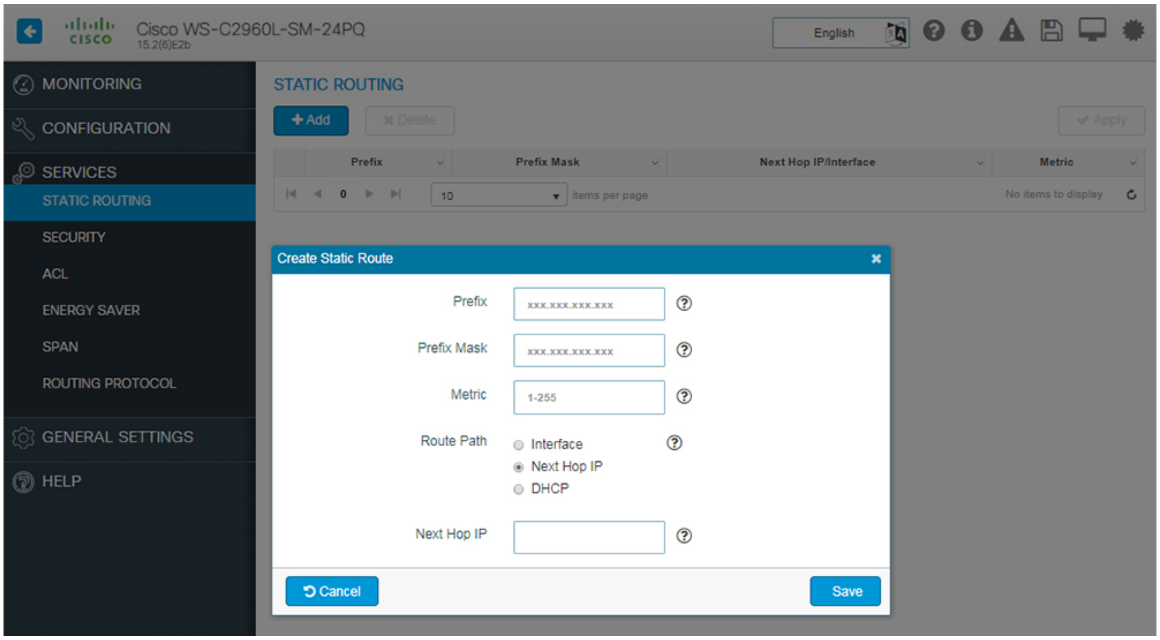
Configuring Services

Configuring Static Routing

Use static routes in environments where network traffic is predictable and where the network design is simple. Routers forward packets using either route information from route table entries that you manually configure or the route information that is calculated using dynamic routing algorithms. Static routing is the simplest form of routing, where you manually enter routes into a routing table.

Static routes define explicit paths between two routers, and cannot be automatically updated. You must manually reconfigure static routes when network changes occur.

Figure 1: Configuring Static Routing



Create Static Route

Prefix: xxx.xxx.xxx.xxx

Prefix Mask: xxx.xxx.xxx.xxx

Metric: 1-255

Route Path: ○ Interface ● Next Hop IP ○ DHCP

Next Hop IP:

Step 1 Choose **Services > Static Routing**, and click **Add**.

Step 2 In the **Prefix** and **Prefix Mask** fields, type the IP address and the subnet mask for the static route.

Step 3 In the **Metric** field, assign a metric, between 1 and 255, to the static route.

When multiple paths to the same destination are available, the device uses the route with the lowest metric and adds the preferred route into the routing table.

Step 4 In the **Route Path** field, choose one of the following options:

- *Interface* — To indicate the output interface, that is the interface on which all packets are sent to the destination network, Choose an interface from the **Interface** drop-down list. In the **Next Hop IP** field, assign a next-hop IP address to the output interface.
- *Next Hop IP* — To specify a next-hop IP address for the static route. Assign a next-hop IP address in the **Next Hop IP** field.
- *DHCP* — To assign a static route IP address using a DHCP server.

The route is removed when the DHCP lease expires. Using DHCP to determine a route path eliminates the need to configure static routes to an outside interface and the configuration of a next-hop router.

Step 5 Click **Save** to save the static route.

About Security Configuration

AAA (Authentication, Authorization, and Accounting) is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

- **Authentication**—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption. Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods, and then applying that list to various interfaces.

- **Authorization**—Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

  AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database can be located locally on the access server or router or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user. All authorization methods must be defined through AAA.

  As with authentication, you configure AAA authorization by defining a named list of authorization methods, and then applying that list to various interfaces.

- **Accounting**—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

  Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces.

In many circumstances, AAA uses protocols such as RADIUS, TACACS+, or Kerberos to administer its security functions. If your device acts as a network access server, AAA is the means through which you establish communication between your network access server and your security server.

Configuring Security

To use the AAA feature, you can enable it on the **Services** > **Security** > **AAA Server** page. After enabling, you need to set up the authentication servers that contain the AAA database.

Configure RADIUS Servers

Step 1 On the **Services > Security > AAA Server** page, click **Add**.

Step 2 Select the authentication protocol from the **Protocol** drop-down list.

Step 3 Enter a name for the server and, and enter the IP address in the **Server Address** field.

Step 4 In the **Shared Secret** field, enter the shared secret key to be used for authentication between the server and your device. Confirm the shared secret.

Step 5 In the **Auth Port** and **Acct Port** fields, enter the RADIUS server's UDP port numbers. The valid range is 1 to 65535, and the default value is 1812 for authentication and 1813 for accounting.

Step 6 Click **Save & Apply to Device**.

Configure TACACS+ Server

Step 1 On the **Services > Security > AAA Server** page, click **Add**.

Step 2 Enter a name for the server and, and enter the IP address in the **Server Address** field.

Step 3 In the **Shared Secret** field, enter the shared secret key to be used for authentication between the server and your device. Confirm the shared secret.

Step 4 In the **Port** field, enter the TACACS server's UDP port number. The valid range is 1 to 65535, and the default value is 49.

Step 5 Click **Save & Apply to Device**.

Configure LDAP Server

Step 1 On the **Services > Security > AAA Server** page, click **Add**.

Step 2 Enter a name for the server and, and enter the IP address in the **Server Address** field.

Step 3 In the **Port** field, enter the LDAP server's UDP port number. The valid range is 1 to 65535, and the default value is 389.

Step 4 In the **User Base DN** field, enter the distinguished name (DN) of the subtree in the LDAP server that contains a list of all the users. For example, ou=organizational unit, .ou=next organizational unit, and o=corporation.com. If the tree containing users is the base DN, type. o=corporation.com, or dc=corporation, dc=com.

Step 5 Click **Save & Apply to Device**.

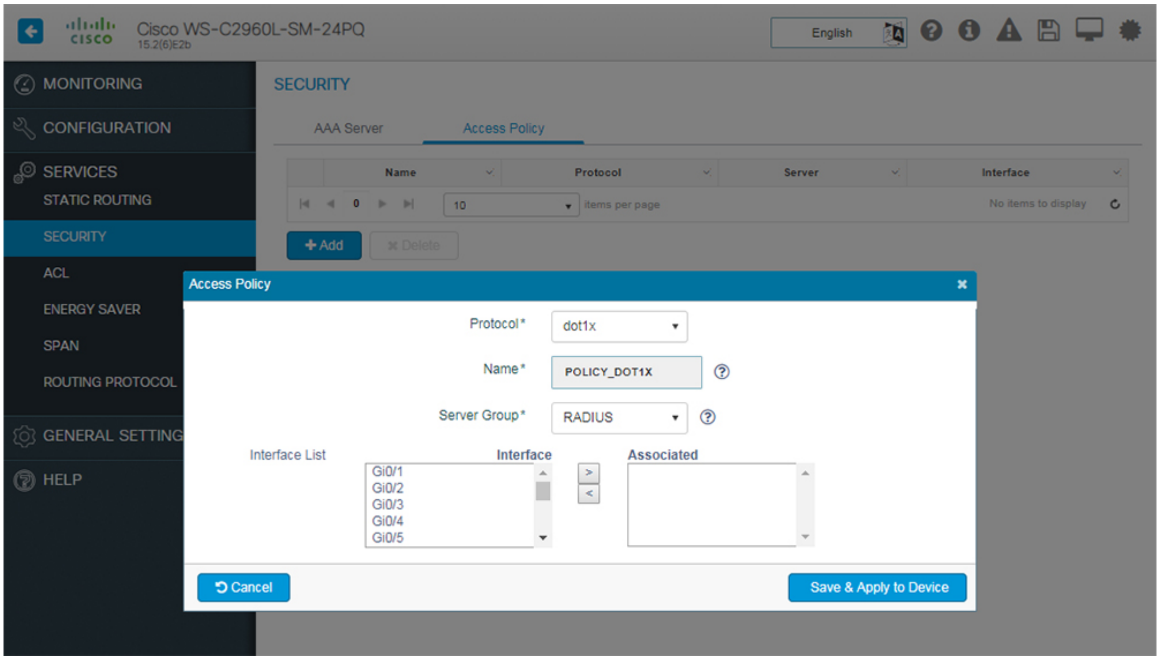
What to do next

The configured list of AAA servers along with their name, address and protocol are displayed in the table listed on the page. If you need to check the status of a server, click **Ping**.

Configure Access Policy

You can configure any combination of the following authentication and authorization methods to control administrative login access to a switch.

Figure 2: Configure Access Policy



Protocol* dot1x

Name* POLICY_DOT1X

Server Group* RADIUS

Step 1 On the **Services** > **Security** > **Access Policy** page, click **Add**.

Step 2 From the **Protocol** drop-down list, select the AAA authentication and authorization method as per the following choices:

- *dot1x* — 802.1X Port-Based authentication helps prevent unauthorized client devices from gaining access to the network. It can be chosen only when a RADIUS authentication server has been configured and the network access switch can route packets to it.
- *mab* — MAC Authentication Bypass (MAB) uses the MAC address of the connecting device to grant or deny network access. The RADIUS server maintains a database of MAC addresses that require access. When this feature detects a new MAC address on a port, it generates a RADIUS request with both username and password as the device's MAC address. After authorization succeeds, the port is accessible to the particular device through the same code path.
- *web* — The web-based authentication feature, known as Web Authentication Proxy, enables you to authenticate end users on host systems that do not run the IEEE 802.1X supplicant.

Note When configuring web-based authentication, note that fallback is configured on switch ports in access mode. Ports in trunk mode are not supported. Also, it is not supported on EtherChannels or EtherChannel members.

Step 3 From the **Server Group** drop-down list, select a server group host to associate it with this method.

Step 4 Select the interface from the **Interface List** and move it to the **Associated** column to associate it with the selected AAA authentication and authorization method.

Step 5 Click **Save & Apply to Device**.

Configuring ACL

Access Control List (ACL) performs packet filtering to control the movement of packets through a network. Packet filtering provides security by limiting the access of traffic into a network, restricting user and device access to a network, and preventing traffic from leaving a network. IP access lists reduce the chance of spoofing and denial-of-service attacks, and allow dynamic, temporary user-access through a firewall.

Creating ACLs

Step 1 On the **Services > ACL** page, click **Add**.

Step 2 Enter a name for the ACL.

Step 3 From the **ACL Type** drop-down list, choose the IP version to which the source or destination addresses belong.

Step 4 From the **Action** drop-down list, choose if you want to deny or permit traffic using this ACL.

Step 5 From the **Source Type** drop-down list, if you choose *Host*, enter the hostname to indicate the source address. If you choose *IP*, enter the source IP addressand subnet mask address. For IPv4 addresses, enter the subnet mask and for IPv6 addresses, enter the prefix length.

Step 6 (Only for IPv4 Extended and IPv6 source types) From the **Destination Type** drop-down list if you choose *Host*, enter the hostname to indicate the destination address. If you choose **IP**, enter the destination IP address. For IPv4 Extended addresses, enter the subnet mask and for IPv6 addresses, enter the prefix length.

Step 7 (Only for IPv4 Extended and IPv6 source types) From the **Protocol** drop-down list, choose the protocol you want to use for this ACL. The device can permit or deny only the IP packets in an ACL. Other types of packets (such as Address Resolution Protocol (ARP) packets) cannot be specified. This field is not available if your IP version is IPv4 Standard.

Step 8 Only for IPv4 Extended and IPv6 source types) If you chose TCP or UDP, two additional parameters, a source port and a destination port, are displayed. These parameters enable you to choose a specific source port and destination port or a port range. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for specific applications such as Telnet, SSH, and HTTP.

Step 9 (Only for IPv4 Extended and IPv6 source types) To use the ACL to mark associated packets with a DSCP value, choose a value, from the **DSCP** drop-down list.

Step 10 Select the interfaces to be associated with this ACL and move them to the **Associated** column.

Step 11 Click **Save & Apply to Device** to apply your changes on the device.

Creating an ACE for an ACL

An Access Control Entry (ACE) consists of a series of ACL entries, which are permit or deny entries with criteria for the source IP address, destination IP address, protocol, port, or protocol-specific parameters. Each entry permits or denies inbound or outbound network traffic to the parts of your network specified in the entry.

You can use ACLs with the ACE to permit or deny traffic to or from a specific IP address or an entire network. For example, you can permit all e-mail traffic on a circuit, but block Telnet traffic. You can also use ACLs to allow one client to access a part of the network while preventing other clients from doing so.

Step 1 On the **Security > ACL > Access Control List** page, click the value in the ACE Count field. The Access Control List page for the selected ACL is displayed.

Step 2 Click **Add**. The Add ACE Setup window is displayed.

Step 3 In the **Sequence** field, type a sequence number for the ACE. An ACE sequence number is unique to an ACE and indicates the priority of an ACE within an ACL.

Step 4 From the **Action** drop-down list, choose if you want to deny or permit traffic using this ACE.

Step 5 From the **Source Type** drop-down list, if you choose Host, enter the hostname to indicate the source address.

Step 6 If you choose IP as the source type, enter the source IP address and the subnet mask.

Step 7 From the **Destination Type** drop-down list, choose the destination IP or host to indicate the destination address.

Step 8 Select the **Protocol** to be matched in the IP packet header. Any value matches any protocol in the IP header of the packet.

Step 9 Select the **DSCP** type to specify the specific DSCP values to match in the IP packet header.

Step 10 Click **Save & Apply to Device.**.

Configuring Energy Saver

Cisco EnergyWise is used to manage the energy usage of powered devices in a EnergyWise network. By default, EnergyWise is disabled on the domain member. However, when you add a switch to a Energywise domain, EnergyWise is enabled on the switch and its PoE ports.

Enabling EnergyWise

To enable EnergyWise with default configuration value, click the **Energywise Status** toggle button on the **Services > Energy Saver > Ports** page. You can also override the default configuration values by clicking **Configure a Energywise Domain** link and provide custom values.

Step 1 On the EnergyWise Domain window enter the domain name to which this member switch belongs. Note that for the domain-name and domain-password:

- You can enter alphanumeric characters and symbols such as #, (, $, !, and &.
- Do not enter an asterisk (*) or a space between the characters or symbols.

Step 2 Set the domain security mode.

- *ntp-shared-secret*—Sets a strong password with NTP. If the time between members varies ±30 seconds, the domain member drops events.
- *shared-secret*—Sets a strong password without NTP.

Step 3 Set the domain password to authenticate all communication in the domain and optionally select encryption if you want the password to be encrypted.

- (Optional) 0—Uses a plain-text password. This is the default.
- (Optional) 7—Uses a hidden password.
- If you do not enter 0 or 7, the default is 0.

Step 4 Enter the UDP port number to communicate with the EnergyWise domain.. The range is from 1 to 65000 and the default is 43440.

Step 5 From the **Interface/IP** drop-down list, if you select Interface, choose the interface from the list of available interfaces. Otherwise select IP from the drop-down list and enter the IP address that will be used to communicate with the domain server.

Step 6 Click **Save & Apply to Device** to apply your changes on the device.

Enabling Energy Efficient Ethernet (EEE)

Energy Efficient Ethernet (EEE) is an IEEE 802.3az standard that is designed to reduce power consumption in Ethernet networks during idle periods. EEE can be enabled on devices that support low power idle (LPI) mode. EEE is enabled by default. If you need to disable EEE on all interfaces, click the **EEE Status** toggle button on the **Services > Energy Saver > Ports** page and click **Apply**. This disables EEE on all interfaces. Alternately, if you want to disable EEE on a particular interface, click on the green EEE icon. The green icon turns red is EEE is disabled on an interface.

Enabling Wake-on-LAN (WOL)

Wake-on-LAN (WoL) is an Ethernet computer networking standard, where you can use a network message to wake up a computer. You can send a WoL magic packet to a specific device in the EnergyWise network by clicking the green play icon on the **Services > Energy Saver > Ports** page. However, to do this, the EnergyWise status should be enabled. A red play icon indicates that there are no clients connected to this interface and therefore WoL is not applicable.

Configuring Power Level

EnergyWise uses a set of power levels to consistently manage power usage. A power level is a measure of the energy consumed by devices in an EnergyWise network.

To configure the power level on the Services > Energy Saver > Clients page, ensure that the EnergyWise Status is enabled.

Step 1 Click the Power level drop-down list and make a selection. The available values are:

Option	Description
Level	Description
10	Full
2	Sleep
1	Hibernate
0	Shutoff

Step 2 Click **Apply**. If you want the same power settings for all the devices in the EnergyWiise network, check the **Apply to all** checkbox and click **Apply**.

Configuring SPAN

You can analyze network traffic passing through ports or VLANs by using Switched Port Analyzer (SPAN) to send a copy of the traffic to another port on the switch. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs.

You can use the SPAN destination port to inject traffic from a network security device. For example, if you connect a Cisco Intrusion Detection System (IDS) sensor appliance to a destination port, the IDS device can send TCP reset packets to close down the TCP session of a suspected attacker.

Local SPAN: It supports a SPAN session entirely within one switch; all source ports or source VLANs and destination ports are in the same switch. Local SPAN copies traffic from one or more source ports in any VLAN or from one or more VLANs to a destination port for analysis.

Remote SPAN: Remote SPAN (RSPAN) is not supported on Cisco Catalyst 2960-L and Cisco Catalyst 2960-L Smart Managed Series Switches.

Creating a Local SPAN Session

Step 1 On the **Services > SPAN** page, click **Add**. A new **Create SPAN** window appears.

Step 2 From the **Source** drop-down list, choose *Local*.

Step 3 From the **Source Direction** drop-down list, choose one of the following:

- None
- Ingress
- Egress
- Both

Step 4 From the **Available** column, choose the ports you want into the **Selected** column.

Step 5 From the **Destination** drop-down list, choose *Local*.

Step 6 From the **Available** column, choose the ports you want into the **Selected** column.

Step 7 To enable traffic-filtering, choose the **Enable Filtering** check box and choose one of the following options:

- From the **Filter Type** drop-down list, choose *IPV4* and make a selection from the **Available ACLs** drop-down list.
- From the **Filter Type** drop-down list, choose *IPV6* and make a selection from the **Available ACLs** drop-down list.
- From the **Filter Type** drop-down list, choose **VLAN** and enter a value in the **VLAN ID** field.

Step 8 Choose the interfaces to be associated with this ACL and move them to the **Associated** column.

Step 9 Click **Save & Apply to Device** to apply your changes on the device.

Editing a Session

Step 1 On the **Services > SPAN** page, choose a session in the table and make changes to the **Create SPAN** window.

Step 2 Click **Update & Apply to Device** to apply your changes on the device.

Configuring Routing Protocol

Routing Information Protocol (RIP) is a commonly used routing protocol in small-to-medium TCP/IP networks. It uses broadcast UDP data packets to exchange routing information. It uses hop count as the metric to rate the value of different routes. The hop count is the number of devices that can be traversed in a route. It sends routing-update messages at regular intervals and when the network topology changes. It uses several timers that determine variables such as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters that you can update to suit your inter-network needs.

The Cisco implementation of RIP Version 2 (RIPv2) supports plain text and message digest algorithm 5 (MD5) authentication, route summarization, classless inter-domain routing (CIDR), and variable-length subnet masks (VLSMs).

Configuring RIP

Step 1 On the **Services > Routing Protocol > RIP** page, click **Add**. A new **Create RIP** window appears.

Step 2 From the **Rip Version** radio buttons, choose either *Version1* or *Version2*.

Step 3 In the **Network Address** field, enter a value.

Step 4 In the **Neighbour** field, enter the network address of the neighbouring device.

Step 5 For setting advanced parameters, click the **Advanced** radio button.

a) Check the **No Autosummary** check box to disable automatic network number summarization.
b) Check the **Disable Split Horizon** check box to disable split horizon on the chosen interface.
c) Check the **Passive Interface** check box to suppress routing updates on the chosen interface.
d) Check the **Timers** check box to set timers for *Flush*, *Update*, *Invalid*, and *Holddown*.
e) For the **Distance** field, enter a value to set the administrative distance.
f) For the **Maximum Paths** drop-down list, choose the number of paths for forwarding packets.
g) Check the **Auth Key** check box to enter key-chain name for authentication control.

Step 6 Click **Save & Apply to Device** to apply your changes on the device.

Editing a Routing Protocol Setup

On the **Services > Routing Protocol > RIP** page, choose a setup in the table and make changes to the **Create RIP** window.