Network Setup

The Network Setup windows let you configure various network-related settings for the IP camera.

The following sections describe the Network Setup windows in detail:

Basic Window

The Basic window provides options for identifying the IP camera and controlling basic operations.

To display the Basic window, perform the following steps:

Procedure

Step 1 From the IP camera user interface, click the **Setup** link.

Step 2 Click **Network Setup** to expand the menu.

Step 3 From the Network Setup menu, click **Basic**.

The Basic window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-1 describes the options in the Basic window.

Table 5-1 Basic Window Options

Option	Description
Basic Settings Area	
ID	Enter a unique identification for the IP camera, which is used to identify the IP camera to various external applications. The ID can contain up to 64 numbers.
Name	Enter a name for the IP camera. This name appears in the IP camera log file for information that is associated with this IP camera. The name can contain up to 64 characters, which can include letters, numbers, spaces, and these characters: ! $ % ( ) + , - . / = @ ^ _ ` { } ~. We recommend that you give each IP camera a unique name so that you can identify it easily.
Description	Enter a description of the IP camera. For example, enter the IP camera location, such as "North Entrance Camera 1." The description can contain up to 128 characters, which can include letters, numbers, spaces, and these characters: ! $ % ( ) + , - . / = @ ^ _ ` { } ~
Location	Enter the physical location of the IP camera, such as "North Entrance." The location can contain up to 64 characters, which can include letters, numbers, spaces, and these characters: ! $ % ( ) + , - . / = @ ^ _ ` { } ~
Contact	Enter system contact information for someone such as the system administrator. For example, enter the e-mail address of the system administrator. The contact can contain up to 64 characters, which can include letters, numbers, spaces, and these characters: ! $ % ( ) + , - . / = @ ^ _ ` { } ~
Basic Operations Area	
Enable LED	Check this check box if you want the Power LED on the back of the IP camera to light. If you do not check this check box, this LED does not light.
Disable Session ID	The following camera API mechanisms are available: • SessionID—Tracks each client session. Session IDs are required by Cisco Video Surveillance Media Server (VSMS). For more information about Cisco VSMS, refer to the documentation at: http://www.cisco.com/en/US/customer/products/ps9152/tsd_products_support_series_home.html • Basic Authentication—Requires a user ID and password to be passed with every API command. SessionID is enabled by default. To disable SessionID, and enable Basic authentication, check this option.

Table 5-1 Basic Window Options (continued)

Option	Description
Enable ONVIF	Check this check box if you want the IP camera to work in Open Network Video Interface Forum (ONVIF) mode. The following features are supported: • Device Discovery Service • Device Service • Media Service Enabling ONVIF disables SessionID as indicated by the informational message that appears after you click the check box. Click **Save** to be redirected to the login page. After login, ONVIF service starts working. You can verify this service by using any ONVIF tool. By default, ONVIF is disabled. **Note** We recommend that you do not enable ONVIF when using Cisco VSM to avoid conflicts with configuration.

IP Addressing Window

The IP Addressing window provides options for configuring the IP address of the IP camera.

To display the IP Addressing window, perform the following steps:

Procedure

Step 1 From the IP camera user interface, click the **Setup** link.

Step 2 Click **Network Setup** to expand the menu.

Step 3 From the Network Setup menu, click **IP Addressing**.

The IP Addressing window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-2 describes the options in the IP Addressing window.

Table 5-2 IP Addressing Window Options

Option	Description
IP Addressing Area	
IP Version	Choose the IP version from the pull-down list. Currently, only IPv4 is supported.

Table 5-2 IP Addressing Window Options (continued)

Option	Description
Configuration Type	Choose the method by which the IP camera obtains its IP address: • **Dynamic**—If your network includes a DHCP server for dynamic allocation of IP addresses, choose this option if you want DHCP to assign an IP address and subnet mask to the IP camera. Depending on your router, the default gateway, primary DNS server, and secondary DNS server may also be assigned. The DHCP server must be configured to allocate static IP addresses based on MAC addresses so that the IP camera always receives the same address. • **Static**—Choose this option if you want to manually enter an IP address, subnet mask, default gateway, and DNS server IP addresses for the camera.
IP Address	If you configured the IP camera for a static IP address, enter that IP address.
Subnet Mask	If you configured the IP camera for a static IP address, enter the subnet mask for the IP camera. Use the same value that is configured for the PCs on your network.
Gateway Address	If you configured the IP camera for a static IP address, enter the gateway for the IP camera. Use the same value that is configured for the PCs on your network.
Primary DNS	*Optional*. Enter the IP address of the primary the DNS server that is used in your network. Use the same value that is used for the PCs on your LAN. Typically, your ISP provides this address. This address is required if you use a host name instead of an IP address in any configuration field in the IP camera configuration windows.
Secondary DNS	*Optional*. Enter the IP address of a secondary (backup) DNS server to use if the primary DNS server is unavailable. Enter the DNS server to be used if the primary DNS server is unavailable. This address is required if you have a secondary DNS server an you use a host name instead of an IP address in any configuration field in the IP camera configuration windows.

Time Window

The Time window provides options for setting and maintaining the time of the IP camera.

To display the Time window, perform the following steps:

Procedure

Step 1 From the IP camera user interface, click the **Setup** link.

Step 2 Click **Network Setup** to expand the menu.

Step 3 From the Network Setup menu, click **Time**.

The Time window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-3 describes the options in the Time window.

Table 5-3 Time Window Options

Option	Description
Set Time Mode Area	
Manually Configure Time	Choose this option if you want to set the time for the IP camera manually.
Use NTP Server to Update Time	Choose this option if you want the IP camera to obtain its time from a network time protocol (NTP) server. If you check this check box, the camera contacts the designated NTP server every 64 seconds and synchronizes its internal clock with the time of that server.
Local Time Area **Note** These options do not apply if you choose the Use NTP Server to Update Time option.	
Set Local Date	Enter a date for the IP camera. The camera is updated with this date when you click **Save**.
Set Local Time	Enter a time for the IP camera. The camera is updated with this time when you click **Save**.
Clone PC Time button	Click this button to update the IP camera date and time with the date and time of the PC that you are using.
Time Zone and Daylight Saving Area	
Time Zone	Choose the time zone in which the IP camera is located. The time that appears when you view video from this IP camera reflects this time zone.
Adjust for Daylight Saving Time	Check this check box if you want the time of the IP camera to adjust automatically for daylight saving time.
Edit Default Daylight Saving Configuration for Time Zone	Check this check box if you want the daylight saving time adjustment of the IP camera to be different than the default adjustment for the selected time zone.
Time Offset	If you choose to overwrite the default time zone configuration, enter the number of minutes that the time of the camera adjusts when daylight saving time starts. The camera automatically adjusts its time back by this number of minutes when daylight saving time ends.
Start Date Start Time	If you choose to overwrite the default time zone configuration, enter the day and time (in 24 hour format) that daylight saving time begins. At this day and time, the time of the IP camera adjusts by the value in the Time Offset field.

Table 5-3 Time Window Options (continued)

Option	Description
End Date End Time	If you choose to overwrite the default time zone configuration, enter the day and time (in 24 hour format) that daylight saving time ends. At this day and time, the time of the IP camera adjusts to the non-daylight saving time.
NTP Server Settings Area **Note** These options do not apply if you choose the Manually Configure Time option.	
Primary NTP Server	If you configured the IP camera to obtain its time from an NTP server, identify the primary NTP server by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field.
Primary NTP Server Port	If you configured the IP camera to obtain its time from an NTP server, enter the primary NTP server port number. Valid values are 123 and 1024 through 65535. The default port is 123.
Secondary NTP Server	If you configured the IP camera to obtain its time from an NTP server, identify the secondary NTP server by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field.
Secondary NTP Server Port	If you configured the IP camera to obtain its time from an NTP server, enter the optional secondary NTP server port number. Valid values are 123 and 1024 through 65535. The default port is 123.

Discovery Window

The Discovery window provides options for configuring the IP camera to work with Cisco Discovery Protocol or Bonjour. These applications facilitate monitoring and management of your network.

To display the Discovery window, perform the following steps:

Procedure

Step 1 From the IP camera user interface, click the **Setup** link.

Step 2 Click **Network Setup** to expand the menu.

Step 3 From the Network Setup menu, click **Discovery**.

The Discovery window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-4 describes the options in the Discovery window.

Table 5-4 Discovery Window Options

Option	Description
Cisco Discovery Protocol (CDP) Area	
Show Neighbors button	Displays a new window with information about CDP-enabled device neighbors in your network.
Bonjour Area	
Enable Bonjour	Check this check box if Bonjour is enabled in your network and you want the IP camera to broadcast Bonjour discovery messages.
Cisco Video Surveillance Media Server (VSMS) Area	
Enable Preferred Media Server List	Check this check box if you want the camera to send discovery messages to the media server list.
Media Server IP address	Enter the IP addresses for up to four VSMS to autodiscover your camera. They are to be listed in order of preference, such that when VSMS 1 does not respond to the camera's discovery request, the camera will send a registration request to VSMS 2; and continue down the list until the camera is registered.

Medianet Window

The Media Services Interface (MSI) is a software component that is embedded in video endpoints and collaboration applications. MSI ties the network to user devices and applications that enables an end-to-end architecture called Cisco Medianet.

The Medianet window on the IP cameras contains the Enable Flow Meditate option. By default this setting is enabled to allow metadata about the camera to be sent across the network and to the network elements in the media path.

For more information about Medianet, refer to the *Cisco Video Surveillance Operations Manager User Guide* at the following URL:

http://www.cisco.com/en/US/products/ps10818/products_user_guide_list.html

To display the Medianet window, perform the following steps:

Step 1 From the IP camera user interface, click the **Setup** link.

Step 2 Click **Network Setup** to expand the menu.

Step 3 From the Network Setup menu, click **Medianet**.

The Medianet window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-5 describes the options in the Medianet window.

Table 5-5 Medianet Window Options

Option	Description
Medianet Features Area	
Enable Flow Metadata	Check this check box if Medianet is supported in your network. Flow metadata is the data that describes flow in network. Enabling this feature helps with sending metadata across the network and network elements in the media path. **Note** This feature is enabled by default.

SNMP Window

The SNMP window provides options for configuring Simple Network Management Protocol (SNMP) settings for the IP camera. These settings can help you manage complex networks by sending messages to different devices on the network.

To display the SNMP window, perform the following steps:

Step 1 From the IP camera user interface, click the **Setup** link.

Step 2 Click **Network** Setup to expand the menu.

Step 3 From the Network Setup menu, click **SNMP**.

The SNMP window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-6 describes the options in the SNMP window.

Table 5-6 SNMP Window Options

Option	Description
SNMP v2c Area	
Enable SNMP v2c	Check this check box to enable SNMP v2c.
Read Community String	Enter the SNMP read community string, which identifies the valid read community.
Trap Community String	Enter the SNMP trap community string.
Primary Trap Receiver	Identify the primary trap receiver of the SNMP v2c manager by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field.
Secondary Trap Receiver	Identify an optional secondary trap receiver of the SNMP v2c manager by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field.
SNMP v3 Area	
Enable SNMP v3	Check this check box to enable SNMP v3.

Table 5-6 SNMP Window Options (continued)

Option	Description
Use Default Local Engine ID	Click this radio button if you want to use the default local engine ID for SNMP. The default local engine ID is 8000000903<*MAC*>, where <*MAC*> is the MAC address of the IP camera.
Manually Configure Local Engine ID	Click this radio button if you want to enter a local engine ID manually, then enter a unique local engine ID. Enter this information in a standard format as defined in RFC3411. Valid formats include (but are not limited to) the following: • 8000000903<*MAC*> where <*MAC*> is the MAC address of the IP camera. For example, if the IP camera MAC address is 00:04:9F:11:22:33, enter 800000090300049F112233. This format is the default. • 8000000901<*IPv4_address_hex*> where <*IPv4_address_hex*> is the IPv4 address of the IP camera in hexadecimal format. For example, if the IP camera IPv4 address is 192.168.0.100, enter 8000000901C0A80064. • 8000000904<*text*> where <*text*> is a string of up to 54 characters.
Primary Trap Receiver	Identify the primary trap receiver of the SNMP v3 manager by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field.
Secondary Trap Receiver	Identify an optional secondary trap receiver of the SNMP v3 manager by choosing **IP Address** or **Hostname** from the drop-down list and entering the IP address or host name in the corresponding field.
User #	*Display only*. Lists the user number of each IP camera user who is configured with the administrator privilege level.
User Name	*Display only*. Displays the name that is associated with the corresponding user number
Authentication Method	Choose the authentication protocol for SNMP v3 messages that are sent on behalf of the corresponding user.
Authentication Password	Enter a password for the authentication protocol for SNMP v3 messages that are sent on behalf of the corresponding user. This password can contain from 8 to 63 characters, which can be letters, numbers, and special characters, but no spaces. Special characters are: ! $ ( ) - . @ ^ _ ` { } ~
Privacy Method	Choose **DES** if you want to use this privacy method for SNMP v3 messages that are sent on behalf of the corresponding user. If you do not want to use a privacy method, choose **None**.

Table 5-6 SNMP Window Options (continued)

Option	Description
Privacy Password	If you choose a privacy method, enter a password for SNMP v3 messages that are sent on behalf of the corresponding user. This password can contain from 8 to 63 characters, which can be letters, numbers, and special characters, but no spaces. Special characters are: ! $ ( ) - . @ ^ _ ` { } ~

802.1x Window

The 802.1x window provides options for configuring 802.1x authentication for the IP camera. These settings require that RADIUS be configured on your network to provide the client authentication.

To display the 802.1x window, perform the following steps:

Step 1 From the IP camera user interface, click the **Setup** link.

Step 2 Click **Network Setup** to expand the menu.

Step 3 From the Network Setup menu, click **802.1x**.

The 802.1x window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-7 describes the options in the 802.1x window.

Table 5-7 802.1x Window Options

Option	Description
802.1x Settings Area	
Enable 802.1x	Check this check box to enable 802.1x authentication for the IP camera.
Protocol Type	Choose the protocol for 802.1x authentication. Options are • EAP-TLS • EAP-TTLS • EAP-PEAP • EAP-FAST The remaining fields in this window change depending on the protocol type that you choose.
EAP-TLS Configuration Options **Note** These options appear if you select the protocol type **EAP-TLS**.	
User Name	Enter the user name that the IP camera uses to access the RADIUS server.

Table 5-7 802.1x Window Options (continued)

Option	Description
Device (Client) Certificate	Path and folder where the device certificate for the IP camera is stored. You can click **Browse** to find this location. After you enter this information, click **Upload** to upload the certificate to the IP camera.
Password (for Private Key)	If the private key in the device certificate is password protected, enter the password that is required to unlock the private key.
Root CA Certificate	Path and folder where the root certificate that is required for 802.1x authentication is stored. You can click **Browse** to find this location. After you enter this information, click **Upload** to upload the certificate to the IP camera.
EAP-TTLS Configuration Options **Note** These options appear if you select the protocol type **EAP-TTLS**.	
Inner Authentication	Choose an inner authentication method for EAP-TTLS. Options are **MS-CHAP**, **MS-CHAP v2**, **PEAP**, and **EAP-MDS**.
User Name	Enter the user name that the IP camera uses to access the RADIUS server.
Password	Enter the password that the IP camera uses to access the RADIUS server.
Anonymous ID	*Optional*. Unsigned public identifier to be used instead of a user name for logging in to the RADIUS server.
Validate Server Certificate	Check this check box if you want the identity of the RADIUS server to be validated.
Root CA Certificate	Path and folder where the root certificate that is required for 802.1x authentication is stored. You can click **Browse** to find this location. After you enter this information, click **Upload** to upload the certificate to the IP camera.
EAP-PEAP Configuration Options **Note** These options appear if you select the protocol type **EAP-PEAP**.	
Inner EAP Protocol	Choose an inner authentication method for EAP-PEAP.
User Name	Enter the user name that the IP camera uses to access the RADIUS server.
Password	Enter the password that the IP camera uses to access the RADIUS server.
Anonymous ID	*Optional*. Anonymous identifier to be used instead of a user name for logging in to the RADIUS server.
Validate Server Certificate	Check this check box if you want the identity of the RADIUS server to be validated.
Root CA Certificate	Path and folder where the root certificate that is required for 802.1x authentication is stored. You can click **Browse** to find this location. After you enter this information, click **Upload** to upload the certificate to the IP camera.
EAP-FAST Configuration Options **Note** These options appear if you select the protocol type **EAP-FAST**.	
Inner EAP Protocol	Choose an inner authentication method for EAP-FAST.

Table 5-7 802.1x Window Options (continued)

Option	Description
User Name	Enter the user name that the IP camera uses to access the RADIUS server.
Password	Enter the password that the IP camera uses to access the RADIUS server.
Anonymous ID	*Optional*. Anonymous identifier to be used instead of a user name for logging in to the RADIUS server.
Allow Automatic PAC Provisioning	Check this check box if you want to allow authentication servers to establish a secure connection with the IP camera so that they can provide the IP camera with new Protected Access Credentials (PACs).
PAC file	Path and folder where the PAC file is stored. You can click **Browse** to find this location. After you enter this information, click **Upload** to upload the certificate to the IP camera.

IP Filter Window

The IP Filter window provides options for controlling access to the IP camera by designating up to 10 IP addresses or address ranges that are allowed or denied access to the IP camera.

To display the IP Filter window, perform the following steps:

Procedure

Step 1 From the IP camera user interface, click the **Setup** link.

Step 2 Click **Network Setup** to expand the menu.

Step 3 From the Network Setup menu, click **IP Filtering**.

The IP Filter window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-8 describes the options in the IP Filter window.

Table 5-8 IP Filter Window Options

Option	Description
IP Filter Area	
Enable IP Filtering	Check this check box to cause the IP camera to allow or deny access to IP addresses as configured in the IP Filtering window.
Filter Entries Area	
#	*Display only*. Filter number.

Table 5-8 IP Filter Window Options (continued)

Option	Description
Action	Choose an action for the corresponding IP address or address range: • **Deny**—IP address or address range cannot access the IP camera. • **Allow**—IP address or address range can access the IP camera.
IP Address/Bit Mask	Enter the IP address and bit mask to which the corresponding action applies. Make these entries in Classless Inter-Domain Routing (CIDR) notation. CIDR is defined in RFC 4632.

QoS Window

The QoS window provides options for configuring quality of service (QoS) settings for video streams.

To display the QoS window, perform the following steps:

Procedure

Step 1 From the IP camera user interface, click the **Setup** link.

Step 2 Click **Network Setup** to expand the menu.

Step 3 From the Network Setup menu, click **QoS**.

The QoS window appears. If you change any options in this window, you must click the **Save** button to save the changes. If you do not click this button, changes are not retained when you exit the window. The **Save** button appears at the bottom of the window. You might need to scroll down to it.

Table 5-9 describes the options in the QoS window.

Table 5-9 QoS Window Options

Option	Description
Class of Service (CoS) Area	
Enable CoS for Video Streaming	Check this check box to enable class of service (CoS) control for video streams. If you enable this option, the IP camera specifies a VLAN tag that appends to an Ethernet MAC frame for video streaming data.
Video Priority	Value from 0 (lowest priority) through 7 (highest priority) that specifies the CoS priority value for steaming video data.
Video VLAN ID	Enter the ID of the video VLAN to which CoS packets are directed.
Enable CoS for Audio Streaming	Check this check box to enable class of service (CoS) control for audio streams.
Audio Priority	Value from 0 (lowest priority) through 7 (highest priority) that specifies the CoS priority value for steaming audio data.
Audio VLAN ID	Enter the ID of the audio VLAN to which CoS packets are directed.

Table 5-9 QoS Window Options (continued)

Option	Description
Differentiated Services (DiffServ) Area	
Enable DiffServ for Video Streaming	Check this check box to enable Differentiated Services (DiffServ) for video streams. If you enable this option, the IP camera specifies the DSCP priority value that appends to an IP header for video streaming packets.
Video DSCP Priority Value	Value from 0 (lowest priority) through 63 (highest priority) that specifies the DSCP priority value for steaming video data.
Enable DiffServ for Audio Streaming	Check this check box to enable Differentiated Services (DiffServ) for audio streams.
Audio DSCP Priority Value	Value from 0 (lowest priority) through 63 (highest priority) that specifies the DSCP priority value for steaming audio data.