

- To access the modem enter the following IP address 192.168.100.1 in the address bar of your web browser
- To log into the modem select: Status Tab / DOCSIS WAN
- Leave both User Name and Password section blank
- Select Log In to login to the modem

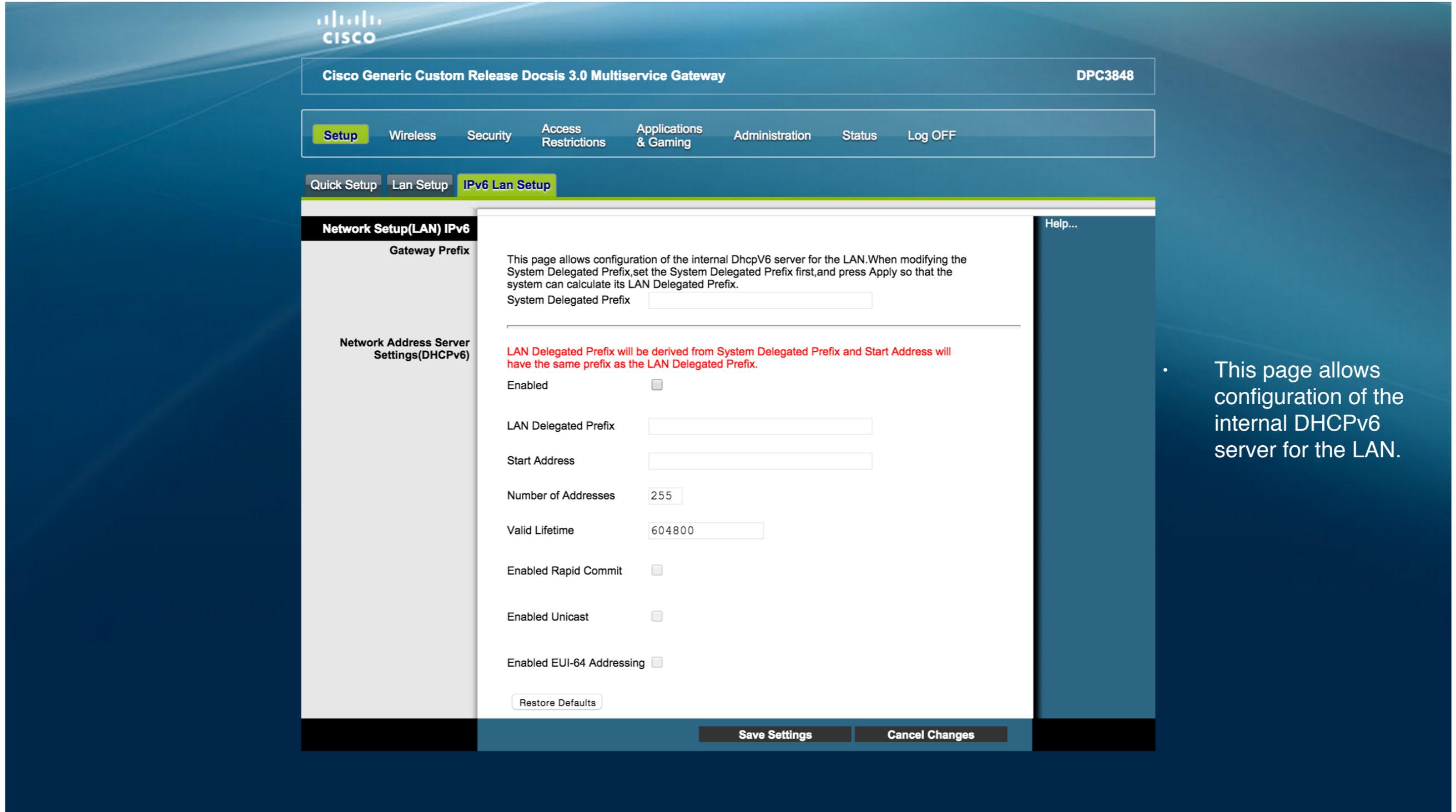
The screenshot shows the Cisco DPC3848 web interface. At the top, it identifies the device as a "Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway" with model number "DPC3848". The navigation menu includes "Setup" (highlighted), "Wireless", "Security", "Access Restrictions", "Applications & Gaming", "Administration", "Status", and "Log OFF". Under the "Setup" tab, there are sub-tabs for "Quick Setup", "Lan Setup", and "IPv6 Lan Setup". The "Quick Setup" sub-tab is active, showing a "Change Password" section and two sections for wireless security: "2.4GHz Wireless Security" and "5GHz Wireless Security". Each wireless security section has the following settings: "Wireless Interface" (radio buttons for "Enable" and "Disable", with "Enable" selected), "Network Name (SSID)" (text field with "E7E525"), "Security Mode" (dropdown menu with "WPA or WPA2-Personal" selected), "Encryption" (dropdown menu with "AES+TKIP" selected), "Pre-Shared Key" (password field with masked characters and a "Show key" checkbox), and "Key Renewal" (text field with "0" and "seconds"). At the bottom of the page, there are "Save Settings" and "Cancel Changes" buttons.

Wireless Security settings and Password to access modem can be changed in this page

The following wireless security mode options are supported: Disable, WEP, WPA-Personal, WPA2-Personal, WPA2-Mixed, WPA-Enterprise, and WPA2-Enterprise.

The screenshot displays the configuration interface for a Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway (DPC3848). The main navigation bar includes 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', 'Status', and 'Log OFF'. The 'Setup' tab is active, and the 'Lan Setup' sub-tab is selected. The left sidebar shows 'Network Setup (LAN)' as the active section, with sub-sections for 'Gateway IP', 'Network Address Server Settings (DHCP)', and 'Time Settings'. The main content area is divided into three sections: Gateway IP, DHCP Server, and Time Settings. The Gateway IP section shows 'Local IP Address' set to 192.168.0.1 and 'Subnet Mask' set to 255.255.255.0. A red warning message states: 'Warning: Changes to LAN IP network settings may require reconfiguration of all attached devices. Some network devices may be out of service until the change is detected.' The DHCP Server section has 'DHCP Server' checked and 'Enable / Disable'. It includes buttons for 'Connected Devices Summary' and 'Pre-assigned DHCP IP Addresses'. The 'Starting IP Address' is 192.168.0.2, 'Maximum Number of DHCP Users' is 252, and 'Client Lease Time' is 604800 seconds. The Time Settings section shows 'Current System Time' as 1970-01-01 07:43:31, 'NTP' is unchecked, 'Time Zone' is '(GMT-12:00) International Date Line West', and 'Automatically adjust clock for daylight saving time' is checked. There are 'Add Server' and 'Remove Server' buttons for the Time Server field. At the bottom, there are 'Save Settings' and 'Cancel Changes' buttons.

This page allows to change LAN IP network settings



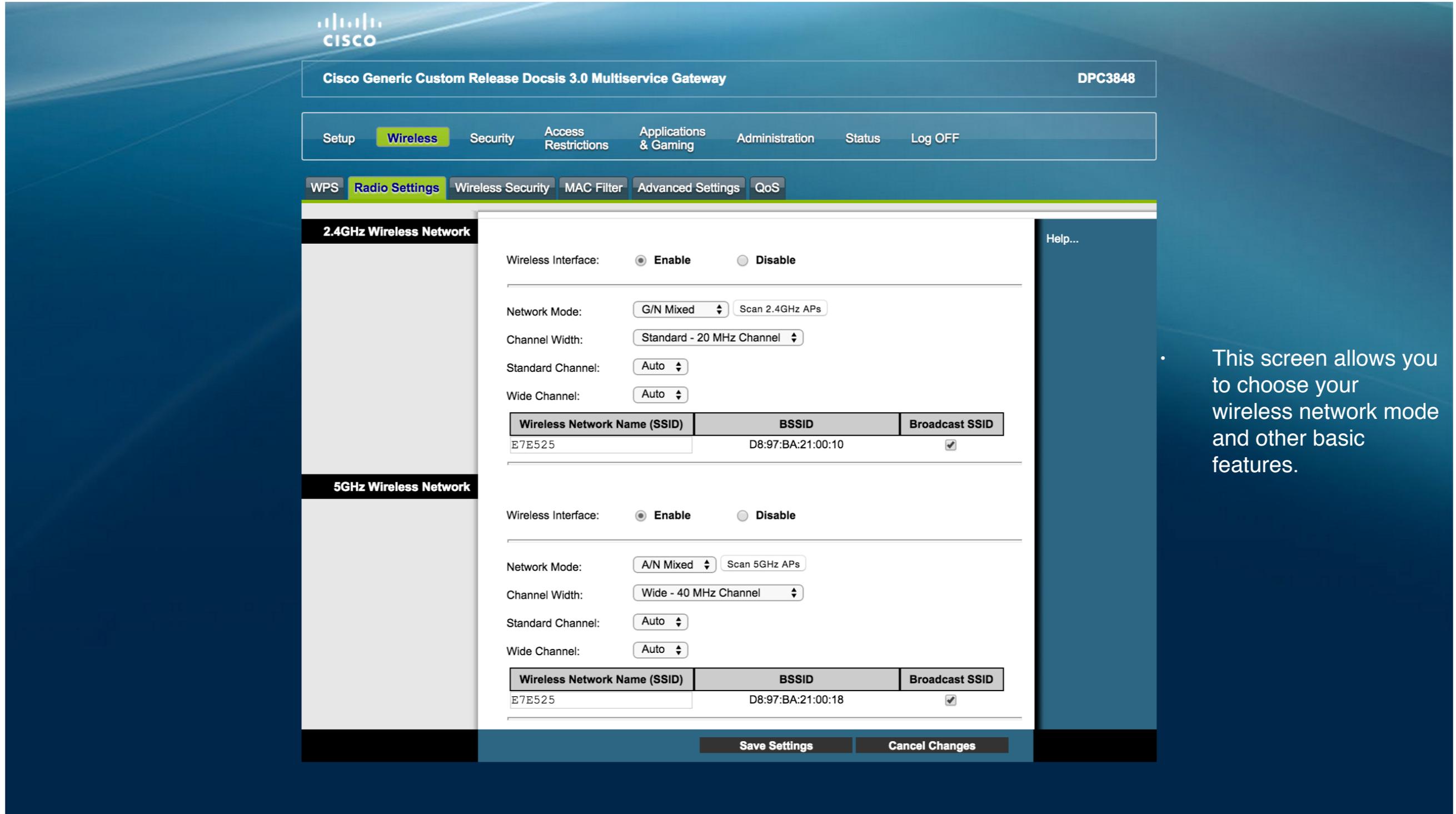
The screenshot shows the Cisco web interface for configuring IPv6 LAN settings. At the top, the Cisco logo and device name 'Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway' are visible, along with the device ID 'DPC3848'. A navigation menu includes 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', 'Status', and 'Log OFF'. Below this, sub-menus for 'Quick Setup', 'Lan Setup', and 'IPv6 Lan Setup' are shown, with 'IPv6 Lan Setup' being the active tab.

The main configuration area is titled 'Network Setup(LAN) IPv6' and contains two sections: 'Gateway Prefix' and 'Network Address Server Settings(DHCPv6)'. The 'Network Address Server Settings(DHCPv6)' section includes a descriptive paragraph: 'This page allows configuration of the internal DhcpV6 server for the LAN. When modifying the System Delegated Prefix, set the System Delegated Prefix first, and press Apply so that the system can calculate its LAN Delegated Prefix.' Below this is a text input field for 'System Delegated Prefix'. A red warning message states: 'LAN Delegated Prefix will be derived from System Delegated Prefix and Start Address will have the same prefix as the LAN Delegated Prefix.' The configuration options include: 'Enabled' (checkbox), 'LAN Delegated Prefix' (text input), 'Start Address' (text input), 'Number of Addresses' (input with value 255), 'Valid Lifetime' (input with value 604800), 'Enabled Rapid Commit' (checkbox), 'Enabled Unicast' (checkbox), and 'Enabled EUI-64 Addressing' (checkbox). A 'Restore Defaults' button is located at the bottom of the form. At the very bottom of the page, there are 'Save Settings' and 'Cancel Changes' buttons.

- This page allows configuration of the internal DHCPv6 server for the LAN.

The screenshot shows the Cisco configuration interface for a DPC3848 gateway. The main navigation bar includes Setup, Wireless (selected), Security, Access Restrictions, Applications & Gaming, Administration, Status, and Log OFF. A secondary navigation bar includes WPS (selected), Radio Settings, Wireless Security, MAC Filter, Advanced Settings, and QoS. The WPS configuration page is titled 'Wi-Fi Protected Setup™' and features a 'WPS Support' section with 'Enable' selected. Below this, instructions are provided for three methods of device registration, accompanied by a circular arrow icon. The configuration fields for both 2.4GHz and 5GHz networks show a Network Name (SSID) of 'E7E525' and a Security Mode of 'WPAWPA2-PSK (TKIP/AES)'. At the bottom, there are 'Save Settings' and 'Cancel Changes' buttons.

• This screen allows you to choose your wireless network mode and other basic features.



The screenshot displays the Cisco Wireless Radio Settings configuration page. At the top, the Cisco logo is visible. The main header identifies the device as a "Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway" with the ID "DPC3848". A navigation menu includes "Setup", "Wireless", "Security", "Access Restrictions", "Applications & Gaming", "Administration", "Status", and "Log OFF". Below this, a sub-menu highlights "Radio Settings" among other options like "WPS", "Wireless Security", "MAC Filter", "Advanced Settings", and "QoS".

The interface is divided into two sections: "2.4GHz Wireless Network" and "5GHz Wireless Network". Each section contains the following settings:

- Wireless Interface:** Radio buttons for "Enable" (selected) and "Disable".
- Network Mode:** A dropdown menu (e.g., "G/N Mixed") and a "Scan" button (e.g., "Scan 2.4GHz APs").
- Channel Width:** A dropdown menu (e.g., "Standard - 20 MHz Channel").
- Standard Channel:** A dropdown menu (e.g., "Auto").
- Wide Channel:** A dropdown menu (e.g., "Auto").

Below these settings are two tables for network configuration:

Wireless Network Name (SSID)	BSSID	Broadcast SSID
E7E525	D8:97:BA:21:00:10	<input checked="" type="checkbox"/>

Wireless Network Name (SSID)	BSSID	Broadcast SSID
E7E525	D8:97:BA:21:00:18	<input checked="" type="checkbox"/>

At the bottom of the page, there are two buttons: "Save Settings" and "Cancel Changes". A "Help..." link is located on the right side of the configuration area.

• This screen allows you to choose your wireless network mode and other basic features.

**Wireless Network:** You can enable or disable wireless network with this radio button.

**Wireless Configuration:** The default is Manual. Select Wi-Fi Protected Setup to set up your network using this option. The Wi-Fi Protected Setup feature automatically configures an encryption-secured, wireless network. To use Wi-Fi Protected Setup, you must have at least one other device that supports Wi-Fi Protected Setup in your network. After you have configured your Wi-Fi Protected Setup devices, you can manually configure other devices. Scroll down to the end of the help page for more information.

**Network Mode:** Determines which Mode the N card will run in.

**Radio Band:** You can select the radio band. If you select Enabled 2.4GHz, the device can support B/G/N Mixed mode. And if you select Enabled 5GHz, it can support A/N mixed mode.

**Channel Width:** You can select the channel bandwidth manually for Wireless-N connections. For best performance in a network using Wireless-N, Wireless-G, and Wireless-B devices, keep the Wide - 40MHz Channel. Wireless-N connections will use the 40 MHz channel, while Wireless-G and Wireless-B will still use the 20 MHz channel. For Wireless-G and Wireless-B networking only, select Standard - 20MHz Channel. Then only the 20 MHz channel will be used.

**Standard Channel:** If you selected Wide - 40 MHz Channel for the Radio Band setting, then the appropriate Standard Channel setting will be automatically selected, depending on the Wide Channel setting. If you selected Standard - 20 MHz Channel as the Radio Band setting, select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must broadcast on the same channel in order to communicate.

**Wide Channel:** If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N channel. Select any channel from the drop-down menu, and then the appropriate Standard Channel setting will be automatically selected.

**Wireless Network Name (SSID):** You may choose an easy remember name for your wireless network or simply use the default value. The value you enter here will be viewable on PCs and other wireless client devices as the wireless network name.

**Wireless SSID Broadcast:** If this feature is enabled, wireless clients will detect the SSID broadcast by the device when they survey the local area for wireless networks to join. To broadcast the devices SSID, keep the default setting, Enable. If you do not want to broadcast the devices SSID, then select Disable.

**Wi-Fi Protected Setup Option 1:** An administrator can push the Wi-Fi Protected Setup button on the Basic Wireless Settings screen or the button on the front panel of the Gateway to allow a user to register a wireless client with the Gateway. The user needs to push the Wi-Fi Protected Setup software button on the client side at the same time as the Wi-Fi Protected Setup button is pushed on the Gateway. The connection will be automatically set up.

**Wi-Fi Protected Setup Option 2:** This is the most secure option for an administrator to register a user's wireless client with the Gateway. The user needs to give the administrator their Wi-Fi Protected Setup PIN number, which is found in the client Wi-Fi Protected Setup utility. After entering the client's Wi-Fi Protected Setup PIN number, the administrator registers the user. The user can then connect to the Gateway.

**Wi-Fi Protected Setup Option 3:** The Gateway's Wi-Fi Protected Setup PIN number is on the label on its bottom panel. Using any Wi-Fi Protected Setup client utility or Microsoft Vista, the user needs to enter the Gateway's Wi-Fi Protected Setup PIN number into the client device.



Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway

DPC3848

Setup **Wireless** Security Access Restrictions Applications & Gaming Administration Status Log OFF

WPS Radio Settings **Wireless Security** MAC Filter Advanced Settings QoS

## 2.4GHz Wireless Security

Security Mode: WPA or WPA2-Personal  
Encryption: AES+TKIP  
Pre-Shared Key: .....  Show key  
Key Renewal: 0 seconds

## 5GHz Wireless Security

Security Mode: WPA or WPA2-Personal  
Encryption: AES+TKIP  
Pre-Shared Key: .....  Show key  
Key Renewal: 0 seconds

Save Settings

Cancel Changes

The following wireless security mode options are supported: Disable, WEP, WPA-Personal, WPA2-Personal, WPA2-Mixed, WPA-Enterprise, and WPA2-Enterprise.



Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway

DPC3848

Setup **Wireless** Security Access Restrictions Applications & Gaming Administration Status Log OFF

WPS Radio Settings Wireless Security **MAC Filter** Advanced Settings QoS

## MAC Filter

Enable  Disable

### Access Restriction

Block computers listed below from accessing the wireless network

Permit computers listed below to access the wireless network

### MAC Address Filter List

#	Device Name	MAC Address	Delete
---	-------------	-------------	--------

### Manual Add A Device

Device Name	MAC Address	Add
<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>

### Auto Detected Devices

Device Name	Interface	IP Address	MAC Address	Status	Add
-------------	-----------	------------	-------------	--------	-----

Save Settings

Cancel Changes

Help...

Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network radius.



Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway

DPC3848

Setup **Wireless** Security Access Restrictions Applications & Gaming Administration Status Log OFF

WPS Radio Settings Wireless Security MAC Filter **Advanced Settings** QoS

## 2.4GHz Advanced Settings

Transmission Rate:  (Default: Auto)  
CTS Protection Mode:  (Default: Disable)  
Beacon Interval:  (Default: 100 msec, Range: 1-65535)  
DTIM Interval:  (Default: 1, Range: 1-255)  
Fragmentation Threshold:  (Default: 2346, Range: 256-2346)  
RTS Threshold:  (Default: 2347, Range: 0-2347)

## 5GHz Advanced Settings

Transmission Rate:  (Default: Auto)  
CTS Protection Mode:  (Default: Disable)  
Beacon Interval:  (Default: 100 msec, Range: 1-65535)  
DTIM Interval:  (Default: 1, Range: 1-255)  
Fragmentation Threshold:  (Default: 2346, Range: 256-2346)  
RTS Threshold:  (Default: 2347, Range: 0-2347)

Save Settings

Cancel Changes

Help...

This screen is used to set up the advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

**CISCO**

Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway DPC3848

Setup **Wireless** Security Access Restrictions Applications & Gaming Administration Status Log OFF

WPS Radio Settings Wireless Security MAC Filter Advanced Settings **QoS**

**2.4GHz Quality of Service**

WMM Support:  **Enable**  **Disable** (Default: Enable)

No ACK:  **Enable**  **Disable** (Default: Disable)

---

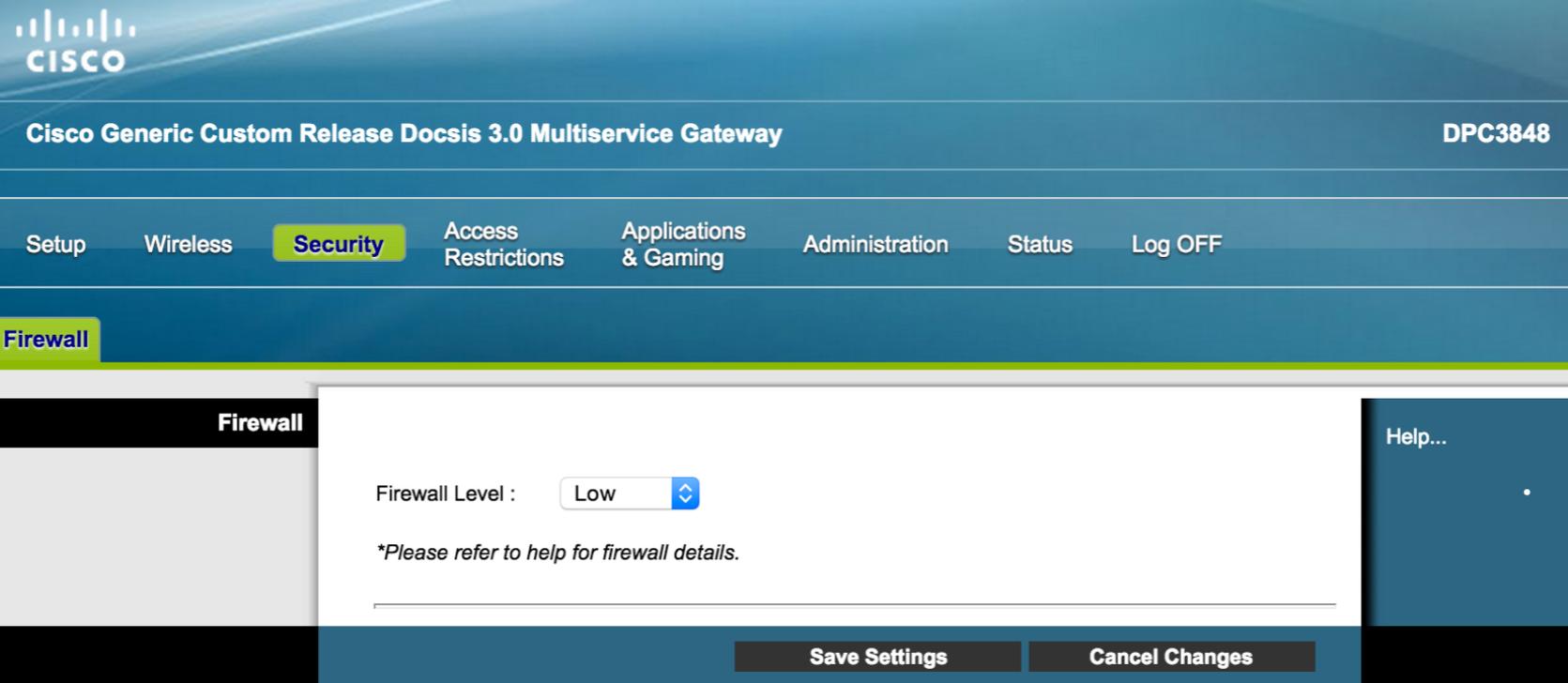
**5GHz Quality of Service**

WMM Support:  **Enable**  **Disable** (Default: Enable)

No ACK:  **Enable**  **Disable** (Default: Disable)

**Save Settings** **Cancel Changes**

The Quality of Service (QoS) settings allow you to specify priorities for different types of traffic. Lower priority traffic will be slowed down to allow greater throughput or less delay for high priority traffic.



The screenshot shows the Cisco management interface for a DPC3848 gateway. At the top left is the Cisco logo. Below it, the device name "Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway" and the ID "DPC3848" are displayed. A navigation menu includes "Setup", "Wireless", "Security" (highlighted), "Access Restrictions", "Applications & Gaming", "Administration", "Status", and "Log OFF". Under the "Security" tab, the "Firewall" sub-tab is active. The main content area shows "Firewall Level" set to "Low" with a dropdown arrow. Below this is a note: "\*Please refer to help for firewall details." At the bottom of the configuration area are two buttons: "Save Settings" and "Cancel Changes". A "Help..." link is visible on the right side of the configuration area.

The Firewall screen is used to configure a firewall that can filter out various types of unwanted traffic on the Gateway local network.



Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway

DPC3848

Setup Wireless Security **Access Restrictions** Applications & Gaming Administration Status Log OFF

**Managed Sites** Managed Services Managed Devices Reports

**Managed Sites**

Enable  Disable

---

[Hide](#)

Device Name	IP address	Trustd
Joses-MBP	192.168.0.129	<input type="radio"/> YES <input checked="" type="radio"/> NO

---

URL	When	ADD
		ADD

---

Keywords	When	ADD
		ADD

Help...



Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway

DPC3848

Setup Wireless Security **Access Restrictions** Applications & Gaming Administration Status Log OFF

Managed Sites **Managed Services** Managed Devices Reports

## Managed Services

### Trusted Devices

Enable  Disable

[Hide](#)

Device Name	IP address	Trustd
Joses-MBP	192.168.0.129	<input type="radio"/> YES <input checked="" type="radio"/> NO

### Blocked Services

Services	TCP/UDP	Starting Port	Ending Port	When	ADD
----------	---------	---------------	-------------	------	-----

Help...



Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway

DPC3848

Setup Wireless Security **Access Restrictions** Applications & Gaming Administration Status Log OFF

Managed Sites Managed Services **Managed Devices** Reports

## Managed Devices

Access Type

Allowed Devices

Enable  Disable

Allow all  Block all

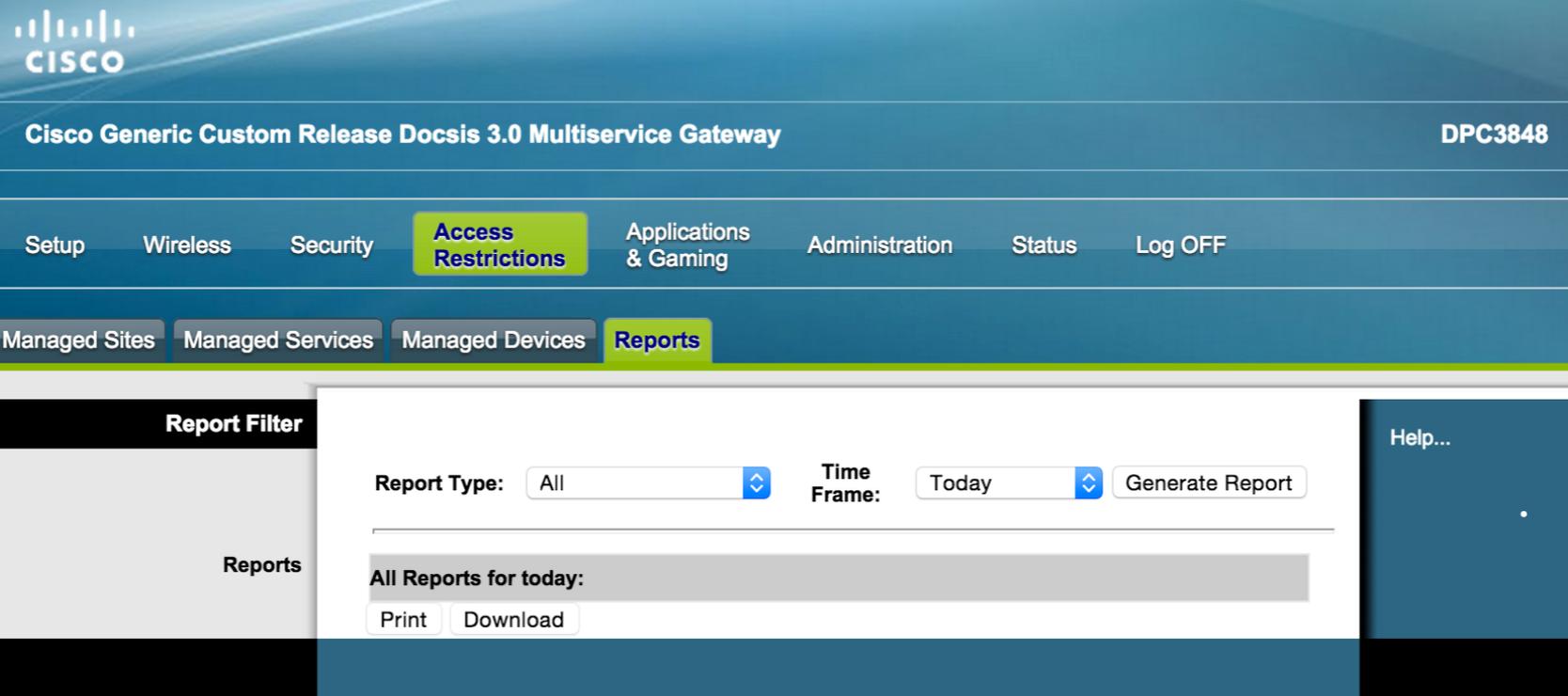
Device Name

MAC Address

When

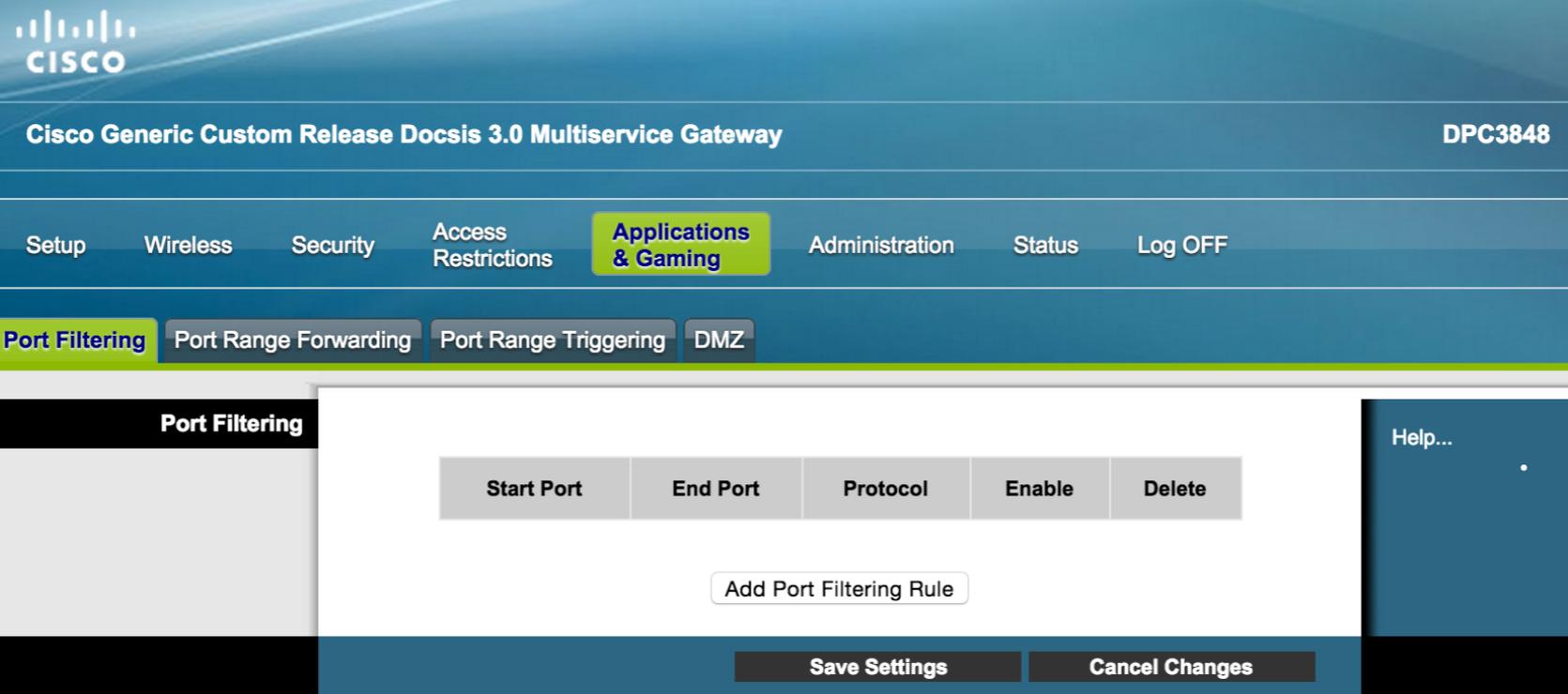
ADD

Help...



The screenshot shows the Cisco management interface for a 'Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway' (ID: DPC3848). The 'Access Restrictions' menu item is highlighted in green. Below it, the 'Reports' sub-tab is also highlighted. The 'Report Filter' section contains a 'Report Type' dropdown set to 'All' and a 'Time Frame' dropdown set to 'Today', with a 'Generate Report' button. Below these are 'All Reports for today:' and 'Print' and 'Download' buttons. A 'Help...' link is visible on the right side of the report area.

The log displayed on this page provides detailed information for all user restriction events.



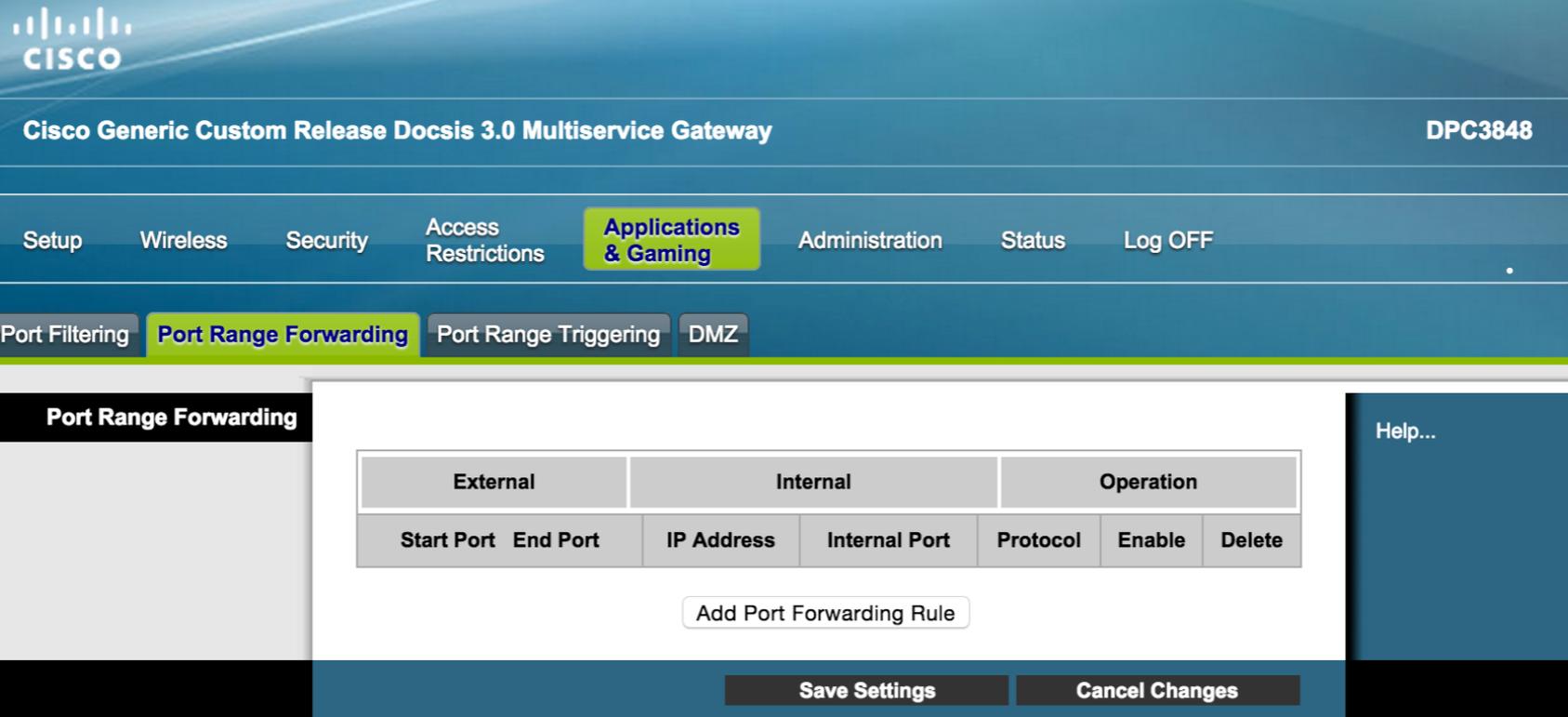
The screenshot shows the Cisco web interface for a Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway (DPC3848). The navigation menu includes Setup, Wireless, Security, Access Restrictions, Applications & Gaming (selected), Administration, Status, and Log OFF. Under the Applications & Gaming tab, the Port Filtering sub-tab is selected. The main content area displays a table with columns for Start Port, End Port, Protocol, Enable, and Delete. Below the table is an 'Add Port Filtering Rule' button. At the bottom of the page are 'Save Settings' and 'Cancel Changes' buttons.

Start Port	End Port	Protocol	Enable	Delete
------------	----------	----------	--------	--------

[Add Port Filtering Rule](#)

[Save Settings](#) [Cancel Changes](#)

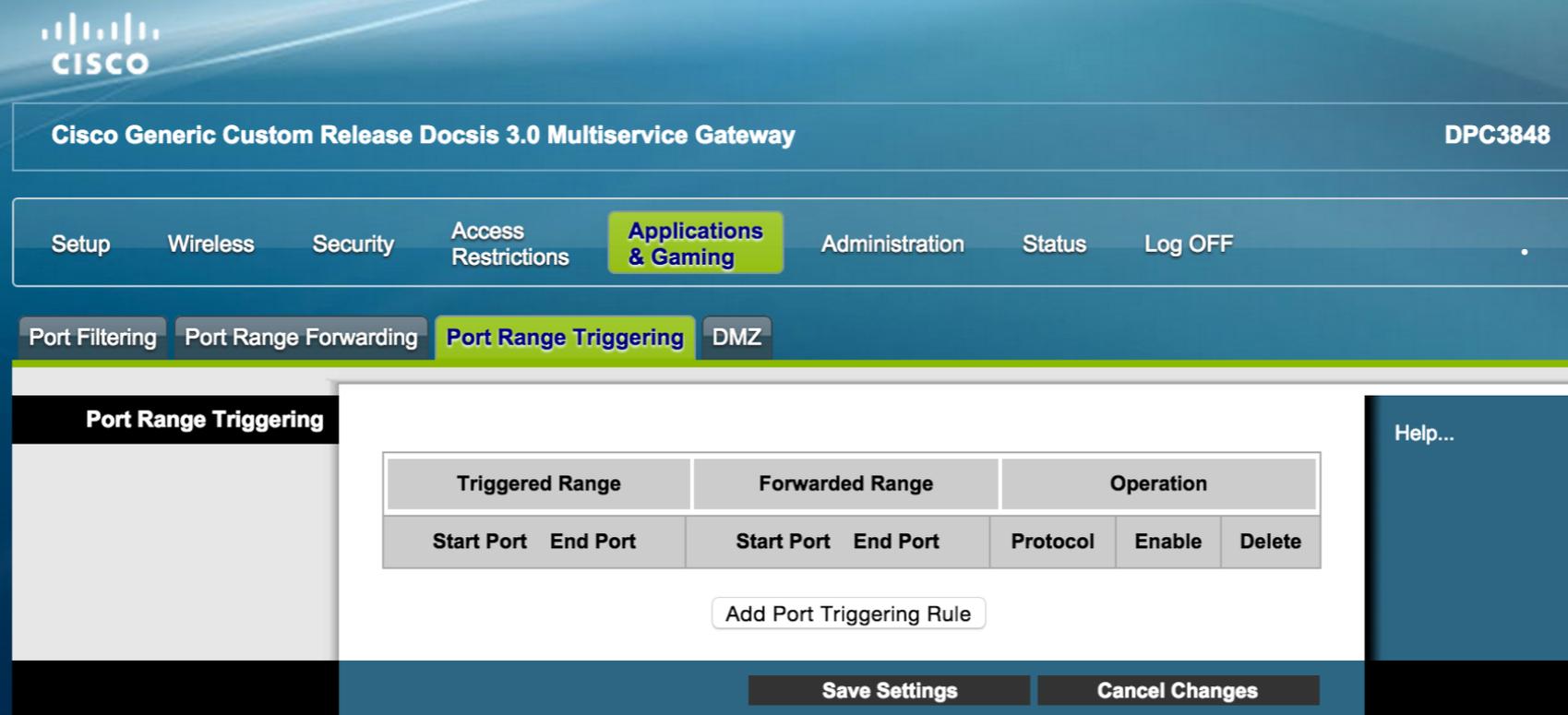
Use the Port Filtering page to configure and enable TCP and UDP port filters. These filters prevent a range of TCP/UDP ports from accessing the Internet.



The screenshot shows the Cisco web interface for a DPC3848 gateway. The top navigation bar includes 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming' (highlighted), 'Administration', 'Status', and 'Log OFF'. Below this, there are sub-tabs for 'Port Filtering', 'Port Range Forwarding' (highlighted), 'Port Range Triggering', and 'DMZ'. The main content area is titled 'Port Range Forwarding' and contains a table with columns for 'External' (Start Port, End Port), 'Internal' (IP Address, Internal Port), and 'Operation' (Protocol, Enable, Delete). An 'Add Port Forwarding Rule' button is located below the table. At the bottom, there are 'Save Settings' and 'Cancel Changes' buttons.

External		Internal		Operation		
Start Port	End Port	IP Address	Internal Port	Protocol	Enable	Delete
<input type="button" value="Add Port Forwarding Rule"/>						

This screen allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as video conferencing or online gaming. Some Internet applications may not require any forwarding.)

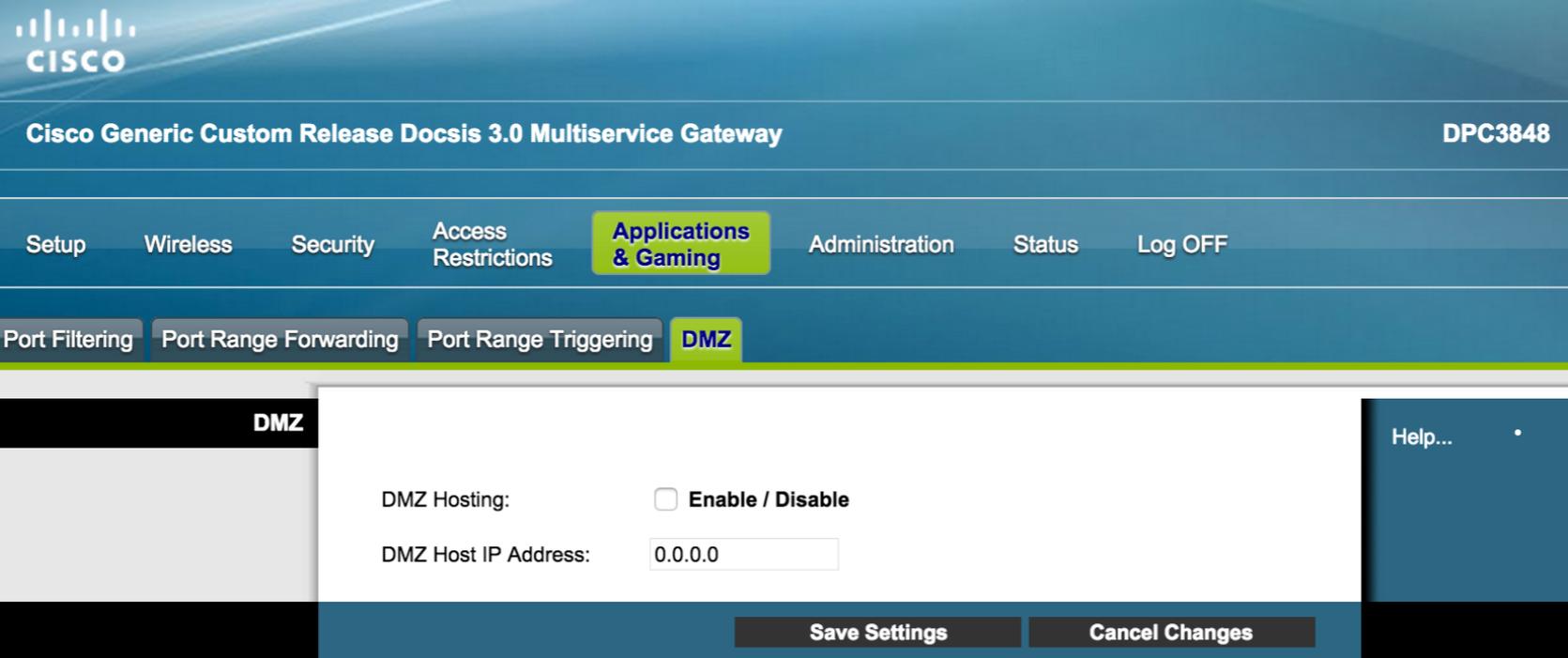


The screenshot shows the Cisco WebUI configuration page for a Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway (DPC3848). The navigation menu includes Setup, Wireless, Security, Access Restrictions, Applications & Gaming (highlighted), Administration, Status, and Log OFF. Under the Applications & Gaming tab, there are sub-tabs for Port Filtering, Port Range Forwarding, Port Range Triggering (highlighted), and DMZ. The Port Range Triggering configuration area contains a table with the following structure:

Triggered Range		Forwarded Range		Operation		
Start Port	End Port	Start Port	End Port	Protocol	Enable	Delete
<input type="button" value="Add Port Triggering Rule"/>						

At the bottom of the configuration area, there are two buttons: **Save Settings** and **Cancel Changes**. A Help... link is visible on the right side of the page.

This screen allows the device to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the device, so that when the requested data returns through the device, the data is sent back to the proper computer by way of IP address and port mapping rules. To trigger a port range, enter the information on each line for the criteria required.



The screenshot shows the Cisco web interface for a DPC3848 gateway. The top navigation bar includes 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming' (highlighted), 'Administration', 'Status', and 'Log OFF'. Under 'Applications & Gaming', there are sub-tabs for 'Port Filtering', 'Port Range Forwarding', 'Port Range Triggering', and 'DMZ' (highlighted). The DMZ configuration panel is open, showing 'DMZ Hosting' with an unchecked checkbox and the text 'Enable / Disable'. Below it, 'DMZ Host IP Address' is set to '0.0.0.0'. At the bottom of the panel are 'Save Settings' and 'Cancel Changes' buttons.

The DMZ feature allows one network user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or video conferencing. DMZ hosting forwards all the ports at the same time to one computer.

Setup Wireless Security Access Restrictions Applications & Gaming **Administration** Status Log OFF

**Management** Reporting Diagnostics Back Up & Restore Factory Defaults Device Restart

**Gateway Setup(WAN)**

Internet Connection Type

Working Mode: Router Mode

Connection Mode: DHCP

Host Name: Docsis-Gateway

**Gateway Access**

Local Access

Current User Name:

Change Current User Name to:

Change Password to:

Re-Enter New Password:

**Remote Access**

Remote Management:  Enable  Disable

Management Port: 80

**UPnP**

UPnP:  Enable  Disable

**IGMP**

IGMP Proxy:  Enable  Disable

Help...

**Save Settings** **Cancel Changes**

- This screen allows you to manage specific functions for access and security.



Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway

DPC3848

Setup Wireless Security Access Restrictions Applications & Gaming **Administration** Status Log OFF

Management **Reporting** Diagnostics Back Up & Restore Factory Defaults Device Restart

## Reporting

E-Mail Alerts:  Enable  Disable

SMTP Mail Server:

E-Mail Address for Alert Logs:

SMTP Username

SMTP Password

Save Settings

Cancel Changes

Help...

If enabled, an e-mail will be sent immediately if a Denial of Service (DoS) attack is detected. To use this feature, provide the necessary e-mail address information.

**CISCO**

Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway DPC3848

Setup Wireless Security Access Restrictions Applications & Gaming **Administration** Status Log OFF

Management Reporting **Diagnostics** Back Up & Restore Factory Defaults Device Restart

### Ping Test

**Ping Test Parameters**

Ping Target IPv4:  .  .  .

Ping Target IPv6:  :  :  :  :  :  :  :

Ping Size:  bytes

Number of Pings:  (Range: 1-100)

Ping Timeout:  seconds

Ping Results: Not Start

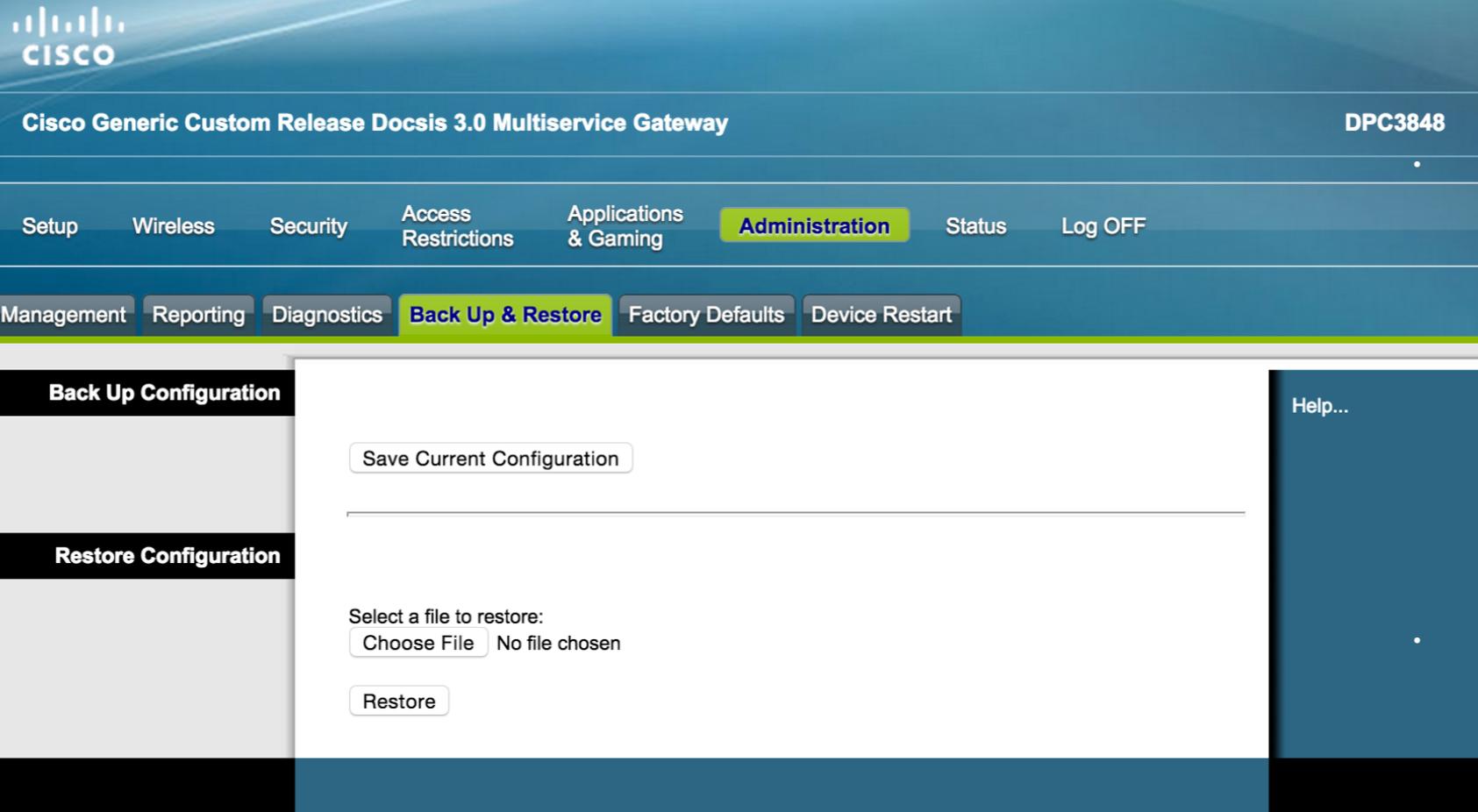
Packets Sent: 0

Packets Received: 0

Average Trip Time: 0

Help...

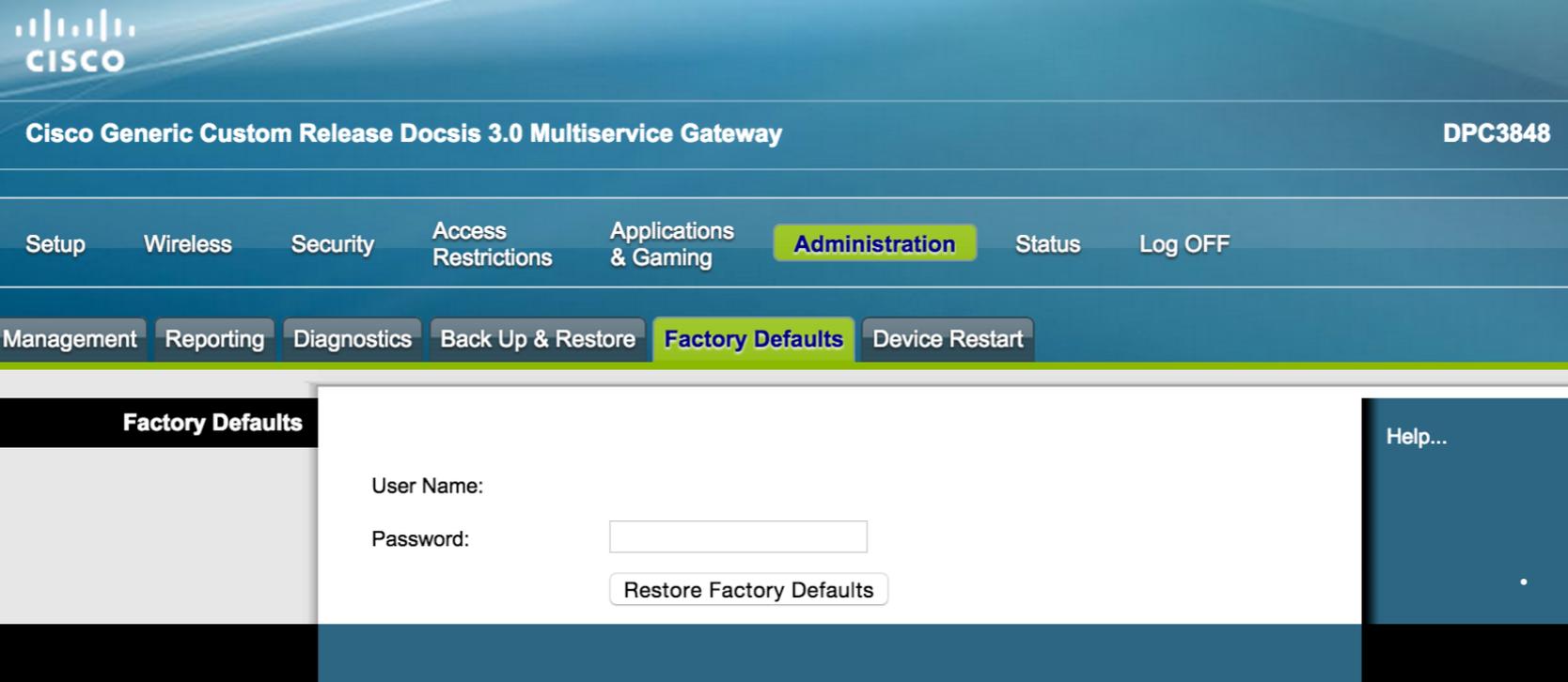
• The ping test allows you to check the status of your Internet connection.



The screenshot shows the Cisco Administration web interface for a DPC3848 gateway. The top navigation bar includes tabs for Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration (highlighted), Status, and Log OFF. Below this, a secondary navigation bar contains Management, Reporting, Diagnostics, Back Up & Restore (highlighted), Factory Defaults, and Device Restart. The main content area is split into two sections: 'Back Up Configuration' with a 'Save Current Configuration' button, and 'Restore Configuration' with a file selection area (labeled 'Choose File' and 'No file chosen') and a 'Restore' button. A 'Help...' link is visible on the right side of the interface.

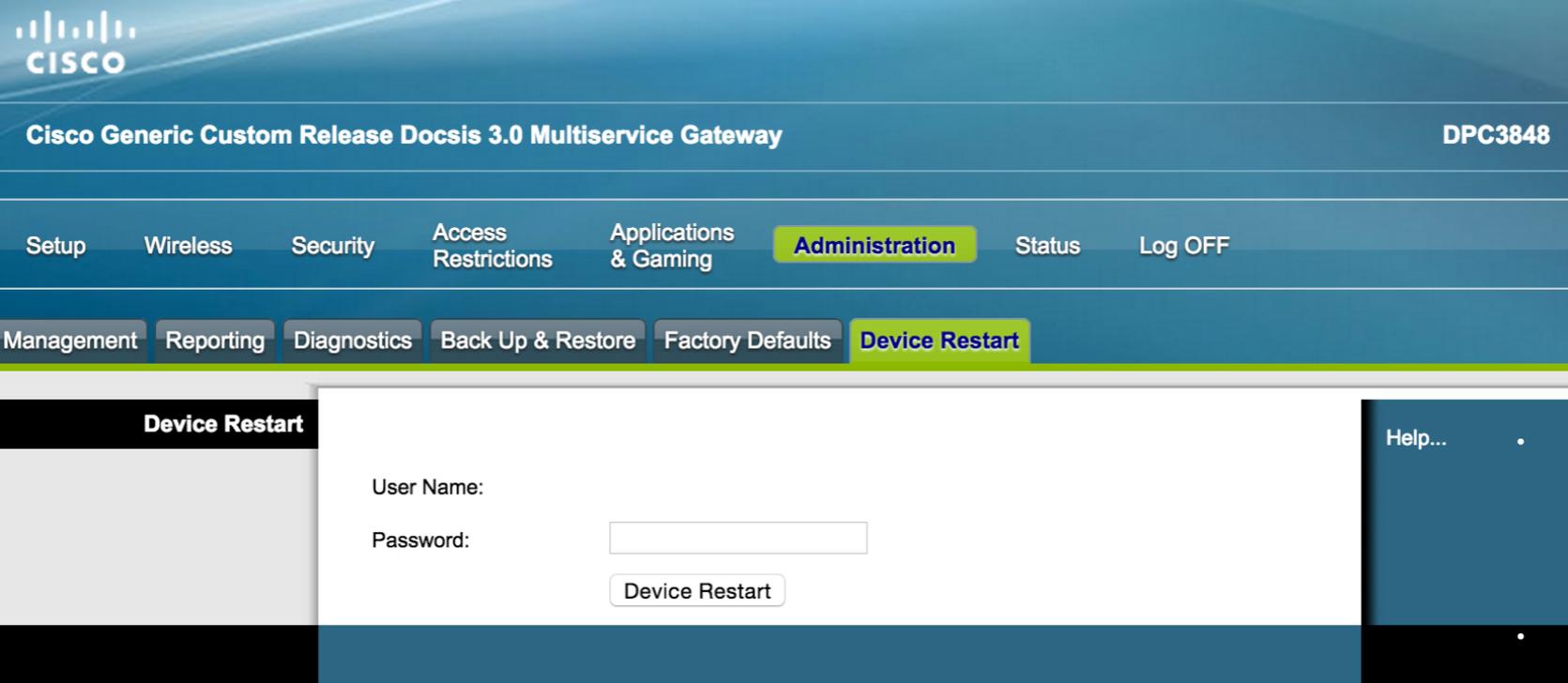
**Back Up Configuration:** Use this feature to download a copy of the current configuration, and store the file on your computer. Click the Backup button to start the download.

**Restore Configuration:** Use this feature to restore a previously saved configuration file. Click the Browse button to select the configuration file, and then click the Restore button to upload the configuration file to the device.



The screenshot shows the Cisco administration interface for a "Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway" (DPC3848). The "Administration" tab is selected, and the "Factory Defaults" sub-tab is active. The interface includes a navigation menu with options like Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, Status, and Log OFF. Below this, there are sub-tabs for Management, Reporting, Diagnostics, Back Up & Restore, Factory Defaults, and Device Restart. The main content area contains a "Factory Defaults" section with a "User Name:" label, a "Password:" label, a text input field, and a "Restore Factory Defaults" button. A "Help..." link is visible on the right side of the page.

Use this feature to restore all modem into its factory defaults



The screenshot shows the Cisco administration interface for a 'Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway' (DPC3848). The 'Administration' tab is selected, and the 'Device Restart' sub-tab is active. The interface includes a navigation menu with options like Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, Status, and Log OFF. Below this, there are sub-tabs for Management, Reporting, Diagnostics, Back Up & Restore, Factory Defaults, and Device Restart. The main content area contains a 'Device Restart' section with a 'User Name:' label, a 'Password:' label, a text input field, and a 'Device Restart' button. A 'Help...' link is visible on the right side of the page.

This screen allows you to reboot the DUT.

Note: This is just reboot , all configuration settings will not lost.



Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway

DPC3848

Setup Wireless Security Access Restrictions Applications & Gaming Administration **Status** Log OFF

**Gateway** Local Network Wireless DOCSIS WAN DOCSIS Status Channels Selection DOCSIS Log

### Gateway Information

Firmware Version: **dpc3800-v303r2042161-140428a**  
MAC Address: **84:8d:c7:e7:e5:26**  
Current Time: **1970-01-01 09:46:54**  
Router Mode: **router**

### Internet IPv4 Connection

IPv4 Address: **0.0.0.0**  
Subnet Mask: **0.0.0.0**  
Default Gateway:  
Primary DNS:  
Secondary DNS:

Help...

This screen displays information about the Gateway and its current settings. The on-screen information will vary depending on the Internet Connection Type you use.

Refresh



Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway

DPC3848

Setup Wireless Security Access Restrictions Applications & Gaming Administration **Status** Log OFF

Gateway **Local Network** Wireless DOCSIS WAN DOCSIS Status Channels Selection DOCSIS Log

## Local Network

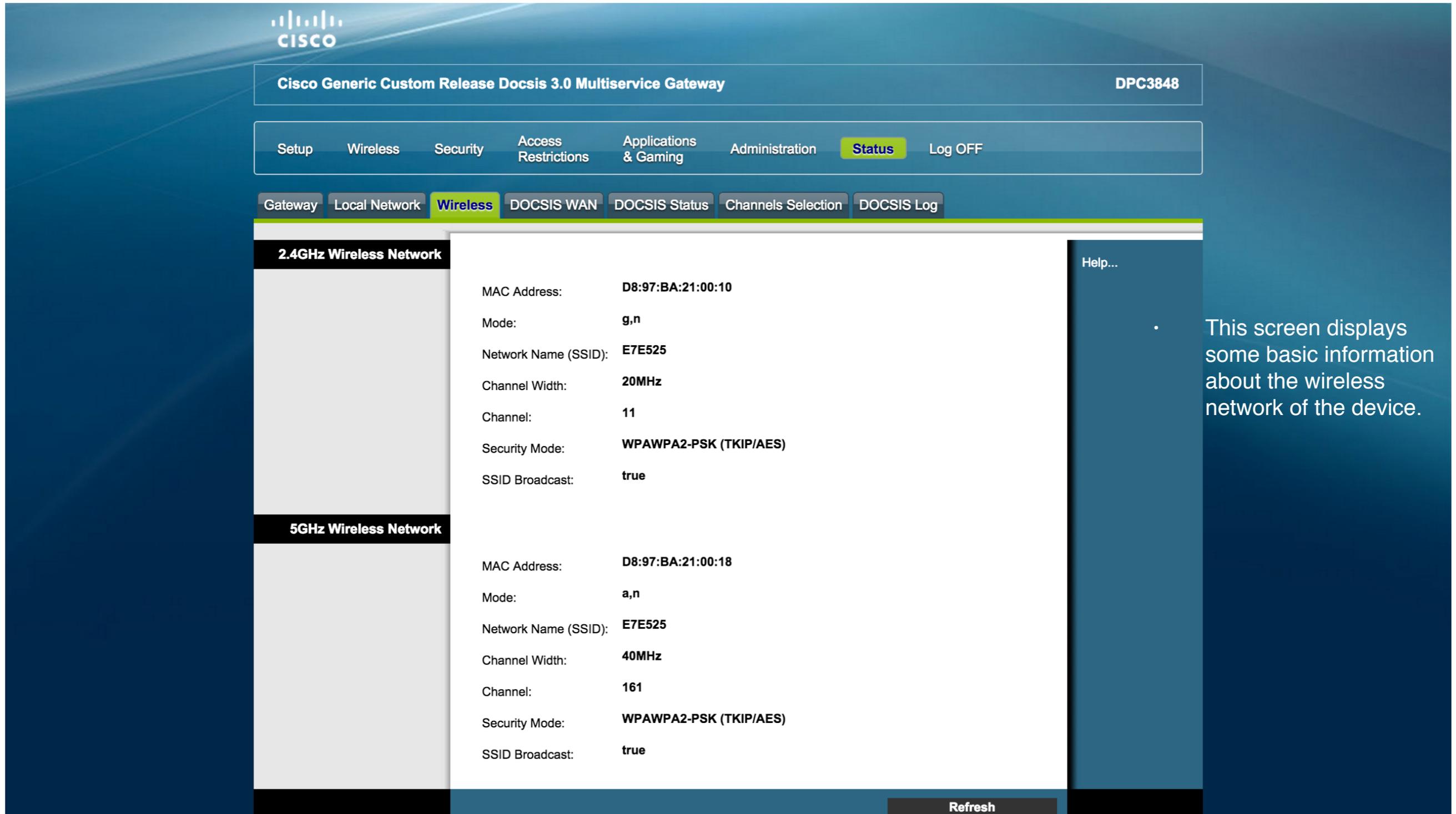
MAC Address: **00:50:f1:80:00:00**  
Internet IP Address: **192.168.0.1**  
Subnet Mask: **255.255.255.0**  
DHCP Server: **Enabled**  
Starting IP Address: **192.168.0.2**  
End IP Address: **192.168.0.253**

[DHCP Client Table](#) [ARP/RARP Table](#)

**Refresh**

Help...

This screen displays the status of your Local Area Network.



The screenshot displays the Cisco Gateway configuration interface. At the top, the Cisco logo and the device name "Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway" are visible, along with the device ID "DPC3848". A navigation menu includes "Setup", "Wireless", "Security", "Access Restrictions", "Applications & Gaming", "Administration", "Status" (highlighted), and "Log OFF". Below this, a sub-menu shows "Gateway", "Local Network", "Wireless" (highlighted), "DOCSIS WAN", "DOCSIS Status", "Channels Selection", and "DOCSIS Log".

The main content area is divided into two sections: "2.4GHz Wireless Network" and "5GHz Wireless Network". Each section lists the following parameters:

Parameter	2.4GHz Wireless Network	5GHz Wireless Network
MAC Address:	D8:97:BA:21:00:10	D8:97:BA:21:00:18
Mode:	g,n	a,n
Network Name (SSID):	E7E525	E7E525
Channel Width:	20MHz	40MHz
Channel:	11	161
Security Mode:	WPAWPA2-PSK (TKIP/AES)	WPAWPA2-PSK (TKIP/AES)
SSID Broadcast:	true	true

A "Refresh" button is located at the bottom right of the content area. A "Help..." link is visible on the right side of the page.

• This screen displays some basic information about the wireless network of the device.

[Gateway](#)
[Local Network](#)
[Wireless](#)
[DOCSIS WAN](#)
[DOCSIS Status](#)
[Channels Selection](#)
[DOCSIS Log](#)

**About**

**Model:** Cisco DPC3848  
**Vendor:** Cisco  
**Hardware Revision:** 2.0  
**Serial Number:** 271294899  
**MAC Address:** 84:8d:c7:e7:e5:25  
**Bootloader Revision:** 3.4.20  
**Firmware Version:** dpc3800-v303r2042161-140428a.p7b  
**Firmware Build Time:** 04-28-2014 17:07:45  
**Cable Modem Status:** NOT\_SYNCHRONIZED

---

**Cable Modem State**

**DOCSIS Downstream Scanning:** Complete  
**DOCSIS Ranging:** NotStarted  
**DOCSIS DHCP:** NotStarted  
**DOCSIS TFTP:** NotStarted  
**DOCSIS Data Reg Complete:** NotStarted  
**DOCSIS Privacy:** NotStarted

---

**Downstream Channels**

Channel	Power Level:	Signal to Noise Ratio:
Channel 1:	-51.800 dBmV	4.70dB

---

**Upstream Channels**

Channel	Power Level:

- Information about the modem such as MAC address, Serial Number, Firmware version can be found in this page
- This is 24\*8 channel modem. This page shows how many DS and US channels are bonding



Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway

DPC3848

[Setup](#)
[Wireless](#)
[Security](#)
[Access Restrictions](#)
[Applications & Gaming](#)
[Administration](#)
[Status](#)
[Log OFF](#)

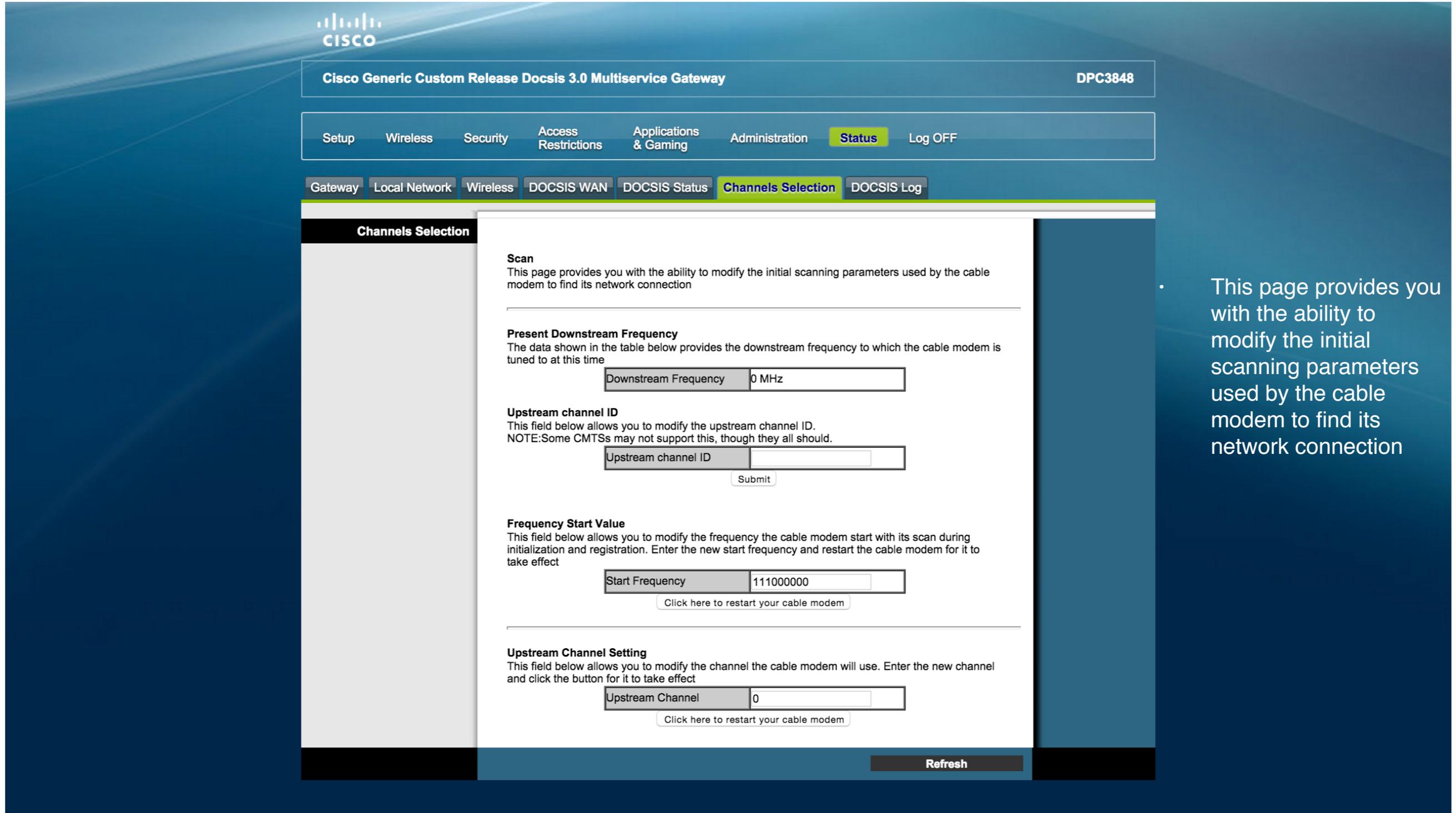
[Gateway](#)
[Local Network](#)
[Wireless](#)
[DOCSIS WAN](#)
[DOCSIS Status](#)
[Channels Selection](#)
[DOCSIS Log](#)

## DOCSIS Status

**Cable Modem Status: Scanning**  
**Cable Modem IPv4 Address: 0.0.0.0**  
**Cable Modem IPv6 Address: ::**  
**Cable Modem Mask: 0.0.0.0**  
**Cable Modem Gateway: 0.0.0.0**  
**Cable Modem TFTP Server: 0.0.0.0**  
**Current Time: 1970-01-01 09:49:30**  
**Time Server: 0.0.0.0**  
**Time Offset: 0**  
**Time Since Last Reset: 35371**  
**Configuration File:**  
**Cable Modem Certificate: Not Installed**  
**IP Time Lease: 0**  
**IP Time Rebind: D: 91 H: 4 M: 22 S: 4**  
**IP Time Renew: D: 91 H: 4 M: 37 S: 24**

## Ethernet

Interface Name	LINK Status	LINK Speed	LINK Duplex
Interface1	Up	100 Mbits	Full
Interface2	Down	0 Mbits	Auto
Interface3	Down	0 Mbits	Auto
Interface4	Down	0 Mbits	Auto
Interface5	Down	1000 Mbits	Auto



The screenshot shows the Cisco web interface for a Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway (DPC3848). The interface includes a navigation menu with tabs for Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, Status, and Log OFF. The Status tab is selected, and the Channels Selection sub-tab is active. The main content area is titled "Channels Selection" and contains several sections for configuring scanning parameters:

- Scan**: This page provides you with the ability to modify the initial scanning parameters used by the cable modem to find its network connection.
- Present Downstream Frequency**: The data shown in the table below provides the downstream frequency to which the cable modem is tuned to at this time. The input field shows "0 MHz".
- Upstream channel ID**: This field below allows you to modify the upstream channel ID. NOTE: Some CMTSs may not support this, though they all should. The input field is empty, and there is a "Submit" button below it.
- Frequency Start Value**: This field below allows you to modify the frequency the cable modem start with its scan during initialization and registration. Enter the new start frequency and restart the cable modem for it to take effect. The input field shows "111000000", and there is a "Click here to restart your cable modem" button below it.
- Upstream Channel Setting**: This field below allows you to modify the channel the cable modem will use. Enter the new channel and click the button for it to take effect. The input field shows "0", and there is a "Click here to restart your cable modem" button below it.

A "Refresh" button is located at the bottom right of the main content area.

• This page provides you with the ability to modify the initial scanning parameters used by the cable modem to find its network connection



Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway

DPC3848

Setup Wireless Security Access Restrictions Applications & Gaming Administration **Status** Log OFF

Gateway Local Network Wireless DOCSIS WAN DOCSIS Status Channels Selection **DOCSIS Log**

### DOCSIS Log

Time	ID	Level	Description
Wed May 13 08:25:48 2015	90000000	Warning (5)	MIMO Event MIMO: Stored MIMO=-1 post cfg file MIMO=-1;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.0;CM-VER=3.0;
Thu Jan 1 00:02:22 1970	82000800	Critical (3)	16 consecutive T3 timeouts while trying to range on upstream channel 4;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:02:22 1970	82000300	Critical (3)	Ranging Request Retries exhausted;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:01:40 1970	82000200	Critical (3)	No Ranging Response received - T3 time-out;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:01:26 1970	84020200	Warning (5)	Lost MDD Timeout;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:01:26 1970	84020300	Warning (5)	MDD message timeout;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Wed May 13 08:19:34 2015	90000000	Warning (5)	MIMO Event MIMO: Stored MIMO=-1 post cfg file MIMO=-1;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.0;CM-VER=3.0;
Thu Jan 1 00:01:20 1970	84020200	Warning (5)	Lost MDD Timeout;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:01:19 1970	84020300	Warning (5)	MDD message timeout;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Wed May 13 08:16:19 2015	69011200	Notice (6)	SW download Successful - Via Config file
Wed May 13 08:12:53 2015	69010200	Notice (6)	SW Download INIT - Via Config file main.cfg
Wed May 13 08:11:19 2015	90000000	Warning (5)	MIMO Event MIMO: Stored MIMO=-1 post cfg file MIMO=-1;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.0;CM-VER=3.0;
Thu Jan 1 00:02:11 1970	82000800	Critical (3)	16 consecutive T3 timeouts while trying to range on upstream channel 4;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:02:11 1970	82000300	Critical (3)	Ranging Request Retries exhausted;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:01:41 1970	82000200	Critical (3)	No Ranging Response received - T3 time-out;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:01:27 1970	84020200	Warning (5)	Lost MDD Timeout;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;

This page provides Logs