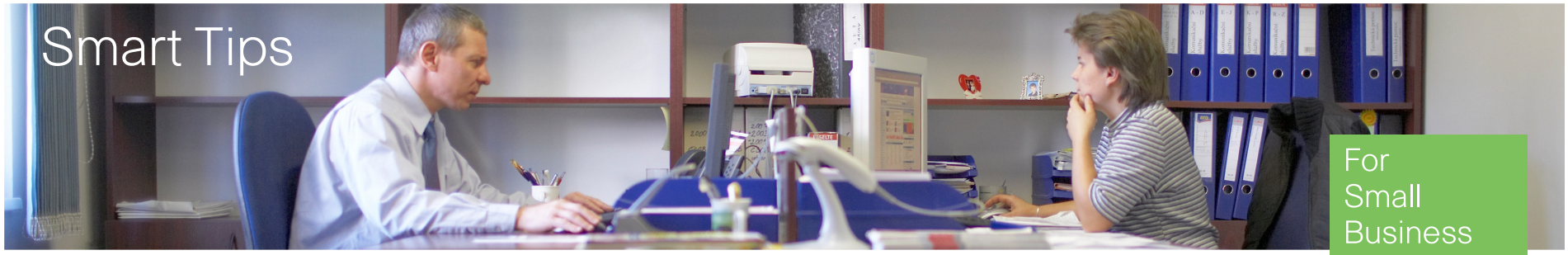


Configuring LAN Quality of Service for Cisco IP Telephony (ESW500)

As the number of devices and LAN traffic increases, traffic segregation, access control, and prioritizing traffic become key requirements. Cisco Small Business Managed Switches have advanced network management and other features that support business growth by providing greater control over network traffic.

Featured Products

Cisco Small Business Pro series of Managed Ethernet Switches with Power over Ethernet (PoE):

- ESW-520-8P-K9
- ESW-520-24P-K9
- ESW-520-48P-K9
- ESW-540-24P-K9

ESW-520-8P-K9 is used as example for this Smart Tip. For details about the other Pro series of PoE switches visit: http://www.cisco.com/go/esw500

Quality of Service

Call quality may be degraded if voice traffic is treated like ordinary data. Unless voice traffic receives priority treatment, voice packets may be dropped and calls may become choppy and jittery if overall traffic exceeds the network capacity. Quality of Service (QoS) provides priority treatment for real-time applications, such as voice traffic.

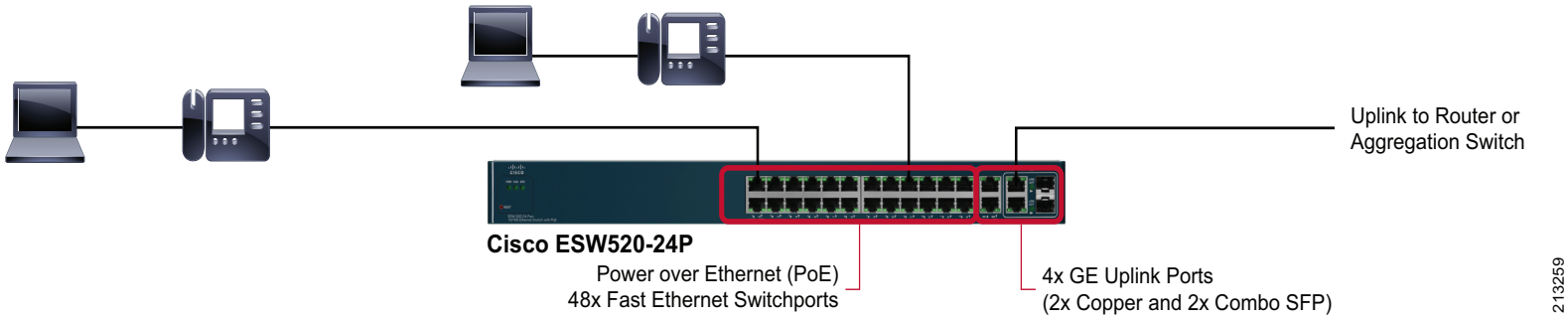
Design Tips

To ensure that voice traffic receives the necessary quality of service, the features described in this section must be enabled and configured on each Ethernet port to which a Cisco IP Phone is connected.

Virtual Local Area Network (VLAN)—A VLAN is a virtual network that segments different types of traffic and users, and that is identified by a port VLAN ID (PVID), such as 1, 10, 12, and so forth. When adding voice to a network, a separate VLAN should be added to the network for the voice traffic. Features that help ensure higher network quality, which is required by a voice VLAN, include the following:

- **Port Fast**—Allows a device, such as an IP Phone, to quickly connect and disconnect from the network.
- **Bridge Protocol Data Unit (BPDU) Guard**—Helps secure the network by preventing attackers from changing from one VLAN to another without authorization.

Figure 1 Voice-Ready LAN



- **Storm Control**—Helps prevent storms, which are unusual bursts of traffic on the network that can damage network performance and disrupt business processes.
- **Port Security**—Helps protect the network from threats, including viruses and worms, by preventing users from adding unauthorized devices to the network.

Quality of Service (QoS)—Helps ensure that sensitive applications, such as voice, get through the network with limited interruptions to maintain the quality of a voice call. The following lists features that should be enabled or customzied when setting up QoS on the network:

- **Class of Service (CoS)**—Used within an Ethernet network to set the priority of the traffic traversing the network and to help ensure the quality of voice calls.
- **Differentiated Service Code Point (DSCP) classification**—Helps ensure voice quality across the entire network by classifying packets and providing guaranteed service for specific packets, such as voice packets.
- **Access Control List (ACL)**—Used to create security policies for a business, such as limiting access to specific servers and preventing unauthorized access from the public Internet.
- **Priority processing (Queuing & Scheduling)**—Helps ensure that sensitive traffic, such as voice calls, get through the network first by managing traffic precedence.

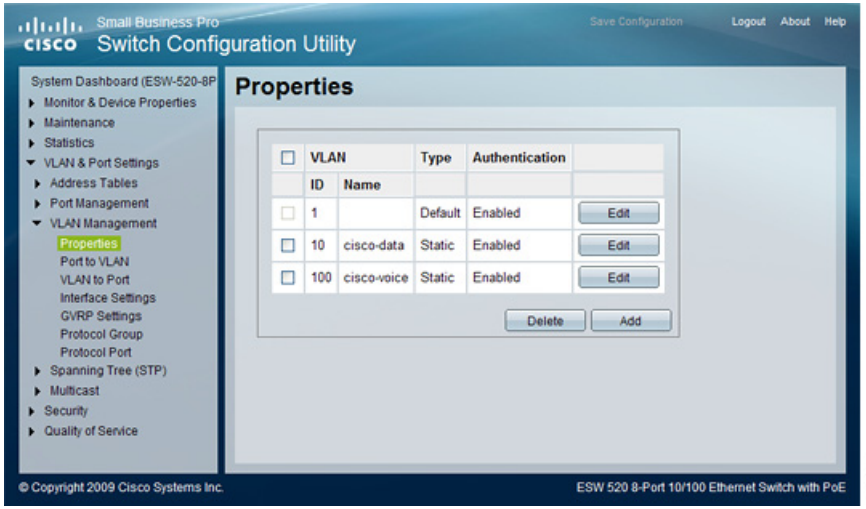
Configuration Tips

The following steps assume you can access the web-based administration for the Cisco Small Business Pro series of Managed Switches. It is also assumed that the Data and Voice VLANs have been created on the router that connects to the Expansion/Uplink port of the managed switch, as shown in Figure 1.

To configure LAN QoS, complete the following steps:

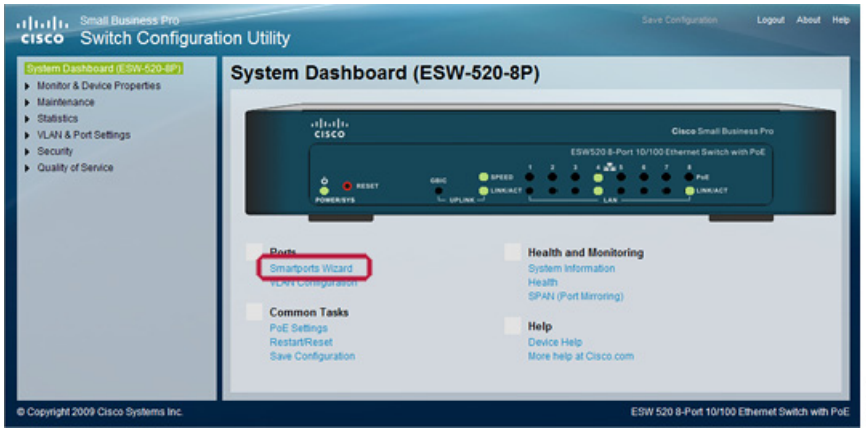
Step 1 Select **VLAN & Port Setting > VLAN Management > Properties** and verify that separate VLANs exist for data and voice traffic.

Figure 2 Switch Configuration Utility



Step 2 Click **System Dashboard**.

Figure 3 System Dashboard



Step 3 Click **Smartports Wizard** in the Ports section.

This launches the Smart Port Settings window.

Figure 4 Smart Ports Setting

Step 4 Select the ports to be configured, and then select the role of device from the drop-down menu.

Step 5 Click **Next**.

You can choose to modify the configuration, such as allowing a specific VLAN in a trunk, or just verify the recommended configuration, as shown for IP phones in Figure 5.

Figure 5 IP Phone Desktop

Step 6 Click **Apply** to configure the port based on the settings listed in the window.