Configure Network Settings

Revised: May 4, 2015

Concepts

Glossary

Timesaver Go to terms that start with... [**numerals** | **A** | **C** | **D** | **E** | **L** | **M** | **P** | **S** | **T** | **W**].

numerals

802.11b A wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g A wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibilitywith 802.11b devices.

A

AAA Authentication, Authorization, and Accounting.

See also EAP-FAST, EAP-MD5 server, LEAP server, and PEAP server.

access point A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

autoregistration *See* MSI registration service.

Auto Smartports[1] A collection of interface-level switch commands bundled together as a macro that configures a switchport without human intervention. Upon detecting a connection to one of its physical interfaces (or "ports"), a Medianet-ready switch uses CDP packets or a similar mechanism[2]—in tandem with a *port-based network access control* (PNAC) standard such as 802.1x/MAB—to learn what type of device has connected to it. Device identification triggers the appropriate Auto Smartports macro to run automatically on the switch and configure its interface appropriately for the detected device type. This behavior eases the administrative burden of configuring multiple switchports manually. (Similarly, when there is a "link-down" event on the port, the switch removes the macro.) In the ITU model and framework for network management, known as *FCAPS*, Auto Smartports macros act in support of what's called *configuration management*.

See *Auto Smartports Configuration Guide, Release 12.2(58)SE* at http://cisco.com/en/US/docs/switches/lan/auto_smartports/12.2_58_se/configuration/guide/aspcg.html.

1. Infrequently abbreviated as *ASP*.
2. Such as Link-Level Discovery Protocol (LLDP) packets, packets that include specific MAC addresses or Organizational Unique Identifiers (OUIs), or attribute-value pairs within a RADIUS response.

C

Return to Top

CCMP

Based on the Advanced Encryption Standard (AES) defined in the National Institute of Standards and Technology's FIPS Publication 197, AES-CCMP is a symmetric block cipher that can encrypt and decrypt data using keys of 128, 192, and 256 bits. AES-CCMP is superior to WEP encryption and is defined in the IEEE 802.11i standard.

See also WEP keys.

CDP

Cisco Discovery Protocol. DMPs and other devices that support CDP can communicate facts about themselves, amongst themselves, over any physical network medium that supports *Subnetwork Access Protocol* (SNAP) encapsulation. CDP uses the *data link layer*, which connects physical network media to upper-layer protocols. And because CDP operates at this level, two or more CDP devices that support different network layer protocols (for example, IP and *Novell IPX*) can learn about each other.

Specifically, CDP causes devices to advertise not only their existence, but also their platform types, protocols, IP addresses, and SNMP-agent addresses to neighboring devices on their LAN switch or WAN. And when their connected switch is Medianet-ready, device identification can also trigger an Auto Smartports macro to run automatically.

Thus, CDP facilitates discovery—by network management applications—of Cisco devices that are neighbors of known devices. And this is particularly useful when such previously undiscovered neighbors use lower-layer, transparent protocols. After they possess information about such devices, network management applications can send SNMP queries to them.

In addition, CDP detects native VLAN and port duplex mismatches.

D

↑ *Return to Top*

DHCP

Dynamic Host Configuration Protocol. A standard method for devices to request, and servers to allocate, IP addresses in a network without human intervention.

DHCP option 125

An optional DHCP relay class that:

- Injects “vendor-identifying, vendor-specific information” into the request (within a DHCP DISCOVER message) to receive a dynamic IP address.
- Identifies the type of client sending the DHCP DISCOVER message.

In turn, a DHCP server that is configured to support Option 125 can relay the client-generated request to some other DHCP server. This mechanism allows an organization to designate DHCP servers for clients that meet particular criteria. For example, you might want all of your DMPs to receive their IP addresses from a DHCP server that you reserve for this purpose exclusively.

E

Return to Top

EAP

EAP is the Extensible Authentication Protocol that WPA uses to authorize user access to wireless networks. Common implementations include EAP-FAST and EAP-MD5.

EAP-FAST

EAP-FAST is a two-phase implementation of the EAP authentication protocol:

- Phase 0, provisioning. Provision client with a credential called PAC (Protected Access Credentials).
- Phase 1, authentication. Use the PAC to establish a tunnel with the server and authenticate the username and password.

See also AAA and EAP.

EAP-MD5 server

Servers that use EAP to provide dynamic, session-specific wireless encryption keys, central user administration, and authentication between clients and access points. EAP-MD5 uses MD5 hashing on client and challenge passwords.

See also AAA and EAP.

L

Return to Top

Location Services

Mechanism by which a device can learn its actual physical ("civic") location through its connection to a Medianet-ready switch. Upon learning its location, the device can then share this information with peers, management servers, and other equipment on its network. The physical location of a DMP is almost always an important factor in which central management server it should trust, which assets it should play, which commands it should run, and which schedule it should follow.

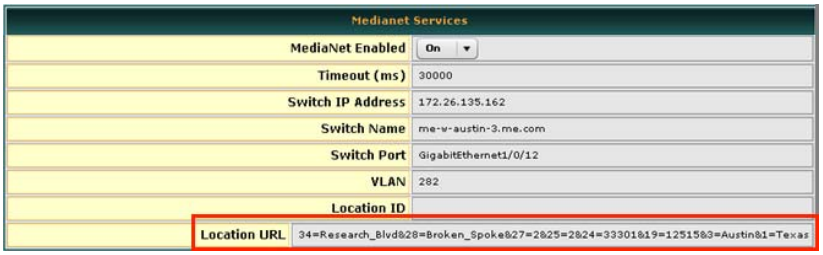
Someone must configure two essential values on your Medianet-enabled switch: "*civic-location-id*" and "*additional-location-information*." These values are encapsulated into a CDP message that endpoints receive.

civic-location-id

This value describes the physical site—including the municipality, street address, floor designation, and so on—where a switch and its attached nodes are deployed.

additional-location-information

This value describes any additional details to inject into the encapsulated CDP message. As this is a data injection, it depends wholly on the presence of a defined *civic-location-id* value. Absent **that** value, there is no way for **this** value to reach any endpoint. Later, when you plug a Medianet-ready DMP into a properly configured switch, the Location Services feature of MSI populates the Location URL field automatically in DMPDM.



Note **CDP and LLDP constrain how much location information you can store on a Medianet-enabled switch.** Make sure that this information never exceeds 255 bytes.

Note **A DMP 4400G cannot receive or use Location Services information over Wi-Fi.** Its connection type to your Medianet-enabled switch must be Ethernet.

M

Return to Top

Medianet

End-to-end intelligent architecture for optimized delivery of rich media to a variety of endpoints throughout an enterprise. Cisco Medianet is media-aware, endpoint-aware, and network-aware.

MSI

Media Services Interface. Announces services to a DMP or any other Medianet-ready device that you connect to a Medianet-enabled switch. MSI tells devices about their neighbors and their civic location.

MSI registration service

Medianet feature by which:

- Devices send encrypted registration requests to management servers.
- Servers receive such requests, respond to them, and store records in a local database.

MSI service discovery

Mechanism that applies DHCP option 125 packets to advertise—and poll for—the availability of particular services in a network. Service Discovery also notes which hosts provide these services. For your purposes as a DMP administrator, Medianet should know that a DMM server is available and know exactly which addressable node it is on your network. So naturally, you must configure your DHCP server to facilitate this information-sharing model. Configuration methods vary among platforms and implementations.

An example here shows entries in the **dhcpd.conf** file for a Linux-based DHCP server called *dhcpd*. Entries like these advertise the IP address of your authoritative DMM appliance—converted here from decimal to hex and shown in red—to any DMPs that should trust its directives implicitly.

```
option domain-name "example.com";
option domain-name-servers 192.168.1.1;
option option-125 code 125 = string;
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.200 192.168.1.210;
  option routers 192.168.1.1;
  option subnet-mask 255.255.255.0;
}
class "DMM" {
match if option option-125 = "\x00\x00\x00\x09\x06\x13\x04\x01\x44\x4d\x4d";
option option-125
"\x00\x00\x00\x09\x0b\x14\x09\x01\x80\x6b\xe0\xbc\x1f\x90\x00\x01";
}
```

Tip **The Linux CLI can easily convert IP address octets from decimal to hexadecimal.**

```
$ echo 'ibase=10;obase=16;[ octet ]' | bc
```
← *(Remember to use a closing quote mark before the pipe.)*

And so, in keeping with the previous conversion example, shown in red....

- **128** becomes **x80**
- **107** becomes **x6b**
- **224** becomes **xe0**
- **188** becomes **xbc**

In contrast, the DHCP offering in Windows Server 2008 (and, likewise, Windows Server 2003) cannot handle DHCP option 125 queries natively. Therefore, you must install a "callout" DLL that injects this ability into the server before you can configure it to advertise the availability of any service.

Note For **32-bit** Windows Server, the DLL filename is DHCPSDDLL**x86**.DLL.
For **64-bit** Windows Server, the DLL filename is DHCPSDDLL**x64**.DLL.

Afterward, you must edit **\Medianet\msi\apps\dhcpsddll\src\dhcpsdconfig.reg** to include a *3-tuple* (**IP,port,transport**), converted to hexadecimal, that identifies your DMM appliance as a provider of centralized management for DMPs.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\DhcpSd\Settings]
"DebugLevel"=dword:00000000
"IgnoreProcessItFromChain"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\DhcpSd\Records\1]
"DMM"=hex:0a,c2,33,2a,1f,90,00,01
```

And finally, you must add two keys to the Windows registry, under
`\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Paramters`

- **CalloutEnabled REG_DWORD 1**
- **CalloutDlls REG_MULTI_SZ** <*full_path_to_DLL*>

Note **See the Medianet documentation on Cisco.com for detailed instructions.**

P

Return to Top

PEAP server Protected EAP server, which combines centralized two-way authentication with dynamically generated wireless equivalent privacy keys or WEP keys.

See also AAA, EAP-MD5 server, and WEP keys.

PSK Pre-Shared Key.

S

Return to Top

SSID Service Set ID. It is a unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish among multiple wireless networks in the same vicinity. The SSID can be any alphanumeric entry up to 32 characters long.

T

Return to Top

TKIP Temporal Key Integrity Protocol, also known as key hashing, is used as part of server-based EAP authentication.

W

Return to Top

WEP Wired Equivalent Privacy is a method to encrypt data transmitted on a wireless network.

WEP keys Wired equivalent privacy (WEP) keys are the IEEE 802.11b standard that offers a mechanism for securing wireless LAN data streams. The goals of WEP include access control to prevent unauthorized users who lack a correct WEP key from gaining access to the network, and privacy to protect wireless LAN data streams by encrypting them and allowing de-encryption only by users with the correct WEP keys.

WPA Wi-Fi Protected Access. WPA is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP for data protection and 802.1X for authenticated key management.

Understand WEP Keys and Passphrases

Timesaver **Does your wireless network use WPA instead of WEP?** If so, you can ignore this topic.

Many 802.11 access points (wireless routers) accept only a hexadecimal passphrase for WEP-64 and WEP-128. And yet, DMPs accept only an ASCII passphrase for WEP. For this reason, it might be necessary at times to translate your WEP passphrase from ASCII to hexadecimal.

Note **Many third-party converters are available.** We do not offer any Cisco converter for this purpose.

The typical WEP process is as follows.

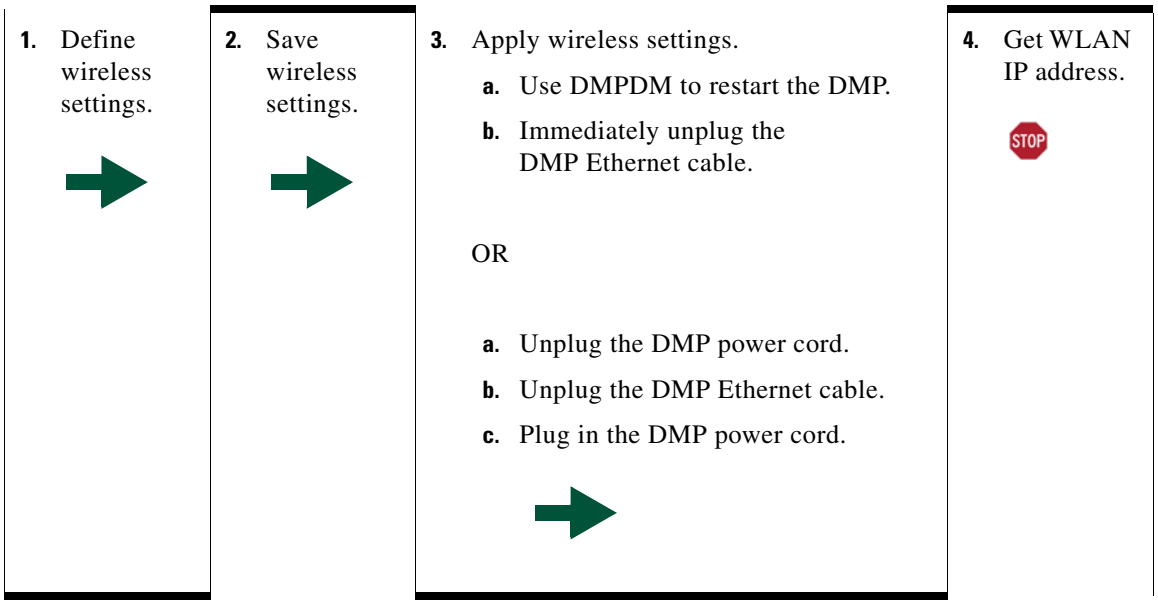
1. Pick an ASCII passphrase. For example, *PassphraseWEP128*.
2. Convert your string of ASCII characters to the hexadecimal key or keys for your network.
   - WEP-64 uses four short hexadecimal keys.
   - WEP-128 uses one long hexadecimal key.
3. Configure your DMP to use the ASCII from which you derived the hexadecimal.
4. Configure your wireless router to use the appropriate hexadecimal key or keys.

Related Topics

- Configure a Wireless Network Connection, page 10-16
- Configure a Wireless Network Connection, page 10-16

Workflow to Define Wi-Fi Settings

It is not necessary, useful, or correct to restart a DMP immediately after you define its 802.11 settings. Instead, the typical workflow is as follows.



Partial Support for Cisco Medianet 2.1 Features

Cisco Medianet is an end-to-end architecture for networks that deliver rich-media experiences. Some DMP endpoints support some Cisco Medianet 2.1 features.

Note **We do not support any Medianet features on DMP 4305G endpoints.**

Tip

- **To assess your network for Medianet readiness, see http://cisco.com/go/mra.**
- **To review solution reference network designs (SRNDs) for Medianet, see http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns819/landing_vid_medianet.html.**

 **DMP 4310G**	DMP 4310G endpoints support discovery via DHCP and can learn their physical location. In addition, they know and can broadcast their product type, model, and software version. Through their use of your Medianet, they can receive their IP address, VLAN assignment, and network configuration settings automatically. Furthermore, they receive information from Medianet through DHCP[1] that helps them to autoregister themselves with your DMM server. Later, after a successful autoregistration, the splash screen on these DMPs includes key parameters and states explicitly that setup succeeded.
 **DMP 4400G**	Medianet 2.1 feature support by DMP 4400G endpoints is equivalent to support by DMP 4310G endpoints, **with just one exception**. Ordinarily, a DMP 4400G can participate in networks via either an Ethernet connection or a Wi-Fi connection. **However:** A Wi-Fi connection by a DMP 4400G prevents it from obtaining or using any Location Services information that Medianet might be configured to provide.

1. With DHCP option 125 (V-I Vendor-Specific Information) for service discovery, after you configure your supported DHCP server to support this option. See **RFC 3925**.

Note **These features are designed to simplify the largest deployments, whereas DMPDM is designed to support the smallest deployments.** If you manage your DMP primarily via DMPDM, your benefit from Medianet integration will be minimal.

Understand Medianet Autoconfiguration for DMP 4310G Endpoints

DMP 4310G and 4400G endpoints can use CDP to announce and identify themselves on networks.

AND

You might use Ethernet cables to connect such DMPs to switches where the autoconfiguration (Auto Smartports) features of Medianet are enabled.

When you do, these switches recognize from the CDP announcements that the newly connected devices are DMPs.

After recognizing that a DMP is attached to one of its Ethernet ports, the switch can apply to this port a set of built-in configuration macros (Auto Smartports) that are optimized specifically for DMPs. By configuring so many settings automatically, Medianet can accelerate and simplify DMP mass deployments, QoS configuration, and asset tracking. In turn, these simplified deployments can lower your operating costs.

Information That Medianet and DMPs Exchange

Medianet and a DMP 4310G can exchange these types of data.

- name of the chassis
- system name
- system object
- hardware revision
- firmware revision
- software revision
- seial number
- manufacturing name
- model name
- asset identifier
- CDP timeout
- VLAN assignment
- switch port assignment
- switch name and model
- switch IP address
- loation string

If you would like to learn more about Medianet, see http://cisco.com/go/medianet.

Restrictions

Wireless Networks

- **Ethernet connections take priority over Wi-Fi connections on DMPs where both are active.**
- We do not support “open” Wi-Fi networks. They are a security risk.
- We do not support media streams to DMPs over Wi-Fi networks. The experience is poor.
- DMP 4305G endpoints do not support Wi-Fi.

Autoregistration

- Autoregistration depends upon the Cisco TAC Troubleshooting Access option for DMPs and fails unless this option is enabled.

Login Credentials

- All DMPs that you manage centrally in DMM must share one identical set of DMPDM login credentials.

Medianet

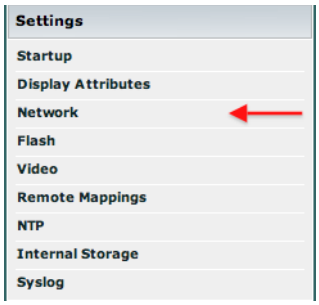
- When a DMP 4310G relies upon a Medianet switch where more than one VLAN uses DHCP, the DMP might come to use the wrong IP address. For this to occur, temporary conditions that do not sever the DMP's AC power connection must nonetheless interrupt its network connection through the switch. (Thus, this problem cannot possibly occur while the DMP uses PoE.) Specifically, the Medianet switch assigns its default VLAN to your DMP. But then—after your DMP’s network connection is interrupted and restored—your Medianet switch assigns to your DMP a dynamic IP address from another VLAN on your Medianet switch. This easily prevented mismatch disrupts centralized management of your DMP. To prevent this problem or to recover from it, you can download and run the patch from Cisco.com.

Procedures

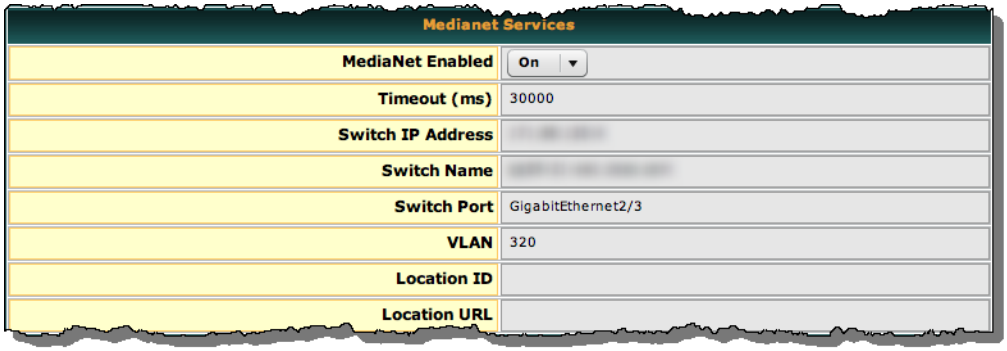
Activate Medianet Support

Procedure

Step 1 Click **Network** in the Settings area.



Step 2 Choose **On** from the Medianet Enabled list in the Medianet Services area.



Step 3 Save this changed setting, and then restart your DMP.

Configure HTTP Proxy Server Settings for a DMP 4310G

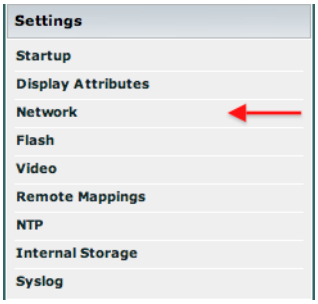
Note

- **The only transport protocol that we can proxy in this release is HTTP over :80 or :8080.**
- **The only asset types that we can proxy in this release are video and SWF.**

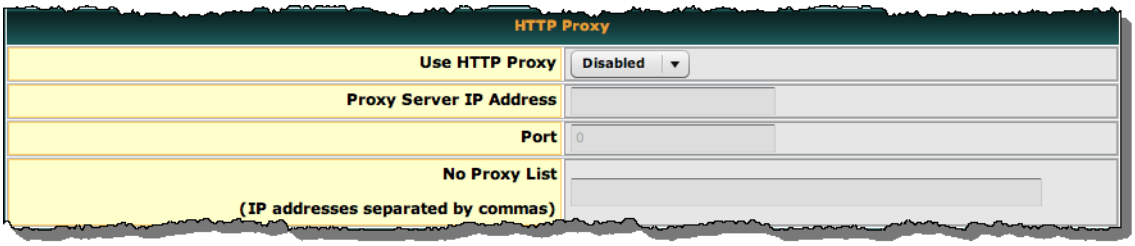
You can configure a DMP 4310G to use a proxy server and you can specify which of your content servers should be exempt from this proxy service.

Procedure

Step 1 Click **Network** in the Settings area.



Step 2 Choose Enabled from the Use HTTP Proxy list.



Step 3 Three fields become editable.

Proxy Server IP Address

- To proxy the playback of **video assets** from an HTTP server, you must enter the routable IP address of your proxy server. Do not enter a hostname. Do not use any wildcards.
- To proxy the playback of **SWF assets** from an HTTP server, you can enter *either* the routable IP address *or* the FQDN (DNS-resolvable hostname) of your proxy server. Do not enter any wildcards.

Port—Enter either **80** or **8080**. Do not enter any other value.

No Proxy List (IP addresses separated by commas)

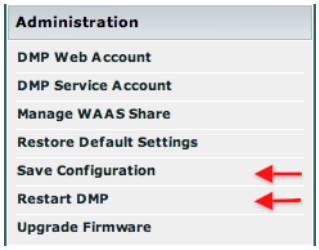
- To bypass your proxy when you play **video assets** from particular HTTP servers, you must enter comma-separated IP addresses. These identify each content server that should be excluded from proxy. Nonetheless, we continue to proxy video playback from any other HTTP server. Do not enter any hostnames. Do not enter any wildcards.
- To bypass your proxy when you play **SWF assets** from particular HTTP servers, you can enter *either* comma-separated IP addresses *or* comma-separated FQDNs (DNS-resolvable hostnames). These identify each content server that should be excluded from proxy. Nonetheless, we continue to proxy video playback from any other HTTP server. Do not enter any wildcards.

Note **Proxy settings do not have any effect on RSS traffic.** When an RSS request crosses from one Internet domain to another, your DMP is its own proxy.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration** in the Administration list, and then click **Save**.

Step 6 Click **Restart DMP** in the Administration list, and then click **Restart**.



Configure HTTP Proxy Server Settings for a DMP 4400G or DMP 4305G

Note **The only transport protocol that we can proxy in this release is HTTP over :80 or :8080.**

You can configure a DMP 4400G or DMP 4305G to use a proxy server and you can specify which of your content servers should be exempt from this proxy service.

Procedure

Step 1 Click **Network** in the Settings area.

Step 2 Choose **Enabled** from the Use HTTP Proxy list.

Step 3 Three fields become editable.

- **Proxy Server IP Address or Hostname**—The routable IP address *or* the FQDN (DNS-resolvable hostname) of your proxy server. Do not enter any wildcards..
- **Port**—Enter either **80** or **8080**. Do not enter any other value.
- **No Proxy List**—To bypass your proxy when you play assets from particular HTTP servers, you can enter *either* comma-separated IP addresses *or* comma-separated FQDNs (DNS-resolvable hostnames). These identify each content server that should be excluded from proxy. Nonetheless, we continue to proxy content from any other HTTP server. Do not enter any wildcards.

Note **Proxy settings do not have any effect on RSS traffic.** When an RSS request crosses from one Internet domain to another, your DMP is its own proxy.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration** in the Administration list, and then click **Save**.

Step 6 Click **Restart DMP** in the Administration list, and then click **Restart**.

Configure a Wireless Network Connection

Timesaver **Complete this optional procedure at your discretion.**

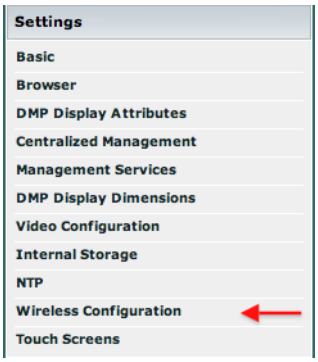
Before You Begin

- Do the hardware and firmware for your DMP support wireless networking? DMP 4305G and DMP 4310G endpoints **do not**.
  - To verify whether you must use an Ethernet cable, see Table 2 on page 2-5.
  - Alternatively, if Table 2 on page 2-5 does not describe your DMP model, see its datasheet at http://cisco.com/go/dms/dmp/datasheets.

- The Broadcast SSID setting must be enabled on your wireless access points (also known as *wireless routers* or *WLAN controllers*). Otherwise, your DMPs cannot connect to your WLAN and are prevented from obtaining IP addresses.
- We do not support "open" wireless networks. They are a security risk.
- Does a security policy in your network restrict DHCP address assignments to known MAC addresses? If so, locate the **WLAN** address printed on a sticker that is affixed to your DMP. Then, share this address with your security policy administrator.
- Verify that your wireless network is working correctly, is available, and you understand how it authenticates connection requests.
- Connect Over Ethernet.
- Log in to DMPDM, page 7-5.

Procedure

Step 1 Click **Wireless Configuration** in the Settings list.



Tip **Do you see this option in DMPDM?** If not, your DMP might not support it. But you can learn whether any firmware upgrade is available that adds this feature to your DMP model.

- See our release notes—http://cisco.com/go/dms/releasenotes.
- See our compatibility information—http://cisco.com/go/dms/compatibility.

If newer firmware is available, follow the published instructions to obtain it. Then, complete the firmware upgrade procedure in your DMPDM user guide at http://cisco.com/go/dms/dmpdm.

The nature of your Cisco DMS service contract might limit:

- Which upgrades are available to you.
- Where and how you obtain upgrades.
- Whether you must pay anything to obtain upgrades.

To learn about Cisco service contracts, see http://cisco.com/go/cscc.

Step 2 Choose **Enabled** from the Wireless Interface list.

Each 802.11 wireless network is assigned a name to distinguish it from other networks. The technical term for this network name is *Service Set Identifier*, or SSID.

Step 3 Double-click the SSID for your network in the Detected Networks table.

OR

When you do not see your SSID in the Detected Networks table, do the following.

a. Enter in the Network SSID field the SSID for your network.

b. Choose from the Security list the security method for your network. Its options are:

- WEP-64bit
- WEP-128bit
- WPA-PSK
- WPA-EAP
- WPA2-PSK
- WPA2-EAP

The security method that you choose controls, in part, which fields and options this DMPDM page shows to you.

- When you see the PSK field and you chose a WEP-based security method, enter in it the key from which your 64-bit or 128-bit passphrase is cryptographically derived.
- When you see the PSK field and you chose a WPA-based or WPA-2-based security method, enter in it the pre-shared key for your network.
- When you see the Encryption list, choose from it either **TKIP** or **CCMP AES**.
- When you see the EAP list, choose from it either **FAST**, **MD5**, or **PEAP (ver.0)**.
- When you see the Username and Password fields, enter in them respectively a valid username for your wireless network and the password for that username.

c. Choose **Enabled** from the Dynamic IP Addressing (DHCP) list.

Tip **Will you ever deploy your DMP in a wireless network that does not have any DHCP server?** If so, you can configure your DMP to use a static IP address.

d. (**Optional**) Click **Probe** to check whether these settings work correctly with your wireless network.

e. When you are satisfied with your choices, Click **Select**.

f. Click **Save Configuration** in the Administration list, and then click **Save**.

Step 4 Disconnect the Ethernet cable from your DMP.

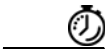
Step 5 Click **Restart DMP** in the Administration list, and then click **Restart**.

Step 6 Stop. You have completed this procedure.

Related Topics

- DMP Physical Specifications and Interfaces (I/O Ports), page 2-3
- Connect Over Ethernet, page 2
- Assign a Static IP Address to a Wireless DMP 4400G, page 10-21

Prepare Your DMP to Use a Static IP Address Over Ethernet



Timesaver **Complete this optional procedure at your discretion.** It explains what to do when a DMP's ultimate deployment site does not use DHCP.

Before You Begin

- Connect Over Ethernet, page 2.

  OR

  Obtain an Ethernet crossover cable.
- Do one of the following.
  - Transport your DMP to a site where the local network segment includes a DHCP server and ensure that you have access there to a web browser.
  - Configure any system at your current location to run temporarily as a DHCP server and ensure that you have access to a web browser.

Procedure

Step 1 Connect your DMP to its presentation system.

Step 2 Turn **On** the presentation system and then do one of the following.

- Use a standard, category 5 (RJ-45) Ethernet cable—either 10/100 or 10/100/1000, depending on your DMP model—to connect your DMP to the network segment that includes the DHCP server.
- Use an Ethernet crossover cable to connect your DMP directly to the DHCP server.

Step 3 If the DHCP server process is not running yet on the DHCP server, start that process now—along with any processes that it uses.

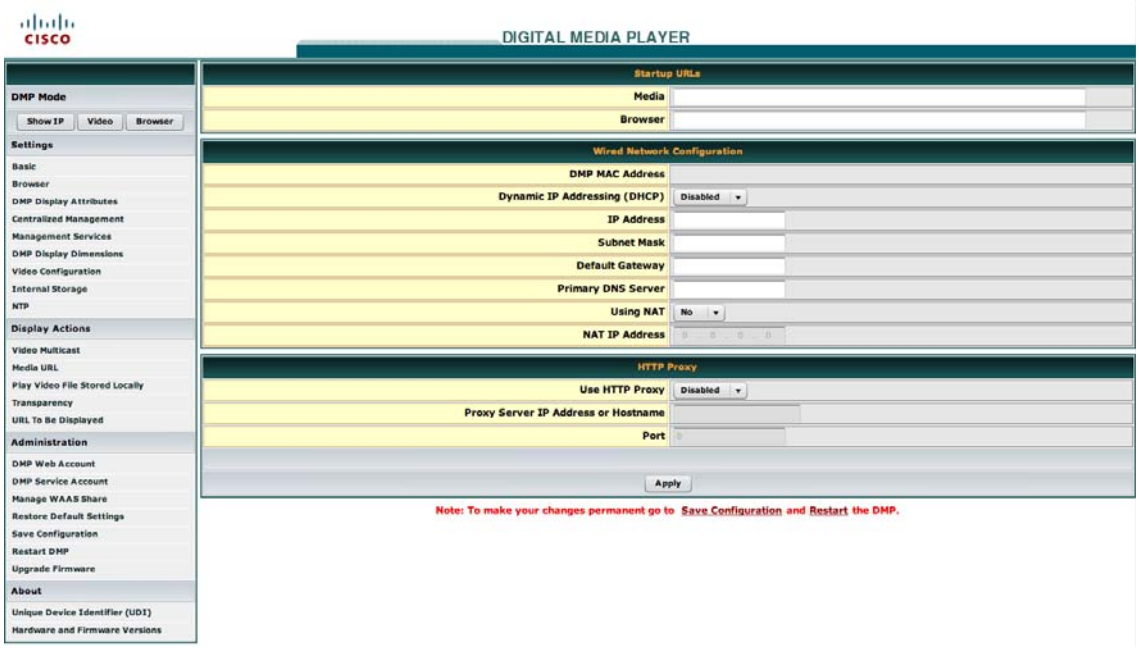
Step 4 Turn **On** your DMP and make a note of the IP address that it shows on its presentation system.

Step 5 Point your browser to the IP address.

Note **Is your DMP brand-new?** Or, have its settings been restored to factory defaults? If so, DMPDM prompts you to define a master password for your DMP. You must do this before you can do anything else. See the "Log in to DMPDM" section on page 7-5.

Step 6 When prompted to log in, use the master username and password that you defined.

DMPDM loads its basic settings page in your browser.



Step 7 Choose **Disabled** from the Dynamic IP Addressing (DHCP) list, and then:

a. Enter in the IP Address field the static IP address that your DMP should use.

b. Enter in the Subnet Mask field the netmask that your DMP should use with its static IP address.

c. Enter in the Default Gateway field the network gateway that your DMP should use with its static IP address.

d. Enter in the Primary DNS Server field the DNS server that your DMP should use with its static IP address.

Step 8 (**Optional**) Will a network address translation (NAT) service give your DMP a private IP address? If so:

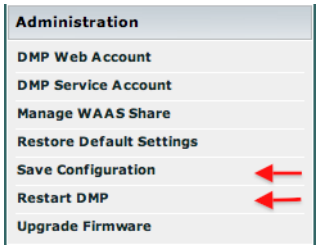
a. Choose **Yes** from the Using NAT list.

b. Enter in the NAT IP Address field the 1-to-1 public address (which is configured on the local router) that corresponds to the private IP address.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration** in the Administration list, and then click **Save**.

Step 11 Click **Restart DMP** in the Administration list, and then click **Restart**.



Step 12 Ship or deliver the DMP to its deployment site, and then:

a. Connect it to its presentation system.

b. Connect it to its local network segment.

c. Connect it to its power source.

Step 13 Stop. You have completed this procedure.

Related Topics

- Assign a Static IP Address to a Wireless DMP 4400G, page 10-21

Assign a Static IP Address to a Wireless DMP 4400G

Procedure

Step 1 Log in to your wireless access point as an administrator.

Step 2 Use its administrative features to assign a static IP address to your DMP.

Step 3 Stop. You have completed this procedure.

Related Topics

- Prepare Your DMP to Use a Static IP Address Over Ethernet, page 10-19

Show the Assigned IP Address

Before You Begin

- If you have not yet obtained an IP address for your DMP, see the quick start guide for your DMP model type to learn how to connect and set up your DMP.

Procedure

Step 1 Click Show IP to learn the IP address of your DMP.

The address is briefly visible on your DMP display.

Step 2 Stop. You have completed this procedure.

Reference

Network Settings Reference

UI Reference: Elements to Define Basic Network Settings

Table 10-1 Elements on the Basic Page

Element	Description
Startup URLs	
Media	The URL or local path that points to an encoded digital video file, which your DMP should load automatically and show immediately after every restart. The URL or pathname cannot contain any more than 254 characters, cannot contain any spaces, and must use ISO/IEC-8859 (Latin-1) character encoding. The value that you enter is case-sensitive. Supported transport protocols and URL types are as follows: • **http://**<*ip_address*>**/**<*path_and_filename*> • **udp://**<*ip_address_of_multicast_server*>**/**<*port_number*> • **file:**///tmp/ftproot/usb_1/<*path_and_filename*> **—For files on the internal flash drive** • **file:**///tmp/ftproot/usb_2/<*path_and_filename*> **—For files on a mounted USB drive** • **file:**///tmp/ftproot/CIFS/<*path_and_filename*> **—For files on a mounted network share** **Note The video file must be encoded in a way that your DMP supports.** **Tip To simulate an audio-only file if your DMP does not support their use directly, play an MPEG-2 file that contains all of the audio data that you want to play and contains just one frame of video data.**
Browser	The HTTP URL of any document that the embedded browser should load automatically and show immediately after each restart. For example, the URL that you enter might point to an HTML page with an embedded Flash file that animates the logo for your organization. The URL cannot contain any more than 254 characters, cannot contain any spaces, and must use ISO/IEC-8859 (Latin-1) character encoding. **Tip We recommend that you do not point to any document or site that requires human interaction to be useful, interesting, or entertaining, because there is no keyboard or mouse that you can use to interact with what you show on your DMP display.**
Wired Network Configuration	
DMP MAC Address	An uneditable representation of the MAC address that is associated with the NIC in your DMP.
Dynamic IP Addressing (DHCP)	Indicates whether your DMP uses a static IP address or a dynamic IP address. Options in the list are as follows: • **Enabled**— Your DMP uses a dynamic IP address that it obtained from a DHCP server. • **Disabled**— Your DMP uses a static IP address.
IP Address	The IP address that is assigned to your DMP. **Note If your DHCP server changes the IP address assignment for a centrally managed DMP while the DMP is running, instead of waiting for the DMP to restart, you must restart the DMP.** Otherwise, you cannot use DMM-DSM to centrally manage that DMP.

Table 10-1 Elements on the Basic Page (continued)

Element	Description
Domain Name	The DNS-resolvable domain name for your organization, such as **example.com**. When you disable DHCP and assign a static IP address to your DMP, its configuration to resolve local hostnames is no longer completely automatic. You must specify the domain name so that your DNS server can convert local device names, such as **server**, to fully qualified domain names, such as **server.example.com** —which are then resolvable to IP addresses for routing.
Subnet Mask	The IPv4 netmask that the DMP-local network segment uses.
Default Gateway	The IP address that is assigned to whatever router provides outside network access to and from devices on the DMP-local network segment.
Primary DNS Server	The routable IP address or DNS-resolvable hostname of the primary DNS server for whichever network segment is local to your DMP. We recommend that you enter the IP address, not the hostname.
Using NAT	Indicates whether your DMP uses private IP addressing. Choose an option from the list. • **Yes**—Your DMP uses a private IP address. • **No**—Your DMP does not use a private IP address.
NAT IP Address	The globally routable IP address that DMM-DSM should use to manage your DMP, if your DMP has a private IP address due to network address translation (NAT).
HTTP Proxy	
Use HTTP Proxy	Indicates whether your DMP uses a proxy server. Choose an option from the list. • **Enabled**—Your DMP sends and receives HTTP traffic through the specified proxy. • **Disabled**—Your DMP does not use a proxy.
Proxy Server IP Address or Hostname	The routable proxy server IP address or DMS-resolvable hostname. DMPDM ignores any address that you enter unless you chose Enabled from the Use HTTP Proxy list.
Port	The logical TCP port number through which the proxy server provides HTTP proxy services. DMPDM ignores any port that you enter unless you chose Enabled from the Use HTTP Proxy list.
No Proxy List	Either comma-separated IP addresses *or* comma-separated FQDNs (DNS-resolvable hostnames). These identify each content server that should be excluded from proxy. Nonetheless, we continue to proxy content from any other HTTP server. Do not enter any wildcards.

FAQs and Troubleshooting

DMP Network Connectivity

Q. What prevents me from centrally managing my DMP?

A. Ask yourself these questions.

- Has your DHCP server changed the IP address assignment for your DMP?
- Was your DMP running when its address changed?

If these statements are true, do not wait for your DMP to restart automatically. Instead, restart it manually. Until it is restarted, it cannot be centrally managed.