).
- ◆ Device Name: UbeeAP

Login Default Values

◆ Standard User Web Interface Login

Username: admin

Password: <random password>

❖ Example password: oF?47Hc%*;hZ

(The random password can be found on the device label)

1.8 Understanding the Device Label

The following is an example of the housing label for the DDW36C. Descriptions are provided in the table below.



Item	Description
CABLE RF MAC Address	Displays the MAC address of the RF interface of the device.
WAN-MAN MAC Address	Displays the address of the cable home interface of the device.
S/N	Displays the serial number of the device.
SSID	The first SSID displays the SSID (service set identifier), or the wireless network name, for the 2.4GHz wireless band. See Understanding Default Values and Logins on page 9 for more information.
SSID	The second SSID displays the SSID (service set identifier), or the wireless network name, for the 5GHz wireless band. See Understanding Default Values and Logins on page 9 for more information.

Item	Description
GUI access URL	Displays the URL or web address to use when accessing the Web User Interface to configure the device. See Accessing the Web User Interface Locally on page 19 for more information.
GUI username	Displays the username to be entered when accessing the Web User Interface for the device.
GUI password	Displays the random password to be entered when accessing the Web User Interface for the device.
WPA2-PSK	Displays the unique WPA pre-shared key for the device. It is also called the network key, the wireless key, or the wireless password.
WPS PIN	A randomly generated 8-digit number in accordance with the WPS specification.
H/W Version	Displays the internal version number that identifies the hardware design.
DC	DC (Date Code) indicates the date of manufacture.
ASSEMBLED IN	Displays the country in which the device was assembled.

2 Installing the DDW36C

Use the information in this chapter to set up and connect the DDW36C, connect additional devices, and troubleshoot the installation.



Topics

See the following topics:

- ◆ [Setting Up and Connecting the DDW36C on page 12](#)
- ◆ [Connecting Devices to the Network on page 15](#)
- ◆ [Troubleshooting the Installation on page 17](#)

2.1 Setting Up and Connecting the DDW36C

Use the following instructions to set up and connect the DDW36C. When the device is set up and connected, refer to [Accessing the Web User Interface Locally on page 15](#) to configure the device.

Important: You must contact your service provider (Time Warner Cable) to enable Internet access and wireless networking.

Typically, your service provider initially configures and connects the device. The installation steps are provided below if you wish to confirm the setup, or add devices to your network. Refer to [Connecting Devices to the Network on page 15](#).



Steps

To set up the device:

3. Remove the contents from the device packaging.
4. Place the DDW36C in the best location to connect to other devices, such as PCs or gaming consoles.
 - ◆ Place the DDW36C and wireless clients in open areas far away from transformers, heavy-duty motors, microwave ovens, refrigerators, fluorescent lights, and other manufacturing equipment. These items can impact wireless signals. A wireless signal can become weaker after it has passed through metal, concrete, brick, walls, or floors.
 - ◆ Place the device in a location that has an operating temperature of 0° C to 40° C (32° F to 104° F). Refer to [Understanding Safety and Regulatory Information on page 1](#) for more safety information.
5. Power on your PC. The PC must have an Ethernet network adapter or Ethernet port and an Internet browser installed, such as Google or Internet Explorer. The following browsers are supported:
 - ◆ For Windows 2000, XP, Vista, Windows 8, Windows 7, Google Chrome, Firefox 1.07 and higher, Internet Explorer v7 and above, Netscape.

- ◆ For MAC OS X, 10.2, and higher: Firefox 1.07 and higher, Safari 1.x and higher.
- 6. Connect the power cable included in the product package to the back of the cable modem and plug the other end into the power outlet.
- 7. Connect the network cable included in the product package to your computer's Ethernet port. Connect the other end to the ETHERNET 1, 2, 3, or 4 port on the back panel of the DDW36C.
- 8. Connect a coaxial cable from the **CABLE** port on the back of the device to the cable wall outlet, or to a cable splitter connected to the wall outlet.
- 9. Validate the network connection using the device LEDs to confirm operations.
 - ◆ The 2.4G and/or 5G LED must be flashing or solidly lit.
 - ◆ The POWER, US, DS, and ONLINE LEDs are solidly lit.

Refer to [Understanding LED Behavior on page 5](#) for more information.

2.1.1 Wall Mount Installation

You can mount the DDW36C on a wall using a mounting kit, which is provided by the service provider installation technician.

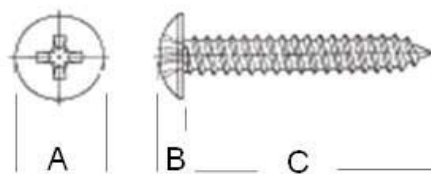
The mounting kit includes:

- ◆ (2) mounting brackets
- ◆ (2) new housing screws

In addition to the mounting kit, you will also need:

- ◆ (2) round or pan head screws for attaching the brackets to the wall (see figure below)
- ◆ (1) Torx T10 screwdriver for modem housing screws
- ◆ (1) screwdriver for the round or pan head screws

Round or Pan Head Screws:



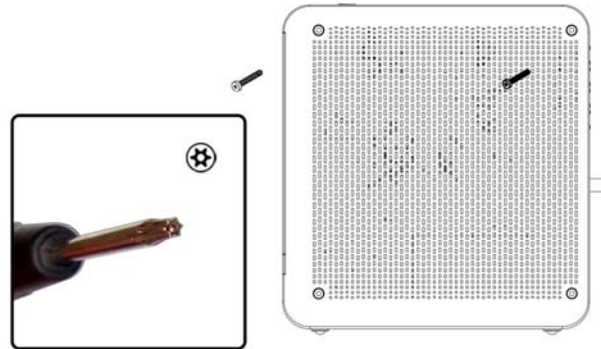
Label	Size In Millimeters (mm)
A	5.5 - 9.0
B	1.5 +/- 0.34
C	19.0 +/- 1.2



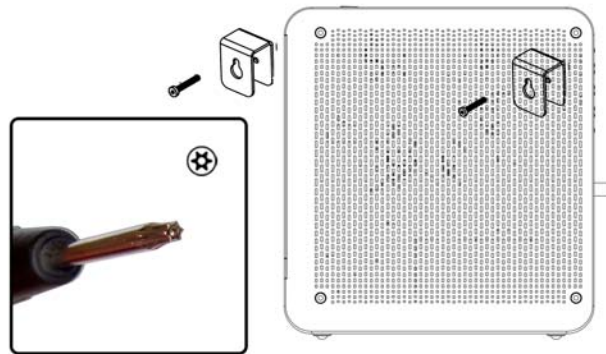
Steps

To mount the DDW36C on a wall:

1. Unscrew both screws from the top right side of the DDW36C using a Torx T10 screwdriver.

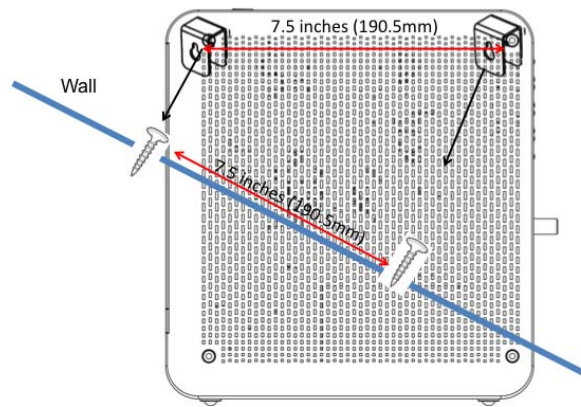


2. Screw each wall bracket to your device using the 2 new housing screws (these are longer than the original housing screws). Make sure the brackets are pointing down and that the smallest opening is closest to the device. **Note:** When attaching the brackets, take care to properly align the screws to prevent cross threading.



Important: To avoid internal device damage, do not use the longer housing screws without brackets.

3. Install the 2 round or pan head screws horizontally on the wall 7.5 inches (190.5 mm) apart. The screws should protrude from the wall so that you can fit the bracket between the head of the screw and the wall. If you install the screws in drywall, use hollow wall anchors to ensure the unit does not pull away from the wall due to prolonged strain from the cable and power connectors.



4. Once the screws have been installed on the wall, position the screws through the brackets and gently push down to secure the brackets over the head of each screw.

2.2 Connecting Devices to the Network

Use the instructions below to connect network devices and validate device functionality.



Topics

See the following topics:

- ◆ [Connecting an Ethernet Device on page 15](#)
- ◆ [Connecting a Wireless Device on page 16](#)

2.2.1 Connecting an Ethernet Device

You can connect up to three additional Ethernet devices to the DDW36C.



Steps

To connect another Ethernet device to the network:

1. Connect the Ethernet cable from the Ethernet device (for example, a PC or gaming console) to an open Ethernet port on the back of the DDW36C.
2. Use the device LEDs to confirm operations. Refer to [Understanding LED Behavior on page 5](#) for more information.
3. Open a Web browser and go to any Web site to validate network/Internet connectivity (for example, <http://www.wikipedia.org>).
4. If the connected device is a gaming console, perform any on line task supported by the console (for example, log into the gaming server, play an on line game, download content).



Note

Refer to [Troubleshooting the Installation on page 17](#) for troubleshooting information.

2.2.2 Connecting a Wireless Device

Use the following steps to connect a wireless device to the DDW36C (for example, a laptop computer).

Default values are shown in the steps below.



Steps

To connect a wireless device to the DDW36C:

1. Access the wireless networking feature on your wireless device.

- ◆ Windows Users: Double-click the Wireless Network Connection icon in the system tray (lower-right side of the Windows desktop). Click **View Wireless Networks**.



- ◆ Mac Users: Click on the wireless icon (Airport) on the right side of the top menu bar. All available wireless networks will appear in the drop-down menu.



2. Click **View Wireless Networks**. The device is shipped with a default SSID. The SSID is the name of the wireless network broadcast from the device so that wireless clients can connect to it.

- ◆ Double-click your **SSID** in the wireless networks window. "WIFI" plus the last 6 characters of the Cable Modem (CM) MAC address. "-5G" is added when the 5GHz band is being used.

❖ Examples:

1. 2.4G radio with CM MAC address 0071CC8E54C7
SSID: WIFI8E54C7
2. 5G radio with CM MAC address 0071CC8E54C7
SSID: WIFI8E54C7-5G

- ◆ **Notes:** You can find the MAC address on the device label or by opening an Internet browser window to the device. Refer to [Using the Software Option on page 19](#) for instructions. If you change the SSID, the device does not revert to this default SSID upon any power reset of the device, except in the case of a manual reset using the device's Web UI. See [Using the Account Option on page 22](#).

- ◆ When prompted, enter the network key, also called the pre-shared key. The WPA pre-shared key is a randomly generated character string, 16 characters in length. It can be found on the device label and on the Wireless Primary Network screen. Refer to [Using the Primary Network Option on page 99](#).
 - ❖ Example WPA PSK: HP3WZ7IHXCT6D9QS
 - ◆ If using WPS, enter the WPS personal identification number (PIN). The WPS PIN is a randomly-generated number. It can be found on the device label and on the Wireless Primary Network screen. Refer to [Using the Primary Network Option on page 76](#).
 - ◆ **Default Security and Encryption Methods:** WPA2-PSK with AES encryption.
3. Confirm connectivity by opening a Web browser and going to any Web site (for example, <http://www.wikipedia.org>) or access the Web interface for the DDW36C.



Note

The Web interface allows you to customize the configurations and capabilities for the device. For a full explanation of all Web interface functions, refer to [Using the Web User Interface on page 15](#).

If you have wireless issues or questions, refer to [Deploying and Troubleshooting the Wireless Network on page 92](#).

2.3 Troubleshooting the Installation

Use the following tips to troubleshoot the installation.

- ❑ **None of the LEDs are on when I power on the DDW36C.**
 - ◆ Check the connection between the power outlet and the power cord. Verify the power outlet is energized and the power cord is connected to the power outlet.
 - ◆ Check the connection between the power cord and the cable modem. Power off the cable modem and wait for 5 seconds and power on the modem again. If the problem still exists, there may be a hardware problem.
- ❑ **The ETHERNET 1, 2, 3, or 4 LEDs on the back of the modem are not lit where Ethernet cables are connected.**
 - ◆ Restart the computer so that it can re-establish a connection with the cable modem.
 - ◆ Check for a resource conflict (Windows users only):
 1. Right-click **My Computer** on your desktop and choose **Properties**.
 2. Choose the **Device Manager** tab and look for a yellow exclamation point or red **X** over the network interface card (NIC) in the Network Adapters field. If you see either one, you may have an interrupt request (IRQ) conflict. Refer to the manufacturer's documentation or ask your service provider for further assistance.
 - ◆ Verify that TCP/IP is the default protocol for your network interface card.
 - ◆ Power cycle the cable modem by removing the power cord from the electrical outlet and plugging it back in. Wait for the cable modem to re-establish communications with your cable service provider.

☐ **Check General Connectivity Issues:**

- ◆ If your PC is connected to a hub or gateway, connect the PC directly into an Ethernet port on the DDW36C.
 - ◆ If you are using a cable splitter, remove the splitter and connect the DDW36C directly to the cable wall outlet. Wait for the device to re-establish communications with the cable service provider.
 - ◆ Try a different cable. The Ethernet cable may be damaged.
- ☐ If none of these suggestions work, contact your service provider's tier II support for further assistance.

3 Using the Web User Interface

The Web user interface (UI) for the DDW36C is easy to use and allows you to view and configure several settings for your wireless gateway device. You can validate the installation by accessing the Web user interface on the device.



Topics

See the following topics:

- ◆ [Accessing the Web User Interface Locally on page 19](#)
- ◆ [Logging Out of the Web User Interface on page 21](#)

3.1 Accessing the Web User Interface Locally

Access the Web user interface for the DDW36C from a Web browser, such as Internet Explorer on a Windows computer.

Default values are shown in the steps below.



Steps

To access the Web user interface:

1. Launch an Internet browser, such as Internet Explorer, from your computer.
2. Enter the following IP address in the address bar of the browser window and press the Enter key.

<http://192.168.100.1>

3. The following screen is displayed. Click **Login**.



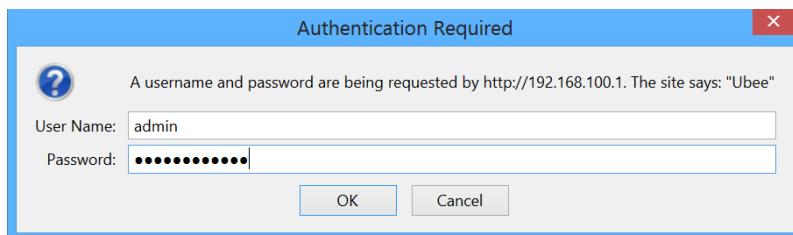
4. Enter the username and password in the authentication dialog box.

◆ **Standard User Web Interface Login:**

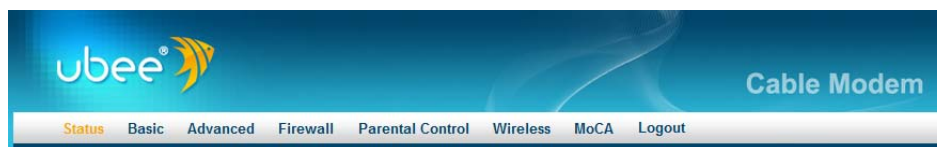
Username: **admin**

Password: **<random password>**

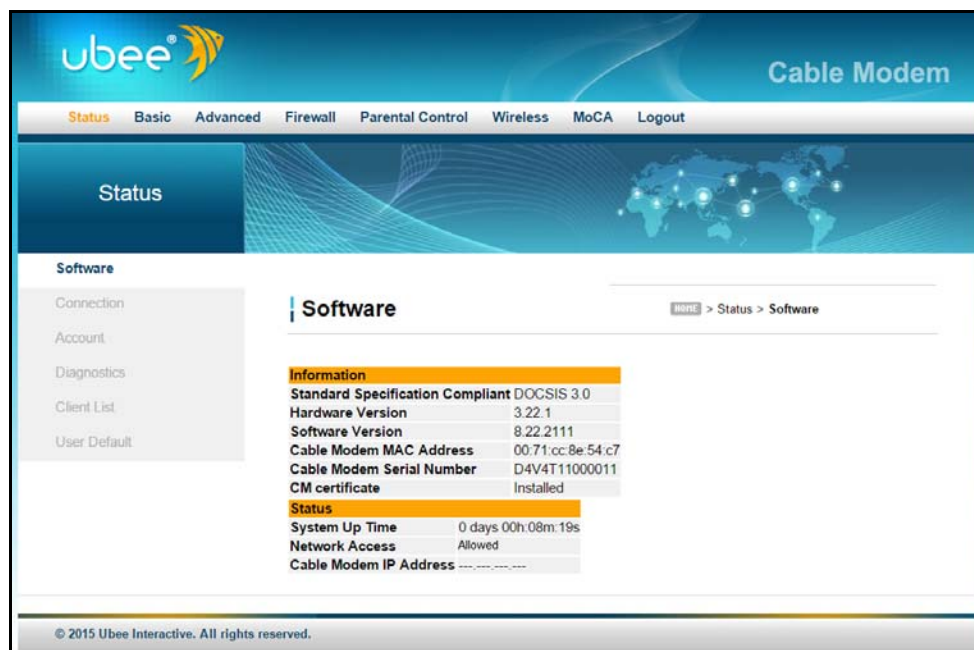
(The random password can be found on the device label)



The following menu options are available:



After logging in, the Status > Software screen displays software information about the DDW36C.

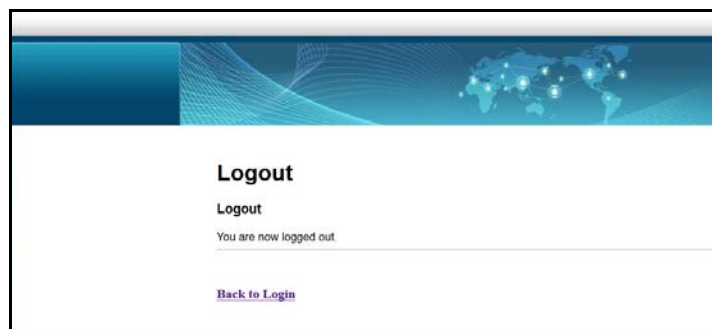


3.2 Logging Out of the Web User Interface

To log out of the Web user interface, click Logout on the top right of the menu bar.



The following screen confirms that you are logged out and gives you the opportunity to return to the Login page.



4 Understanding the Status Menu

The **Status** menu of the Web user interface allows you to access information about the DDW36C, such as software, connection (downstream and upstream), diagnostics, and event log.



Topics

See the following topics:

- ◆ [Using the Software Option on page 22](#)
- ◆ [Using the Connection Option on page 23](#)
- ◆ [Using the Account Option on page 26](#)
- ◆ [Using the Diagnostics Option on page 26](#)
- ◆ [Using the Client List Option on page 29](#)
- ◆ [Using the User Default Option on page 31](#)



Steps

To access status options:

1. Access the Web user interface. Refer to [Accessing the Web User Interface Locally on page 14](#).
2. Click **Status** from the main menu.

4.1 Using the Software Option

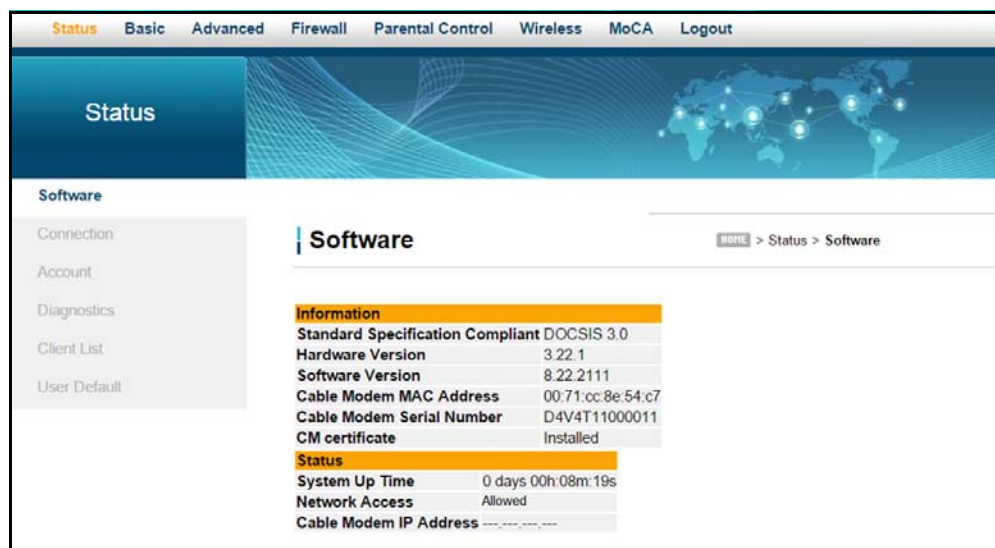
The **Software** option displays the device's internal software and hardware configuration.



Steps

To view software information:

1. Click **Status** from the main menu.
2. The **Software** screen is shown. Field descriptions are listed below the screen example.



Label	Description
Information	
Standard Specification Compliant	Defines the current DOCSIS standard supported by the DDW36C.
Hardware Version	Defines the internal version number that identifies the hardware design.
Software Version	Defines the firmware version of the device.
Cable Modem MAC Address	Defines the unique media access control (MAC) hardware address of the DDW36C.
Cable Modem Serial Number	Defines the unique manufacturer serial number of the device.
CM certificate	Indicates if the cable modem certificate is installed.
Status	
System Up Time	Displays how long the device has been connected.
Network Access	Defines if network access is enabled. When enabled, the user is allowed to access the network.
Cable Modem IP Address	Displays the IP address for the cable modem.

4.2 Using the Connection Option

The **Connection** screen displays information about the device's connection status and downstream and upstream channel bonding statistics.

- ◆ **Downstream** displays detailed information on the network traffic from the service provider **to** the local computer (downstream channels).
- ◆ **Upstream** displays detailed information on the network traffic **from** the computer to the remote destination (upstream channels).



Steps

To view connection information:

1. Click **Status** from the main menu.
2. Click **Connection** from the left side menu. Field descriptions are listed below the screen example.

Ubee DDW36C Advanced Wireless Gateway MSO Operations Guide

Navigation: Status | Basic | Advanced | Firewall | Parental Control | Wireless | MoCA | Logout

Status

Left Menu: Software | **Connection** | Account | Diagnostics | Client List | User Default

Connection Home > Status > Connection

Startup Procedure

Procedure	Status	Comment
Acquire Downstream Channel	555000000 Hz Locked	
Connectivity State	OK	Operational
Boot State		
Configuration File	OK	
Security	Enabled	BPI+

Downstream Bonded Channels

Channel	Lock Status	Modulation	Channel ID	Frequency	Power	SNR	Correctables	Uncorrectables
1		QAM256		555000000 Hz	-10.3 dBmV	36.8 dB	0	0
2		QAM256		561000000 Hz	-10.3 dBmV	37.0 dB	0	0
3		QAM256		567000000 Hz	-10.3 dBmV	36.9 dB	0	0
4		QAM256		573000000 Hz	-10.5 dBmV	37.1 dB	0	0
5		QAM256		579000000 Hz	-10.7 dBmV	36.1 dB	0	0
6		QAM256		585000000 Hz	-10.8 dBmV	36.9 dB	0	0
7		QAM256		591000000 Hz	-10.9 dBmV	36.7 dB	0	0
8		QAM256		597000000 Hz	-11.0 dBmV	36.3 dB	0	0
9		QAM256		603000000 Hz	-11.3 dBmV	36.5 dB	0	0
10		QAM256		609000000 Hz	-11.2 dBmV	36.7 dB	0	0
11		QAM256		615000000 Hz	-11.2 dBmV	36.6 dB	0	0
12		QAM256		621000000 Hz	-11.6 dBmV	36.3 dB	0	0
13		QAM256		627000000 Hz	-11.9 dBmV	36.0 dB	2	0
14		QAM256		633000000 Hz	-11.9 dBmV	36.0 dB	4	0
15		QAM256		639000000 Hz	-11.5 dBmV	35.9 dB	4	0
16		QAM256		645000000 Hz	-11.1 dBmV	36.3 dB	3	0

Upstream Bonded Channels

Channel	Lock Status	US Channel Type	Channel ID	Symbol Rate	Frequency	Power
1		ATDMA		5120 Ksym/sec	237000000 Hz	48.8 dBmV
2		ATDMA		5120 Ksym/sec	365000000 Hz	50.0 dBmV
3		ATDMA		5120 Ksym/sec	301000000 Hz	49.3 dBmV
4		ATDMA		2560 Ksym/sec	173000000 Hz	47.8 dBmV

CM IP Address Duration Expires

D: -- H: -- M: -- S: -- -- -- -- --

Current System Time: Thu Jan 08 11:19:25 2015

Label	Description
Startup Procedure: (Procedure, Status, Comment)	
Acquire Downstream Channel	Displays the Downstream channel status and if the device has locked to a channel.
Connectivity State	Displays connection status and if the DDW36C is operational.
Boot State	Displays the status on boot up and if the device is operational.
Configuration File	Provides the status and file name of the configuration file currently used by the DDW36C.
Security	Displays the status of the security settings: enabled/disabled.
Downstream Bonded Channels	
Channel	Numbers the downstream channels.
Lock Status	Displays if the device has locked successfully to a downstream channel.
Modulation	Displays the modulation method required for the downstream channel to lock on to by device. This method is determined by the service provider.
Channel ID	Displays the downstream channel ID.
Frequency	Displays the downstream channel frequency on which the DDW36C is scanning.
Power	Displays the receiver power level in decibel millivolts (dBmV) after ranging process.
SNR	Displays the signal-to-noise ratio, the desired signal level to the background noise level.
Correctables	Displays the quantity of codewords which are correctable.
Uncorrectables	Displays the quantity of codewords which are not correctable.
Upstream Bonded Channels	
Channel	Numbers the upstream channels.
Lock Status	Displays if the device has locked successfully to an upstream channel.
US Channel Type	Displays the channel type.
Channel ID	Displays the current upstream channel ID.
Symbol Rate	Displays the symbol rate in 1000 symbols per second.
Frequency	Displays the current upstream frequency in hertz.
Power	Displays the current upstream transmit power in decibel millivolts (dBmV).
CM IP Address	Displays the DDW36C's IP address.

Label	Description
Duration	Displays the time the device has been active.
Expires	Displays when the cable modem's certificate expires.
Current System Time	Displays the current system time.

4.3 Using the Account Option

Use the **Account** option to change the end user username and password.



Steps

To reset the DDW36C's username and password:

1. Click **Status** from the main menu.
2. Click **Account** from the left side menu. Field descriptions are listed below the screen example.

Label	Description
End User	
User Name	Enter the new User name.
New Password	Enter the new User password.
Confirm Password	Confirm the new User password.
Apply	Saves the changes.

4.4 Using the Diagnostics Option

Use the **Diagnostics** option to test network connectivity. Two utilities are available: Ping and Traceroute.



Topics

See the following topics:

- ◆ [Using the Ping Option on page 27](#)
- ◆ [Using the Traceroute Option on page 28](#)

4.4.1 Using the Ping Option

Use the **Ping** utility to test network connectivity between devices by sending a test message to a specific device. You can also confirm the size of data sent is the same as the size of data received.



Steps

To test connectivity between devices:

1. Click **Status** from main menu.
1. Click **Diagnostics** from the left side menu.
2. Choose **Ping** from the Utility drop-down menu.
3. Enter new parameter values or accept the default values.
4. Click **Start Test**. Field descriptions are listed below the screen example.

The screenshot shows the 'Status' page of the Ubee DDW36C Advanced Wireless Gateway MSO Operations Guide. The 'Diagnostics' section is active, showing the 'Ping Test Parameters' form. The form includes a 'Utility' dropdown menu set to 'Ping'. The 'Ping Test Parameters' section has the following fields: 'Target' (google.com), 'Ping Size' (64 bytes), 'No. of Pings' (3), and 'Ping Interval' (1000 ms). There are buttons for 'Reset Defaults', 'Start Test', 'Abort Test', and 'Clear Results'. Below the form is a 'Results' section showing the output of the ping test.

Label	Description
Utility	Provides a drop-down menu to choose Ping or Traceroute.
Ping Test Parameters	
Target	Defines the IP address to which you want to send a ping.

Label	Description
Ping Size	Defines the packet size (bytes of data) to send for the ping operation. Default is 64.
No. of Pings	Defines the number of ping commands to send to the ping target. Default is 3 pings.
Ping Interval	Defines the interval between ping operations in milliseconds.
Reset Defaults	Resets the Ping Test Parameters to the default values.
Start Test Abort Test Clear Results	Defines what action to take. ♦ Start Test begins the ping. ♦ Abort Test stops the ping. ♦ Clear Results deletes previous test results in the Results table.
Results	Displays the results of the ping test.

4.4.2 Using the Traceroute Option

The **Traceroute** utility determines the IP addresses of hosts in the network path. By checking the Resolve Host names box, Traceroute tries to find which name matches the address. Some hosts have no names, and might still be shown as IP addresses, even if this option is active.



Steps

To trace host IP addresses along a route:

1. Click **Status** from main menu.
2. Click **Diagnostics** from the left side menu.
3. Choose **Traceroute** from the Utility drop-down menu.
4. Enter new parameter values or accept the default values.
5. Click **Start Test**. Field descriptions are listed below the screen example.

Status

Software
Connection
Account
Diagnostics
Client List
User Default

Diagnostics HOME > Status > Diagnostics

Utility Traceroute ▼

Traceroute Parameters

Target IP address or Name

Max Hops

Data Size bytes

Base Port

Resolve Host Off ▼

Results

08 68.86.82.186 20 ms 20 ms 20 ms
09 23.30.206.106 30 ms 30 ms 20 ms
10 72.14.234.59 30 ms 30 ms 20 ms
11 209.85.251.9 30 ms 20 ms 20 ms
12 74.125.225.160 20 ms * 20 ms
Traceroute complete.

Utility	Provides a drop-down menu to choose Ping or Traceroute.
Traceroute Parameters	
Target	Defines the specific IP address or domain (for example, google.com) to which you want to trace a route.
Max Hops	Defines the maximum number of hops. Hops are the number of routers the traceroute traverses. Default is 255.
Data Size	Defines the data size to send for the traceroute operation. Default is 32 bytes.
Base Port	Defines the destination port number. Default is 33434.
Resolve Host	Enable (on) or disables (off) this option. When checked, traceroute tries to find the name that matches the IP address. Default is Off.
Reset Defaults	Resets the Traceroute Parameters to the default values.
Start Test/Clear Results	Defines what you want to do. ♦ Start Test begins the traceroute. ♦ Clear Results deletes previous test results in the Results table.
Results	Displays the results of the trace.

4.5 Using the Client List Option

The **Client List** screen displays computers and devices connected to the DDW36C.



Steps

To view a list of connected devices:

1. Click **Status** from the main menu.
2. Click **Client List** from the left side menu. Field descriptions are listed below the screen example.

Client List

HOME > Status > Client List

CPE Interface Status

Interface	Status
Eth-Switch Lan(0)	enabled
Eth-Switch Lan(1)	enabled
Eth-Switch Lan(2)	enabled
Eth-Switch Lan(3)	enabled

Tools - Client List

Host Name	IP Address	MAC Address	Interface
Home	192.168.0.260	a4:4c:09:f2:10	Eth-Switch Lan(0)

Refresh

Label	Description
CPE Interface Status	
Interface	Displays the interface.
Status	Displays whether the CPE Interface is Enabled or Disabled.
Tools - Client List	
Host Name	Displays the host name of the DHCP client connected to the DDW36C.
IP Address	Displays the IP address of the DHCP client connected to the DDW36C.
MAC Address	Displays the MAC address of the DHCP client connected to the DDW36C.
Interface	Displays the method of how clients are connected to the device (for example, Ethernet LAN, Wireless).
Refresh	Refreshes the client list. This may be useful when testing network connectivity between connecting clients and the DDW36C.

4.6 Using the User Default Option

The **User Default** option allows you to restore the DDW36C to the factory default values.



Steps

To restore factory defaults:

1. Click **Status** from the main menu.
2. Click **User Default** from the left side menu. Field descriptions are listed below the screen example.

Label	Description
Restore User Defaults	Restores settings to factory defaults. Select Yes to have the device reset all configured options in the device to factory default settings. The device reboots if Reset The System is also selected.
Reset The System	Resets the system. Select Yes to power cycle the device. When you select Apply, you will be notified that the device has been reset. Click RELOAD . The Login screen will then appear.
Apply	Applies the options selected on this screen.

5 Understanding the Basic Menu

Basic gateway options provide the majority of configuration for the device including WAN IP addresses, LAN IP addresses, and DHCP. Advanced gateway options provide settings like MAC filtering and port forwarding.



Topics

See the following topics:

- ◆ [Using the Setup Option on page 32](#)
- ◆ [Using the DHCP Option on page 34](#)
- ◆ [Using the DDNS Option on page 39](#)
- ◆ [Using the DHCPv6 Option on page 36](#)
- ◆ [Using the LAN IPv6 Option on page 38](#)
- ◆ [Using the Static Lease Option on page 40](#)
- ◆ [Using the Backup Option on page 41](#)
- ◆ [Using the Time Option on page 45](#)



Steps

To access the basic menu:

1. Access the Web user interface. Refer to [Accessing the Web User Interface Locally on page 14](#).
2. Click **Basic** from the main menu.

5.1 Using the Setup Option

Use the **Setup** option to configure common gateway parameters.



Steps

To configure setup options:

1. Click **Basic** from the main menu.
2. The **Setup** screen is displayed. Field descriptions are listed below the screen example.

[Status](#)
[Basic](#)
[Advanced](#)
[Firewall](#)
[Parental Control](#)
[Wireless](#)
[MoCA](#)
[Logout](#)

Basic

Setup

[DHCP](#)
[DHCPv6](#)
[LAN IPv6](#)
[DDNS](#)
[Static Lease](#)
[Backup](#)
[Time](#)

Setup

HOME > Basic > Setup

Network Configuration

LAN

IPv6 Address: Unspecified
 IPv6 Prefix: ::
 IPv4 Address: 192 . 168 . 0 . 1
 MAC Address: 00:71:cc:8e:54:c9

Interface/Prefix

None Specified

WAN

IPv6 Address: fe80::271:ccff:fe8e:54c8/64
 IPv4 Address: 10.2.1.10
 MAC Address: 00:71:cc:8e:54:c8
 Duration: D: 00 H: 01 M: 00 S: 00
 Expires: Wed Nov 12 13:26:50 2014
 IPv4 DNS Servers: 192.168.250.221
 8.8.8.8
 75.75.75.75
 IPv6 DNS Servers: None

WAN Connection Type:

Host Name: (Required by some ISPs)
 Domain Name: (Required by some ISPs)
 IPv4 MTU Size: (256-1500 octets, 0 = use default)

Label	Description
LAN	
IPv6 Address	Defines the local IPv6 address.
IPv6 Prefix	Defines the IPv6 prefix.
IPv4 Address	Defines the local IPv4 address, which is the default gateway address for all wired LAN hosts that connect to the DDW36C.
MAC Address	Displays the LAN interface's hardware address.
Interface/Prefix	
None Specified	Indicates no interface or prefix has been specified.
WAN	
IPv6 Address	Displays the current WAN public IPv6 address obtained from the service provider.
IPv4 Address	Displays the current WAN public IPv4 address obtained from the service provider.
MAC Address	Displays the WAN interface's hardware address.
Duration	Displays the accumulated time since successfully acquiring a WAN public IP address.
Expires	Displays the remaining time before the WAN IP address expires, if applicable.
IPv4 DNS Servers	Lists the IPv4 DNS servers available on the network.

Label	Description
IPv6 DNS Servers	Lists the IPv6DNS servers available on the network.
Release WAN Lease	Releases the WAN public IP address when clicked.
Renew WAN Lease	Renews the WAN IP address when clicked.
WAN Connection Type	Selects the WAN connection type. For each type, different data entry is required, as explained below: ♦ DHCP: The WAN interface is set to a DHCP client, and the IP address is assigned by the service provider's DHCP server. ♦ Static IP: For Static IP, you must manually enter the IP address for the WAN interface. ♦ PPTP (dhcp): For Point to Point Tunneling Protocol (PPTP), you must enter a username, password, and the PPTP server's IP address. ♦ PPTP (static): ♦ L2TP (dhcp): ♦ L2TP (static):
Host Name	Defines the host name for the router. This may be required by some service providers.
Domain Name	Defines the domain name for the router. This may be required by some service providers.
IPv4 MTU Size	Defines the maximum transmission unit (MTU) size. MTU defines the largest size of the packet or frame that the device can transfer (256-1500). If this is not given by your service provider, use 0 for the default.
Apply	Saves changes.

5.2 Using the DHCP Option

Use the **DHCP** option to configure dynamic host configuration protocol-specific behavior on the device.



Steps

To configure DHCP settings:

1. Click **Basic** from the main menu.
2. Click **DHCP** from the left side menu. Field descriptions are listed below the screen example.

The screenshot shows the 'Basic' configuration page for the DHCP service. The 'DHCP Server' is set to 'Yes'. The 'Starting Address Set' is 'Private Starting Address' with a value of 192.168.0.2 and 253 CPEs. The 'Lease Time' is 3600 seconds. The 'DHCP Clients' table shows one client with MAC address 60:A4:4C:09:F2:10 and IP address 192.168.0.2.

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
60:A4:4C:09:F2:10	192.168.0.2	255.255.255.0	D:00 H:01 M:00 S:00	Wed Nov 12 13:26:32 2014	☐

Label	Description
DHCP Server	Enables (Yes) or disables (No) DHCP on the device. If No is selected, all the static DHCP rules in this screen are ignored.
Starting Address Set	
Private Starting Address	Defines the starting private IP address for the pool of IP addresses that can be used by connecting clients. Private addresses are translated to public IPs to be used on the network.
Public Starting Address	Defines the starting public IP address. Public addresses can be recognized on the network.
Number of CPEs	Defines the maximum number of customer premises equipment devices (CPE) that can connect to the network through the DDW36C.
Lease Time	Defines the DHCP lease time duration in minutes between 1 and 71582788. A DHCP user's PC gets an IP address with a lease time. When the lease time expires, the PC must connect to the DHCP server and be issued a new unused IP address. Note: The default DHCP lease time is 3600 seconds and should be changed to 86400 seconds (24 hours). This helps resolve connectivity issues with some iMAC and Windows 7 devices that turn off the network interface when they go into standby mode. This results in slow Web browsing until the device gets a new IP address via DHCP.
Apply	Saves changes.

Label	Description
DHCP Clients	Lists all DHCP clients currently connected to the device, either via an Ethernet connection, or via a wireless connection. Each client is listed with the following information: ♦ MAC Address / IP Address / Subnet Mask ♦ Duration: Duration displays the accumulated time since the client acquired the IP address. ♦ Expires: Expires is the time until the IP expires and must be recycled. If the IP address is reserved to a certain host, it shows STATIC IP ADDRESS. ♦ Select: Reserves the current private IP address to be assigned to this host statically when selected.
Current System Time	Displays the current system time.
Force Available	Activates a selected rule in the DHCP Clients list and assigns IP addresses. Note: The Select button must be activated in the DHCP list.

5.3 Using the DHCPv6 Option

Use the **DHCPv6** option to configure IPv6 host IP addresses, IPv6 prefixes, and various configuration data required to operate in an IPv6 network.



Steps

To configure DHCPv6 settings:

1. Click **Basic** from the main menu.
2. Click **DHCPv6** from the left side menu. Field descriptions are listed below the screen example.

Basic

Setup
DHCP
DHCPv6
LAN IPv6
DDNS
Static Lease
Backup
Time

DHCPv6 [HOME](#) > Basic > DHCPv6

System Delegated Prefix

User defined prefix ☐

Server Settings
LAN Delegated Prefix will be derived from System Delegated Prefix and Start Address will have the same prefix as the LAN Delegated Prefix.

Enabled ☒

LAN Delegated Prefix

Start Address

Valid Lifetime

Enable Rapid Commit ☒

Enable Unicast ☐

Label	Description
System Delegated Prefix	This is the IPv6 prefix from the Setup Web UI, disabled (grayed out) by default. It is enabled buy the user defined prefix box below.
User defined prefix	Enables the System Delegated Prefix, which is disabled by default. Once enabled and Apply is clicked, the device restarts.
Server Settings	
Enabled	Enables the Ethernet Switch LAN Interface and Prefix listed in the Setup Web UI.
LAN Delegated Prefix	Displays the Ethernet Switch LAN Interface and Prefix listed in the Setup Web UI.
Start Address	Displays the Ethernet Switch LAN start IPv6 address.
Valid Lifetime	Defines the DHCPv6 lease time duration in minutes between 1 and 71582788. A DHCPv6 user's PC gets an IPv6 address with a lease time. When the lease time expires, the PC must connect to the DHCPv6 server and be issued a new, unused IPv6 address. Note: The default DHCPv6 lease time is 3600. For optimum performance, it should be changes to 86400 seconds (24 hours). This helps resolve connectivity issues with some MAC and Windows 7 devices that turn off the network interface when they go into standby mode. This results in slow Web browsing until the device gets a new IPv6 address via DHCPv6.

Label	Description
Enable Rapid Commit	Enables Rapid Commit. When enabled, the server recognizes this option in Solicit messages sent from the DHCPv6 client. The server and client then use a two-message exchange (Solicit and Reply) to configure clients, rather than the default four-message exchange (Solicit, Advertise, Request, and Reply). This provides faster client configuration when networks are under heavy traffic loads.
Enable Unicast	Enables Unicast, which is disabled by default. Unicast transmission is defined to be between a single sender and a single user over a network.
Apply	Saves changes.
Restore DhcpV6 Defaults	Restores default DHCPv6 values.

5.4 Using the LAN IPv6 Option

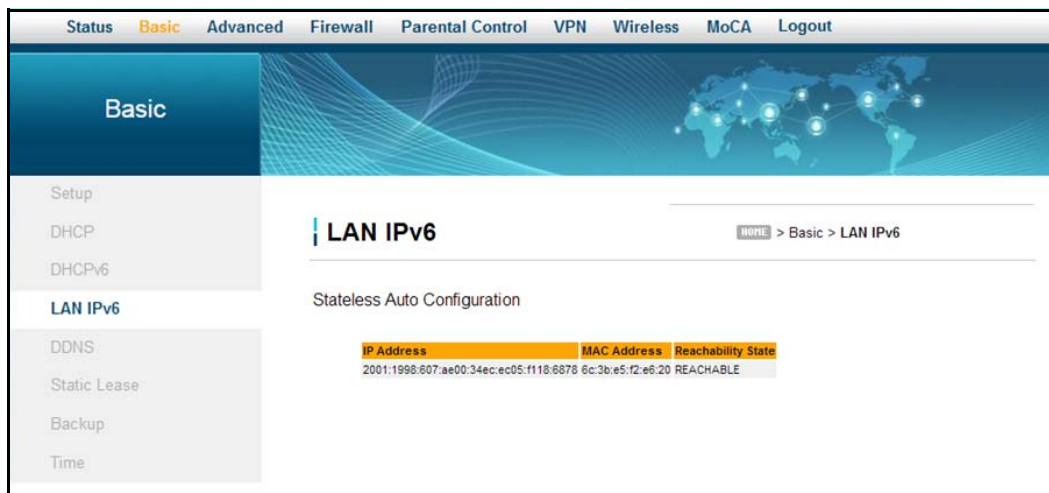
Use the **LAN IPv6** option to connect clients with LAN IPv6 addresses.



Steps

To configure LAN IPv6 settings:

1. Click **Basic** from the main menu.
2. Click **LAN IPv6** from the left side menu. Field descriptions are listed below the screen example.



Label	Description
Stateless Auto Configuration	

Label	Description
IP Address	Displays the IPv6 address of the client.
MAC Address	Displays the MAC address of the client connected to the device with an IPv6 address.
Reachability State	Displays whether the client is reachable or unreachable by neighboring nodes.

5.5 Using the DDNS Option

Use the dynamic domain name system (DDNS) to assign a changing IP address to a constant pre-defined host name. The host can then be contacted by other hosts on the Internet, even if its IP address changes.

The DDNS service for the DDW36C is provided through a third-party and can be purchased from Dynamic Network Services Inc. at www.dynDNS.com.



Steps

To use the DDNS option:

1. Click **Basic** from the main menu.
2. Click **DDNS** from the left side menu. Field descriptions are listed below the screen example.

Label	Description
DDNS Service	Enables or disables the DDNS service. When enabled, this service is available from www.dynDNS.org .
User Name	Defines the user name for the DDNS account.
Password	Defines the password for the DDNS account.
Host Name	Defines the host name for the DDNS account.

Label	Description
IP Address	Displays the IP address for the DDNS account.
Status	Displays if the DDNS service is enabled or disabled.
Apply	Saves changes.

5.6 Using the Static Lease Option

You can use the **Static Lease** option to assign IP addresses to clients on your network that do not change. A static lease ensures a specific device always gets the same IP address, especially if the devices are powered on and off or disconnected and reconnected. This may be useful in a variety of networking scenarios where you need more control over the network and the clients connected to it. Examples is which you may need to use a static lease include:

- ◆ [Using the IP Filtering Option on page 47](#)
- ◆ [Using the Port Filtering Option on page 49](#)
- ◆ [Using the DMZ Host Option on page 57](#)



Steps

To assign static IP addresses:

1. Click **Basic** from the main menu.
2. Click **Static Lease** from the left side menu. Field descriptions are listed below the screen example.

Note: If some IP addresses turn to red color, you should check the DHCP pools!
Current DHCP Server IP Ranges' information
Private IP Range: 192.168.0.2 -- 192.168.0.254
Public IP Range: 0.0.0.0 -- 0.0.0.0

Index	MAC Address	IP Address	Enabled	Clear
1.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
2.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
3.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
4.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
5.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
6.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
7.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
8.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
9.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
10.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
11.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
12.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
13.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
14.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
15.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
16.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
17.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
18.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
19.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
20.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
21.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
22.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
23.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐
24.	00 : 00 : 00 : 00 : 00 : 00	0.0.0.0	☐	☐

Apply

Label	Description
Index	Provides an index number for each client that connects to your network.
MAC Address	Defines the MAC address of the client to which you want to assign a static IP address.
IP Address	Defines an IP address to the specific client/host.
Enabled	Activates this rule when Enable is checked.
Clear	Deletes the rule when Clear is checked.
Apply	Saves changes.

5.7 Using the Backup Option

The Backup option lets you backup your gateway configuration or restore the DDW36C to a previously saved configuration.



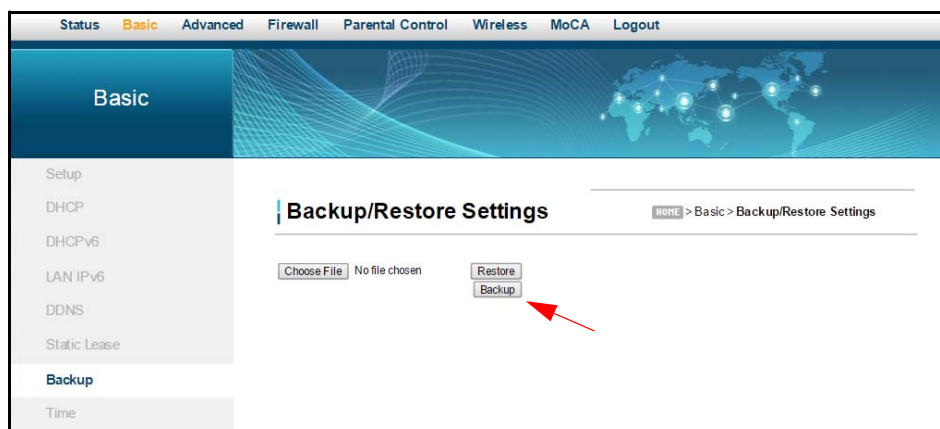
Steps

To use the backup option:

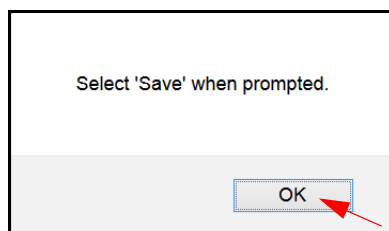
1. Click **Basic** from the main menu.
2. Click **Backup** from the left side menu.

5.7.1 Backing Up the Current Configuration

To backup and save the current device configuration, click the **Backup** button.



A pop-up window appears instructing you to select 'Save' when prompted. Click 'OK'.



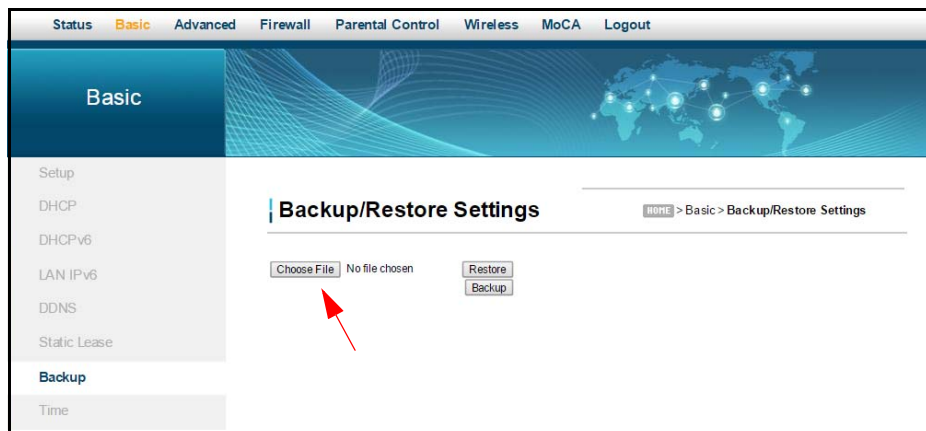
The following window appears, giving you the option to save the file. Click the 'Save File' option and click 'OK'.



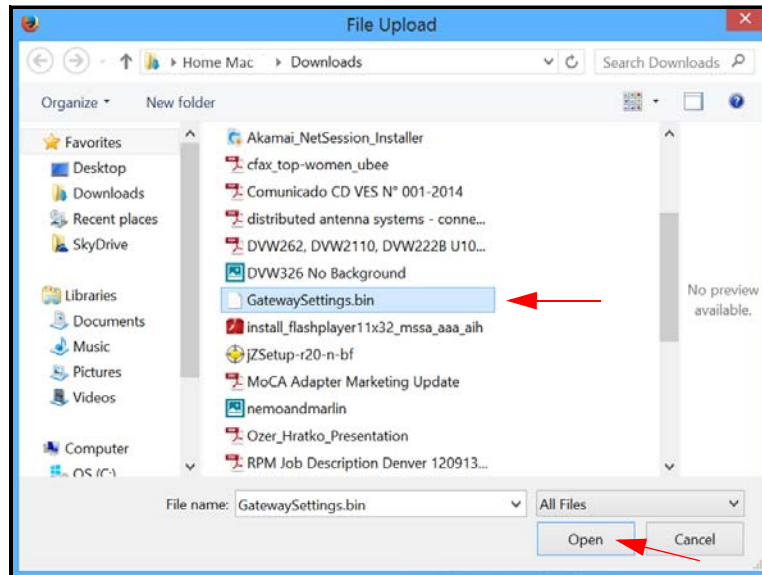
The file will be saved to your Downloads folder as a binary file (.bin) titled 'GatewaySettings.bin.'

5.7.2 Restoring the DDW36C to a Previously Saved Configuration

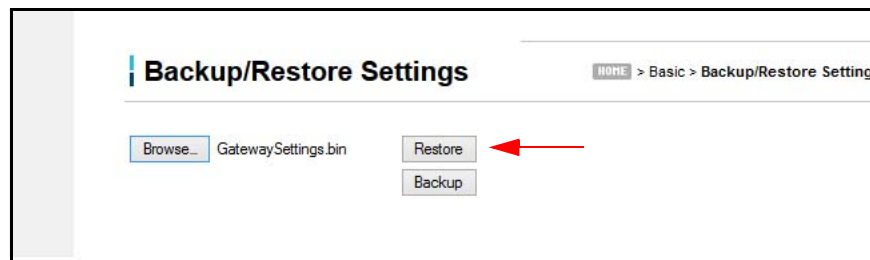
To restore the device to a previously saved configuration, click the **Browse** button.



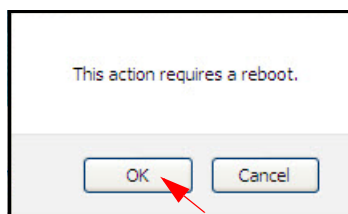
The File Upload dialog box appears and allows you to select the previously saved backup file. Highlight the file and click '**Open**'.



The location for the backed up file appears in the box to the left of the Browse button. Click the **Restore** button.



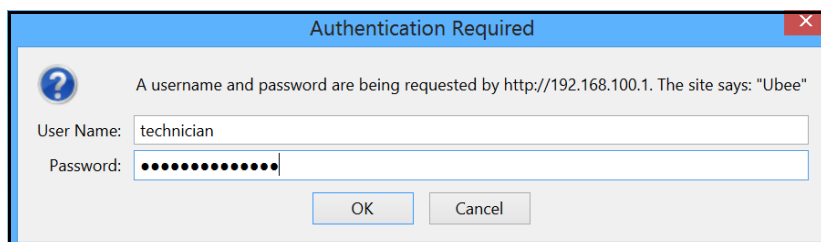
You are advised that you will be required to reboot the device. Click '**OK**'.



You are then notified that the device has been reset. Click '**RELOAD**'.

The device has been reset...[RELOAD](#)

You are then presented with the login screen. Enter the Username and Password to return to the User Interface.



5.8 Using the Time Option

The **Time** option allows you to configure the system time obtained from the network servers via Simple Network Time Protocol (SNTP). SNTP is a protocol for synchronizing the clocks of computing devices over networks. The device must be reset for changes to take effect.



Steps

To configure system time:

1. Click **Basic** from the main menu.
2. Click **Time** from the left side menu. Field descriptions are listed below the screen example.

 A screenshot of the Ubee DDW36C web interface. The top navigation bar includes "Status", "Basic" (highlighted), "Advanced", "Firewall", "Parental Control", "Wireless", "MoCA", and "Logout". The left sidebar shows a tree view with "Setup", "DHCP", "DHCPv6", "LAN IPv6", "DDNS", "Static Lease", "Backup", and "Time" (highlighted). The main content area is titled "Time" and shows the following configuration options:

- Enable SNTP: ☒ Yes ☐ No
- Current Time: Wed Nov 12 13:07:57 2014
- System Start Time: Wed Nov 12 11:56:01 2014
- Time Server 1: clock.via.net
- Time Server 2: ntp.nasa.gov
- Time Server 3: tick.ucla.edu
- Timezone Offset: Hours [0] Minutes [0]

 At the bottom are "Apply" and "Reset Values" buttons.

Label	Description
Enable SNTP	Enables (Yes) or disables (No) the SNTP feature.
Current Time	Displays the current system time.
System Start Time	Displays the accumulated time since the system was started.
Time Server 1	Defines the IP address or domain name of the time server. Use the one provided or enter an alternative choice.
Time Server 2	Defines the IP address or domain name of the time server. Use the one provided or enter an alternative choice.

Label	Description
Time Server 3	Defines the IP address or domain name of the time server. Use the one provided or enter an alternative choice.
Time Zone Offset	Defines the time zone offset in hours and minutes from Greenwich Mean Time. For example: 8 hours means GMT +8, -1 hour means GMT -1.
Apply	Saves changes.
Reset Values	Resets the screen to factory defaults when clicked.

6 Understanding the Advanced Menu

Advanced options provide settings to configure your DDW36C, such as MAC filtering and port forwarding.



Topics

See the following topics:

- ◆ [Using the Options Option on page 47](#)
- ◆ [Using the IP Filtering Option on page 50](#)
- ◆ [Using the MAC Filtering Option on page 51](#)
- ◆ [Using the Port Filtering Option on page 52](#)
- ◆ [Using the Forwarding Option on page 54](#)
- ◆ [Using the Port Triggers Option on page 59](#)
- ◆ [Using the Pass Through Option on page 60](#)
- ◆ [Using the DMZ Host Option on page 61](#)



Steps

To access the advanced menu:

1. Access the Web User Interface. Refer to [Accessing the Web User Interface Locally on page 14](#).
2. Click **Advanced** from the main menu.

6.1 Using the Options Option

Use the **Options** option to define which networking protocols are enabled or disabled on the device. The network address translation application-level gateway (NAT ALG) settings provide additional security beyond the firewall.



Steps

To enable or disable network protocols:

1. Click **Advanced** from the main menu.
2. The **Options** screen is displayed. Field descriptions are listed below the screen example.

The screenshot shows the 'Advanced' tab of the Ubee DDW36C router's web interface. The 'Options' section is active, displaying a list of settings. On the left, a sidebar lists navigation options: IP Filtering, MAC Filtering, Port Filtering, Forwarding, Port Triggers, Pass Through, and DMZ Host. The main content area, titled 'Options', shows the following settings, all of which are checked and labeled 'Enable':

- WAN Blocking
- IPsec PassThrough
- PPTP PassThrough
- Multicast Enable
- UPnP Enable
- Primary Network Bridged
- DNS Relay
- NAT ALG Status
- RSVP
- FTP
- TFTP
- Kerb88
- NetBios
- IKE
- RTSP
- Kerb1293
- H225
- PPTP
- MSN
- SIP
- ICQ
- IRC666x
- ICQTalk
- Net2Phone
- IRC7000
- IRC8000

An 'Apply' button is located at the bottom right of the settings list.

Label	Description
WAN Blocking	Blocks connection requests initialized from Internet users when enabled. WAN Blocking must be disabled to be able to PING the WAN gateway IP.
Ipsec PassThrough	Forces the router to redirect the IPsec request to the local host when enabled. NAT fails this attempt if Internet users initialize an IPsec VPN request to a host located behind the router.
PPTP PassThrough	Forces the router to redirect the PPTP request to the local host when enabled. NAT fails this attempt if Internet users initialize a PPTP VPN request to a host located behind the router.
Multicast Enable	Optimizes the bandwidth utilization compared with unicast (especially video streaming applications).
UPnP Enable	Activates Universal Plug and Play (UPnP) when enabled. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. Gaming consoles and Web cameras are examples of devices that can use UPnP.

Label	Description
Primary Network Bridged	When enabled, this allows bridging of traffic to and from the Internet for <u>ALL</u> LAN side primary interfaces (Ethernet, MoCA, and Wireless Primary Network). Note: When the Primary Network Bridged option is enabled, menu items for other functions can still be seen, but are not active.
DNS Relay	Allows the DDW36C to act as the “relay” device. Each PC that wants to access a URL does not have to send a DNS request to a DNS server on the Internet. DNS is used to resolve a URL (Web site name) to an IP address. DNS Relay is typically used for commercial applications where each device/PC connected to the device uses the DNS Relay address rather than going to a public DNS server hosted by an ISP to look up a URL.
NAT ALG Status – Filters to allow (enable) or disallow (disable) protocols to pass through the DDW36C to connected devices (computers, game consoles, and so on).	
RSVP	Enables or disables resource reservation protocol (RSVP). RSVP defines how applications reserve resources and how they free the reserved resources once they are no longer needed.
FTP	Enables or disables the file transfer protocol (FTP) used to transfer files from one host to another.
TFTP	Enables or disables the trivial file transfer protocol (TFTP) – a simpler protocol generally used for automated file transfers.
Kerb88	Enables or disables the Kerberos network authentication protocol which allow nodes to communicate over a non-secure network using “tickets” on port 88 to prove their identity to one another.
NetBios	Enables or disables the network basic input/output system (NetBIOS) services related to the OSI session layer. NetBIOS allows applications on separate computers to communicate over a LAN.
IKE	Enables or disables the network key exchange (IKE) protocol used to set up a security association (SA) in the IPsec protocol suite.
RTSP	Enables or disables the real time streaming protocol (RTSP) network control protocol used to establish and control media sessions between end points.
Kerb1293	Enables or disables the Kerberos network authentication protocol which allows nodes to communicate over a non-secure network using “tickets” on port 1293.
H225	Enables or disables the H.225 protocol used to define messages and procedures for call signaling, media packetization, and registration, admission, and status (RAS) functions.
PPTP	Enables or disables the point-to-point tunneling protocol (PPTP) used to implement a virtual private network.

Label	Description
MSN	Enables or disables the Microsoft network protocol used for instant messaging.
SIP	Enables or disables the session initiation protocol application layer gateway (SIP ALG). SIP ALG inspects protocol packets and formats SIP message headers and SDP body to ensure proper signaling. Note: Some hosted VoIP services prefer this function to be performed by their own session border controller (SBC) and require the SIP ALG to be disabled. Some IP-PBXs may require SIP ALG enabled.
ICQ	Enables or disables the ICQ instant messaging program.
IRC666x	Enables or disables the Internet relay chat (IRC) protocol used for text messaging.
ICQTalk	Enables or disables the ICQTalk instant messaging program.
Net2Phone	Enables or disables Net2Phone SIP- and PacketCable-based VoIP.
IRC7000	Enables or disables the Internet relay chat protocol on TCP port 7000 used for text messaging and group forums.
IRC8000	Enables or disables the Internet relay chat protocol on UDP port 8000 used for text messaging and group forums.
Apply	Saves changes.

6.2 Using the IP Filtering Option

Use the **IP Filtering** option to filter IP addresses to block Internet traffic to specific network devices on the LAN. Any host on this list is not accessible to Internet traffic.



Note

You may also filter by the MAC address which does not require setting a static lease. Refer to [Using the MAC Filtering Option on page 51](#).



Steps

To filter IP addresses:

1. Make sure a PC is connected to the DDW36C and both devices are powered on and functioning.
2. Log in to the DDW36C Web user interface. Refer to [Accessing the Web User Interface Locally on page 14](#).
3. Click **Advanced** from the main menu.
4. Click **IP Filtering** from the left side menu. Field descriptions are listed below the screen example.

Start Address	End Address	Enabled
192.168.0.4	192.168.0.4	☒
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐

Label	Description
Start Address	Defines the starting IP address to block.
End Address	Defines the ending IP address to block.
Enabled	Activates the rule when enabled is checked.
Apply	Saves changes.

6.3 Using the MAC Filtering Option

The **MAC Filtering** option allows you to filter MAC addresses to block Internet traffic from specific network devices on the LAN. MAC filtering establishes a list and any host on this list is not able to access the network through the DDW36C.



Steps

To filter MAC addresses:

1. Note the MAC addresses of the devices that you want to deny Internet access.
Be sure all devices to which you potentially deny Internet access are connected to the DDW36C network.
2. Click **Advanced** from the main menu.
3. Click **MAC Filtering** from the left side menu.
4. Enter the MAC address to block in the text box to the left of the **Add MAC Address** button.
5. Click the **Add MAC Address** button. The MAC address is displayed in the filtered

MAC address list. Field descriptions are listed below the screen example.

Label	Description
MAC Addresses	Specifies the MAC address to block. Enter the MAC address in the field.
Add MAC Address	Adds a MAC address to the list of addresses to block.
Addresses entered: n/20	Displays the MAC addresses to be blocked. The number of MAC addresses entered is shown as 1/20 where 1 is the number of addresses in the list. You can filter up to twenty MAC addresses at one time.
Remove MAC Address	Deletes the selected MAC address from the list of addresses to be blocked.
Clear All	Removes all MAC addresses from the list.

6.4 Using the Port Filtering Option

Use the **Port Filtering** option to configure port filters to block to all devices on the LAN Internet services that use the ports specified.



Steps

To configure port filters:

1. Click **Advanced** from the main menu.
2. Click **Port Filtering** from the left side menu. Field descriptions are listed below the screen example.

For example:

To prevent all Telnet access into and across your LAN:

1. Enter the **Start** and **End** ports to be 23.
2. Select **Both** for Protocol to include TCP and UDP.
3. Check **Enabled**.
4. Click **Apply**. Field descriptions are listed below the screen example.



Caution

Use caution when assigning port filtering by port range. You may accidentally prevent traffic that should pass through your network, such as http or email. Pre-assigned application ports are displayed on the Forwarding screen. Refer to [Using the Forwarding Option on page 54](#).

Start Port	End Port	Protocol	Enabled
1	65535	Both	☒
		Both	☐
		Both	☐
		Both	☐
		Both	☐
		Both	☐
		Both	☐
		Both	☐
		Both	☐
		Both	☐
		Both	☐

Label	Description
Start Port	Defines the starting port number
End Port	Defines the ending port number.
Protocol	Selects the protocol type. Options are UDP, TCP, or Both.
Enabled	Activates the rule and filters out all traffic on the specified ports.
Apply	Saves changes.

6.5 Using the Forwarding Option

Forwarding tells the DDW36C to which computer on the local area network to send data. If your host systems or applications have communications issues with the Internet, you can use forwarding to resolve the following issues:

- ☐ Data is sent from a local host to the Internet, but the return path of expected data is not received by your local host.
- ☐ An application or service running on your local network (on local host) cannot be accessed from the Internet directly (for example, a request to a local audio server). Examples are:
 - ◆ Xbox/PlayStation – Games/applications
 - ◆ Home Security Systems – Security systems that use the Internet
 - ◆ Audio Servers/VoIP – Audio and VoIP applications and services



Topics

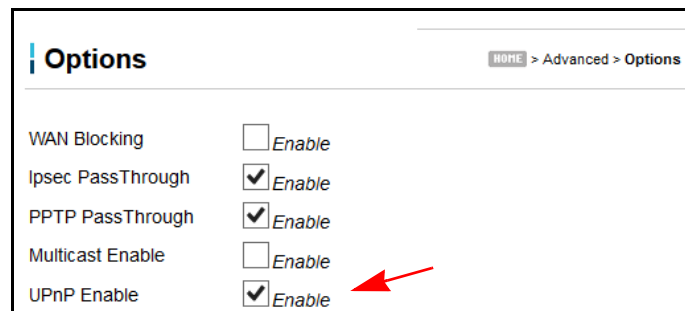
See the following topics:

- ◆ [Before Setting Up Forwarding on page 54](#)
- ◆ [Setting Up Forwarding on page 55](#)
- ◆ [Setting Up Port Forwarding for an Xbox Example on page 58](#)

6.5.1 Before Setting Up Forwarding

Try the following options before you assign forwarding rules:

1. Enable Universal Plug and Play (UPnP). This may resolve the issue you have without setting up forwarding rules.
 - a. Access the Web interface of the DDW36C, see [Accessing the Web User Interface Locally on page 14](#).
 - b. Click **Advanced** from the main menu.
 - c. Click **Options** from the left menu.
 - d. Check the **UPnP Enable** box



- e. Click **Apply**.

- f. Test your local host or application such as your Xbox to see if it is functioning properly. Continue with port forwarding if the host or application is not communicating correctly.
2. Assign a Static IP lease to the client/host to which you are setting up forwarding. This way, the IP does not change and disrupt your forwarding rules. For example, if you are hosting a Web server in your internal network, and you wish to setup a forwarding rule for it, assign a static IP lease to that system to keep the IP from renewing and disrupting the forwarding rule.

6.5.2 Setting Up Forwarding

If the suggestions in [Before Setting Up Forwarding on page 54](#) did not correct your communication problem, use port forwarding.

You need the following information to set up port forwarding:

- ☐ **IP address** of each local host system (for example, Xbox) for which you need to setup a port forwarding rule.
- ☐ **Port numbers** the local host's application listens to for incoming requests/data (for example, a game or other service). These port numbers should be available in the documentation associated with the application.



Note

For detailed information on port forwarding, including how to set it up for specific applications using specific network devices (for example, cable modems), refer to: <http://portforward.com> or consult your host device or application user manual.



Steps

To set up port forwarding:

1. Access the Web interface of the DDW36C, see [Accessing the Web User Interface Locally on page 14](#).
2. Click **Advanced** from the main menu.
3. Click **Forwarding** from the left menu.
4. Click either **Create IPv4** or **Create IPv6**.



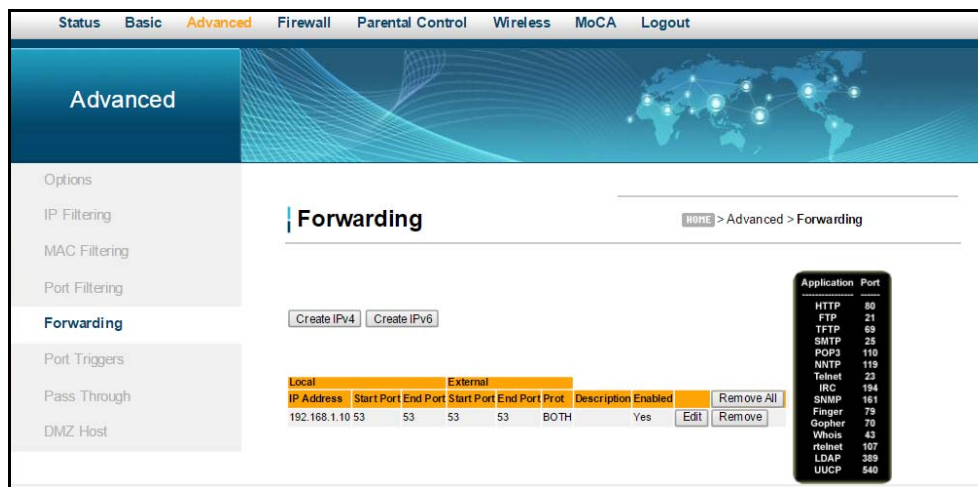
5. Enter information in the forwarding fields as shown in the screen shot below. **Create IPv4** was selected for the following screen shots. Field descriptions follow.



Label	Description
Local IP	Defines the IP address of the local LAN device to which the forwarding rule applies. For example, an Xbox or PC.
Local Start Port	Defines the starting port number listened to by the server host located in your LAN.
Local End Port	Defines the ending port number listened to by the server host located in your LAN.
External Start Port	Defines the port number to start the range of ports to publish to the Internet.

External End Port	Defines the port number to end the range of ports published to Internet. Note: Be very careful with ranges. Ports within a range are not usable by other applications that may require them. It is common and safer to enter the same port number as the start and end of the range.
Protocol	Selects the protocol type. Options are UDP, TCP, or BOTH.
Description	Specifies the forwarding rule name.
Enabled	Disables (Off) or enables (On) the forwarding rule.
Cancel	Stops the forwarding rule creation process and returns you to the previous Forwarding screen.
Apply	Saves changes.
Port Map	Shows a list of common applications and their ports.
Forwarding Table – Lists existing forwarding rules.	
Remove All	Deletes all entries in the forwarding table.

6. Click **Apply**. The forwarding rule is created and displayed in the table as shown below. Additional field descriptions follow.



Label	Description
Remove All	Deletes all entries in the forwarding table.
Edit	Displays fields for the rule selected in order to change values.
Remove	Deletes the selected rule.

6.5.3 Setting Up Port Forwarding for an Xbox Example

The following is an example of how you would set up a single Xbox running Modern Warfare 2. Since multiple ports are used for the Xbox and the Modern Warfare 2 game, a separate forwarding rule is set for each port. Multiple ports and forwarding rules may not be required for other applications.



Steps

To set up port forwarding for an Xbox:

1. Click **Advanced** from the main menu.
2. Click **Forwarding** from the left side menu.
3. Enter the Xbox IP address in the **Local IP** field.
4. Define ports used by the Xbox in the **Local Start Port** and **Local End Port** fields. Define the same ports used by the Xbox in the **External Start Port** and **External End Port** fields.
5. Create Port Forwarding rules per port. A rule set up for port 53 works for port 53. A port can be used only by one program at a time.

Local IP Address	Local Start Port	Local End Port	External Start Port	External End Port	Prot	Description	Enabled	Edit	Remove
192.168.1.10	53	53	53	53	BOTH		Yes	Edit	Remove
192.168.1.10	80	80	80	80	BOTH		Yes	Edit	Remove
192.168.1.10	88	88	88	88	BOTH		Yes	Edit	Remove
192.168.1.10	3074	3074	3074	3074	BOTH		Yes	Edit	Remove

Application	Port
HTTP	80
FTP	21
TFTP	69
SMTP	25
POP3	110
NINTP	119
Telnet	23
IRC	184
SNMP	161
Finger	79
Gopher	70
Whois	43
Relnet	107
LDAP	389
UUCP	540



Note

You can set up applications/services to listen on one internal port. External Internet users who want to access that application, address it using an external port, such as an Audio server. Internal Ports are the ports to which local servers listen. External Ports are the ports that the cable modem listens to from the WAN.

6.6 Using the Port Triggers Option

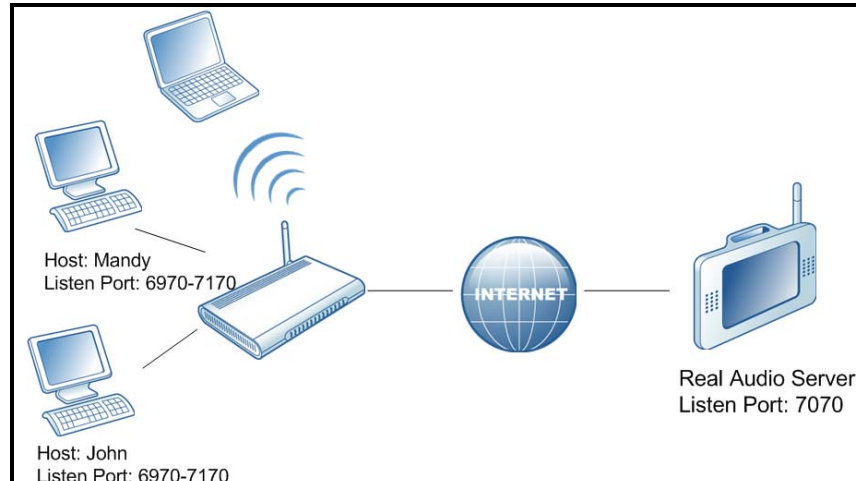
Port Triggers define dynamic triggers for specific devices on the LAN. This allows special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. The difference between port forwarding and triggering is:

- ◆ Port forwarding sets a rule to send a service to a single LAN IP address.
- ◆ Port triggering defines two kinds of ports: trigger port and target port. The trigger port sends a service request from a LAN host to a specific destination port number. The port the LAN host is required to listen to by the application is called the target port. The server returns responses to these ports.

For example:

1. John requests a file from the Real Audio server (port 7070). Port 7070 is a “trigger” port and causes the device to record John’s computer IP address. The DDW36C associates John’s computer IP address with the “target” port range of 6970-7170.
2. The Real Audio server responds to a port number ranging between 6970-7170.
3. The DDW36C forwards the traffic to John’s computer IP address.
4. Only John can connect to the Real Audio server until the connection is closed or expires.



Steps

To set up port triggering:

1. Click **Advanced** from the main menu.
2. Click **Port Triggers** from the left side menu.
3. Click **Create** and enter information in the trigger fields.

- Click **Apply**. The port trigger rule is created and displayed in the table. Field descriptions are listed below the screen example.



Note

The following example shows the Port Triggering option set up for a dual Xbox configuration.

Trigger		Target		Prot	Description	Enabled		
Start Port	End Port	Start Port	End Port				Edit	Remove
53	53	53	53	BOTH	Yes	Edit	Remove	
80	80	80	80	UDP	Yes	Edit	Remove	
88	88	88	88	TCP	Yes	Edit	Remove	
3074	3074	3074	3074	BOTH	Yes	Edit	Remove	

Label	Description
Trigger Start Port	Defines a port number or the starting port number in a range of port numbers.
Trigger End Port	Defines a port number or the ending port number in a range of port numbers.
Target Start Port	Defines a port number or the starting port number in a range of port numbers.
Target End Port	Defines a port number or the ending port number in a range of port numbers.
Protocol	Defines the protocol type for this rule, UDP, TCP, or Both.
Description	Names the triggering rule.
Enabled	Enables (on) or disables (off) the triggering rule.
Remove All	Deletes all port triggering rules.
Edit	Allows you to edit a port triggering rule.
Remove	Deleted a port triggering rule.

6.7 Using the Pass Through Option

Use the **Pass Through** option to configure a pass through table. Devices in the pass through table are treated as bridge devices, storing and forwarding data between LAN interconnections.



Steps

To configure a pass through table:

1. Click **Advanced** from the main menu.
2. Click **Pass Through** from the left side menu. The pass through fields are explained following this screen example.

The screenshot shows the 'Advanced' configuration page of the Ubee DDW36C. The left sidebar lists various options: IP Filtering, MAC Filtering, Port Filtering, Forwarding, Port Triggers, **Pass Through** (selected), and DMZ Host. The main content area is titled 'Pass Through' and includes a breadcrumb trail: HOME > Advanced > Pass Through. Below the title, there is a text input field for 'PassThrough Mac Addresses (example: 01:23:45:67:89:AB)' with an 'Add Mac Address' button. A list box below shows a single entry '00:25:c1:d2:c4:e3' with up and down arrows. To the right of the list box, it says 'Addresses entered: 1/32'. At the bottom of the list box are 'Remove Mac Address' and 'Clear All' buttons.

Label	Description
Pass Through MAC Addresses	Defines the input host's MAC address.
Add MAC Address	Adds the input host's MAC address.
Addresses entered: n/32	Displays the MAC addresses to be blocked. The number of MAC addresses is shown as 0/32 where 0 is the number of addresses in the list. You can add up to 32 MAC addresses at one time.
Remove MAC Address	Removes the input host's MAC address.
Clear All	Removes all of the input host's MAC addresses.

6.8 Using the DMZ Host Option

Use the **DMZ Host** option to expose a host IP address to the WAN (public Internet). You can use this option when applications do not work with port triggers or other networking strategies.



Steps

To set up a DMZ host:

1. Connect a PC to an Ethernet port on the DDW36C. Make sure both devices are powered on and functioning.
2. Connect a Home Gateway (or other device you wish to be in the DMZ) to an Ethernet

- port on the DDW36C.
3. Log in to the DDW36C Web user interface.
 4. Click **Advanced** from the main menu.
 5. Click **DMZ Host** from the left side menu.
 6. Enter the IP address you just configured in the Static Lease section.
 7. Test the device to ensure Internet access is available and the device is functional. For example, connect to the Internet from a PC connected to the Home Gateway, or make calls from a VoIP phone.



Label	Description
DMZ Address	Defines the IP address of the host to be exposed.
Apply	Saves changes.

7 Understanding the Firewall Menu

Use these instructions to configure the DDW36C firewall settings to control what types of traffic are allowed on your network. The firewall can block certain Web-oriented cookies, Java scripts, and pop-up windows. It is highly recommended the Firewall is left enabled at all times to protect against denial of service (DoS) attacks. Refer to [Using the Basic Option on page 63](#) to block Internet access to specific sites.

Note: Firewall menu options are not available when the device is in Bridge mode.



Topics

See the following topics:

- ◆ [Using the Basic Option on page 63](#)
- ◆ [Using the Local Log Option on page 64](#)
- ◆ [Using the Remote Log Option on page 65](#)



Steps

To access the firewall menu:

1. Access the Web user interface. Refer to [Accessing the Web User Interface Locally on page 14](#).
2. Click **Firewall** from the main menu.

7.1 Using the Basic Option

Use the **Basic** option to filter Web content to block certain Web-oriented cookies, Java scripts, and pop-up windows.



Steps

To filter Web content:

1. Click **Firewall** from the main menu.
2. The **Basic** screen is displayed. Field descriptions are listed below the screen example.

The screenshot shows the 'Firewall' configuration page. The 'Basic' tab is selected. On the left, there are links for 'Local Log' and 'Remote Log'. The main area is titled 'Web Content Filter'. It includes settings for 'IPv4 Firewall Protection' (set to 'Low') and 'IPv6 Firewall Protection' (set to 'On'). Below these are checkboxes for 'Block Fragmented IP Packets', 'Port Scan Detection', 'IP Flood Detection', and 'Optimize for XBOX (may stabilize video streaming)', all of which are checked. An 'Apply' button is at the bottom. On the right, the 'Allowed Services' window is open, showing 'No Ports Restricted'.

Label	Description
IPv4 Firewall Protection	Defines the level of IPv4 protection. Choices are Off, Low, Medium, and High. Services are based on the protection level and displayed in the Allowed Services window.
IPv6 Firewall Protection	Defines whether IPv6 firewall protection is On or Off.
Block Fragmented IP Packets	Detects fragmented IP packets and blocks them.
Port Scan Detection	Detects port scans that probe for available ports and potentially use these ports to detect weakness in the network.
IP Flood Detection	Detects IP flood attacks that send excessive information to the device, using up bandwidth.
Optimize for XBOX	When enabled, this feature stabilizes and improves video streaming. This disables LDPC (low-density parity-check) for some Xbox implementations, like the older Xbox Slim, that do not properly support the protocol.
Apply	Saves changes.

7.2 Using the Local Log Option

Use the **Local Log** to define firewall event log reporting through email alerts and report on possible attacks on the system.



Steps

To define local log reporting:

1. Click **Firewall** from the main menu.
2. Click **Local Log** from the left side menu. Field descriptions are listed below the screen example.

Description	Count	Last Occurrence	Target	Source
TCP- or UDP-based Port Scan	7	Tue Jun 24 09:09:24 2014	10.2.1.61:55722	8.8.8.8:53
TCP- or UDP-based Port Scan	3	Wed Nov 12 12:24:38 2014	10.2.1.10:61486	192.168.250.221:53
TCP- or UDP-based Port Scan	4	Wed Nov 12 12:46:01 2014	10.2.1.10:50522	8.8.8.8:53
TCP- or UDP-based Port Scan	2	Wed Nov 12 12:36:54 2014	10.2.1.10:63002	75.75.75.75:53

E-mail Log Clear Log

Label	Description
Contact Email Address	Defines the email address where you want to send the log.
SMTP Server Name	Defines the name of the SMTP server, such as smtp.example.com.
SMTP Username	Defines the username for the email address, such as contact@company.com.
SMTP Password	Defines the password for the email address.
E-mail Alerts	Enables or disables log reporting.
Apply	Saves the settings and completes the setup.
E-mail Log	Sends the log to the specified email address.
Clear Log	Deletes the log.

7.3 Using the Remote Log Option

Use the **Remote Log** option to define events and send the log to a local SysLog server.



Steps

To configure the firewall remote log:

1. Click **Firewall** the main menu.
2. Click **Remote Log** from the left side menu. The **Remote Log** fields are explained following this screen example.

Ubee DDW36C Firewall Remote Log configuration page. The page shows a navigation bar with tabs: Status, Basic, Advanced, Firewall (selected), Parental Control, Wireless, MoCA, and Logout. The Firewall section is active, showing a sidebar with 'Basic', 'Local Log', and 'Remote Log' (selected). The main content area is titled 'Remote Log' and includes a breadcrumb 'HOME > Firewall > Remote Log'. It contains a section 'Send selected events' with four checkboxes: 'Permitted Connections', 'Blocked Connections', 'Known Internet Attacks', and 'Product Configuration Events'. Below these is a text field 'to SysLog server at 192.168.0.0' and an 'Apply' button.

Label	Description
Permitted Connections	Logs all access attempts that are allowed by the firewall.
Blocked Connections	Logs all access attempts that are blocked by the firewall.
Known Internet Attacks	Logs all known attacks from the Internet.
Product Configuration Events	Logs when the DDW36C is configured/modified by a user or administrator.
to SysLog server at 192.168.0.	Defines the IP address of the Syslog server.
Apply	Saves changes.

8 Understanding the Parental Control Menu

Parental Controls allow you to control Internet access for users on the DDW36C network. Parental Controls provides the following features:

- ◆ Define user/password access.
- ◆ Block specific Web sites and Web sites based on keywords.
- ◆ Define the times users are allowed to access the Internet.
- ◆ View a local log to view Internet activity.



Topics

See the following topics:

- ◆ [Using the Parental Control User Setup Option on page 67](#)
- ◆ [Using the Basic Option on page 69](#)
- ◆ [Using the ToD Filter Option on page 71](#)
- ◆ [Using the Local Log Option on page 72](#)



Steps

To access the parental control menu:

1. Access the Web interface. Refer to [Accessing the Web User Interface Locally on page 14](#).
2. Click the **Parental Control** link from the top of the screen.

8.1 Using the Parental Control User Setup Option

The **User Setup** option allows you to configure which user accounts can or cannot connect to your wireless or wired network, and the parameters of each connection.



Steps

To configure user accounts:

1. Click the **Parental Control** link from the top of the screen.
2. The **User Setup** screen is displayed. The **User Setup** fields are explained following the screen example.

Note: To enable Parental Control, refer to [Using the Basic Option on page 69](#).

The screenshot shows the 'Parental Control' interface. The 'User Setup' section is active, displaying a list of users. The 'User Settings' for '2 User 1' are shown, including a password field, a re-enter password field, a 'Trusted User' checkbox, a 'Content Rule' dropdown, a 'Time Access Rule' dropdown, a 'Session Duration' field (1440 min), and an 'Inactivity time' field (60 min). Below these are 'Trusted Computers' and 'No Trusted Computers' sections with 'Add' and 'Remove' buttons.

Label	Description
Add User Remove User Enable	Defines user accounts. ♦ To select an existing user, choose the user from the User Settings drop-down menu. ♦ To add a new user, add the user name and click Add. Note that the user name cannot contain any spaces. ♦ To activate the user, check Enable. ♦ To remove a user, select the user from the drop-down menu and click Remove User.
Password	Defines the password for this user. It is required when this user tries to access the Internet via the device.
Re-Enter Password	Confirms the password with the re-entered password.
Trusted User	Each specified user may also be enabled as a “trusted user” which means that person will have access to all Internet content regardless of filters that may be set up. This check box can be used as a simple override to grant a user full access but still having the ability to keep all of the previous settings stored and available.
Content Rule	Provides a drop-down list of existing content rules that define what kind of Websites the user can or cannot visit.
White List Access Only	Selects the White List Access option. If you have created a content rule that defines a black list and white list, select the White List Access Only checkbox to force the DDW36C to execute the policy for the selected user.

Label	Description
Time Access Rule	Selects a defined time access rule to apply to the selected user.
Session Duration	Allows you to enter a time in minutes for the user's session to expire. When the session expires, the user can log in again for the same session duration.
Inactivity Time	Allows you to enter the time out value when a user has no activity on the Internet. When the time expires, the user interface to the Internet is canceled.
Apply	Saves all changes when clicked.
Trusted Computers	Defines the trusted hosts that can bypass the Parental Control Process.
Add	Adds the trusted host's MAC address entered in the given area and Add is clicked.
Remove	Removes a trusted computer from the list when it is highlighted and Remove is clicked.

8.2 Using the Basic Option

The **Basic** option allows you to select rules to block certain Internet content and Web sites. After you change your Parental Control settings, click the appropriate Apply, Add, or Remove button for your new settings to take effect. Refresh your browser's display to see the currently active settings.



Steps

To filter Internet content and Web sites:

1. Click the **Parental Control** link from the top of the screen.
2. Click **Basic** from the left side of the screen. The **Basic** fields are explained following this screen example.

The screenshot displays the 'Parental Control' configuration interface. At the top, a navigation bar includes links for Status, Basic, Advanced, Firewall, Parental Control (highlighted), Wireless, MoCA, and Logout. The main header area features a 'Parental Control' title and a decorative background with a world map. On the left, a sidebar contains links for User Setup, Basic (selected), ToD Filter, and Local Log. The main content area is titled 'Basic' and includes a breadcrumb trail: HOME > Parental Control > Basic. The configuration options are as follows:

- Enable Parental Control:** A checkbox that is currently checked, with an 'Apply' button below it.
- Content Policy Configuration:** A section containing:
 - Add New Policy:** A button to create a new policy.
 - Content Policy List:** A dropdown menu showing '2: SmithFamily' and a 'Remove Policy' button.
 - Keyword List:** A list containing 'anonymizer', with 'Add Keyword' and 'Remove Keyword' buttons.
 - Blocked Domain List:** A list containing 'anonymizer.com', with 'Add Domain' and 'Remove Domain' buttons.
 - Allowed Domain List:** A list containing 'ubee.com', with 'Add Allowed Domain' and 'Remove Allowed Domain' buttons.

Label	Description
Enable Parental Control	Activates the Parental Control feature when checked.
Apply	Saves all changes in the screen and activates Parental Control, if enabled.
Content Policy Configuration	
Add New Policy	Adds a policy to the Policy List. Enter the policy name and click Add New Policy. Note: the policy name cannot contain any spaces.
Content Policy List	Lists existing policies you can choose to use.
Remove Policy	Deletes a policy from the list. Select the policy from the list and click Remove Policy.
Keyword List	Displays keywords you can use to block Web site addresses (URLs) containing those words.
Add Keyword	Adds a keyword to the keyword list. Enter the word in the field next to the Add Keyword button and click Add Keyword. The keyword is added to the list.
Remove Keyword	Removes a keyword from the keyword list. Select the keyword from the list, and click Remove Keyword.
Blocked Domain List	Displays Web domains (for example, unwanted.com) you can use to block access to those domains.
Add Domain	Adds a domain to the Allowed Domain List. Enter a domain, and click Add Domain.

Label	Description
Remove Allowed Domain	Removes a domain from the Allowed Domain List. Select the domain from the list, and click Remove Domain.
Allowed Domain List	Displays domains you can assign to users to visit only the sites allowed.
Add Allowed Domain	Adds allowed domains to the list. Enter the name and click Add Allowed Domain.
Remove Allowed Domain	Removes domain names from the list. Highlight the domain from the list and click Remove Allowed Domain.

8.3 Using the ToD Filter Option

The **ToD** (Time of Day) **Filter** option allows the configuration of time-based access policies to block all Internet traffic at specified times.



Steps

To configure ToD filters:

1. Click the **Parental Control** link from the top of the screen.
2. Click **ToD Filter** from the left side of the screen. The **ToD Filter** fields are explained following this screen example.

The screenshot displays the 'Parental Control' section of the Ubee DDW36C Advanced Wireless Gateway web interface. The left sidebar shows a navigation menu with 'User Setup', 'Basic', 'ToD Filter' (selected), and 'Local Log'. The main content area is titled 'ToD Filter' and includes a breadcrumb trail: 'HOME > Parental Control > ToD Filter'. Below the title is a section for 'Time Access Policy Configuration' with a text input field for a policy name and an 'Add New Policy' button. A 'Time Access Policy List' section shows a table with one policy named 'Weekend', which is 'Enabled' and has a 'Remove' button. Below the table, there are checkboxes for 'Days to Block' (Everyday, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday) and 'Time to Block' (All day). The 'Time to Block' section includes fields for 'Start' (8:00 AM) and 'End' (4:30 PM). The 'Ports to Block' section has checkboxes for 'Enabled', 'Port Start' (80), 'Port End' (80), and 'Protocol' (UDP). An 'Apply' button is at the bottom.

Label	Description
Add New Policy	Adds a new policy. Enter a policy name and click the Add New Policy button.
Time Access Policy List	Lists the existing policies in a drop-down list.
Enabled	Activates a policy. Select the policy from the drop-down list and check Enabled.
Remove	Deletes a policy. Select the policy from the drop-down list and click Remove.
Days to Block	Selects the days to block Internet access.
Time to Block: All Day or a specific time frame	Defines the time to block. ♦ To block all day, check All Day to eliminate all access during the days selected. ♦ To block a specific time frame for the days selected, enter the Start time and the End time. Select AM or PM for each.
Ports to Block	Defines a port range to block if the Enabled box is checked. ♦ Port Start: Enter the starting port number to be blocked. ♦ Port End: Enter ending port number to be blocked. ♦ Protocol: Select the protocol type. Options are UDP, TCP, or Both.
Apply	Saves all changes when clicked.

8.4 Using the Local Log Option

The **Local Log** option displays Parental Control event log reporting.



Steps

To view the parental control local log:

1. Click the **Parental Control** link from the top of the screen.
2. Click **Local Log** from the left side of the screen. The **Local Log** fields are explained following this screen example.



Label	Description
Last Occurrence	Displays the time when the last event occurred.
Action	Displays what is done by parental control, including dropping or permitting access requests.
Target	Displays the destination IP address or URL of a certain access request.
User	Displays the user who triggered this event log.
Source	Displays the source MAC address of this event.
Clear Log	To empty the displayed log entries, click Clear Log.

9 Understanding the Wireless Menu

Use the Wireless menu to configure wireless network settings for both the 2.4GHz and 5GHz radio bands. The DDW36C is a dual-band concurrent wireless gateway, supporting operation of both the 2.4GHz and 5GHz radio bands simultaneously.



Topics

See the following topics:

- ◆ [Selecting the Wireless Radio Band on page 74](#)
- ◆ [Using the Wireless Radio Option on page 75](#)
- ◆ [Using the Primary Network Option on page 77](#)
- ◆ [Using the Access Control Option on page 82](#)
- ◆ [Using the Wi-Fi Multimedia Option on page 84](#)
- ◆ [Using the Wireless Bridging Option on page 86](#)
- ◆ [Deploying and Troubleshooting the Wireless Network on page 87](#)



Steps

To access the wireless menu:

1. Access the Web interface. Refer to [Accessing the Web User Interface Locally on page 14](#).
2. Click **Wireless** from the main menu. The Wireless Radio screen is displayed.

9.1 Selecting the Wireless Radio Band

The DDW36C is a dual-band concurrent wireless gateway, supporting operation of both the 2.4GHz and 5GHz radio bands simultaneously. Each of the radio bands can be configured separately (i.e. changing the wireless network name or password). On the top left side of each screen in the Wireless tab, you can select which radio you want to configure (either the 2.4GHz or the 5GHz). The screen shot below shows the radio band selection boxes (with 2.4GHz being selected/highlighted).



NOTE: Selecting the radio band as above is only an indicator of which band you are actively configuring, both the 2.4GHz and 5GHz bands are enabled by default.

9.2 Using the Wireless Radio Option

The **Radio** option is used to configure the wireless radio, including channel number, and bandwidth control.



Steps

To configure wireless operations:

1. Click **Wireless** from the main menu.
2. The **Radio** screen is displayed. Field descriptions are listed below the screen example (the screen example shows the 2.4GHz radio selected).

Label	Description
2.4GHZ / 5GHz (top left side)	On the top left side of the screen, you can select either the 2.4GHz or 5GHz radio band to configure.
Wireless Status	Displays the selected wireless radio's status, Enabled or Disabled.
Channel Bandwidth	Sets the channel bandwidth and displays the current channel bandwidth. ♦ For the 2.4GHz radio, options are 20MHz (default value) or 20/40MHz. ♦ For the 5GHz radio, options are 20MHz, 20/40MHz, or 20/40/80MHz (default value). NOTE: ♦ 802.11b and 802.11g support 2.4GHz, 20MHz wide channels ♦ 802.11n supports 2.4GHz or 5GHz, 20MHz or 40MHz wide channels ♦ 802.11a supports 5GHz, 20MHz wide channels ♦ 802.11ac supports 5GHz, 20/40/80MHz wide channels

Label	Description
Wireless Channel	Set to Auto by default, the Wireless Channel selects a specific channel to deploy the wireless network. This allows you to set the operating frequency/channel depending on your particular region. Channel selection can have an impact on wireless networking performance. For more information, refer to Selecting a Wireless Channel on page 91 . The current channel is displayed as well as the interference level.
Apply	Saves all screen changes when clicked.
Restore Wireless Defaults	Restores the factory default settings for wireless configurations when clicked.
Scan Wireless APs	Scans for other wireless access points and displays channel, encryption, SSID, RSSI levels, and other information. See the section below for more information.

9.2.1 Scanning for Wireless Access Points (APs)

You can search for nearby wireless access points and display the results in a new window.



Steps

To search for wireless access points:

1. Click **Scan Wireless APs** at the bottom of the Wireless Radio screen. Results are displayed in a new window.

Network Name	Security Mode	Mode	PHY Mode	RSSI	Channel	Bandwidth	BSSID
WIFI8E55E4	WPA2-PSK AES-CCMP	Managed	802.11ac	-64 dBm	6	20 MHz	00:71:cc:8e:55:e8
WSMCorp_Guest	WPA2-PSK AES-CCMP	Managed	802.11n	-69 dBm	6	20 MHz	02:18:4a:a4:14:32
HP-Print-b2-LaserJet 100	NONE	Managed	802.11b/g	-71 dBm	6	20 MHz	9c:2a:70:67:ac:b2
CenturyLink7358	WPA2-PSK TKIP AES-CCMP	Managed	802.11n	-59 dBm	6	20 MHz	12:7b:ef:a1:ef:8c
UBEE-CORP	WPA2-PSK AES-CCMP TKIP	Managed	802.11b/g	-49 dBm	11	20 MHz	dc:9f:db:1c:be:4a
CC33B8	WPA2-PSK AES-CCMP TKIP	Managed	802.11ac	-66 dBm	7 + 11	40 MHz	10:08:b1:cc:33:b8
DVW326.A1CF28-2.4G	WPA2-PSK AES-CCMP TKIP	Managed	802.11n	-70 dBm	6	20 MHz	f8:2f:a8:a1:cf:28
WSMCorp_Guest	WPA2-PSK AES-CCMP	Managed	802.11n	-84 dBm	11	20 MHz	02:18:4a:a5:0a:02
ots-guest	WPA2-PSK AES-CCMP	Managed	802.11b/g	-79 dBm	1	20 MHz	68:bc:0c:35:32:20
WSMCorp_Guest	WPA2-PSK AES-CCMP	Managed	802.11n	-73 dBm	1	20 MHz	02:18:4a:a4:f8:c2
ots-guest	WPA2-PSK AES-CCMP	Managed	802.11b/g	-78 dBm	1	20 MHz	c0:62:6b:8e:99:62
DunkN5	WPA2-PSK AES-CCMP	Managed	802.11n	-74 dBm	6	20 MHz	02:1a:11:f9:f9:4a
Meraki Auth Test	WPA2-PSK AES-CCMP	Managed	802.11n	-69 dBm	6	20 MHz	02:18:4a:a4:14:34
	WPA2-PSK AES-CCMP TKIP	Managed	802.11n	-70 dBm	6	20 MHz	02:18:4a:a4:14:33
	WPA2-PSK AES-CCMP	Managed	802.11n	-69 dBm	6	20 MHz	02:18:4a:a4:14:31
	WPA2 AES-CCMP TKIP	Managed	802.11n	-70 dBm	6	20 MHz	02:18:4a:a4:14:30
DDW365.B30F5E-2.4G	WPA2-PSK AES-CCMP	Managed	802.11n	-68 dBm	1	20 MHz	68:94:23:b3:0f:5e
Ubee73AB	WPA2-PSK AES-CCMP TKIP	Managed	802.11n	-84 dBm	1	20 MHz	00:00:59:e1:73:af
BROADCOM	WPA2-PSK AES-CCMP	Managed	802.11n	-74 dBm	1	20 MHz	68:94:23:b3:0f:fa
DVW3201B7B	WPA2-PSK AES-CCMP	Managed	802.11n	-72 dBm	6	20 MHz	5c:ac:4c:23:d6:5c

2. Click **Refresh** to update the results.

Label	Description
Nearby Wireless Access Points	
Network Name	Displays the name of the wireless network (SSID) broadcast by the access point.
Security Mode	Displays the encryption method used.
Mode	Displays the mode of the wireless access point: Possible modes are: ♦ Master – Communicates with associated wireless cards that are in managed mode. Appears as a normal access point with an SSID and channel. Network communications, such as authentication, conflict, and duplicate packets are managed by the wireless card. ♦ Managed – Communicates with an associated master, not directly with another managed AP. Wireless cards connect to the master network and change their channel to match. The master must accept the credentials of the managed network for it to be associated. ♦ Ad-hoc – Communicates directly with another wireless network. Network cards must be in range and use the same name and channel. ♦ Monitor – Communicates in observation mode and does not transmit. Can be used for troubleshooting wireless links or checking bandwidth usage in the area.
PHY Mode	Displays the physical transceivers (PHY) layer method used.
RSSI	Displays the received signal strength (RSSI) of the wireless access points in range of the device. Lower negative numbers (for example, -1 to -65) indicate the access point is closer. Greater negative numbers (for example, -66 to -95) indicate the access point is farther away.
Channel	Displays the channel on which the DDW36C is operating.
BSSID	Displays the MAC address for the nearby wireless access points.

9.3 Using the Primary Network Option

Use the **Primary Network** option to configure a variety of wireless security settings.



Steps

To configure wireless security options:

1. Click **Wireless** from the main menu.
2. Click **Primary Network** from the left side menu. Field descriptions are listed below the screen example. This example shows the settings when the DDW36C is in the 2.4GHz band.

Wireless default values are discussed in [Understanding Default Values and Logins on page 8](#).

Wireless

2.4G Hz | 5G Hz

Radio

Primary Network

Access Control

WMM

Wireless Bridging

Primary Network

HOME > Wireless > 2.4GHz > Primary Network

MAC-ID: (00:71:CC:8E:54:C8)

Primary Network: Enabled

Network Name (SSID): WIFI8E54C7

Broadcast SSID: On

Wireless Mode: Mixed (11b/gn)

WPA: Disabled

WPA-PSK: Disabled

WPA2: Disabled

WPA2-PSK: Enabled

WPA/WPA2 Encryption: AES

WPA Pre-Shared Key: HP3WZ7IHXT6D9QS

RADIUS Server: 0.0.0.0

RADIUS Port: 1812

RADIUS Key:

Group Key Rotation Interval: 0

WPA/WPA2 Re-auth Interval: 3600

WEP Encryption: Disabled

Shared Key Authentication: Optional

802.1x Authentication: Disabled

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Current Network Key: 1

PassPhrase:

Automatic Security Configuration

WPS: WPS Config State: Configured

Device Name: UbeeAP

WPS Setup AP

UID: a96f5eb05a07b8e6827ea2dd357c01ce

PIN: 15349392

Generate AP PIN

Configure by External Registrar: Allow

WPS Add Client

Add a client: Add

Client PIN:

Authorized Client MAC:

Label	Description
2.4GHZ / 5GHz (top left side)	On the top left side of the screen, you can select either the 2.4GHz or 5GHz radio band to configure.
MAC ID	Displays the MAC Address of the DDW36C.
Primary Network	Enables or disables the primary network.
Network Name (SSID)	Defines the primary network name (SSID) to which client devices connect. -- For the 2.4GHz radio (shown above), the default SSID is "WIFI" plus the last 6 characters of the MAC address with the letters in UPPER case. -- For the 5GHz radio, the default SSID is "WIFI" plus the last 6 characters of the MAC address with the letters in UPPER case, plus "-5G".

Label	Description
Broadcast SSID	When On is selected, the SSID is visible to wireless clients. If Off is selected, the SSID is not visible to wireless clients unless manually set up on the client. Broadcast SSID is On by default to allow broadcasting of the primary network name (SSID). Refer to Enabling a Closed Network on the Primary Network on page 81 to set up a closed network. NOTE: WPS must be disabled before Broadcast SSID can be disabled.
Wireless Mode	Allows you to define the 802.11 wireless networking standard(s). ♦ 2.4GHz band options are: Mixed (11b/g/n), and 11n only. The default is Mixed (11b/g/n). ♦ 5GHz band options are: Mixed (11a/n/ac), Mixed (11n/ac) and 11ac only. The default is Mixed (11a/n/ac).
WPA	Enables or disables the Wi-Fi Protected Access (WPA) security protocol. WPA is a subset of the IEEE 802.11i standard. Key differences between WPA and WEP are user authentication and improved data encryption. Setting WPA alone with a pre-shared key requires a RADIUS or TACACS server for authentication. This method is mostly used in large enterprise implementations.
WPA-PSK	Enables or disables WPA Pre-Shared Key (WPA-PSK). If you do not have an external RADIUS server, use WPA-PSK, which requires a single (identical) password entered into wireless gateway and wireless client. As long as the passwords match, a client is granted access to the wireless LAN.
WPA2	Enables or disables WPA2. This advanced protocol is certified through Wi-Fi Alliance's WPA2 program and implements the mandatory elements of 802.11i. In particular, it has an AES-based algorithm (CCMP) that is considered fully secure. Setting WPA2 alone with a pre-shared key requires a RADIUS or TACACS server for authentication. This method is mostly used in large enterprise implementations.
WPA2-PSK	Enables or disables WPA2-PSK. If you do not have an external RADIUS server, use WPA2-PSK, which requires a single (identical) password entered into wireless gateway and wireless client. As long as the passwords match, a client is granted access to the wireless LAN. This is the default residential setting. It is more secure than WPA-PSK and uses AES encryption.
WPA/WPA2 Encryption	Sets WPA2 encryption to AES for WPA2, and WPA Encryption to AES or TKIP+EAS. The default is WPA2/AES. NOTE: TKIP encryption results in maximum link speed of 54Mbps. Use WPA2+PSK with AES for maximum performance and encryption security.

Label	Description
WPA Pre-Shared Key	Displays the WPA Pre-Shared Key when “Show Key” is checked. The WPA pre-shared key is a unique key for each device. It is a randomly generated character string, 16 characters in length, and can also be found on the device label. The encryption mechanisms for WPA and WPA-PSK are the same, except that WPA-PSK uses a simple common password instead of user-specific credentials.
Show Key	Displays the pre-shared key when checked.
RADIUS Server	Defines the IP address of the RADIUS server, if used.
RADIUS Port	Defines a RADIUS port number when WPA or 802.1x network authentication is selected.
RADIUS Key	Defines the RADIUS Key when WPA or 802.1x network authentication is selected.
Group Key Rotation Interval	Allows the device to generate the best possible random group key and update all the key-management capable stations periodically. This field is set to 0 by default.
WPA/WPA2 Re-auth Interval	Sends a new group key to all clients at the specified interval for a wireless router (if using WPA-PSK key management) or RADIUS server (if using WPA key management). The re-keying process is the WPA equivalent of automatically changing the WEP key for a wireless access point and all stations in the WLAN on a periodic basis. Setting the WPA Group Key Update Timer is also supported in WPA-PSK mode.
WEP Encryption	Enables or disables WEP encryption. If you do not have wireless clients that can use WPA or WPA2, you can use WEP key encrypting. A higher bit key offers better security. WEP encryption scrambles the data transmitted between the wireless stations and the DDW36C to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the DDW36C must use the same WEP key. Data Encryption can be set to WEP 128-bit , 64-bit , or Disable .
Shared Key Authentication	Defines Shared Key Authentication as optional or required. Shared Key is an authentication method used by wireless LANs, which follow the IEEE 802.11 standard. Wireless devices authenticate each other by using a secret key that is kept by both devices.
802.1x Authentication	Enables or disables 802.1x to authenticate wireless clients.
Network Key 1-4	Pre-defines up to 4 keys for 64-bit or 128-bit (64-bit keys require 10 hexadecimal digits) (128-bit key require 26 hexadecimal digits).
Current Network Key	Selects one of the four pre-defined keys as the current network key.

Label	Description
Passphrase	Sets the WEP encryption key by entering a word or group of printable characters in the Passphrase box and clicking Generate WEP keys. These characters are case sensitive.
Generate WEP Keys	Forces the device to generate 4 WEP keys automatically.
Apply	Saves changes.
Automatic Security Configuration — Sets up WPS (Wi-Fi Protected Setup) for devices connecting to the wireless network.	
WPS/Disabled	Enables or disables WPS option. When enabled, the following fields are available:
WPS Config State	Defines if the WPS has been configured or not.
Device Name	Defines a name for the DDW36C for WPS. The default is UbeeAP.
WPS Setup AP	
UUID	Defines the universal unique identifier (UUID) for this device.
PIN	Defines the Personal Identification Number for this device.
Generate AP PIN	Creates a new PIN for this device.
Configure by External Registrar	Options are Allow (default) and Deny.
WPS Add Client	
Add a client	Activates wireless protected setup (WPS) security on the device. To add a client: 1. Click Add a client. The WPS Add Client screen is displayed. 2. Click PUSH on the WPS Add Client screen. The WPS button is activated on the device, indicated by a flashing white light on top of the unit. 3. Press the WPS button on the device.
Client PIN	Defines a PIN number for client access.
Authorized Client MAC	Defines the MAC address of the authorized client.

9.3.1 Enabling a Closed Network on the Primary Network

You can enable a Closed Network so the SSID cannot be broadcast or seen by others.



Steps

To enable a closed network:

1. Access the pull down menu on **Broadcast SSID**.
2. Choose **Off** to enable a closed network, meaning the SSID is not visible to wireless

clients. Automatic Security Configuration is disabled.



Primary Network HOME > Wireless > 2.4GHz > Primary Network

MAC-ID: (00:71:CC:8E:54:CB)

Primary Network:

Network Name (SSID):

Broadcast SSID: Automatic Security Configuration:

Note: WPS must be disabled before Broadcast SSID can be turned to **Off**.

9.4 Using the Access Control Option

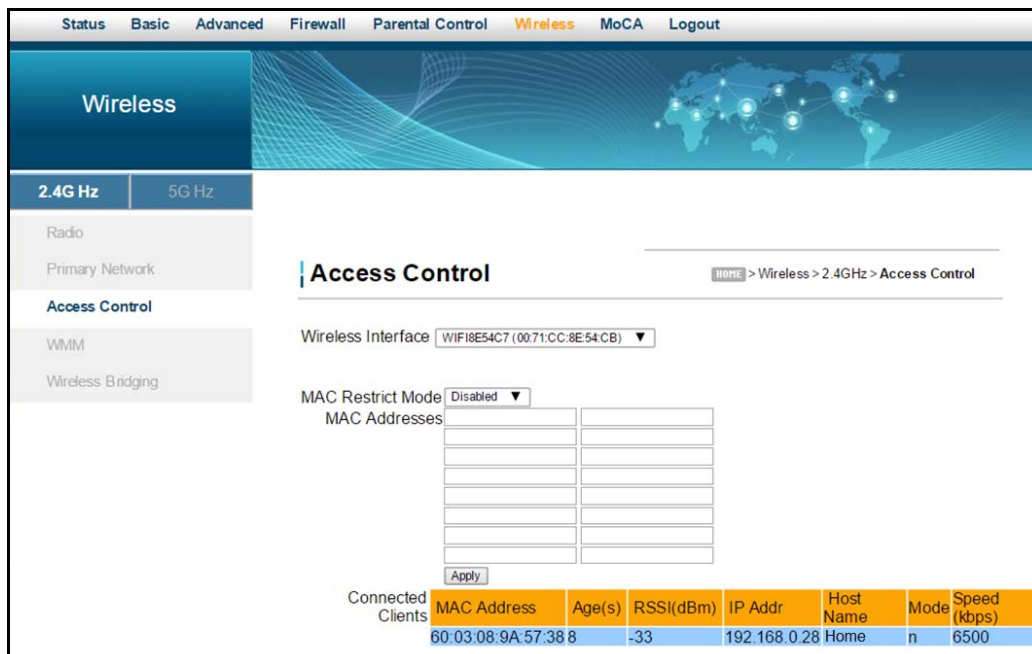
Use the **Access Control** option to configure which clients can access your wireless network.



Steps

To configure client access:

1. Click **Wireless** from the main menu.
2. Click **Access Control** from the left side menu. Field descriptions are listed below the screen example. This example shows the screen when the DDW36C is in the 2.4GHz band.



Wireless HOME > Wireless > 2.4GHz > Access Control

Wireless Interface:

MAC Restrict Mode:

MAC Addresses:

MAC Address	Age(s)	RSSI(dBm)	IP Addr	Host Name	Mode	Speed (kbps)
60:03:08:9A:57:38 8		-33	192.168.0.28	Home	n	6500

Label	Description
2.4GHZ / 5GHz (top left side)	On the top left side of the screen, you can select either the 2.4GHz or 5GHz radio band to configure.
Wireless Interface	Defines the network name (SSID) and MAC address for which you are setting access control parameters. The screen shot above shows the SSID for the 2.4GHz radio.
MAC Restrict Mode	Controls wireless access to your network by MAC address. ♦ Disabled turns off MAC restrictions and allows any wireless client to connect to this device. However, if you use other security mechanisms for access to the wireless network, clients must still adhere to those restrictions. ♦ Allow creates a list of wireless clients that can connect to the wireless network. Enter the MAC addresses of these clients in the MAC Addresses fields. MAC addresses not on the list, are not allowed access to your wireless network. ♦ Deny creates a list of wireless clients that you do not want to have access to your wireless network. Enter the MAC addresses of these clients in the MAC Addresses fields.

Label	Description
MAC Addresses	Defines the MAC addresses. Note: You may cut and paste MAC addresses from the connected clients list at the bottom of the screen.
Apply	Saves changes when clicked.
Connected Clients	Lists wireless clients currently connected listed by MAC address. ♦ MAC Address – Displays the MAC addresses entered in the MAC Addresses field (see above). ♦ Age(s) – Displays the duration since the wireless client's polled values were sent to the device. The values include all information shown on this screen. The lower the number, the more current its data. ♦ RSSI(dBm) – Displays the received signal strength from the device to the DDW36C. This value is commonly used to assist in troubleshooting wireless performance issues. A signal strength between 0dBm and -65dBm is considered optimal. Levels of -66dBm and lower (for example, -70, -80, etc.) have a downward impact on wireless data throughput. Refer to Understanding Received Signal Strength on page 87 for more information. ♦ IP Address – Displays the IP address assigned to this wireless client. ♦ Host Name – Displays the host name of the wireless client. ♦ Mode – Indicates the applicable 802.11a/b/g/n standard used by the connected client device. ♦ Speed (kbps) – Displays the maximum theoretical link speed negotiated between the DDW36C and the client, not including the overhead associated with encryption, and so on. For example, actual speeds with WEP encryption enabled are typically less than half of the negotiated link speed. TKIP encryption can also affect performance. AES is the most efficient and secure with the highest throughput possible.

9.5 Using the Wi-Fi Multimedia Option

Use the Wi-Fi Multimedia option to enable quality of service (QoS) to ensure the best service in your wireless networks.

- ☐ Controls WLAN transmission priority on packets transmitted over the wireless network.
- ☐ Wi-Fi Multi-Media Quality of Service (WMM QoS) is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.
- ☐ WMM QoS prioritizes wireless traffic according to the delivery requirements of the individual user and applications. On wireless access points without WMM QoS, all traffic streams are given the same access priority to the wireless network. If a new traffic stream creates a data transmission demand that exceeds the current network capacity, the new traffic stream reduces the throughput of the other traffic streams.

- ❑ WMM QoS capability allows you to assign access categories (ACs) to various packet streams. The assigned AC of a packet stream depends on the packet's priority, such as a priority assigned by an application (also referred to as a user priority (UP)). An AC may include a common set of enhanced distributed channel access (EDCA) parameters used by QoS to contend for a channel to transmit packets with certain priorities.

Different ACs can be associated with different power saving parameters. For example, one power saving parameter might be the delivery mechanism used by an access point (AP) to deliver packets to a station (STA) that is operating in a reduced power mode.

- ❑ WMM transmit opportunity (TXOP) is assigned to each access point. The bounded time interval during which a station can send as many frames as possible as long as the transmission time does not extend past the maximum duration of the TXOP. If a frame is too large to be transmitted in a single TXOP, it should be fragmented into smaller frames. Using TXOP reduces the problem of low rate stations gaining too much channel time in the legacy 802.11 DCF MAC. A TXOP time interval of 0 means it is limited to a single MAC service data unit (MSDU) or MAC management protocol data unit (MMPDU).



Note

Disabling WMM will break the 802.11n specification and results in speeds that tend toward a maximum speed of 54Mbps (802.11g max speed).



Steps

To enable the multimedia wireless option:

1. Click **Wireless** from the main menu.
2. Click **WMM (Wi-Fi Multimedia)** from the left side menu. Field descriptions are listed below the screen example. This example shows the screen when the DDW36C is in the 2.4GHz band.



Label	Description
2.4GHZ / 5GHz (top left side)	On the top left side of the screen, you can select either the 2.4GHz or 5GHz radio band to configure.
WMM Support	Enables (On) or disables (Off) WMM support. It is enabled by default.
Power Save Support	Enables (On) or disables (Off) power savings. WMM Power Save increases the efficiency and flexibility of data transmission. The wireless client device can “doze” between packets to save power, while the wireless access point buffers downlink frames. The application chooses the time to wake up and receive data packets to maximize power conservation without sacrificing quality of service. Power Save Support is enabled by default.
Apply	Saves changes to the WMM settings.

9.6 Using the Wireless Bridging Option

Use the **Wireless Bridging** option to configure the DDW36C to act as a wireless network bridge and establish wireless links with other wireless access points. To establish a bridge, you need to know the MAC address of the peer device, that must be in wireless bridging mode as well. The DDW36C can establish up to four wireless links with other wireless access points. When wireless devices are in wireless bridging mode, they form a wireless distribution system that allows computers in one LAN to connect to the computers in the other LAN.



Caution

Avoid bridge loops when you enable bridging devices. Bridge loops cause broadcast traffic to circle the network endlessly. This can degrade throughput and disrupt communications.



Steps

To configure the modem as a bridge:

1. Click **Wireless** from the main menu.
2. Click **Wireless Bridging** from the left side menu. Field descriptions are listed below the screen example. This example shows the screen when the DDW36C is in the 2.4GHz band.

Label	Description
2.4GHZ / 5GHz (top left side)	On the top left side of the screen, you can select either the 2.4GHz or 5GHz radio band to configure.
Wireless Bridging	
Wireless Bridging	Enables or disables the wireless bridging function. If enabled, the DDW36C will be able to communicate with a wireless repeater.
Remote Wireless Bridges MAC ID List	Defines the MAC addresses of the wireless bridges that you want to have the DDW36C send traffic to.
Apply	Saves all changes.

9.7 Deploying and Troubleshooting the Wireless Network

Use the information in this section to help you understand, deploy, and troubleshoot your wireless environments:

- ❑ [Understanding Received Signal Strength on page 87](#)
- ❑ [Estimating Wireless Cable Modem to Wireless Client Distances on page 88](#)
- ❑ [Understanding the 2.4GHz and 5GHZ Bands on page 90](#)
- ❑ [Selecting a Wireless Channel on page 91](#)

9.7.1 Understanding Received Signal Strength

Received signal strength (RSSI) is measured from connected wireless client devices to the DDW36C. This value can significantly impact wireless speeds/performance. It is determined by:

- ❑ Materials (for example, open air, concrete, trees)
- ❑ Distance between wireless clients and the wireless cable modem
- ❑ Wireless capabilities of the client devices

To determine the received signal strength, refer to [Using the Access Control Option on page 82](#) and review the **RSSI** value. A receive signal strength indicator between 0 to -64 dBm is considered optimal. Levels of -67dBm and lower (for example, -70, -80, etc.) have a downward impact on wireless data throughput.

9.7.2 Estimating Wireless Cable Modem to Wireless Client Distances

The information in this section helps you to determine how far a wireless cable modem can be placed from wireless client devices. Environmental variances include the capabilities of wireless clients and the types of material through which the wireless signal must pass. When the wireless cable modem and wireless clients reach the distance threshold between each other, network performance degrades.



Steps

To determine wireless cable modem placement:

1. Connect a wireless client to the wireless DDW36C. Refer to [Connecting Devices to the Network on page 11](#) if needed.
2. Place the wireless client at around one meter (three feet) away from the DDW36C.
3. Obtain the **RSSI** value for the connected client. Refer to [Using the Access Control Option on page 82](#). This value is used in the formula further below.
4. Use the following table to determine what materials the wireless signal must travel through to reach the desired wireless coverage distance.
5. Use the following table to determine what materials the wireless signal must travel through to reach the desired wireless coverage distance.

Attenuation Considerations

Material	Attenuation	
	2.4GHZ	5GHz
Free Space	0.24dB / foot	0.3dB / foot
Interior Drywall	3dB to 4dB	3dB to 5dB
Cubicle Wall	2dB to 5dB	4dB to 9dB
Wood Door (Hollow/Solid)	3dB to 4dB	6dB to 7dB
Brick, Concrete Wall (Note 1)	6dB to 18dB	10dB to 30dB
Glass Window (not tinted)	2dB to 3dB	6dB to 8dB
Double Pane Coated Glass	13dB	20dB
Bullet Proof Glass	10dB	20dB
Steel / Fire Exit Door	13dB to 19dB	25dB to 32dB

Attenuation Considerations

Material	Attenuation	
	2.4GHZ	5GHz
Human Body	3dB	6dB
Trees (Note 2)	0.15dB / foot	0.3dB / foot
Note 1: Different types of concrete materials are used in different parts of the world and the thickness and coating differ depending on whether it is used in floors, interior walls, or exterior walls.		Note 2: The attenuation caused by trees varies significantly depending upon the shape and thickness of the foliage.

6. Use the attenuation value from the materials table above in the following formula:

Formula:

(Transmit Power, **use -30dBm**) – (Receiver Sensitivity, **use RSSI value**) = Allowable Free Space Loss

Allowable Free Space Loss ÷ Materials Attenuation Value = Optimal Distance in Feet Between the DDW36C and a Wireless Client

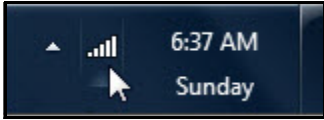
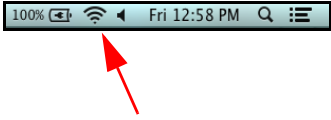
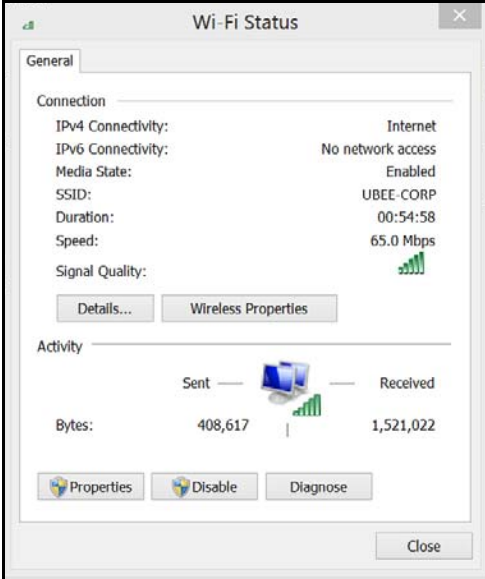
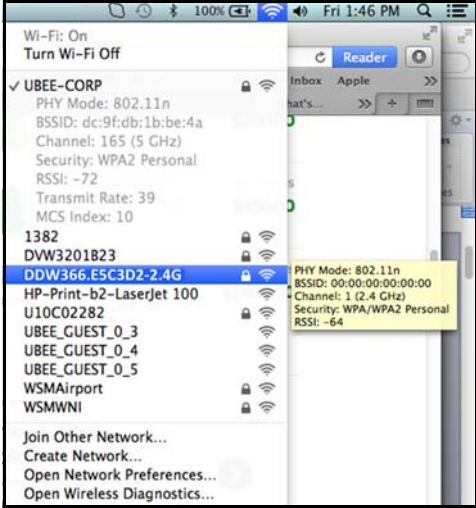
Example:

(-30dBm) - (-67dBm) = 37dBm (allowable free space loss for a 54Mbps connection)

37dBm ÷ .24db/foot (for open space) = 154.16 feet

- Once you know the optimal feet distance between individual wireless clients and the DDW36C, you may resolve and prevent some performance issues.
- Check the wireless signal strength and speed of the computer connected wirelessly to the DDW36C. Instructions for checking speeds are provided for both a Windows and Mac computer in the table below. If the wireless computer is not connected, refer to [Connecting a Wireless Device on page 12](#).

Checking Wireless Signal Strength and Speed

Windows PC	Apple Mac
1. Click the Wireless networking icon in the system tray to display a list of available wireless networks. 	1. Hold down the Option key and click on the wireless icon (Airport) on the right side of the top menu bar. 
2. Click "Open Network and Sharing Center," then click "Wireless Network Connection."	2. Information about the current wireless connection appears below the SSID. If you continue to hold the Option key and hover over any network, information about the connection is visible.
3. Review the speed and signal strength in the Status window. 	

9.7.3 Understanding the 2.4GHz and 5GHz Bands

The DDW36C operates in both the 2.4GHz and 5GHz frequency bands simultaneously. This feature allows you to choose the best band for your device to ensure stability with your local and Internet connection.

The table below provides a comparison between the 2.4GHz and 5GHz bands.

Band	2.4GHz	5GHz
Channels	In the USA, channels 1-11 are used. There are 3 non-overlapping channels (1, 6, and 11). Auto channel should be selected to ensure that the channel with the least interference is used.	23 non-overlapping channels.
Standards	802.11b,g,n	802.11a,n,ac
Network Range	Wider range	Shorter Range
Interference	Higher, as many wireless devices such as cordless phones, microwave ovens, and computers use the 2.4GHz frequency.	Lower chance of picking up interference because fewer types of wireless devices use the 5GHz frequency.
Application	Recommended for simple Internet browsing and email, as these applications don't take too much bandwidth and work fine at a greater distance.	Recommended for applications that require uninterrupted throughput, like media streaming. The wider spectrum delivers better performance.
Note: If you want to use the 5GHz frequency, all wireless client adapters must support 5GHz.		

9.7.4 Selecting a Wireless Channel

You may need to change the wireless channel on which the DDW36C operates when you are in computing, test, and other environments where several wireless access points may be operating in the 2.4GHz range.

In some cases, you may want to segment your wireless traffic where a group of devices operates on one channel and another group operates on another channel, and so on. This is done by configuring the channel on each wireless access point individually (if you have multiples). If you have control over only one wireless device in an environment where there may be several, you can change the wireless channel on your device to one that is not heavily used.

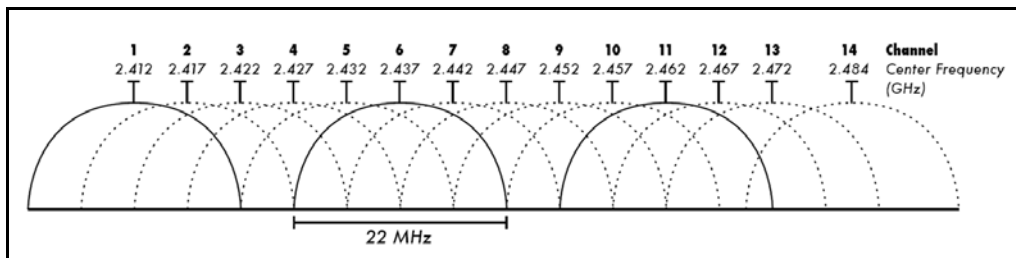


Note

To change the wireless broadcast channel, refer to [Using the Wireless Radio Option on page 75](#).

2.4GHz Channels

The following diagram displays the channels available in the Americas. Each available channel is 22MHz wide. Since channels overlap, it is best to choose channels that have the least overlap (typically 1, 6, and 11 in the Americas, and 1, 5, 9, and 13 in Europe). Overlapping channels can cause wireless network performance issues.



Source: Wikipedia.org, and IEEE article IEEE 802.11n-2009

5GHz Channels

The following table shows the 5GHz channel list and the corresponding frequencies.

Channel	GHz	Channel	GHz
36	5.180	108	5.540
40	5.200	112	5.560
44	5.220	116	5.580
48	5.240	136	5.680
52	5.260	140	5.700
56	5.280	149	5.745
60	5.300	153	5.765
64	5.320	157	5.785
100	5.500	161	5.805
104	5.520	165	5.825

10 .Understanding the MoCA Menu

The **MoCA** menu of the Web user interface displays information about the MoCA status of the DDW36C. MoCA (Multimedia over Coax Alliance) technology is a standard that enables the distribution of high quality digital multimedia content throughout the home over existing coaxial cabling



Topics

See the following topics:

- ◆ [Using the MoCA Software Option on page 93](#)



Steps

To access the MoCA menu:

1. Access the Web user interface. Refer to [Accessing the Web User Interface Locally on page 14](#).
2. Click **MoCA** from the main menu.
3. The **Software** screen is displayed.

10.1 Using the MoCA Software Option

The **MoCA Software** option allows you to view the MoCA status of the DDW36C. Field descriptions are listed below the screen example.



Label	Description
Configure Information	
Status	Indicates whether MoCA is enabled or disabled.
MoCA IP	Displays the DDW36C Gateway IP address, accessed via the MoCA interface.
Security Mode	Enabled means MoCA traffic is encrypted. Disabled means MoCA traffic is not encrypted.
Auto Scan	If true, the DDW36C auto scans the MoCA frequency range to find an existing MoCA network. If one is not found, then the DDW36C will become the Network Coordinator of its own MoCA network.
Frequency	Displays the current MoCA frequency seen by the DDW36C.
Link Local Information	Displays MoCA-related information about the local link.

11 Glossary

This chapter defines terms used in this guide and in the industry.

54G™

The internal wireless adapter from Broadcom.

ALG (Application-Level Gateway)

A type of security device that acts on behalf of the application servers on a network, hiding the servers themselves from traffic that might be malicious.

AP (Access Point)

A device that allows wireless devices to connect to a wired network using WiFi, or related standards.

Broadcast

A packet sent to all devices on a network.

BSS (Basic Service Sets)

A basic service set is the fundamental building block of an 802.11 wireless local area network. The overlapping BSS problem refers to a situation where two or more systems, unrelated to each other are in close enough proximity to hear each other physically. Overlapping BSS may degrade the network performance severely.

BSSID (Basic Service Set Identifier)

The BSSID uniquely identifies a specific access point and is in the same format as a MAC address.

Channel Bonding

A computer networking configuration where two or more network interfaces are combined on a host computer for redundancy or increased throughput. Data is transmitted over these channels as if they are one channel.

CMTS (Cable Modem Termination System)

Typically located in the cable company's headend, the CMTS is equipment that provides high-speed data services to subscribers, such as cable Internet and Voice over IP (VoIP).

CPE (Customer Premises Equipment)

Equipment such as telephones, routers, and modems located at a user's location to enable access to communication services.

Default Gateway

The routing device used to forward all traffic that is not addressed to a computer on the local subnet.

DHCP (Dynamic Host Configuration Protocol)

A protocol that centrally automates the assignment of IP addresses in a network. Using the Internet's set of protocols (TCP/IP), each machine that can connect to the Internet needs a unique IP address. For example, when the service provider sets up computer users with a connection to the Internet, an IP address is assigned to each machine. DHCP lets the service provider distribute IP addresses and automatically sends a new IP address when a computer is plugged in to the high-speed Internet network. DHCP uses the concept of a "lease" or amount of time an IP address is valid for a computer. Lease times can vary.

DMZ (Demilitarized Zone)

Allows one IP address (or computer) to be placed in between the firewall and the Internet (usually for gaming and video conferencing). This allows risky, open access to the Internet.

DOCSIS (Data Over Cable Service Interface Specification)

An International telecommunications standard that permits the addition of high-speed data transfer over an existing cable TV system.

Domain

A subnetwork comprised of a group of clients and servers under the control of one security database.

Domain Name

A descriptive name for an address or group of addresses on the Internet. Domain names are in the form of a registered entity name plus one of a number of predefined top-level suffixes, such as .com, .edu, .org.

DoS (Denial of Service) Attack

An attempt to make a machine or network resources unavailable to its intended users.

DNS (Domain Name System)

An Internet service that locates and translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Every time you use a domain name, a DNS service translates the name into the corresponding IP address. The DNS system is actually its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Downstream

A term to describe the direction of data from the network service provider to the customer.

DTIM (Delivery Traffic Indication Message)

Informs clients about the presence of buffered broadcast data on the access point.

Ethernet

A standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. It forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP, HTTP, and FTP.

Firewall

A highly effective method to block unsolicited traffic from outside the connected computers in your gateway and local network.

FTP (File Transfer Protocol)

A network protocol used to transfer files from one host to another over a TCP-based network.

Gateway

A local device, usually a router, that connects hosts on a local network to other networks – sometimes with different incompatible communication protocols. The DDW36C is an example of a gateway.

Headend

A main facility to process and distribute Internet communication signals. Headend may also refer to cable television signals and power line communication facilities.

ICQ

A free instant-messaging utility introduced by Mirabilis in 1996.

IKE (Internet Key Exchange)

A protocol used to ensure security for VPN negotiation and remote host or network access.

IP (Internet Protocol)

The method or protocol by which data is sent from one computer to another on the Internet. It is a standard set of rules, procedures, or conventions relating to the format and timing of data transmission between two computers that they must accept and use to understand each other. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

IP Address

In the most widely installed level of the IP today, an IP address is a 32-bit binary digit number that identifies each sender or receiver of information that is sent in packet form across the Internet. When you request a Web page or send an e-mail, the IP part of TCP/IP includes your IP address. IP sends your IP address to the IP address obtained by looking up the domain name in the URL you requested or in the e-mail address to which you are sending a note. A dynamic IP address is an IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server.

IPsec (Internet Protocol Security)

A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

IRC (Internet Relay Chat)

A system that facilitates the transfer of messages in the form of text.

ISP (Internet Service Provider)

A company that provides individuals and companies access to the Internet and other related services.

IUC (Interval Usage Code)

Interval usage codes define different profiles for upstream burst profiles to use for the data. IUCs are sent to the cable modem from the CMTS to tell the device important characteristics to use for the burst, such as modulation type, preamble length, and so on.

Kerberos

A network authentication protocol which works on the basis of “tickets” to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

LAN (Local Area Network)

A group of computers and associated devices such as printers and servers that share a common communication line and other resources within a small geographic area.

MAC (Media Access Control Address)

A unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. Usually written in the form 01:23:45:67:89:ab.

Mbps (Megabits per Second)

A unit of measurement for data transmission that represents one million bits per second.

MTU (Maximum Transmission Unit)

The size in bytes of the largest packet that can be sent or received.

NAT (Network Address Translation)

A technique by which several hosts or computers share a single IP address for access to the Internet. NAT enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic, and provides a type of firewall by hiding internal IP addresses.

NetBios (Network Basic Input/Output System)

A program that allows applications on different computers to communicate within a local area network.

Net2Phone

A software/services company whose principal line of business is SIP-based and PacketCable-based voice over IP.

Packet

A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

PPTP (Point-to-Point Tunneling Protocol)

A method for ensuring secure communication between virtual private networks.

Ranging

A process in which a cable modem sends a range request at a power of 8 dBmV (very low power). If it does not receive a range response from the CMTS, the cable modem re-transmits the range request at a 3 dB higher power level and continues the process until a range response is received.

Router

A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

RIP (Routing Information Protocol)

A protocol in which routers periodically exchange information with one another to determine minimum-distance paths between sources and destinations.

RSSI (Received Signal Strength Indicator)

A measurement of the power present in a received radio signal. Lower negative numbers (for example, -1 to -65) indicate the access point is closer. Greater negative numbers (for example, -66 to -95) indicate the access point is farther away. RSSI is optimal between 0dBm and -64dBm.

RSVP (Resource Reservation Protocol)

A set of communication rules that allows channels or paths on the Internet to be reserved for the multicast transmission of video and other high-bandwidth messages.

RTSP (Real Time Streaming Protocol)

A protocol used in the transfer of real-time streaming media such as audio and video.

Service Set Identifier (SSID)

A sequence of characters that uniquely names a wireless local area network (WLAN). The SSID allows stations to connect to the desired network when multiple independent networks are operating in the same physical area.

SIP (Session Initiation Protocol)

A signaling communications protocol that is widely used for controlling multimedia communications sessions such as voice and video over Internet Protocol networks.

SNR (Signal-to-Noise Ratio)

A measure that compares the level of a desired signal to the level of background noise.

SNTP (Simple Network Time Protocol)

A protocol for synthesizing the clocks of computing devices over networks.

STBC (Space-Time Block Code))

A technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas.

Subnet

A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 10.1.10 would be part of the same subnet. IP networks are divided using a subnet mask.

Subnet Mask

Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router. A number that explains which part of an IP address comprises the network address and which part is the host address on that network.

Telnet

A network protocol used on the Internet or a local area network. Provides bi-directional interactive text-oriented communications using a virtual terminal connection.

TACACS (Terminal Access Controller Access-Control System)

A remote authentication protocol used to communicate with an authentication server to determine if the user is allowed to access the network.

TCP (Transmission Control Protocol)

A method (protocol) used with the IP to send data in the form of message units (datagrams) between network devices over a LAN or WAN. While IP handles the actual delivery of the data (routing), TCP keeps track of the individual units of data (packets) that a message is divided into for efficient delivery over the network. TCP requires the receiver of a packet to return an acknowledgment of receipt to the sender of the packet.

TCP/IP (Transmission Control Protocol/Internet Protocol)

The basic communication language or set of protocols to communicate over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols.

TDMA (Time Division Multiple Access)

A method in which cable modems must time-share the upstream channel because there are many cable modems and only one upstream channel frequency.

TFTP (Trivial File Transfer Protocol)

A file transfer protocol used to transfer automatically configuration or boot files.

TPC (Transmit Power Control)

Sometimes called Dynamic Power Control (DPC), TPC is a mechanism used in radio communications to reduce the power of a radio transmitter to the minimum necessary to maintain the link with a certain quality. It is used to avoid interference with other devices and/or to extend battery life.

UDP (User Datagram Protocol)

A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol.

UPNP (Universal Plug and Play)

A set of networking protocols that permits networked devices to seamlessly discover each other's presence on the network to enable data sharing, communications, and entertainment.

Upstream

A term to describe the direction of data from the customer to the network service provider.

URI (Uniform Resource Identifier)

A string of characters used to identify a name or a resource on the Internet.

URL (Uniform Resource Locator)

A uniform resource identifier (URI) that specifies where a known resource is available and how to retrieve it.

WAN (Wide Area Network)

A long-distance link or computer network that spans a relatively large geographical area that connects remotely located LANs. Typically, a WAN consists of two or more LANs. The Internet is a large WAN.

WEP (Wired Equivalent Privacy)

An encryption method used to protect your wireless data communications. WEP uses 64-bit or 128-bit keys to provide access control to your network and security for everyday transmissions. To decode data transmissions, all devices on the network must use an identical key.

WLAN (Wireless Local Area Network)

A communications network that uses high frequency radio signals to allow wireless devices to communicate with each other within a limited geographic area.

WPA (Wi-Fi Protected Access)

A security protocol for wireless networks offering improvements over the WEP protocol in the way it handles security keys and the way users are authorized.

WPS (Wi-Fi Protected Setup)

A security protocol for wireless home networks. Created by the Wi-Fi Alliance, this protocol allows home users to easily set up wireless security and add new devices without needing to enter long passwords.

XML (Extensible Markup Language)

A markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine readable.

XPress™

XPress™ is a standards-based frame-bursting approach to improve 802.11g wireless LAN performance developed by Broadcom.