DEPLOYMENT GUIDE

DISTRIBUTE, MANAGE & CONTROL VIDEO AND AUDIO SIGNALS OVER AN IP NETWORK

KramerAV.com

CONTENTS

NETWORK CONFIGURATION

A network configuration defines how the various network components are arranged. For our purposes, this refers to the various devices that KDS is connected to and how those devices are connected to each other.

Although there are many types of network configurations, KDS is almost always connected to one of the following two types: star or tree. Each of these topologies has its own distinct advantages and disadvantages, which we'll briefly discuss here.

STAR

A star network is a network configuration in which all devices are connected to a common central switch. This configuration, using a fully non-blocking switch, enables all connected devices to communicate with each other in any combination.

Advantages: Relatively simple installation, ability to remove devices without disrupting the system, fast detection of network faults, can accommodate large installations by using large modular switch frames.

Disadvantages: All devices are disconnected if the central switch fails.

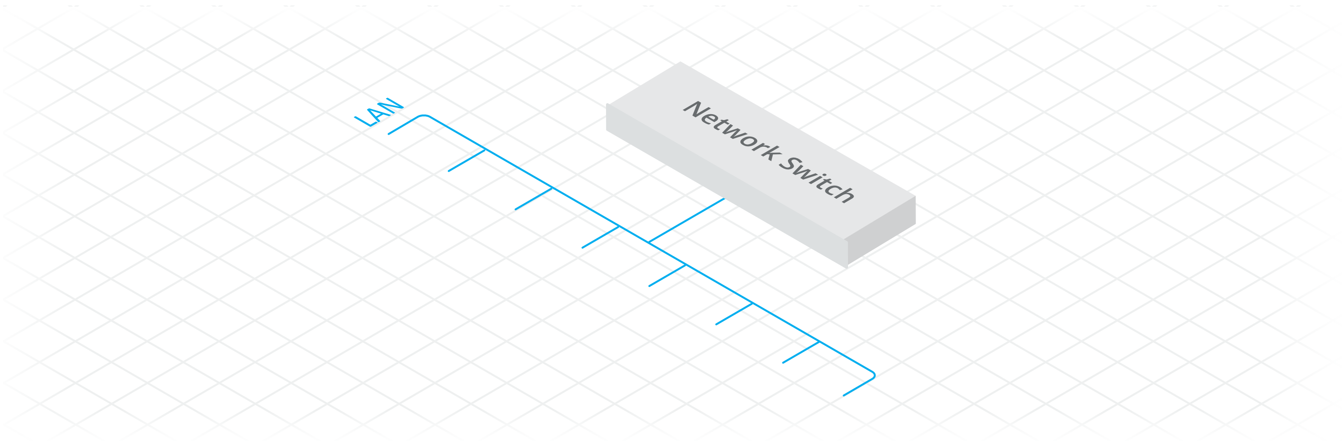


Figure 1: Star Network Using a Non-blocking Switch

TREE

A tree network is a configuration of two or more star networks that are part of a core-switching infrastructure.

The tree network enables a failure to occur in one part of the connected star networks without widely affecting the other star networks in turn. The network designer accomplishes this by configuring the core network with more than one switch for the purposes of redundancy and scalability.

Advantages: Larger capacity and scale.

Disadvantage: Bandwidth management for the lower branches.

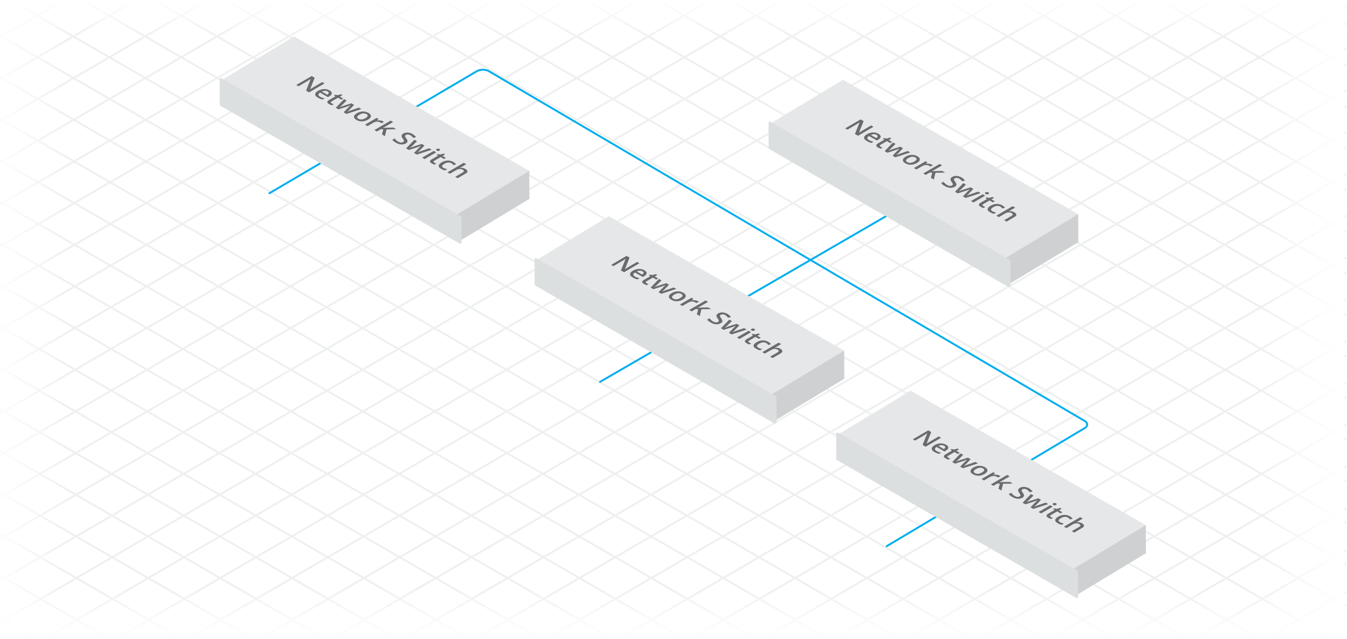


Figure 2: Tree Topology Using Switches on a Core Network

DAISY CHAIN

While not a type of network configuration per se, daisy chaining is a deployment methodology, supported by KDS devices, that is appropriate only for specific deployment applications such as video walls where all displays receive the same video source as the first KDS device in the chain.
Daisy chaining is used for video wall applications and any application where displays are viewed in close proximity to each other and which share the same source.

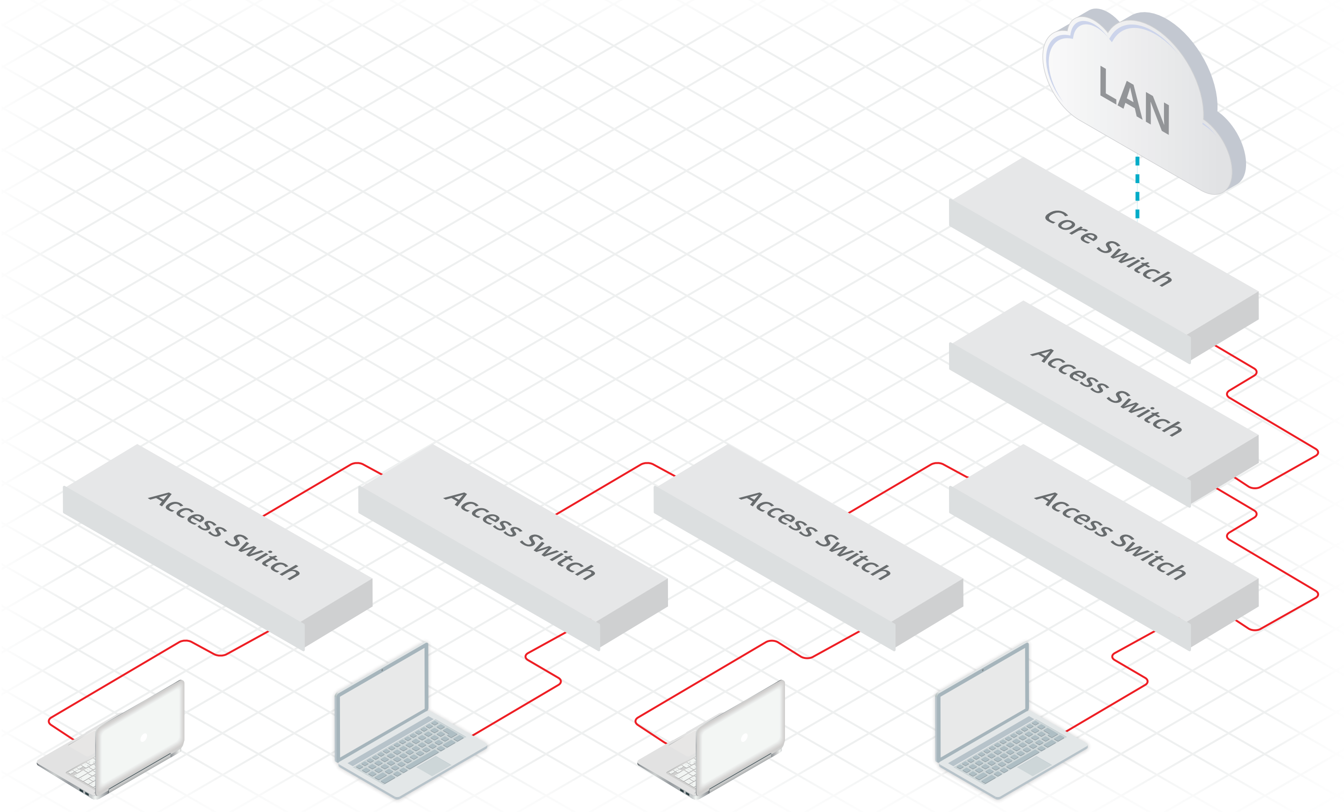


Figure 3: Simple Cascading Switch Networking

POE

PoE (Power over Ethernet) is a feature that enables an Ethernet switch to convey both data and electrical power to a network device through a single cable. PoE reduces the number of wires that are used in the network installation. The advantages of PoE over standard network wiring are lower cost, less downtime, easier maintenance, and greater installation flexibility.

A PoE system consists of the following two components:

- Power Source Equipment (PSE) – a device such as a PoE Ethernet switch that provides and manages the power supply to a Powered Device.
- Powered Device (PD) – a device that receives power provided from a PSE. For example, wireless access points or a TX/RX. Electric modules that receive power from a PSE are called PD modules.

POE STANDARD

The PoE Standard exists in the following two versions:

- IEEE 802.3af – supplies up to 15.4 W of DC power at the PSE. Only 12.95 W is assured to be available at the PD.
- IEEE 802.3at – (also known as PoE+ or PoE plus) provides up to 32 W of DC power at the PSE. Only 25.5W is assured to be available at the PD.

TRUNK PORT DEFINITION

Trunk ports on a switch are used to connect to other switches. Note that multiple physical ports can be bonded to create a higher bandwidth trunk link. Trunk links are always full duplex

TRUNK UPLINK

The trunk uplink bandwidth utilization is the sum of all traffic flowing from the origin switch to the switch connected to the link.
When computing trunk uplink bandwidth utilization, take into account that any multicast sources (encoders) connected to the origin switch must send all their data to the master IGMP querier/multicast router. If another switch is the master IGMP (Internet Group Management Protocol) querier/multicast router, then the multicast traffic must flow to that switch.

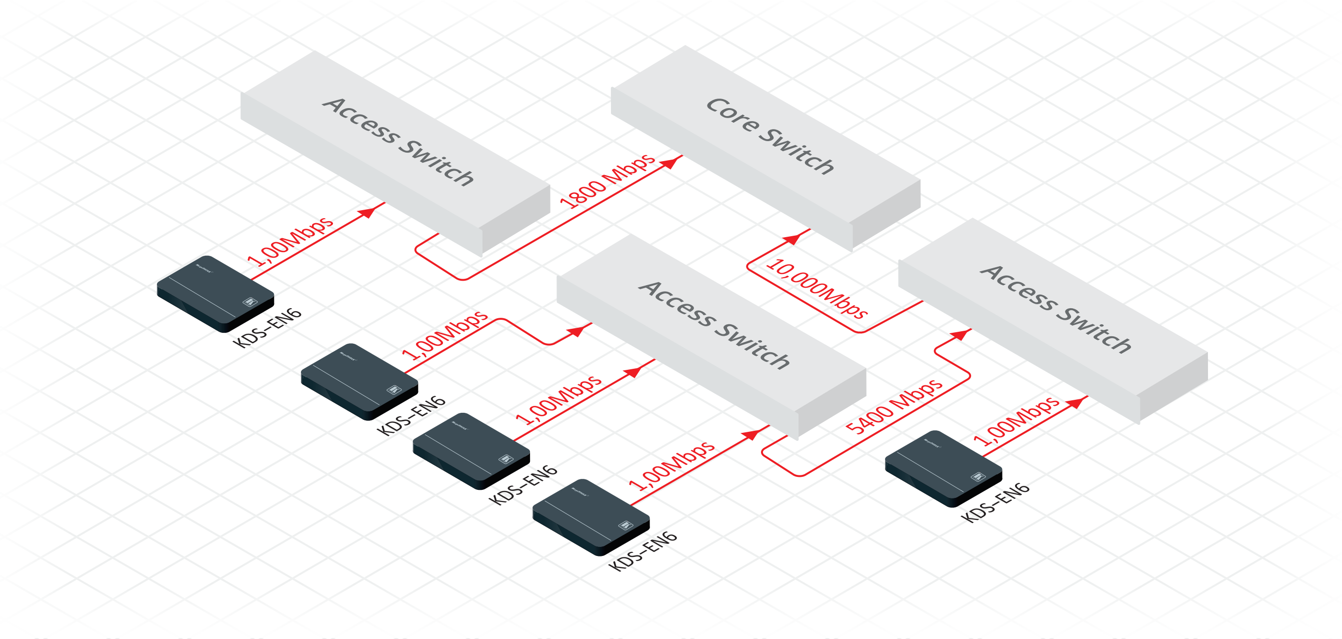


Figure 4: Mulitcast Mode – Uplink Calculation

TRUNK DOWNLINK

The trunk downlink bandwidth utilization is the sum of all traffic flowing to the origin switch from the other switch connected to the link.

When computing trunk downlink bandwidth utilization, it is best practice to assume worst-case by accounting for the maximum amount of multicast traffic possible, coming from another switch.

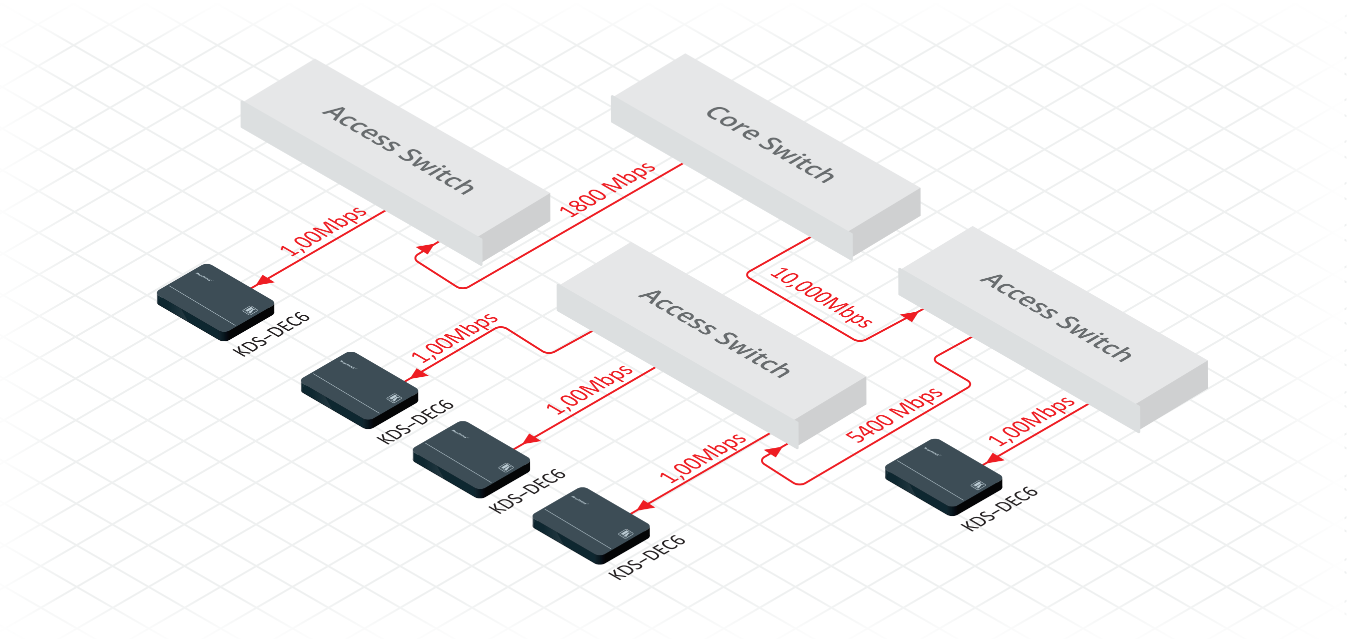


Figure 5: Mulitcast Mode – Downlink Calculation

NETWORK MULTICAST FUNCTIONALITY

KDS networks rely on multicast functionality to send and receive video, IGMP multicast in the Ethernet. The goal is to ensure that the flow of traffic is capable of any permutation of one encoder to many decoders, and vice-versa without adversely affecting or being affected by other network devices.

Generally, the first step in enabling multicast is using a VLAN to segregate KDS traffic. A VLAN maintains KDS traffic on the KDS network, preventing traffic from flowing to and from other network segments, which interferes with operation of both the KDS network and the other network segments. However, within that segment all ports can still be flooded by IGMP traffic whether or not that traffic was intended to be sent or received by a network device at any given point in time. This results in network operation interference and can even be maliciously implemented as a denial-of-service attack on a network.

To ensure that only traffic between intended multicast senders and multicast receivers appears at a given port, a switch feature called IGMP snooping must be enabled. Snooping only allows multicast traffic between ports of intended senders and receivers. To communicate to the switch where route limiting will be specifically implemented in the network for multicast traffic, you must enable a network switch that assesses and maps the network for multicast nodes in the KDS network. This switch is called an IGMP querier. Usually, a single switch is selected by address to act as the IGMP querier, but the switch with the lowest numerical IP address on the network will typically be the default when multiple switches are configured as queriers. The default leave time for the querier (typically around 125s) is usually sufficient for a KDS network, unless there are other specific requirements that a network designer must account for.

NETWORK DESIGN CONSIDERATIONS

Along with an understanding of the main network implications of the KDS design, review and apply the following network design best practices:

- Use non-blocking Layer 3 managed switches with sufficient bandwidth at each segment, from edge to core, to accommodate a non-blocking architecture for KDS
- Select an appropriate network configuration. Consider all network requirements, including basic functionality and redundancy, and whether video walls or repetitive display signage are required. Make sure to involve current network IT staff and experienced network architects in these decisions.
- Enable an IGMP querier on at least one switch in the KDS network. The IGMP querier ensures that all switches know which multicast transmitters and receivers are connected to which switches in the network. Enabling an IGMP querier on multiple switches causes the switch with the lowest value of IP source address to take precedence and act as the querier.
- Ensure VLANs are correctly implemented.
- Enable IGMP multicast snooping on all switches in the KDS network. This is required for all designs to enable multicast delivery to multiple endpoints. Switches without IGMP snooping enabled that receive a multicast stream will transmit that stream to all ports simultaneously, immediately saturating all network links.
- Use daisy chaining to connect video wall endpoints or repetitive display signage. In the case of video walls or endpoints that receive the same source from a single transmitter to feed multiple identical displays or in a video wall using a single source, it is simpler and less expensive to daisy chain the network from device to device.
- Point-to-point mode – each encoder is directly connected to a receiver and the only requirements are that each end-point has a unique ip address and is broadcasting to and “listening” to the same multicast or unicast address

- Point-to-multipoint (daisy chain) – the first decoder in the chain is connected directly to the encoder and every other decoder is connected to another decoder in the chain. Each device needs a unique IP address and each decoder must “listen” to the multicast address of the encoder.
- Point-to-multipoint using a Switch (“star” topology) – offers some redundancy, in that if any decoder should fail, the decoders connected to that decoder are not affected as they would be in the daisy-chain method.
- Any time you use a switch for the KDS-6, the absolute minimum requirement is that the switch support jumbo framing, i.e. a layer 2 MTU > 9000 bytes.
- Multipoint-to-multipoint – the most complex environment and, more often than not, the most typical application. For this to be successful the network switch being used should support jumbo framing, IGMP-snooping and have built in IGMP-querying.
  If you are using more than 2 encoders across multiple switches the switches should support at least 10Gbit links between switches.
  If the encoder will be used in a non-dedicated network other than Jumbo framing – IGMP snooping and querying are imperative in order for the bandwidth intensive streams to not affect network performance.

NETWORK SWITCH CONFIGURATION SUPPORTING AV OVER IP

FEATURE	SINGLE SWITCH NETWORKING	CASCADE NETWORKING	
		CORE SWITCH	EXTENDED SWITCH
Jumbo Frames	frame size to 9216	frame size to 9216	frame size to 9216
IGMP Snooping	Enable	Enable	Enable
Multicast forwarding or filtering	Enable	Enable	Enable
IP address of IGMP Querier	Must be assigned a valid value	Must be assigned a valid value	N/A
IGMP Querier	Enable	Enable	N/A
IGMP snooping fast leave	Enable	Disable	Enable
Dynamic multicast router port	Disable	Disable	Enable
Forwarding unknown multicast	Disable	Disable	Router port only indicates that extended Ethernet switches must forward unknown multicast
Green or energy-saving feature	Disable	Disable	Disable

SETTING UP A SWITCH FOR KDS-6 STREAMING DEPLOYMENT

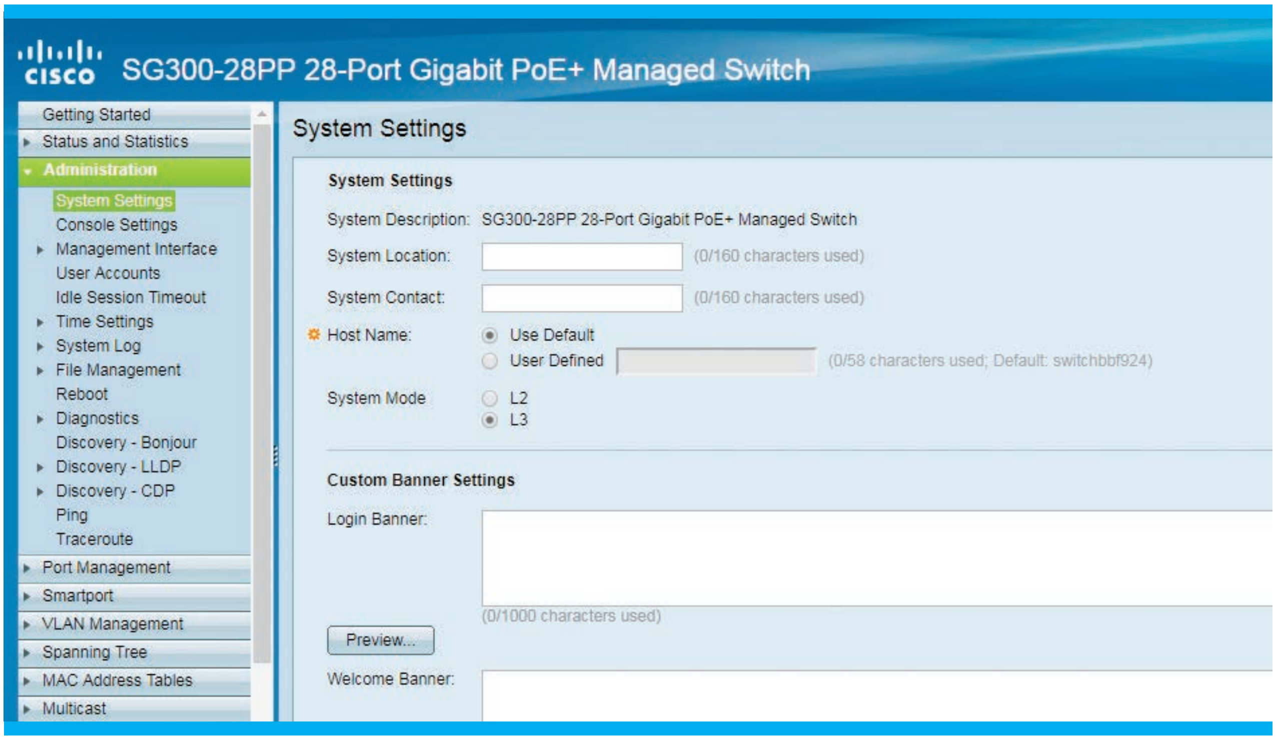
Perform the following procedures in the order that they appear to set up a Switch for KDS-6 Streaming Deployment. The following uses Cisco SG300 as an example, but similar procedures can be applied to any L2/L3 managed switch.

ENABLING LAYER 3 ON THE SWITCH

Setting the switch to Layer 3 mode resets the switch to factory default.

To enable Layer 3 on the switch:

1. On the left pane, click **Administration** > **System Settings.**
   The System Settings page appears.



System Settings

System Settings

System Description: SG300-28PP 28-Port Gigabit PoE+ Managed Switch

System Location: (0/160 characters used)

System Contact: (0/160 characters used)

Host Name: ● Use Default ○ User Defined (0/58 characters used; Default: switchbbf924)

System Mode ○ L2 ● L3

Custom Banner Settings

Login Banner: (0/1000 characters used)

Welcome Banner:

2. Under System Mode, select **L3**.
   Layer 3 mode is enabled on the switch.

FOR YOUR REFERENCE, THE DEFAULT SETTINGS ARE:

- IP Address: 192.168.1.254
- Username: cisco
- Password: cisco

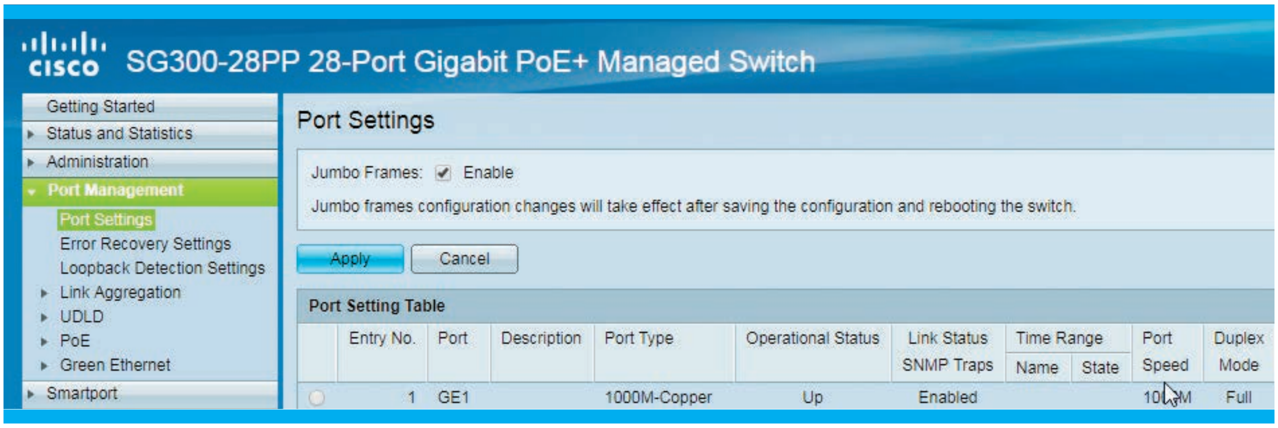
ENABLING JUMBO FRAMES

Enabling jumbo frame support is a prerequisite for streaming with KDS-6.

To enable Jumbo Frames:

1. On the left pane, click **Port Management > Port Settings.**

   The Port Settings page appears.



Port Settings

Jumbo Frames: ☑ Enable

Jumbo frames configuration changes will take effect after saving the configuration and rebooting the switch.

Port Setting Table

	Entry No.	Port	Description	Port Type	Operational Status	Link Status	Time Range		Port	Duplex
						SNMP Traps	Name	State	Speed	Mode
○	1	GE1		1000M-Copper	Up	Enabled			1000M	Full

2. Under Jumbo Frames, select the Enable checkbox.
3. Click **Apply.**

   Jumbo frames support is enabled.

ENABLING IGMP SNOOPING

The following steps are required to enable IGMP snooping:

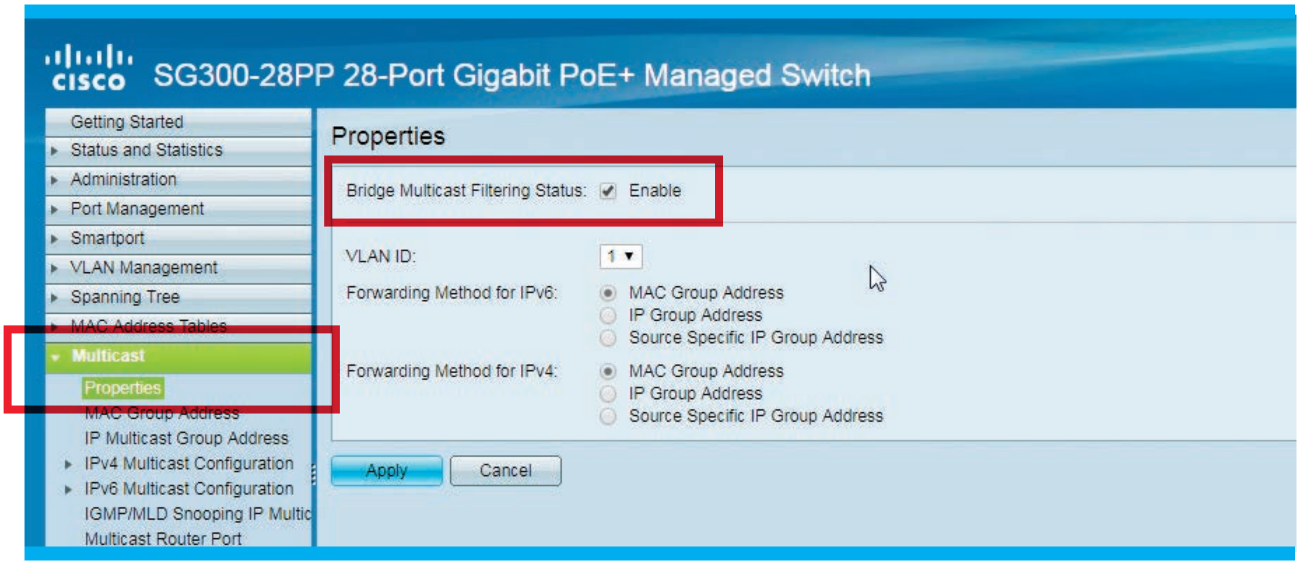
- Setting Bridge Multicast Filter Status
- Setting IGMP Snooping Status
- Setting Additional IGMP Snooping Settings
  - Mrouter Ports Auto Learn
  - Immediate Leave
  - IGMP Querier Status
  - IGMP Querier Election

SETTING BRIDGE MULTICAST FILTER STATUS

To set bridge multicast filter status:

1. Select **Multicast > Properties**.

   The Properties page appears



Properties

Bridge Multicast Filtering Status: ☑ Enable

VLAN ID: 1

Forwarding Method for IPv6: ● MAC Group Address ○ IP Group Address ○ Source Specific IP Group Address

Forwarding Method for IPv4: ● MAC Group Address ○ IP Group Address ○ Source Specific IP Group Address

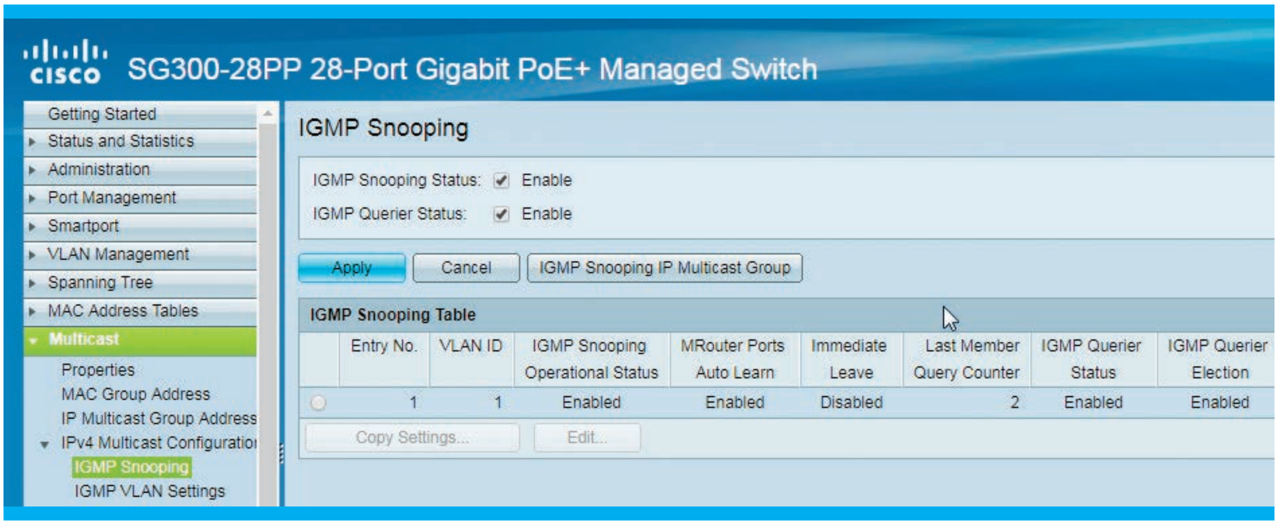
2. Under Bridge Multicast Filter Status select the **Enable checkbox.**
3. Confirm that your settings match the ones in the image above.
4. Click **Apply.**

SETTING IGMP SNOOPING STATUS

To set the IGMP Snooping status:

1. Select **Multicast > IPV4 Multicast Configuration > IGMP Snooping**.

   The IGMP Snooping page appears



IGMP Snooping

IGMP Snooping Status: ☑ Enable

IGMP Querier Status: ☑ Enable

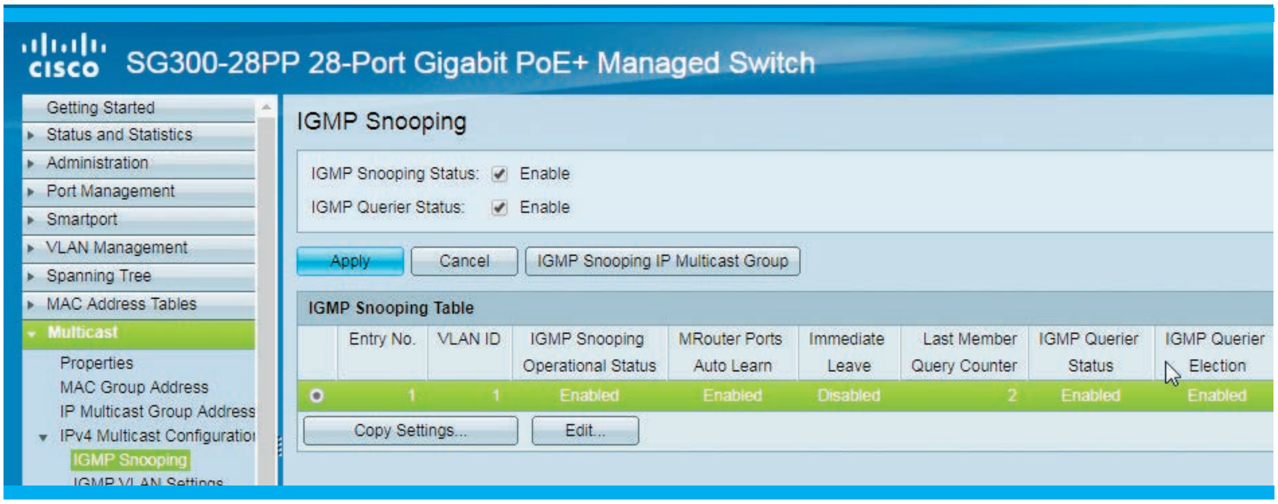
IGMP Snooping Table

	Entry No.	VLAN ID	IGMP Snooping Operational Status	MRouter Ports Auto Learn	Immediate Leave	Last Member Query Counter	IGMP Querier Status	IGMP Querier Election
○	1	1	Enabled	Enabled	Disabled	2	Enabled	Enabled

2. Click the Enable checkboxes under IGMP Snooping Status and under IGMP Querier Status.
3. Make sure that your settings match the image above.
4. Click **Apply.**

SETTING ADDITIONAL IGMP SNOOPING SETTINGS

To set additional IGMP Snooping settings:



IGMP Snooping

IGMP Snooping Status: ☑ Enable

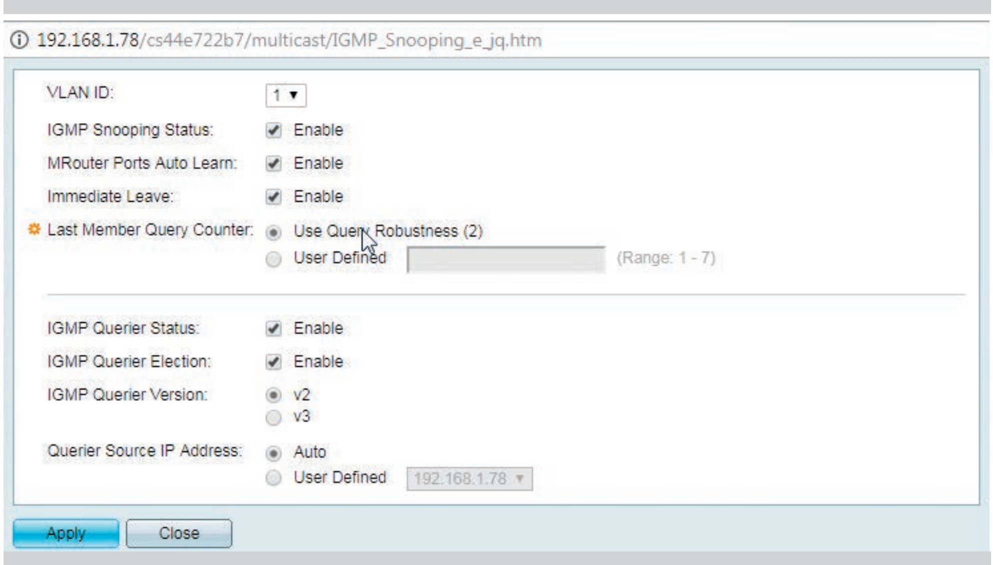
IGMP Querier Status: ☑ Enable

IGMP Snooping Table

	Entry No.	VLAN ID	IGMP Snooping Operational Status	MRouter Ports Auto Learn	Immediate Leave	Last Member Query Counter	IGMP Querier Status	IGMP Querier Election
●	1	1	Enabled	Enabled	Disabled	2	Enabled	Enabled

1. On the IGMP Snooping page, in the IGMP Snooping Table, select the radio button in line one.
2. Click **Edit**.

   The Edit IGMP Snooping Settings window appears.



192.168.1.78/cs44e722b7/multicast/IGMP_Snooping_e_jq.htm

VLAN ID:	1 ▾
IGMP Snooping Status:	☑ Enable
MRouter Ports Auto Learn:	☑ Enable
Immediate Leave:	☑ Enable
Last Member Query Counter:	● Use Query Robustness (2) ○ User Defined (Range: 1 - 7)
IGMP Querier Status:	☑ Enable
IGMP Querier Election:	☑ Enable
IGMP Querier Version:	● v2 ○ v3
Querier Source IP Address:	● Auto ○ User Defined 192.168.1.78 ▾

3. Make sure your settings match the image above for the following:
   - Mrouter Ports Auto Learn
   - Immediate Leave
   - IGMP Querier Status
   - IGMP Querier Election
4. Click **Apply**.

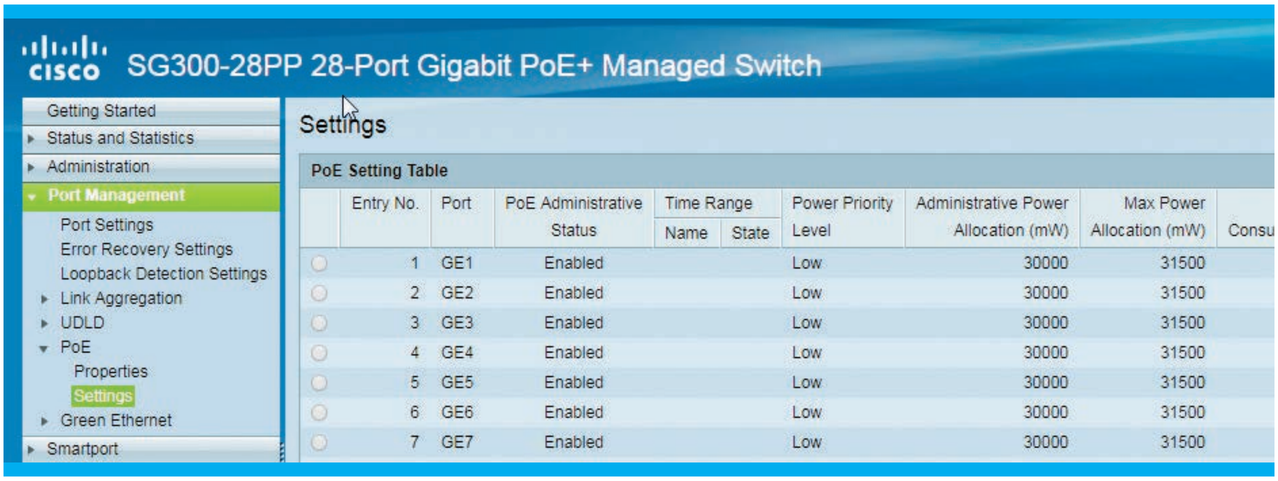
MAKING CHANGES TO POE

MOST SWITCHES SUPPORT POE BY DEFAULT. IF YOUR SWITCH SUPPORTS POE, SKIP THIS STEP. OTHERWISE, FOLLOW THE INSTRUCTIONS BELOW.

To make changes to the PoE default setting:

1. Select **Port Management > PoE > Settings.**

The IGMP Snooping page appears.

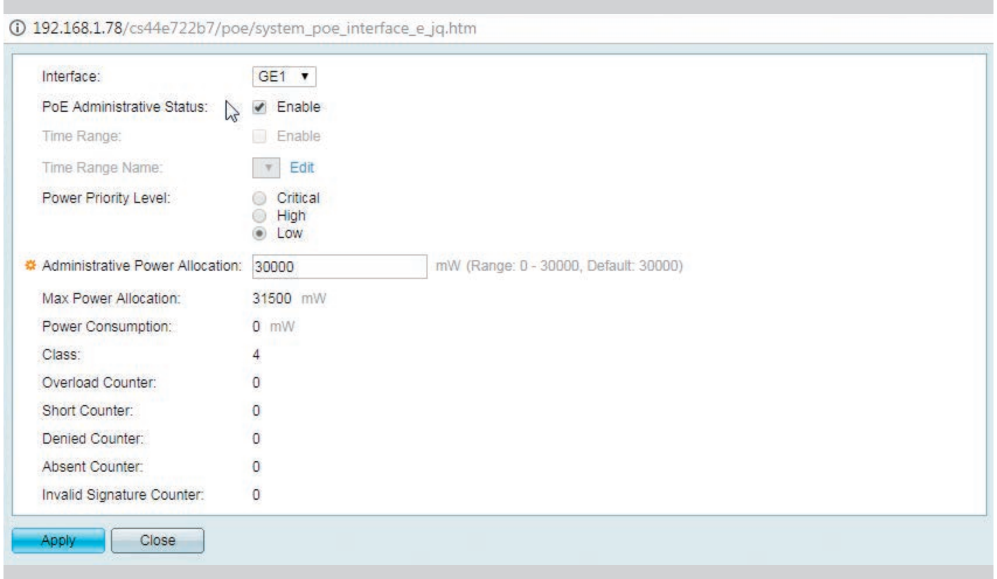


Settings

PoE Setting Table

	Entry No.	Port	PoE Administrative Status	Time Range		Power Priority Level	Administrative Power Allocation (mW)	Max Power Allocation (mW)	Consu
				Name	State				
○	1	GE1	Enabled			Low	30000	31500	
○	2	GE2	Enabled			Low	30000	31500	
○	3	GE3	Enabled			Low	30000	31500	
○	4	GE4	Enabled			Low	30000	31500	
○	5	GE5	Enabled			Low	30000	31500	
○	6	GE6	Enabled			Low	30000	31500	
○	7	GE7	Enabled			Low	30000	31500	

2. In the PoE Setting Table, select the line to be edited and click **Edit.**
   The System PoE Interface page appears.



192.168.1.78/cs44e722b7/poe/system_poe_interface_e_jq.htm

Interface: GE1 ▾

PoE Administrative Status: ☑ Enable

Time Range: □ Enable

Time Range Name: ▾ Edit

Power Priority Level: ○ Critical ○ High ● Low

Administrative Power Allocation: 30000 mW (Range: 0 - 30000, Default: 30000)

Max Power Allocation: 31500 mW

Power Consumption: 0 mW

Class: 4

Overload Counter: 0

Short Counter: 0

Denied Counter: 0

Absent Counter: 0

Invalid Signature Counter: 0

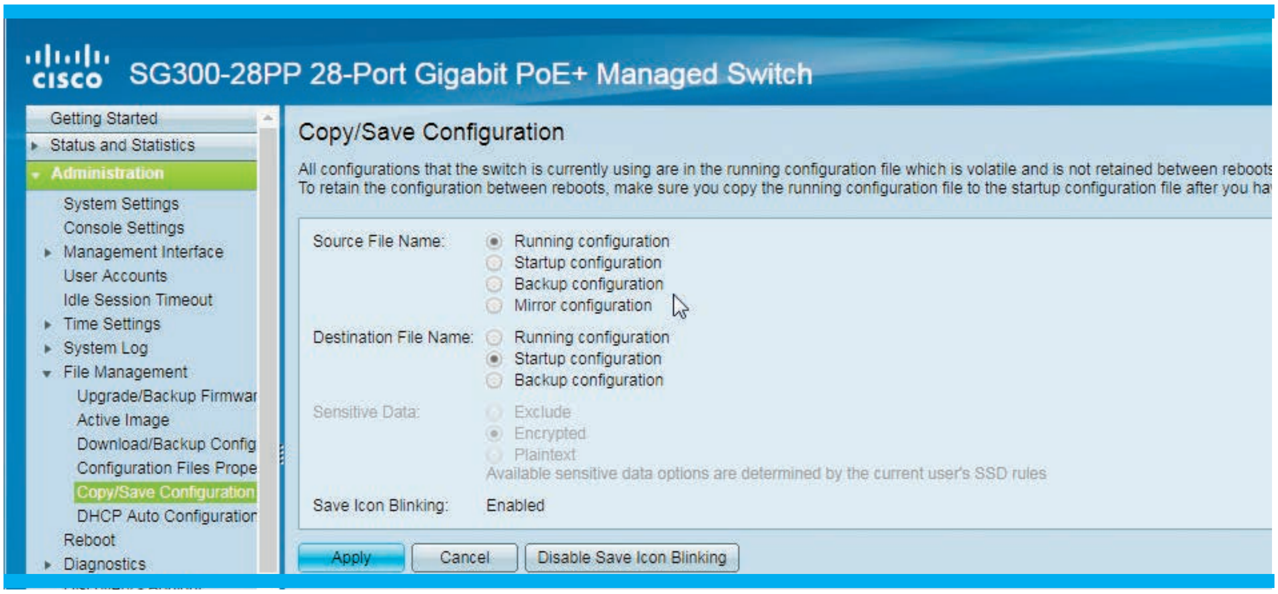
3. Under PoE Administrative Status, select or clear the Enable checkbox to enable/disable PoE on the selected port.

THIS CHECKBOX CAN ALSO BE USED THIS TO POWER CYCLE A DECODER OR ENCODER REMOTELY IF REQUIRED.

APPLYING AND SAVING CHANGES

To apply and save changes to the startup configuration:

1. Select **Administration > Copy/Save Configuration.**
   The Copy/Save Configuration page appears.



SG300-28PP 28-Port Gigabit PoE+ Managed Switch

Copy/Save Configuration

All configurations that the switch is currently using are in the running configuration file which is volatile and is not retained between reboots
To retain the configuration between reboots, make sure you copy the running configuration file to the startup configuration file after you ha

Source File Name: ● Running configuration ○ Startup configuration ○ Backup configuration ○ Mirror configuration

Destination File Name: ○ Running configuration ● Startup configuration ○ Backup configuration

Sensitive Data: ○ Exclude ● Encrypted ○ Plaintext
Available sensitive data options are determined by the current user's SSD rules

Save Icon Blinking: Enabled

2. Click **Copy/Save Configuration**.
3. Click **Apply.**

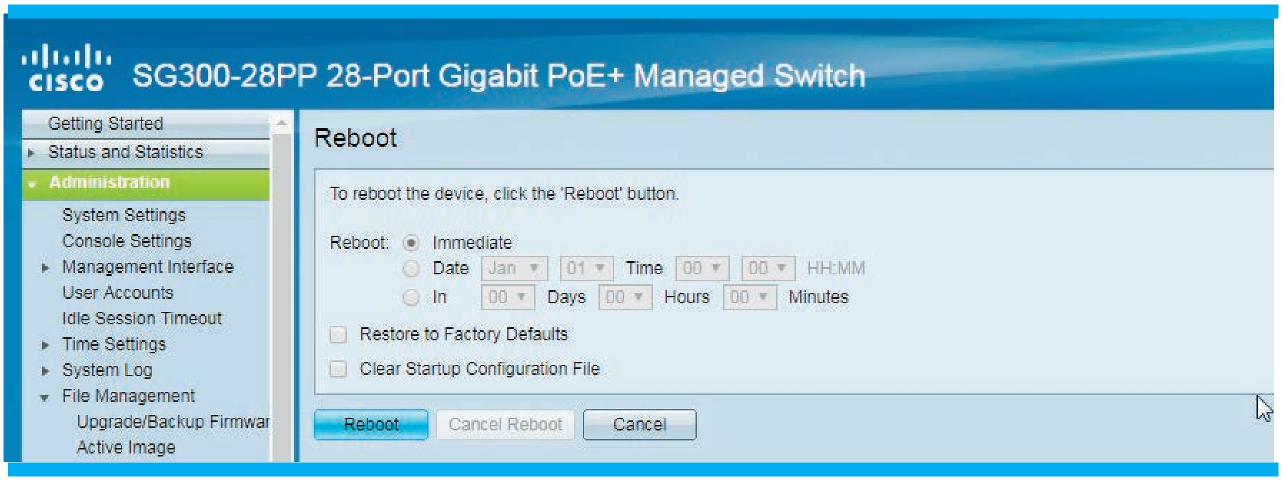
REBOOTING THE SWITCH

Rebooting the switch loads the new start-up configuration that you saved.

To reboot the switch:

1. Select **Administration > File Management > Reboot.**

   The Reboot page appears.



To reboot the device, click the 'Reboot' button.

Reboot: ● Immediate
○ Date Jan ▾ 01 ▾ Time 00 ▾ 00 ▾ HH:MM
○ In 00 ▾ Days 00 ▾ Hours 00 ▾ Minutes

□ Restore to Factory Defaults

□ Clear Startup Configuration File

2. Click **Reboot**.

DISCONNECT THE UNIT FROM THE POWER SUPPLY BEFORE OPENING AND SERVICING

AV BEYOND
THE BOX

For the latest information on our products and a list of Kramer distributors, visit our Web site where updates to this user manual may be found.
We welcome your questions, comments, and feedback.

www.KramerAV.com
info@KramerAV.com

?????????

?????????