Managed PoE Switch

Web Management User Manual

Version: V2.0

Date: 2017.8

TABLE OF CONTENTS

۱. معرفی(Introduction)

۱.۱ مرور اجمالی

با تشکر از خرید سوییچ مدیریتی سپیتام، این سوییچ از طریق رابط کاربری وب مبتنی بر وب (HTML) پیکربندی و نظارت می‌شود. با یک مرورگر استاندارد می‌توانید سوییچ را در هر سایت از راه دور شبکه مدیریت کنید مرورگر به عنوان یک ابزار دسترسی جهانی، از پروتکل HTTP برای برقراری ارتباط مستقیم با سوییچ استفاده می‌کند .

۱.۲ ورود به سیستم مدیریت وب:

مرورگر خود را در رایانه باز کنید، آدرس آی پی سوییچ را مانند فرمت روبه‌رو وارد کنی: http://xxx.xxx.xxx.xxx

آدرس پیش‌فرض سوییچ http://۱۹۲.۱۶۸.۲.۱ می‌باشد. با تأیید این آدرس در مرورگر رایانه با صفحه‌ی زیر روبه‌رو می‌شوید که باید در آن نام کاربری و پسورد را وارد کنید.

به‌صورت پیش‌فرض نام کاربری admin و پسورد ورود system می‌باشد.

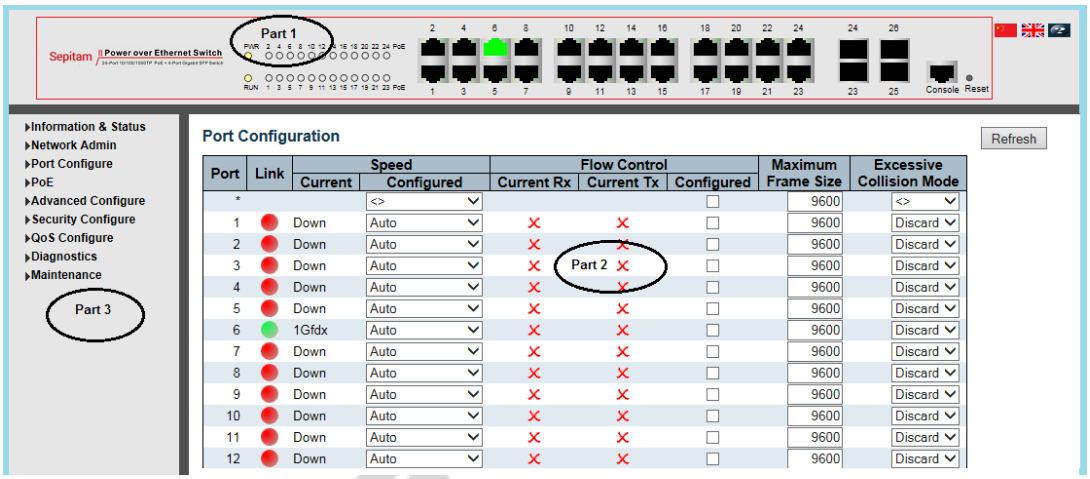
نکته: تمامی حروف به‌صورت کوچک وارد شود.

۱-۱ پنجره ورود به سیستم

Default User Name: admin
Default Password: system

۱.۳ رابط کاربری مبتنی بر وب

۱-۲ پس از وارد کردن نام کاربری و پسورد با صفحه‌ی زیر مواجه می‌شوید.



شکل۲-۱: رابط اصلی صفحه‌ی مدیریت وب

شرکت دانش بنیـــان سپیتـــام

رابط صفحه‌ی اصلی شامل سه بخش است:

Part	توضیحات
Part ۱	آرم شرکت؛ نمایش صفحه شاخص‌های پورت ، از جمله وضعیت کار PoE و Link ؛ دکمه انتخاب زبان ؛ فایل راهنما
Part ۲	منوی اصلی ، به شما امکان می‌دهد به تمام دستورات و آمار دسترسی پیدا کنید.
Part ۳	صفحه اصلی ، نمایش جزئیات پیکربندی.

رنگ‌های مختلف به معنای حالت‌های مختلف است ، آنها به شرح زیر نشان داده‌شده‌اند:

: No link ; : 1000Mbps linked ; : 100Mbps linked

۱.۴منوی اصلی (Main Menu)

با استفاده از سیستم مدیریت وب شما می‌توانید پارامترهای مختلفی از سیستم را تعریف و کنترل نمایید. شما می‌توانید به تمامی درگاه‌ها و همچنین ترافیک شبکه نظارت کامل داشته باشید. در بخش زیر به معرفی اجمالی منوهای سوییچ می‌پردازیم.

Information & Status: کاربران می‌توانند اطلاعات سوئیچ و وضعیت کار را در زیر این فهرست بررسی کنند

Network Admin: کاربران می‌توانند ویژگی‌های مربوط به شبکه را در زیر این فهرست بررسی و پیکربندی کنند.

Port Configure: کاربران می‌توانند مشخصات درگاه‌ها را در زیر این فهرست بررسی و پیکربندی کنند.

PoE: کاربران می‌توانند ویژگی‌های مربوط به Power-over-Ethernet (PoE) را در زیر این فهرست بررسی و پیکربندی کنند.

Advanced Configure: کاربران می‌توانند ویژگی‌های پیشرفته L۲ را در زیر این فهرست بررسی و پیکربندی کنند.

Security Configure: کاربران می‌توانند ویژگی‌های امنیتی سوئیچ را در زیر این فهرست بررسی و پیکربندی کنند.

Qos Configure: کاربران می‌توانند ویژگی‌های Qos سوئیچ را در زیر این فهرست بررسی و پیکربندی کنند.

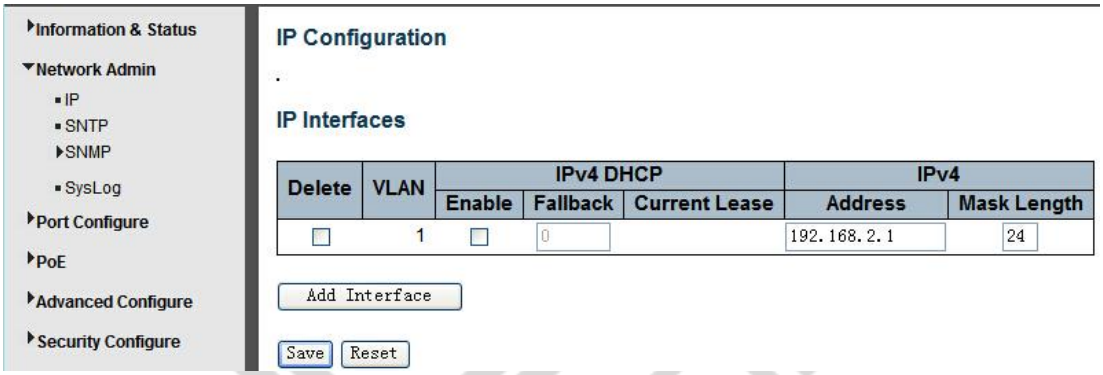
Diagnostics: کاربران می‌توانند ویژگی‌های تشخیصی سوئیچ را در زیر این فهرست بررسی و پیکربندی کنند.

Maintenance: کاربران می‌توانند اطلاعات و ویژگی‌های تعمیر و نگهداری را در زیر این فهرست بررسی و پیکربندی کنند.

۲. مدیریت شبکه (Network Management)

۲.۱پیکربندی آدرس آی پی (IP Configuration)

نکته: آدرس آی پی به‌صورت پیش‌فرض ۱۹۲.۱۶۸.۲.۱ با Subnet (۲۴)۲۵۵.۲۵۵.۲۵۵.۰ می‌باشد. در منوی اصلی بر روی "Network Admin" کلیک کنید سپس بر روی زیر منوی "IP" کلیک کنید که صفحه‌ی زیر برای شما باز می‌شود.



شکل ۲-۱ صفحه پیکربندی IP

در جدول زیر جزئیات توضیحات در مورد پیکربندی IP آورده شده است:

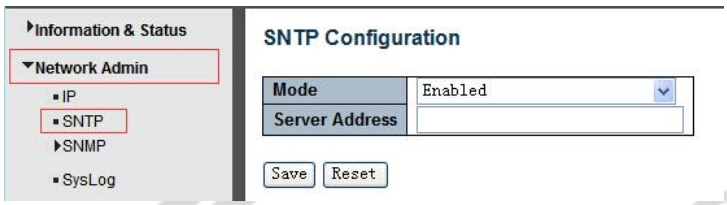
نام	توضیحات
Port Name	نمایش اطلاعات پورت
VLAN	برای دسترسی و مدیریت Vlanهای مختلف بر روی سیستم
IPv۴ DHCP	- اگر فعال باشد ، به این معنی است که پورت VLAN سمت کلاینت IPv۴ DHCP را شروع می‌کند تا آدرس IPv۴ سوییچ را به‌صورت پویا دریافت کند. - در غیر این صورت، از پیکربندی ثابت IP استفاده خواهد کرد - Fallback (ثانیه) ، به معنی زمان انتظار برای دریافت آدرس IP سوییچ به‌صورت پویا از طریق DHCP است. مقدار "۰" در اینجا به معنای عدم دریافت آی پی از DHCP در طول زمان است
IPv۴	- Address : آدرس ثابت IPv۴ که توسط کاربر وارد شده است. - Mask Length: subnet IPv۴ subnet Mask توسط کاربر وارد شده است.

برای ایجاد مدیریت جدید برای آدرس VLAN و IP بر روی "Add Interface" کلیک کنید. برای ذخیره تنظیمات روی "Save" کلیک کنید.

توجه: همه‌ی پورت‌ها به‌صورت پیش‌فرض عضو Vlan1 هستند. اگر کاربر برای مدیریت سوییچ نیاز به استفاده از VLAN دیگر دارد ، ابتدا VLAN را در قسمت VLAN اضافه کرده و پورت مربوطه را به VLAN اضافه کند

۲.۲ پیکربندی SNTP (SNTP Configuration)

SNTPمخفف Simple Network Time Protocol است ، یک پروتکل شبکه برای همگام سازی ساعت سیستم‌های رایانه‌ای است. می‌توانید سرورهای SNTP را مشخص کرده و GMT Time zone را تنظیم کنید. صفحه‌های پیکربندی SNTP بعد از کلیک روی "Network Admin"> "SNTP" ظاهر می‌شوند.



شکل ۲-۲ نمایش تنظیمات SNTP

توضیحات پیکربندی:

Object	توضیحات
Mode	برای SNTP فعال و غیرفعال "Enabled" و "Disable" روی منوی کشویی کلیک کنید. Enabled وقتی عملکرد حالت SNTP را فعال می‌کنید. هنگام فعال کردن عملکرد حالت SNTP، عامل پیام‌های SNTP را بین کلاینت‌ها و سرور انتقال می‌دهد در صورتی که آنها در یک دامنه زیر شبکه نیستند. Disabled: عملکرد حالت SNTP را غیرفعال کنید
SNTP Sever	پس از ورود آدرس IP سرورSNTP ، اطلاعات SNTP از آن سرور دریافت می‌شود .

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

۲.۳ پیکربندی SNMP (SNMP Configuration)

پروتکل مدیریت شبکه ساده (SNMP) یک پروتکل لایه ۲ کاربردی است که تبادل اطلاعات مدیریتی بین دستگاه‌های شبکه را تسهیل می‌کند. این بخشی از مجموعه پروتکل کنترل انتقال اینترنت (TCP/IP) است. SNMP مدیران شبکه را قادر می‌سازد تا عملکرد شبکه را مدیریت کنند، مشکلات شبکه را پیدا و حل کنند و برای رشد شبکه برنامه‌ریزی کنند. این سوییچ از SNMPv۱، v۲c پشتیبانی می‌کند. نسخه‌های مختلف SNMP سطح امنیتی متفاوتی را برای ایستگاه‌های مدیریت فراهم می‌کند.

به زبان ساده SNMP از سیستمی پشتیبانی می‌کند که به یک مدیر شبکه که از یک ایستگاه کاری واحد استفاده می‌کند، امکان می‌دهد تا از راه دور کامپیوترها، مسیریابی‌ها و دیگر تجهیزات شبکه را مدیریت و بر آنها نظارت کند.

۱. public - به ایستگاه مدیریت احراز هویت اجازه دهید اشیا MIB را فقط بخواند.
۲. private - به ایستگاه مدیریت احراز هویت اجازه دهید اشیا MIB را هم بخواند، بنویسد و ویرایش کند.

Trap

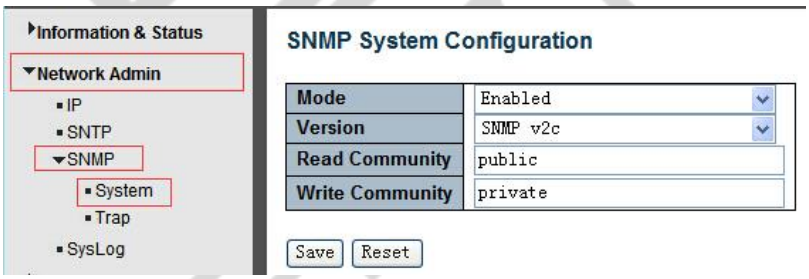
سرویس و پروتکل **SNMP** می‌توانند اطلاعات بسیار زیادی در خصوص دستگاه‌های شبکه به شما ارائه بدهند اما ما به همه این اطلاعات نیازی نداریم و صرفاً برخی از این اطلاعات برای ما مهم است. با استفاده از **Trap** شما می‌توانید تعریف کنید که فقط در صورت بروز یک رویداد خاص اطلاع رسانی شود. اگر یکی از سوییچ‌های شبکه خاموش شود و یا یکی از پورت‌های آن خاموش شود بلافاصله **Trap** مورد نظر ایجاد شده و برای **NMS** شبکه ارسال می‌شود تا در خصوص این رویداد اطلاع رسانی شود و مشکل به وجود آمده برطرف شود.

MIB

MIB مجموعه‌ای از اشیا **managed** مدیریت شده است که در یک شبکه مجازی وجود دارند. مجموعه اشیا **managed** مدیریت شده مرتبط در ماژول‌های خاص **MIB** تعریف می‌شوند. سوییچ از ماژول استاندارد مدیریت اطلاعات **MIB II** استفاده می‌کند. بنابراین، مقدار شی **object MIB** توسط هر نرم‌افزار **SNMP** تحت وب قابل خواندن است.

۲.۳.۱پیکربندی سیستم SNMP (SNMP System Configuration)

می‌توانید پیکربندی سیستم SNMP را فعال یا غیرفعال کنید. با کلیک بر روی "Network Admin" در منوی اصلی و بعد SNMP و در آخر System را انتخاب نمایید تا صفحه‌ی زیر برای شما نمایان گردد.



شکل ۳-۲ صفحه پیکربندی SNMP

توضیحات پیکربندی:

Object	توضیحات
Mode	عملکرد SNMP را فعال و غیرفعال کنید
Version	با استفاده از این منو ورژن SNMP را مشخص کنید
Read Community	Public: به ایستگاه مدیریت احراز هویت اجازه دهید اشیا MIB را فقط بخواند
Write Community	Private: به ایستگاه مدیریت احراز هویت اجازه دهید اشیا MIB را هم بخواند، و بنویسد و ویرایش کند

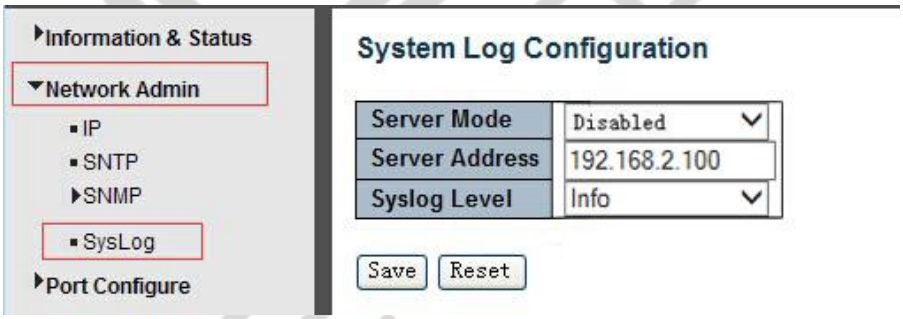
۲.۳.۲پیکربندی SNMP Trap (SNMP Trap Configuration)

می‌توانید عملکرد SNMP Trap را فعال یا غیرفعال کنید و پیکربندی را تنظیم کنید. روی "Trap"> "SNMP" <"Network Admin" کلیک کنید، سپس این صفحه به‌صورت زیر نمایش داده می‌شود:

شکل ۳-۲ صفحه پیکربندی SNMP Trap

۲.۴پیکربندی ورود به سیستم (System Log Configuration)

پس از کلیک بر روی" SysLog" < "Network Admin" می‌تواند ثبت سیستم سوییچ را از طریق صفحه زیر پیکربندی کنید.



شکل ۴-۲ صفحه پیکربندی ورود به سیستم

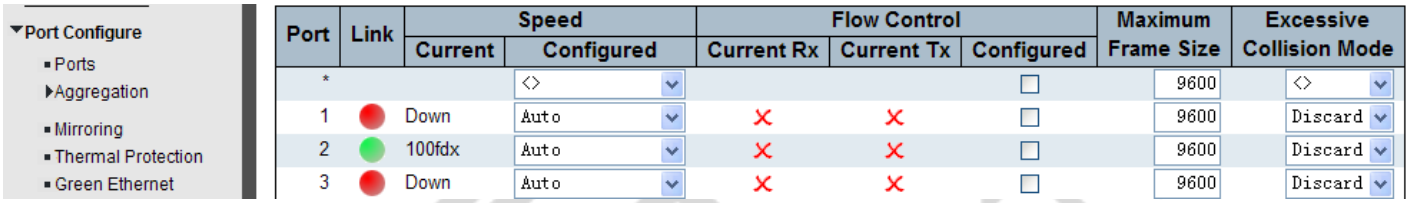
توضیحات پیکربندی:

Object	توضیحات
Server Mode	عملکرد ورود به سیستم SNMP را فعال یا غیرفعال کنید. اگر فعال انتخاب شده باشد اگر فعال انتخاب شده باشد گزارش ورود به سیستم را برای سرور تعریف شده ارسال می‌کند
Server Address	آدرس سرور
Syslog Level	برای تعریف سطح ورود به سیستم از جمله: **Info** : اطلاعات ، هشدارها و خطاها **Warning** : اطلاعات ، هشدارها و خطاها **Error**: ارور ها

۳. (port Configure) پیکربندی پورت‌ها

۳.۱ نحوه پیکربندی پورت‌ها (Port Configuration)

این صفحه برای پیکربندی مشخصات پورت‌ها می‌باشد "Port Configure" > "Ports"



شکل ۳-۱ صفحه پیکربندی پورت

توضیحات پیکربندی:

Object	توضیحات
Link	رنگ قرمز به معنی غیر فال بودن پورت و رنگ سبز به معنی فعال بودن آن پورت می‌باشد
Speed	با استفاده از این زیر منو می‌توانید پورت را فعال یا غیرفعال کنید یا سرعت آن را انتخاب کنید
Flow Control	برای مکانیسم کنترل جریان هر پورت استفاده می‌شود
Maximum Frame Size	برای تنظیم حداکثر اندازه فریم اترنت استفاده می‌شود که به‌صورت پیش‌فرض ۹۶۰۰بایت است

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

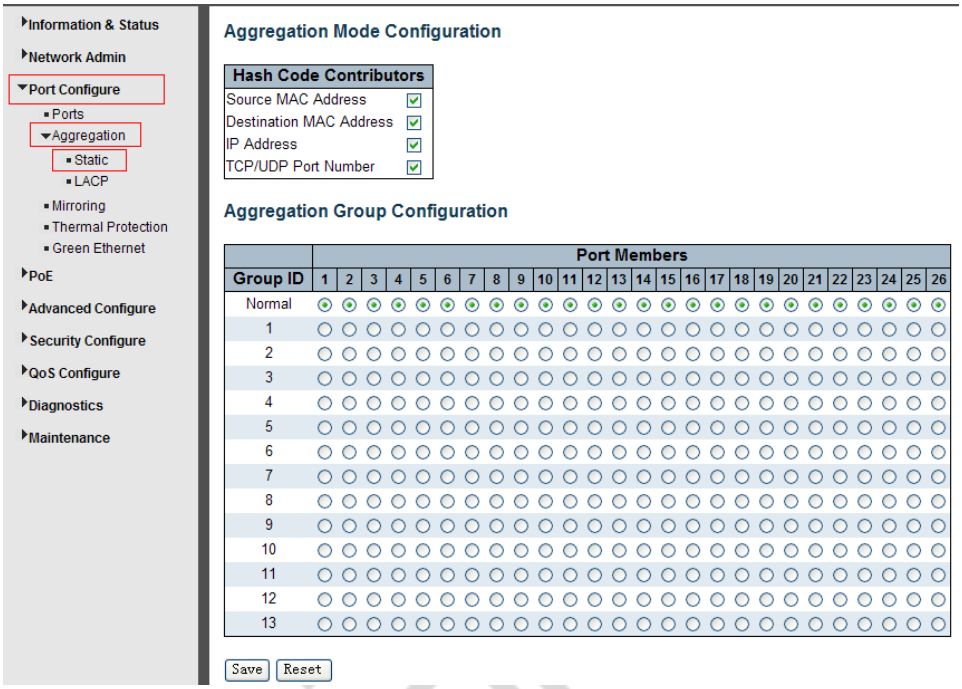
۳.۲ پروتکل تجمیع لینک (Link Aggregation)

Link Aggregation تکنیکی است که برای افزایش پهنای باند، سرعت، افزونگی و تضمین ارتباط میان دستگاه‌های یک شبکه کابلی استفاده می‌کنند. وقتی از Link Aggregation استفاده می‌کنید؛ اگر یک درگاه یا کابل خراب یا قطع شود؛ هنوز ارتباط میان سوییچ و دستگاه دیگر برقرار است. استاندارد تجمیع لینک بانام ad۸۰۲/۳ شناخته می‌شود ولی در حال حاضر از AX۸۰۲/۱ نیز استفاده می‌شود. این سوییچ حداکثر از ۱۳ گروه از پیوند ، ۲ تا ۸ پورت به عنوان یک گروه پشتیبانی می‌کند.

این روش تعدادی پورت فیزیکی را با هم ترکیب می‌کند تا یک مسیر داده با پهنای باند بالا ایجاد کند ، به طوری که بتواند تقسیم بار ترافیکی را بین پورت‌های عضو در گروه پیاده سازی کند و قابلیت اطمینان از اتصال را تقویت کند.

۳.۲.۱تنظیم استاتیک پروتکل تجمیع لینک (Static Aggregation)

در این صفحه ، کاربر می‌تواند تجمع استاتیک درگاه‌های سوییچ را پیکربندی کند. پس از کلیک بر روی منوی <"Port Configure" "Static" <"Aggregation"، برای انجام تنظیمات تجمع استاتیک پنجره زیر ظاهر می‌شود.



شکل ۲-۳ صفحه پیکربندی تجمیع استاتیک لینک

توضیحات پیکربندی:

Object	توضیحات
Aggregation Mode Configuration	این پارامتر الگوریتم هش جریان در میان پورت‌های LAG (گروه تجمع پیوند) است.
Group ID	شناسه گروه تجمع استاتیک
Port Members	این سوییچ از ۱۳ گروه پشتیبانی می‌کند، ۲ تا ۸ پورت به عنوان یک گروه می‌توان انتخاب کرد.

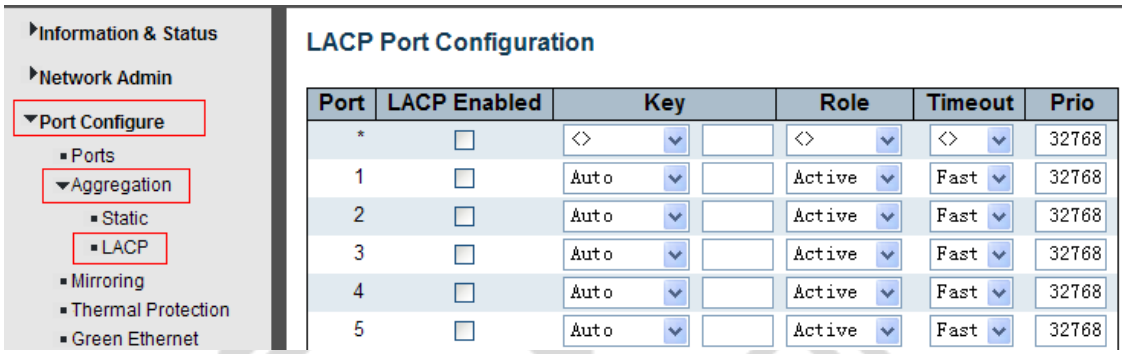
پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

توجه: این دستگاه اجازه می‌دهد که تا حداکثر ۸ پورت تجمیع شده و به عنوان یک گروه به‌صورت هم‌زمان انتخاب شوند.

۳.۲.۲ پروتکل کنترل تجمع پیوند LACP (LACP Aggregation)

پروتکل کنترل تجمع پیوند (LACP) ابزاری استاندارد برای تبادل اطلاعات بین سیستم‌های شریک فراهم می‌کند که به پیوندهای زائد با سرعت بالا نیاز دارند. تجمیع پیوند به شما امکان می‌دهد تا حداکثر هشت پورت متوالی را در یک اتصال اختصاصی گروه‌بندی کنید. این ویژگی می‌تواند پهنای باند را به دستگاهی در شبکه گسترش دهد. عملکرد LACP به حالت دوبلکس کامل نیاز دارد. برای اطلاعات دقیق‌تر، به استاندارد IEEE ۸۰۲.۳ad مراجعه کنید.

برای ساختن لینک تجمیع شده به‌صورت دینامیک به‌صورت روبه‌رو عمل نمایید "Port Configure"> "Aggregation"> "LACP"، کاربران می‌توانند پیکربندی LACP را در صفحه دنبال شده تنظیم کنند.



شکل ۳-۳ صفحه پیکربندی پروتکل LACP

توضیحات پیکربندی:

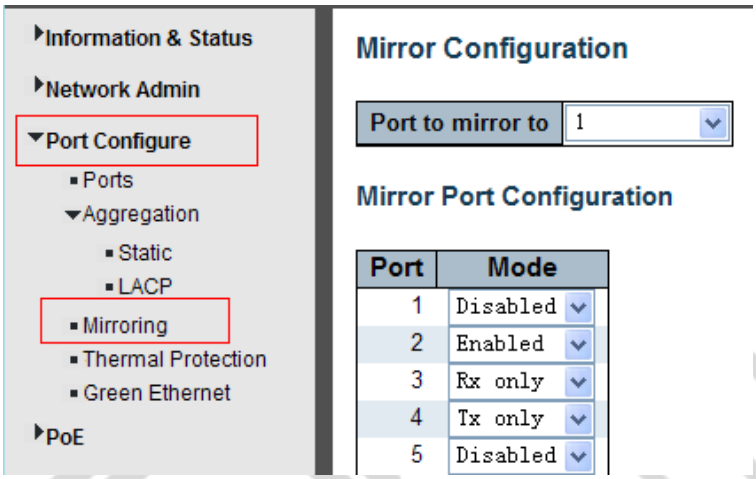
Object	توضیحات
LACP	Enable or disable: عملکرد LACP آن پورت را فعال یا غیرفعال کنید.
Key	مقدار رنج قابل قبول برای این پورت ۱-۶۵۵۳۵ Auto تنظیم خودکار سرعت اتصال با توجه به نرخ تبادل داده در اتصال فیزیکی شبکه. ۳ = 1Gb, ۲ = ۱۰۰Mb, ۱ = ۱۰Mb , Specific یک مقدار تعریف شده توسط کاربر می‌تواند وارد شود.پورت‌های با کلید یکسان می‌توانند در تجمیع لینک شرکت کنند، در حالی که پورت‌های با کلیدهای دیگر نمی‌توانند..
Role	Role: نقش فعالیت پروتکل LACP را مشخص می‌کند. Active: بسته‌های LACP را در هر ثانیه منتقل می‌کند. Passive: این در حالی است که Passive منتظر بسته‌های LACP از یک شریک خواهد ماند.
Timeout	Timeout: فاصله بین انتقال BPDU را کنترل می‌کند. Fast: بسته‌های LACP را در هر ثانیه منتقل می‌کند. Slow: قبل از ارسال بسته LACP به مدت ۳۰ ثانیه صبر می‌کند.
Prio	Prio : اولویت پورت را کنترل می‌کند. اگر شریک LACP بخواهد گروهی بزرگ‌تر از آنچه توسط این دستگاه پشتیبانی می‌شود تشکیل دهد، این پارامتر کنترل می‌کند که کدام درگاه‌ها فعال هستند و کدام درگاه‌ها نقش پشتیبان را دارند. تعداد کمتر به معنای اولویت بیشتر است.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

۳.۳ عملکرد Port Mirroring در سوییچ (Port Mirroring)

پورت میرورینگ یکی از روش‌های آنالیز ترافیک شبکه است. در این روش سوییچ و یا روتر شبکه یک کپی از تمام پکت‌های شبکه را که از یک پورت خاص یا کل شبکه LAN عبور می‌کنند را به یک پورت دیگر می‌فرستد تا مورد بررسی و آنالیز قرار گیرند در نتیجه پورت میرورینگ به یک کامپیوتر خاص امکان می‌دهد تا پکت های را دریافت کند که در حالت عادی از دید آن پنهان است. این قابلیت سبب بهبود مانیتورینگ شبکه توسط مدیر شبکه می‌شود.

برای پیکربندی تنظیمات Mirror، روی "Mirroring" <"Port Configure" کلیک کنید. سپس صفحه‌ای به‌صورت زیر ظاهر می‌شود:



شکل ۳-۴ صفحه‌ی پیکربندی پورت Mirror

توضیحات پیکربندی:

Object	توضیحات
Port mirror to	Disabled: قابلیت پورت Mirror را غیرفعال می‌کند. با استفاده از اعداد ۱ تا ۱۰ می‌توانیم پورتی که دیتاها و فریم‌ها در آن کپی می‌شوند را مشخص کنیم
Mode	انتخاب حالت‌های پورت Mirror: Rx only: فقط فریم‌های دریافتی را بر روی پورت Mirror کپی می‌کند Tx only: فقط فریم‌های ارسالی را بر روی پورت Mirror ارسال می‌کند Disabled: هیچ دیتای از آن پورت بر روی پورت Mirror کپی نمی‌شود. Enabled: تمامی فریم‌های ارسالی و دریافتی بر روی پورت Mirror مشخص شده کپی می‌شوند

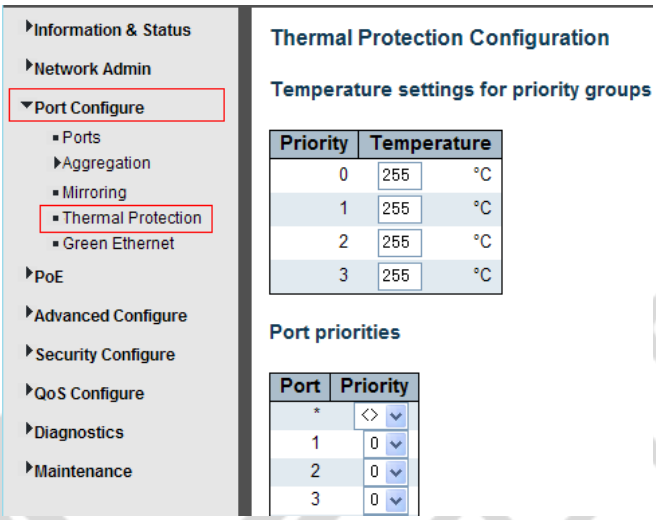
پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

توجه: شما نمی‌توانید در Mirror پورت (های) سریع را روی پورت کم سرعت تنظیم کنید. به عنوان مثال، اگر بخواهید پورت (های) ۱۰۰ مگابیت بر ثانیه را به پورت ۱۰ مگابیت در ثانیه منتقل کنید، مشکلی پیش می‌آید. بنابراین مقصد پورت باید در مقایسه با پورت منبع دارای سرعت برابر یا بالاتر باشد. علاوه بر این، پورت منبع و پورت مقصد نباید یکی باشند.

۳.۴پیکربندی حفاظت حرارتی (Thermal Protection Configuration)

حفاظت حرارتی برای شناسایی و محافظت از کلید کار است. هنگامی‌که سوییچ دمای پورت را تشخیص دهد که بالاتر از دمای تعریف شده باشد، سیستم برای محافظت از خود سوییچ، پورت را غیرفعال می‌کند، برای دسترسی به این قابلیت مسیر زیر را دنبال می‌کنیم.

"Port Configure" > "Thermal Protection"



صفحه پیکربندی حفاظت حرارتی۵-۳شکل

توضیحات پیکربندی:

Object	توضیحات
Temperature settings for priority groups	این سوییچ از ۴ گروه اولویت محافظت حرارتی پشتیبانی می‌کند و هر یک از آنها می‌توانند درجه حرارت مشخصی برای محافظت داشته باشند.
Port priorities	از طریق این گزینه مشخص کنید که پورت‌ها به کدام یک از اولویت‌ها اختصاص دارد

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

- توجه به طور پیش‌فرض، تمام پورت‌های سوئیچ با درجه حرارت محافظت شده ۲۲۵ درجه سانتی‌گراد به گروه اولویت تعلق دارند.

۴.پیکربندی PoE (PoE Configuration)

Power Over Ethernetیا PoE ، مکانیزم استاندارد IEEE ۸۰۲.۳af است که وظیفه ارسال برق بر روی کابل شبکه CAT۵ و CAT۶ را بر عهده دارد. در صورتی که شما دوربین‌های مدار بسته تحت شبکه یا IP Camera دارید، می‌توانید با استفاده از سوییچPoE ، آن‌ها را روشن کنید. علاوه بر این، در صورتی که سازمان شما دارای IP Phone و یا آنتن وایرلس است، می‌توانید برق این تجهیزات را نیز از طریق سوییچPoE ، تأمین نمائید. ارسال برق بر روی کابل شبکه با استفاده از PoE ، اهمیت زیادی دارد. در آغاز باعث تمیزتر شدن کار می‌شود. بجای اینکه به IP Phone ها یاIP Camera ، دو کابل متصل شده باشد (یکی برای دیتا و دیگری برق آداپتور)، فقط یک کابل شبکه متصل خواهد شد. از طرفی، هنگامی‌که برق تجهیزات را از طریق PoE تأمین می‌کنید، کافیست سوییچ PoE را به UPS متصل کنید تا در صورت قطع برق، IP Phone ها و دوربین‌ها، خاموش نشوند. در غیر این صورت، باید ساختمان را برایUPS ، کابل کشی نمائید.

سیستم منبع تغذیه PoE این محصول دارای استاندارد واحد ، IEEE ۸۰۲.۳af/at است. بنابراین دستگاه‌های تولیدکنندگان مختلف مشکلی در استفاده عمومی ندارند ، به شرطی که از این استانداردها پیروی کنند.

PD: مخفف کلمه power devices به معنی دستگاه‌های که از استاندارد POE پشتیبانی می‌کنند است. که شامل دوربین‌های IP اکسس پوینت‌های وایرلس، تلفن‌های VOIP و... می‌باشد.

روند شناسایی دستگاه‌های POE از دستگاه‌های غیر POE :

۱. ردیابی: در ابتدا ، سوییچ ولتاژ بسیار کمی در خروجی آزاد می‌کند تا تشخیص دهد که آیا PD متصل شده آن سازگار با IEEE۸۰۲.۳af IEEE۸۰۲.۳at /است. این امر فقط برای تشخیص اینکه دستگاه متصل شده سازگار با استاندارد af/at است ، سپس به مرحله بعدی می‌رود.

۲ .طبقه‌بندی مصرف کننده‌ها: پس از شناسایی مصرف کننده‌ها در خروجی، سوییچ آنها را طبقه‌بندی می‌کند و تشخیص می‌دهد که توان مورد نیاز PD چه مقدار است.

۳.روشن شدن: پس از انجام دو مرحله بالایی ، سوییچ تغذیه مورد نیاز PD را با ولتاژ خروجی ۴۴ ~ ۵۷ ولت DC شروع می‌کند.

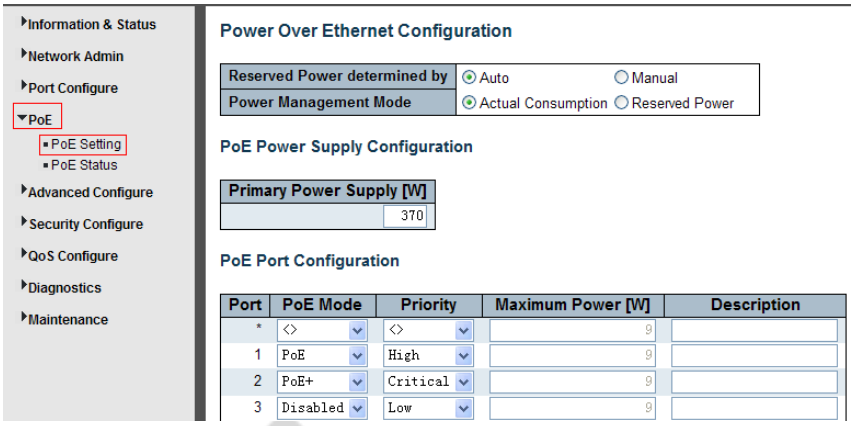
۴. منبع تغذیه PSE : دستگاه به‌صورت پایدار ولتاژ ۴۴ ~ ۵۷ ولت DC را به PD تحویل می‌دهد و تغذیه پورت را به‌صورت خودکار فراهم می‌کند. حداکثر توان تحویلی POE در استاندارد IEEE۸۰۲.۳af ۱۵/۵ وات و برای استاندارد IEEE۸۰۲.۳at ۲۵/۵ وات به ازای هر پورت می‌باشد.

۵.قطع اتصال: اگر PD قطع شود یا کاربر PoE را از نرم‌افزار مدیریت غیرفعال کند ، سوییچ به سرعت (۳۰۰-۴۰۰ میلی ثانیه) تأمین برق PDرا متوقف می‌کند.

توجه: در هر لحظه از تأمین انرژی PD توسط سوییچ، فرآیند ارائه توان به‌صورت پویا و دینامیک چک می‌شود. در صورت بروز هرگونه وضعیت غیر عادی، مانند اتصال کوتاه PD ، مصرف برق بالاتر از توان تغذیه و غیره ، تغذیه خودکار پورت دیگر متوقف می‌شود و سپس از مرحله ۱ دوباره راه‌اندازی می‌شود.

۴.۱تنظیمات POE (PoE Settings)

پس از کلیک روی" PoE Setting "PoE"> "، می‌توانید تنظیمات PoE را مانند صفحه زیر دنبال کنید:



شکل ۴-۱ تنظیمات POE

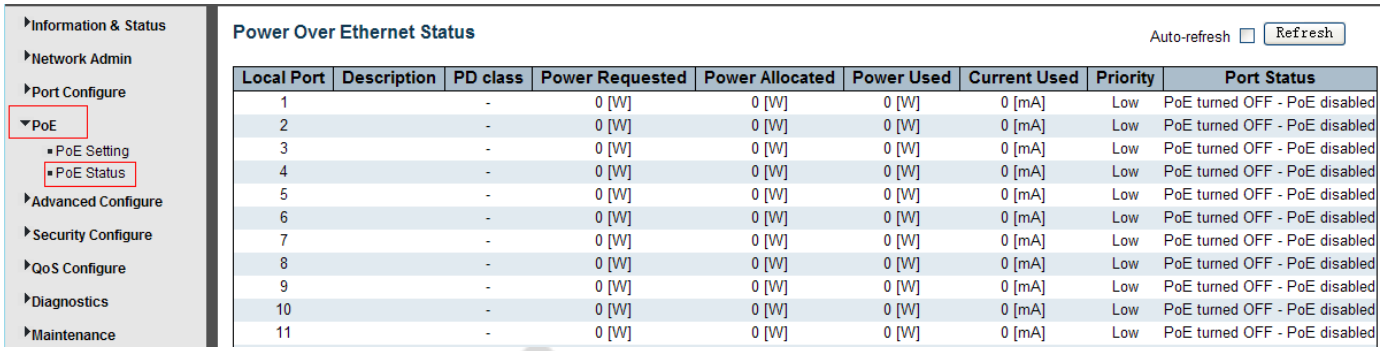
توضیحات پیکربندی:

Object	توضیحات
Reserved Power determined by	این سوییچ از دو حالت برای اختصاص توان POE بهره می‌برد. Auto: سوییچ با توجه به کلاس PD شناسایی شده ، حداکثر قدرت پورت سوییچ را به طور خودکار در خروجی ظاهر می‌کند. این سوییچ از دو استاندارد IEEE.۸۰۲.۳af/at پشتیبانی می‌کند . Manual: به‌صورت دستی توسط کاربر می‌توان توان خروجی پورت را سفارش سازی کرد.
Power Management Mode	این سوییچ از دو حالت برای مدیریت POE استفاده می‌کند. ۱.Actual Consumption(مصرف واقعی): در این حالت ، وقتی که میزان واقعی مصرف برق همه پورت‌ها از بودجه برق سوییچ بیشتر شود ، کمترین درگاه اولویت خاموش خواهد شد. اگر همه درگاه‌ها اولویت یکسانی داشته باشند ، حداکثر تعداد درگاه خاموش خواهند شد. ۲.Reserved Power (پاور تضمین شده): در این حالت اگر مقدار مصرف واقعی پورت‌ها از مقدار بودجه پاور کل بیشتر شود، دستگاه جدیدی که به سوییچ متصل کنیم تغذیه نخواهد شد.
Primary Power Supply [W]	کاربر می‌تواند حداکثر توان اولیه کل سوییچ را تنظیم کند. تنظیمات پیش‌فرض ۲۵۰ وات است.
PoE Mode	این سوییچ از حالت ۸۰۲.۳af (PoE) و ۸۰۲.۳at (PoE +) پشتیبانی می‌کند. تنظیم پیش‌فرض ۸۰۲at است.
Priority	اولویت پورت PoE را مشخص کنید. اولویت از پایین به بالا کم ، زیاد ، خیلی زیاد است.
Maximum Power(W)	این برای تعیین حداکثر توان پورت است که کاربر کتابچه راهنمای PD ها به عنوان حالت تعیین قدرت ذخیره شده تنظیم می‌کند.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

۴.۲وضعیت PoE (PoE Status)

در این صفحه ، کاربر می‌تواند پس از کلیک بر روی " PoE Status" <"PoE"، وضعیت PoE همه درگاه‌ها را بررسی و بررسی کند.



Local Port	Description	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
2		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
3		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
4		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
5		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
6		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
7		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
8		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
9		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
10		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
11		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled

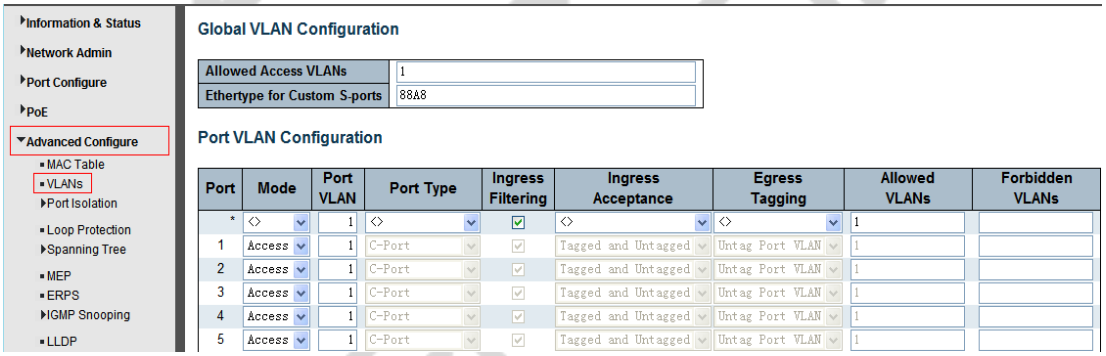
شکل ۴.۲ نمایش وضعیت POE همه‌ی پورت‌ها

۵. پیکربندی پیشرفته (Advanced Configure)

VLAN ۵.۱

LAN مجازی ((Virtual LANبه قسمت جدا و تقسیم شده در لایه Data Link شبکه کامپیوتری که باعث ایجاد چندین Broadcast Domain های مختلف می‌شود، گفته می‌شود. LAN مخفف Local Area Network به معنی شبکه محلی و Virtual یک حالت منطقی (Logic) بازسازی شده و جایگزین شده به‌جای یک قطعه فیزیکی در شبکه اشاره دارد. به عنوان مثال در یک مجموعه به دو شبکه نیاز است و می‌بایست برای این کار حداقل دو سوییچ تهیه نماییم (با در نظر گرفتن هزینه‌های جانبی). با استفاده از VLAN می‌توان به‌جای خرید دو سوییچ از یک سوییچ با قابلیت VLAN استفاده کرد و به‌صورت مجازی دو شبکه B و A ایجاد نمود که هر دستگاه متصل به شبکه یا در شبکه مجازی A قرار گیرد یا در شبکه مجازیB. قابلیت VLAN به‌صورت اعمال تگ‌ها بروی داده‌های شبکه و هدایت آنها بروی سیستم‌های شبکه عمل می‌کند؛ در عملکرد شبکه به‌صورت فیزیکی تغییری ایجاد نمی‌شود و فقط به‌صورت ارسال داده در شبکه‌های مجازی تفکیک شده ایفای نقش می‌کند. به این ترتیب، VLANها می‌توانند عملکردهای شبکه را با وجود وصل بودن به همان شبکه فیزیکی واحد (یعنی سوییچ) به‌صورت جدا از هم نگه دارند و نیاز به چندین دستگاه و کابل کشی اضافی را برطرف نمایند.

بر روی " "VLANs" <">Advanced Configureکلیک کنید تا صفحه پیکربندی VLAN ۸۰۲.۱Q را به‌صورت زیر مشاهده کنید



شکل ۵-۱ صفحه پیکربندی ویلن‌ها

توضیحات پیکربندی:

Object	توضیحات
Allowed VLANs	در اینجا شناسه VLAN ایجاد شده نمایش داده می‌شود. به طور پیش‌فرض ۱ است. اگر می‌خواهید VLAN جدید ایجاد کنید ، کافیست شناسه VLAN را در اینجا اضافه کنید.
Ether type for Custom S-ports	این قسمت (ether type / TPI) را مشخص می‌کند. هدر فریم‌های اترنت را برای ارتباط با لایه‌های بالاتر مشخص می‌کند که بر اساس هگزادسیمال مشخص شده است و برای درگاه‌های S سفارشی استفاده می‌شود. این تنظیم برای همه پورت‌هایی که نوع پورت آنها روی S-Custom-Port تنظیم شده است ، لازم الاجرا است.

Mode	در این بخش می‌توان مدهای Vlan را مشخص نمود که مد Access (پورتی که عضو Vlan می‌شود). مد Trunk (همه‌ی Vlan ها از آن عبور می‌کند و به همه‌ی Vlan ها دسترسی دارد و جز هیچ‌کدام از Vlan ها نیست. مد Hybrid که در این حالت به‌صورت مذاکره با طرف مقابل نوع Access یا Trunk انتخاب می‌شود.
Port VLAN	از این طریق می‌توان بین پورت‌های مختلف Vlan های متفاوتی ساخت و آنها را از یکدیگر تفکیک کرد. به‌صورت پیش‌فرض همه‌ی پورت‌ها عضو Vlan ۱ هستند و می‌توان از ۱ تا ۴۰۹۶، Vlan بر روی سوییچ تعریف کرد.
Port Type	پورت‌ها در حالت (ترکیبی) امکان تغییر نوع پورت را فراهم می‌کنند ، یعنی اینکه آیا از برچسب VLAN یک قاب برای طبقه‌بندی فریم در ورودی به یک VLAN خاص استفاده می‌شود یا خیر ، و در این صورت ، بر روی کدام TPID واکنش نشان می‌دهد. به همین ترتیب ، در حالت خروج ، در صورت نیاز به برچسب ، نوع ورودی TPID برچسب را تعیین می‌کند. **Unaware:** هنگام ورود ، همه فریم‌ها ، خواه دارای یک برچسب VLAN باشند یا نه ، در Port VLAN طبقه‌بندی می‌شوند و برچسب‌های احتمالی در خروج حذف نمی‌شوند. **C-Port:** اگر هنگام ورود، فریم‌های دارای برچسب VLAN با ۰x۸۱۰۰ = TPID در VLAN تعبیه شده طبقه‌بندی می‌شوند. اگر یک قاب برچسب گذاری نشده یا اولویت بندی شده باشد ، قاب به Port VLAN طبقه‌بندی می‌شود. اگر فریم‌ها باید در egress برچسب گذاری شوند ، آنها با برچسب C برچسب گذاری می‌شوند. **S-Port :** اگر هنگام ورود، فریم‌های دارای برچسب VLAN با ۰x۸۱۰۰ = TPID یا ۰x۸۸A۸ به شناسه VLAN تعبیه شده در برچسب طبقه‌بندی می‌شوند. اگر یک قاب برچسب گذاری نشده یا اولویت بندی شده باشد، قاب به Port VLAN طبقه‌بندی می‌شود. اگر فریم‌ها باید در egress برچسب گذاری شوند، آنها با برچسب S برچسب گذاری می‌شوند. **S-Custom-Port :** اگر هنگام ورود، فریم‌هایی با برچسب VLAN با ۰x۸۱۰۰ = TPID یا برابر با Ether type پیکربندی شده برای درگاه‌های S سفارشی، به شناسه VLAN تعبیه شده در برچسب طبقه‌بندی می‌شوند. اگر یک قاب برچسب گذاری نشده یا اولویت بندی شده باشد، قاب به Port VLAN طبقه‌بندی می‌شود. اگر فریم‌ها باید در egress برچسب گذاری شوند، با برچسب S سفارشی برچسب گذاری می‌شوند.
Ingress Filter	پورت‌های ترکیبی امکان تغییر فیلتر ورودی را فراهم می‌کنند. دسترسی و درگاه‌های Trunk همیشه فیلتر ورودی را فعال می‌کنند. اگر فیلتر کردن ورودی فعال باشد (کادر تأیید علامت گذاری شده است)، فریمهایی که به VLAN طبقه‌بندی شده‌اند و درگاه عضوی از آن نیستند، کنار گذاشته شوند. اگر فیلتر کردن ورودی غیرفعال باشد، فریم‌های طبقه‌بندی شده به VLAN که پورت عضو آن نیست، پذیرفته شده و به موتور سوییچ ارسال می‌شوند. با این حال، پورت هرگز فریم‌های طبقه‌بندی شده به VLAN را که عضو آن نیست، منتقل نخواهد کرد.
Ingress Acceptance	Hybridپورت امکان تغییر نوع فریم‌هایی را که هنگام ورود پذیرفته می‌شوند را می‌دهد . **Tagged and Untagged** فریم‌های بدون برچسب و با برچسب پذیرفته می‌شوند. **Tagged Only** فقط فریم‌های دارای برچسب در هنگام ورود پذیرفته می‌شوند. فریم‌های بدون برچسب کنار گذاشته می‌شوند. **Untagged Only** فقط فریم‌های بدون برچسب هنگام ورود پذیرفته می‌شوند و فریم‌های برچسب گذاری شده کنار گذاشته می‌شود.
Egress Tagging	پورت‌ها در حالت Trunk و Hybrid ممکن است برچسب گذاری قاب‌ها را در خروجی کنترل کنند. **Untag Port VLAN** فریم‌های طبقه‌بندی شده به Port VLAN بدون برچسب منتقل می‌شوند. سایر فریم‌ها با برچسب مربوطه منتقل می‌شوند. **Tag All** همه فریم‌ها ، چه به Port VLAN طبقه‌بندی شده باشند یا نه ، با برچسب منتقل می‌شوند.

	Untag All همه فریم‌ها ، چه به Port VLAN طبقه‌بندی شوند یا نه ، بدون برچسب منتقل می‌شوند. این گزینه فقط برای پورت‌ها در حالت Hybrid فعال است.
Allowed VLANs	پورت‌ها در حالت Trunk و Hybrid کنترل می‌کنند که کدام Vlan ها اجازه عضویت دارند. پورت‌های دسترسی یا Access فقط می‌توانند عضو یک VLAN باشند. به طور پیش‌فرض یک پورت Trunk یا Hybrid به دیتای تمام Vlan ها دسترسی دارد که به عنوان آپلینک از آن استفاده می‌شود.
Forbidden VLANs	پورت‌ها را می‌توان به نحوی برنامه‌ریزی نمود که هرگز به عضویت یک یا چندین Vlan خاص نگردند. این امر زمانی اهمیت پیدا می‌کند که شما از پروتکل‌های پویایی مانند MVRP، GVRP استفاده می‌کنید که سبب ارتباط بین Vlan های مختلف خواهد شد. با این قابلیت شما می‌تواند دیتای Vlan های که هرگز نباید با دیگر Vlan ها ارتباط برقرار کنند را در این لیست قرار دهید تا تضمین امنیت داده‌های شما برقرار باشد. این فیلد به‌صورت پیش‌فرض خالی است.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

۵.۲ ایزولاسیون پورت‌ها (Port Isolation)

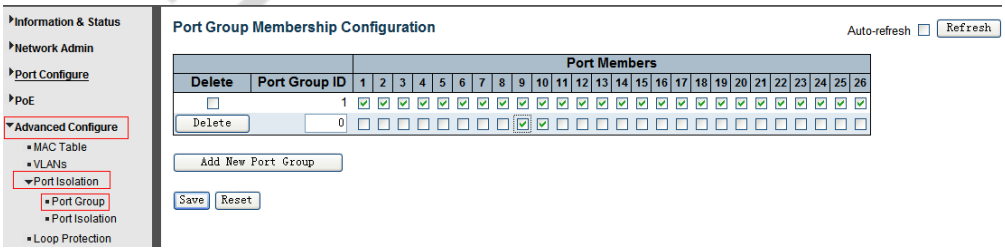
به جداسازی پورت برای محدود کردن داده‌ها بین پورت‌ها گویند که شبیه VLAN بوده اما به روشی سخت گیرانِ تر عمل می‌کند.

۵.۲.۱ گروه‌بندی پورت‌ها (Port Group)

به گروه‌بندی پورت‌های شبکه (Logical) ماشین‌های مجازی بر روی vSwitch می‌باشد تمامی ماشین‌های مجازی در داخلPort Group می‌توانند با ماشین‌های مجازی دیگر و یا ماشین‌های فیزیکی ارتباط داشته باشند.

نکته: یک پورت می‌تواند به چندین گروه تعلق داشته باشد و پورت‌های یک گروه به آسانی می‌توانند بایکدیدگر به تبادل داده بپردازند.

پس از کلیک روی "Port Group"> "Port Isolation"> "Advanced Configure"، صفحه زیر برای پیکربندی گروه‌بندی پورت‌ها ظاهر می‌شود.



شکل ۲-۵ صفحه گروه‌بندی پورت‌ها

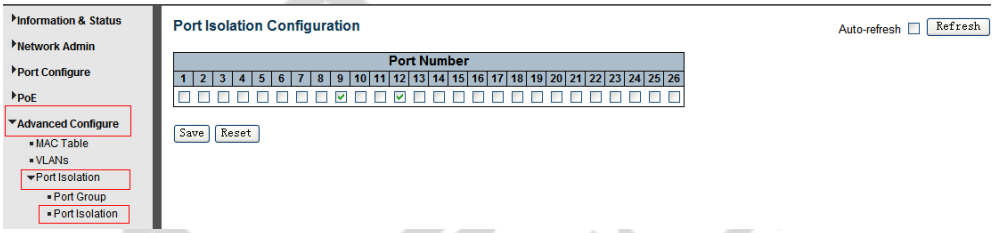
توضیحات پیکربندی:

Object	توضیحات
Port Members	کادر علامت را بزنید تا پورت‌ها به عنوان یک گروه انتخاب شوند

برای ایجاد گروه جدید بر روی "Add New Port Group" کلیک کرده و علامت شماره آن پورت را انتخاب کنید. و برای حذف گروه جدید ایجاد شده بر روی "Delete" کلیک کنید تا گروه جدید ایجاد شده حذف گردد.

Port Isolation ۵.۲.۲

پس از کلیک بر روی "Port Isolation"> "Port Isolation"> "Advanced Configure" ، سپس صفحه زیر برای پیکربندی جداسازی پورت ظاهر می‌شود.



شکل ۳-۵ صفحه پیکربندی ایزولاسیون پورت‌ها.

توضیحات پیکربندی:

Object	توضیحات
Port Number	برای تنظیم پورت مربوطه به عنوان "Port Isolation" کادر مشخص شده را علامت گذاری کرده تا آنها نتوانند جریان داده را ارسال کنند.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

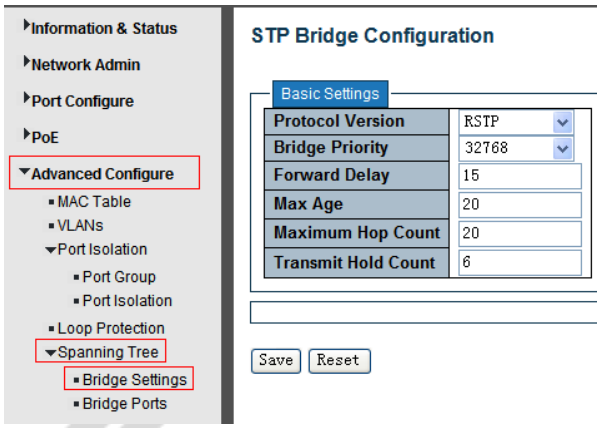
۵.۳پروتکل جلوگیری از حلقه در شبکه یا (STP)

هنگامی‌که در شبکه چندین سوییچ را به هم وصل می‌کنید، ممکن است شبکه کند و سپس مختل شود. علت این اختلال به وجود آمدن حلقه (Loop) در شبکه است. به‌صورت ساده‌تر هر سوییچ به سوییچ‌های متصل به خود، اطلاعات دریافتی خود را ارسال می‌کند و سوییچ‌های دیگر نیز اطلاعات دریافتی را برای همه سوییچ‌های متصل دیگر ارسال می‌کنند و این داستان تا بی‌نهایت ادامه دارد. در حقیقت اطلاعات دریافتی سوییچ‌ها مانند طوفانی با سرعت زیاد بین یکدیگر مبادله می‌شود تا شبکه درنهایت مختل شده و از کار میافتد. پروتکل STP به منظور جلوگیری از ایجاد Loop های لایه ۲ ای به دنیای شبکه معرفی شد. پروتکل STP از مکانیزم های هوشمندانه برای جلوگیری از ایجاد Loopاز طریق مسدود کردن لینک‌های پشتیبان استفاده می‌کند .

STP Bridge Settings ۵.۳.۱

این صفحه به شما امکان می‌دهد تنظیمات پورت STP را پیکربندی کنید.

پس از کلیک روی "Bridge Settings"> "Spanning Tree"> "Advanced Configure"، صفحه زیر ظاهر می‌شود.



شکل ۴-۵ صفحه پیکربندی پورت STP

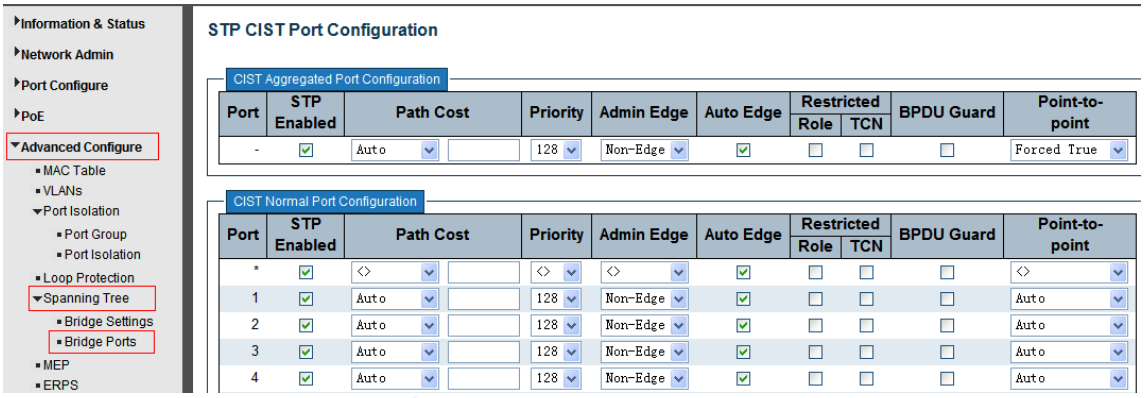
توضیحات پیکربندی:

Object	توضیحات
Protocol Version	برای انتخاب نسخه پروتکل STP روی منوی کشویی کلیک کنید ، که دارای موارد زیر است: - STPپروتکل جلوگیری از حلقه (IEEE۸۰۲.۱D) ؛ - RSTPپروتکل جلوگیری از حلقه سریع (IEEE۸۰۲.۱w)
Bridge Priority	اولویت Bridge را کنترل می‌کند. سوییچی که دارای کمترین Bridge ID باشد به عنوانRoot Bridge انتخاب می‌شود. Port Priority متغیر ۸ بیتی است که بین ۰ تا ۲۵۵ مقداردهی می‌شود و مقدار پیش‌فرض آن ۱۲۸ است.
Forward Delay (۴-۳۰)	دامنه تنظیم Forward Delay از ۴ تا ۳۰ ثانیه است. مقدار پیش‌فرض ۱۵ ثانیه است.
Max Age (۶-۴۰)	حداکثر زمانی که سوییچ صبر می‌کند تا از تغییرات توپولوژی شبکه مطمئن شود که به‌صورت پیش‌فرض ۲۰ ثانیه است
Maximum Hop Count (۶-۴۰)	تعیین کننده آن است که بسته اطلاعاتی BPDU ها از چه تعداد Hop یا همان تعداد Root های که می‌تواند از آن عبور کند و به مقصد برسد. در غیر این صورت بسته BPDU دور انداخته شود. که از ۶ تا ۴۰ Hop می‌توان انتخاب کرد.
Transmit Hold Count (۱-۱۰)	تعداد بسته‌های BPDU های که Bridge port می‌تواند در هر ثانیه ارسال کند قابل تغییر است. اگر حجم این بسته‌ها در یک بازه‌ی زمانی بیشتر از حد مجاز باشند، بسته بعدی BPDU با تأخیر ارسال خواهد شد. مقدار بسته‌های ارسالی از ۱ تا ۱۰ قابل تنظیم است .

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

STP Bridge Port ۵.۳.۲

پس از کلیک روی "Bridge Ports" >"Spanning Tree"> "Advanced Configure" ، صفحه زیر را مشاهده می‌کنید.



شکل ۵-۵ صفحه پیکربندی پروتکلSTP

توضیح پیکربندی:

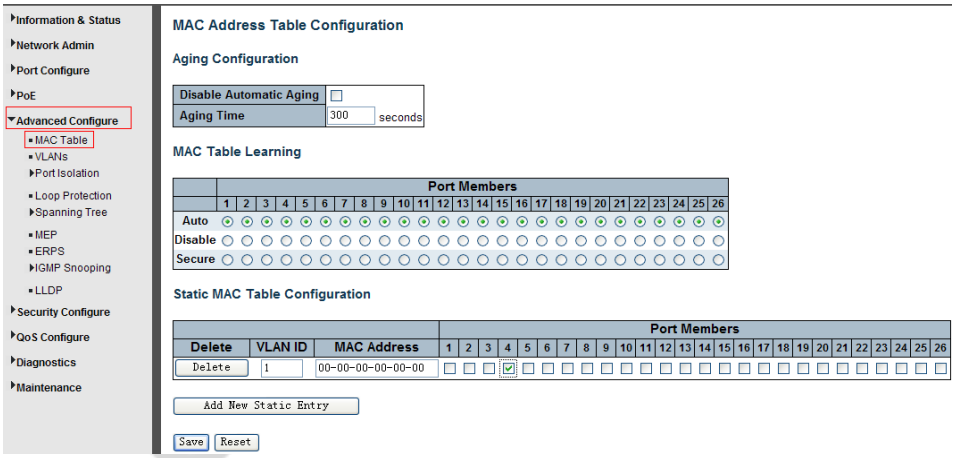
Object	توضیحات
STP Enabled	بر روی کادر مشخص شده کلیک کرده و علامت گذاری کنید تا عملکرد پروتکل STP فعال گردد.
Path Cost(۰=Auto) Path Cost(۰=Auto)	مسیر Cost متحمل شده هر پورت را کنترل می‌کند Auto: تنظیم خودکار Costمسیر با بهره‌گیری از پروتکل IEEE۸۰۲.۱D که با توجه به سرعت پورت، بهترین مسیر را انتخاب می‌کند. Specific: با استفاده از این تنظیمات می‌توان مقادیر دلخواه توسط کاربر وارد شود.
Priority	اولویت پورت را کنترل می‌کند. این می‌تواند برای کنترل اولویت پورت‌هایی که Cost های یکسانی دارند، استفاده شود. (هرچه کمتر اولویت بالاتر)
Auto Edge	برای تنظیم پورت مربوطه به عنوان Auto Edge کادر را علامت بزنید.
Restricted Role	برای تنظیم پورت مربوطه به عنوان نقش Restricted ، کادر را علامت بزنید
Restricted TCN	برای تنظیم پورت مربوطه به عنوان Restricted TCN، کادر را علامت بزنید
BPDU Guide	برای فعال کردن راهنمای BPDU کادر مشخص شده را علامت بزنید. بنابراین وقتی پورتی بسته BPDU را دریافت می‌کند ، به وضعیت Disable (Shut Down) تغییر وضعیت می‌دهد.
Point-to-point	به‌صورت خودکار کنترل می‌کند که پورت به‌صورت مستقیم به یک شبکه (Point-to-Point) وصل است یا یک رسانه مشترک. انتخاب حالت Forwarding در اتصال به شبکه Point-to-Point سریع‌تر از رسانه مشترک است.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

توجه: Hop Count به معنی تعداد روترهایی است که یک داده بایستی از آنها عبور کند تا به شبکه مقصد برسد ، یا به بیان دیگر Hop Count به تعداد روترهايي گفته می‌شود که داده ما باشد از شبکه مبدأ تا شبکه مقصد از آنها عبور کند. اگر مقدار cost یک interface پایین باشد به معنای بالا بودن سرعت و اگر مقدار cost یک interface بالا باشد به معنای پایین بودن سرعت آن interface است. برای مثال cost یک لینک WAN که ۱ مگابیت بر ثانیه است از cost یک لینک WAN با سرعت ۸ مگابیت بر ثانیه بالاتر است.

۵.۴ جدول MAC Address(MAC Address Table)

این صفحه به شما امکان می‌دهد تنظیمات جدول آدرس Mac را پیکربندی کنید. بعد از کلیک روی "Mac Table"> "Advanced Configure"، صفحه زیر را مشاهده خواهید کرد.



شکل ۶-۵ صفحه پیکربندی جدول شناسه سخت‌افزاری

توضیحات پیکربندی:

Object	توضیحات
Disable Automatic Aging	اگر کادر علامت گذاری شده باشد، عملکرد automatic aging غیرفعال است.
Aging Time	مقدار زمانی که بعد از آن یک ورودی از بین می‌رود. دامنه ۱۰ ۱۰۰۰۰۰۰ ثانیه؛ پیش‌فرض: ۳۰۰ ثانیه
MAC Table Learning	این سوییچ از ۳ نوع برای یادگیری جدول MAC پشتیبانی می‌کند ۱. خودکار: پورت به طور خودکار آدرس مک را فرا می‌گیرد. ۲. غیرفعال: در این حالت شناسه سخت‌افزاری را فرا نمی‌گیرد. ۳. پایدار: فقط انتقال داده‌های شناسه سخت افزا استاتیک پیکربندی شده را انجام می‌دهید.
Static MAC Table Configuration	ورودی‌های ثابت در جدول شناسه سخت‌افزاری در این جدول نشان داده‌شده است. برای ایجاد رکورد جدید، Add "New Static Entry" را کلیک کنید.

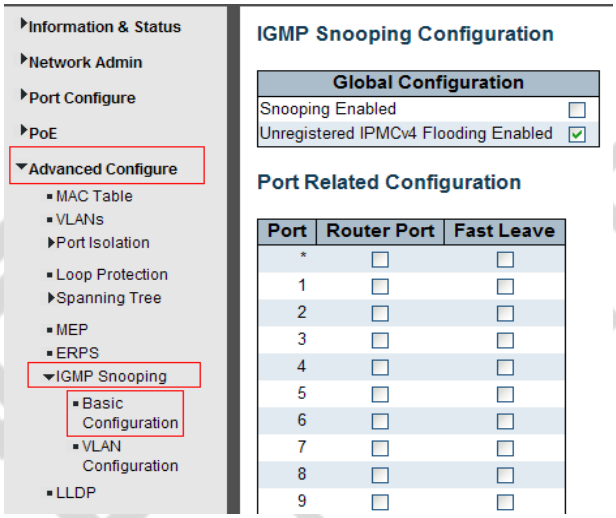
پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

۵.۵ IGMP Snooping

پروتکل مدیریت گروه اینترنت (IGMP) به میزبان و روترها امکان می‌دهد اطلاعات مربوط به عضویت در گروه‌های چندپخشی را به اشتراک بگذارند. (IGMP snooping) یک ویژگی سوییچ است که تبادل پیام‌های IGMP را کنترل می‌کند و آنها را برای پردازش ویژگی در CPU کپی می‌کند. هدف کلی IGMP Snooping محدود کردن بازار سال فریم‌های چندپخشی فقط به درگاه‌هایی است که عضوی از گروه چندپخشی هستند.

۵.۵.۱پیکربندی پایه(Basic Configuration)

پس از کلیک به روی "Basic Configuration" > "IGMP Snooping" > "Advanced Configure"، صفحه زیر ظاهر می‌شود.



شکل ۷-۵ پیکربندی پایه پروتکل مدیریت گروه اینترنتی

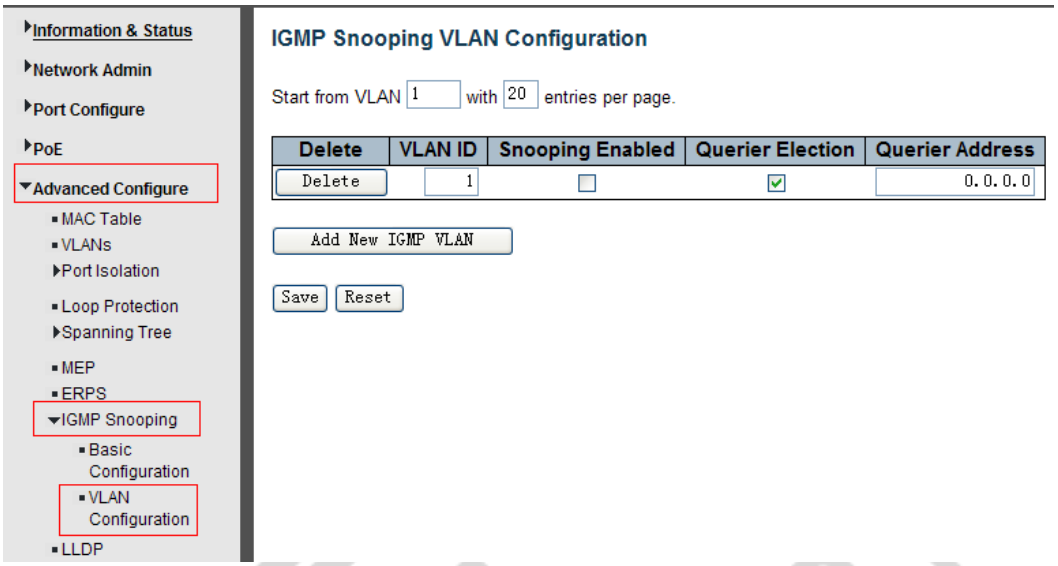
توضیحات پیکربندی:

Object	توضیحات
Snooping Enabled	فعال و غیرفعال کردن تجسس مدیریت گروه اینترنتی .مقدار پیش‌فرض "Disabled" Enable: علامت بزنید؛ Disabled: علامت نزنید.
Unregistered IPMCv۴ Flooding Enabled	برای فعال کردن بارگیری IPMCv۴ ثبت نشده، کادر را علامت بزنید.
Router Port	مشخص کنید کدام پورت‌ها به عنوان پورت‌های روتر عمل می‌کنند. پورت روتر پورتی است که روی سوییچ اترنت است که به سمت دستگاه چندپخشی لایه ۳ یا پرسشگر IGMP هدایت می‌شود. اگر پورت عضو تجمع به عنوان پورت روتر انتخاب شود، کل تجمع به عنوان یک پورت روتر عمل می‌کند.
Fast Leave	خروج سریع هنگام دریافت پیام برای ثبت‌نام گروه، حذف ورودی هدایت شده شناسه سخت‌افزاری را فوراً انجام می‌دهد.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

۵.۵.۲پیکربندی IGMP Snooping VLAN

پس از کلیک روی"VLAN Configuration"><"IGMP Snooping"><"Advanced Configure" ، صفحه زیر ظاهر می‌شود.



شکل۷-۵ پیکربندی تجسس مدیریت گروهی اینترنتی VLAN

توضیحات پیکربندی:

Object	توضیحات
Snooping Enabled	فعال کردنVLAN IGMP Snooping. حداکثر تا ۳۲ VLAN را می‌توان در پروتکل IGMP Snooping فعال کرد
Querier Election	فعال کردن برای پیوستن به انتخابات پرسش و پاسخ IGMP در.VLAN غیرفعال کردن به عنوان یک IGMP غیر پرسشگر.
Querier Address	آدرس IPv۴ را به عنوان آدرس منبع استفاده شده در سرآیند IP برای انتخاب پرسشنامه IGMP تعریف کنید. وقتی آدرس پرسشگر تنظیم نشده باشد، سیستم از آدرس مدیریت IPv۴ رابط IP مرتبط با این VLAN استفاده می‌کند. وقتی آدرس مدیریت IPv۴ تنظیم نشده باشد، سیستم از اولین آدرس مدیریت IPv۴ موجود استفاده می‌کند. در غیر این صورت، سیستم از یک مقدار از پیش تعریف شده استفاده می‌کند. به طور پیش‌فرض، این مقدار ۱۹۲.۰.۲.۱ خواهد بود.

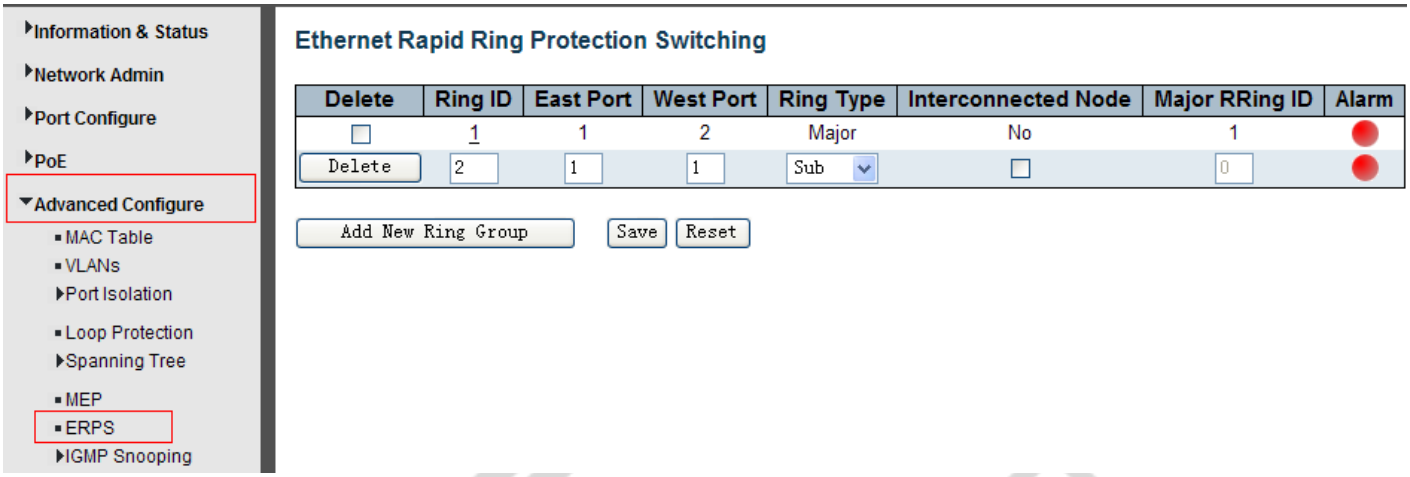
پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

ERPS ۵.۶

(Ethernet Ring Protection Switching) ERPS، عملکرد OAM و پروتکل APS را ادغام می‌کند. اگر شبکه حلقه‌ای به طور تصادفی قطع شود ، زمان بازیابی خطا می‌تواند کمتر از ۵۰ میلی ثانیه باشد تا شبکه به سرعت به حالت عادی برگردد. ITU-T G.۸۰۳۲ اولین استاندارد صنعتی برای ERPS است.

توجه: قبل از فعال کردن ERPS ، STP رینگ پورت باید غیرفعال شود.

پس از کلیک روی "ERPS" <"Advanced Configure" ، صفحه زیر ظاهر می‌شود.



شکل ۵-۸ پیکربندی EPRS

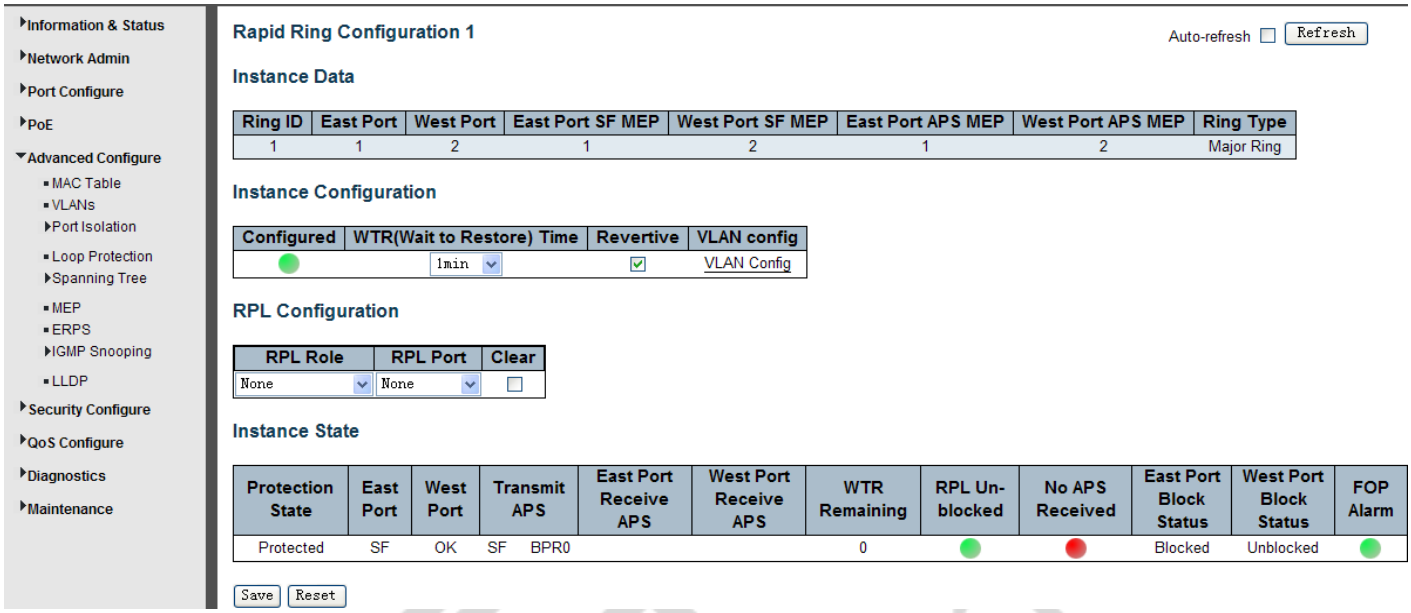
توضیحات پیکربندی:

Object	توضیحات
Ring ID	نمایش اطلاعات ERPS Ring
East Port	تعداد درگاهی که در این محافظت از Ring شرکت می‌کنند.
West Port	تعداد پورت‌های دیگری که در این محافظت از Ring شرکت می‌کنند.
Ring Type	انتخاب موجود: "Major Ring" یا "Sub Ring" فقط در صورت استفاده از چند حلقه ، "Sub Ring" برای پیکربندی مورد نیاز است. نوع حلقه پیش‌فرض: "Major Ring" فقط در صورت وجود برنامه چند حلقه‌ای ، لازم است تنظیم شود.
Interconnected Node	در برنامه Multi Ring ، گره متقابل گره‌ای است که ۲ یا چند حلقه را به هم متصل می‌کند.
Major Ring ID	در برنامه Single Ring، Major Ring ID همان شناسه Ring است. در برنامه Multi Ring، Sub Ring باید به عنوان Major Ring ID باشد.
R-APS VLAN(۱-۴۰۹۴)	VLANرا برای R-APS VLAN تعریف کنید.

برای ایجاد برنامه جدید حلقه ERPS ، روی "Add New Ring Group" کلیک کنید.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

بعد از کلیک روی شماره زیر "Ring ID" ، همانند صفحه زیر به صفحه تنظیمات Ring می‌رود:



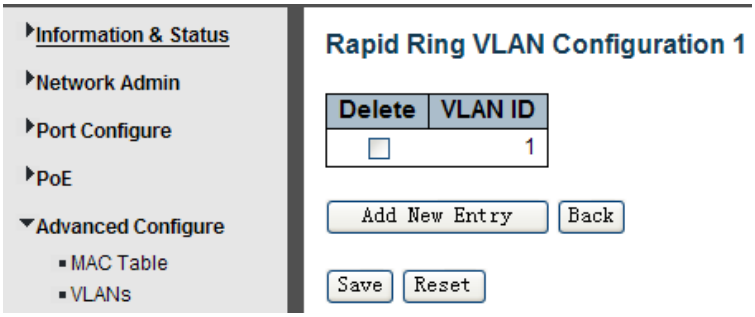
شکل ۵-۹ پیکربندی حلقه EPRS

توضیحات پیکربندی:

Object	توضیحات
WTR(Wait to Restore) Time(۱-۱۲)	برای انتخاب زمان WTR برای R-APS روی منوی کشویی کلیک کنید. انتخاب موجود: ۱-۱۲ دقیقه پیش‌فرض: ۱ دقیقه
Revertive	برای فعال کردن وضعیت بازگشتی R-APS علامت بزنید.
VLAN config	پس از کلیک بر روی "VLAN config" ، به صفحه پیکربندی Rapid Ring VLAN می‌روید.
RPL Role	برای انتخاب نقش " None"، "RPL Owner" یا "RPL Neighbor" روی منوی کشویی کلیک کنید.
RPL Port	برای انتخاب "None"، "East Port" یا "West Port"روی منوی کشویی کلیک کنید.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

پس از کلیک روی "VLAN config" ، به صفحه زیر هدایت می‌شوید:



شکل ۵-۱۰ پیکربندی سریع حلقه VLAN

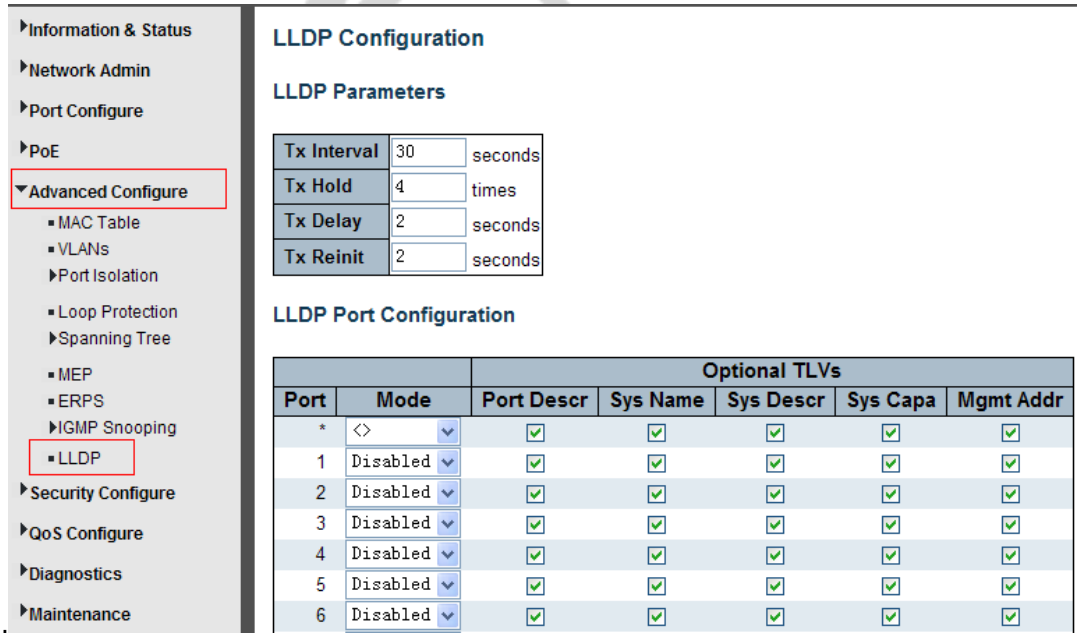
برای ایجاد ورودی جدید ، روی "Add New Entry" کلیک کنید.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

LLPD ۵.۷

پروتکل کشف لایه Link (LLDP) برای کشف اطلاعات اساسی در مورد دستگاه‌های همسایه در دامنه پخش محلی استفاده می‌شود. LLDP یک پروتکل لایه ۲ است که از پخش دوره‌ای برای انتشار اطلاعات مربوط به دستگاه ارسال کننده استفاده می‌کند. اطلاعات منتشر شده با توجه به استانداردIEEE۸۰۲.۱ab در قالب Type Length Value (TLV) نمایش داده می‌شود و می‌تواند شامل جزئیاتی مانند شناسایی دستگاه ، قابلیت‌ها و تنظیمات پیکربندی باشد. LLDP همچنین نحوه ذخیره و نگهداری اطلاعات جمع‌آوری شده در مورد گره‌های شبکه همسایه را که کشف می‌کند ، تعریف می‌کند.

پس از کلیک روی "LLDP"> "Advanced Configure" ، صفحه دنبال شده ظاهر می‌شود



شکل ۵-۱۰ صفحه پیکربندی LLDP

توضیحات پیکربندی:

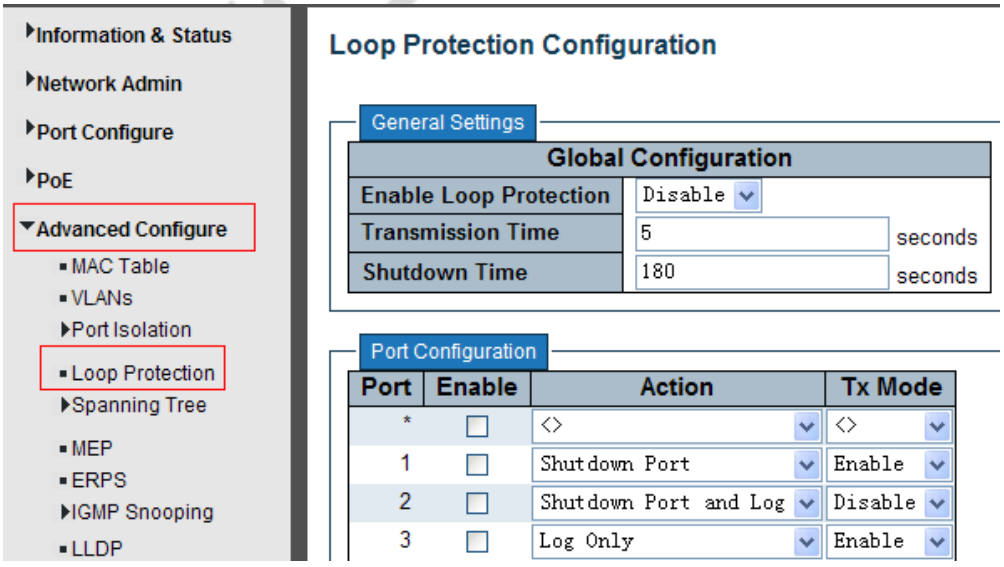
Object	توضیحات
LLDP Parameters	در اینجا به کاربر اجازه می‌دهد تنظیمات فعلی پورت LLDP را بازرسی و پیکربندی کند: ➢ Tx Interval : فاصله زمانی انتقال ➢ Tx Hold : نگه‌داشتن ضریب زمانی ➢ Tx Delay : انتقال Delay ➢ Tx Remit : انتقال Remit time
Mode	پیام‌های LLDP حالت‌های انتقال و دریافت را برای واحدهای داده پروتکل LLDP انتخاب کنید. گزینه‌ها فقط Tx only، Rx only ، Enabled و Disabled هستند.
Optional TLVs	برای پیکربندی اطلاعات مندرج در حوزه TLV پیغام‌های آگهی شده. هنگامی‌که گزینه مورد نظر بررسی می‌شود، اطلاعات مربوطه در اطلاعات LLDP گنجانده خواهد شد. ➢ Port Descr: توضیحات پورت ➢ Sys Name: نام سیستم ➢ Sys Descr: توضیحات سیستم ➢ Sys Capa: قابلیت سیستم ➢ Mgmt Addr: آدرس مدیریت

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

۵.۸محافظت از حلقه (Loop Protection)

محافظت از حلقه برای جلوگیری از پخش حلقه‌ها است.

پس از کلیک روی "Loop protection" > "Advanced Configure" ، صفحه زیر ظاهر می‌شود.



شکل ۵-۱۱ صفحه پیکربندی محافظت از حلقه

توضیحات پیکربندی:

Object	توضیحات
Global Configuration	Enable Loop Protection :برای غیرفعال یا فعال کردن محافظت از حلقه، روی منوی کشویی کلیک کنید. Transmission Time : یک عدد وارد کنید تا به عنوان زمان فاصله محافظت از حلقه تنظیم شود. Shutdown Time: برای تنظیم زمان خاموش کردن پورت، یک عدد وارد کنید.
Enable	علامت بزنید تا محافظت از حلقه پورت مربوطه فعال شود.
Action	وقتی پورت حلقه را شناسایی کرد، عملیات آغاز می‌شود. ۳ نوع عملکرد برای انتخاب وجود دارد، Shutdown port / Shutdown port / Log / Log Only
Tx Mode	برای فعال و غیرفعال کردن حالت Tx

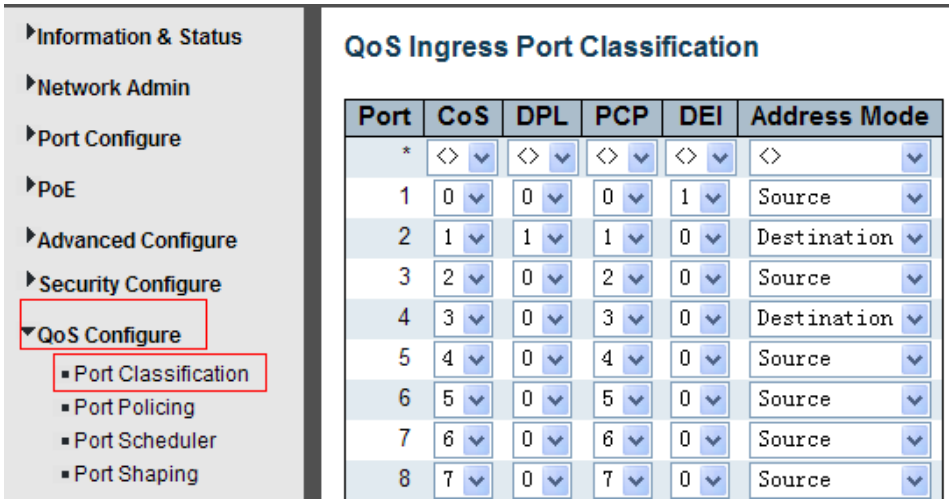
پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

۶. QoS Configure

Quality of Service (QoS) یکی از ویژگی‌های پیشرفته اولویت بندی ترافیک است که به شما امکان می‌دهد ترافیک شبکه را کنترل کنید. QoS شما را قادر می‌سازد درجه‌های مختلفی از خدمات شبکه را به انواع مختلف ترافیک ، مانند ترافیک چندرسانه‌ای ، ویدئویی ، ویژه پروتکل ، زمان حساس و پشتیبان گیری از پرونده اختصاص دهید. این قابلیت نه‌تنها می‌تواند پهنای باند را ذخیره کند ، بلکه ترافیک دیگری را که چندان مهم نیستند نیز محدود می‌کند.

۶.۱ QoS Port Classification

پس از کلیک روی "Port Classification" > "QoS Configure"، صفحه زیر ظاهر می‌شود.



شکل ۶-۱ صفحه پیکربندی طبقه‌بندی پورت‌ها

توضیحات پیکربندی:

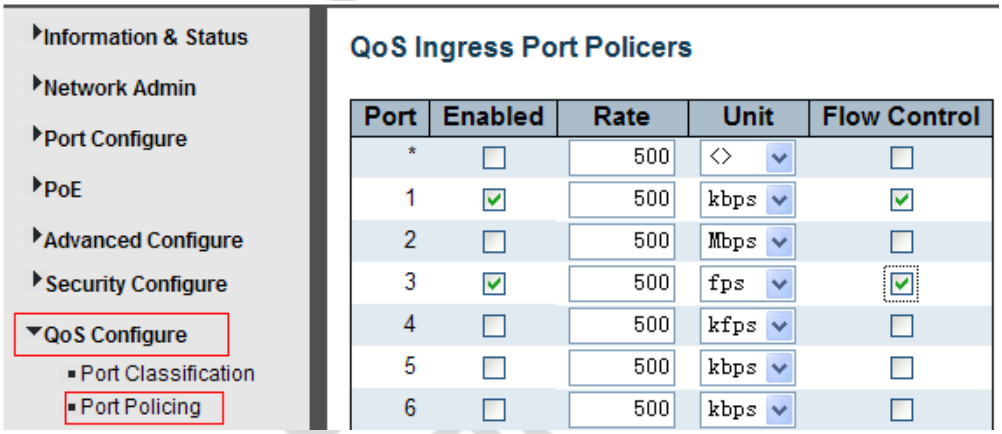
Object	توضیحات
CoS	کلاس پیش‌فرض سرویس را کنترل می‌کند، از ۰ (کمترین) تا ۷ (بالاترین). همه فریم‌ها به CoS طبقه‌بندی می‌شوند. بین CoS ، صف و اولویت نقشه برداری یک به یک وجود دارد ۰ CoS (صفر) کمترین اولویت را دارد. CoSطبقه‌بندی شده را می‌توان با یک ورودی QCL لغو کرد. توجه: اگر CoS پیش‌فرض به‌صورت پویا تغییر کرده باشد، CoS پیش‌فرض واقعی پس از CoS پیش‌فرض پیکربندی شده در پرانتز نشان داده می‌شود.
DPL	سطح تقدم پیش‌فرض را کنترل می‌کند. همه فریم‌ها به یک سطح تقدم طبقه‌بندی می‌شوند. DPLطبقه‌بندی شده را می‌توان با یک ورودی QCL لغو کرد.
PCP	مقدار PCP پیش‌فرض را کنترل می‌کند. همه فریم‌ها به مقدار PCP طبقه‌بندی می‌شوند. اگر پورت عضو Vlan باشد و فریم برچسب گذاری شود ، آنگاه فریم به مقدارPCP بر اساس برچسب طبقه‌بندی می‌شود. در غیر این صورت فریم بر اساس مقدار پیش‌فرض PCP طبقه‌بندی می‌شود.
DEI	مقدار پیش‌فرض DEI را کنترل می‌کند. همه فریم‌ها بر اساس مقدار DEI طبقه‌بندی می‌شوند. اگر پورت عضو VLAN باشد و فریم برچسب گذاری شود ، آنگاه فریم به مقدار DEI بر اساس برچسب طبقه‌بندی می‌شود. در غیر این صورت فریم به مقدار پیش‌فرض DEI طبقه‌بندی می‌شود.

Address Mode	حالت آدرس IP/MAC مشخص می‌کند که طبقه‌بندی QCL باید بر اساس آدرس منبع (SMAC / SIP) یا مقصد (DMAC / DIP) در این پورت انجام شود. مقادیر مجاز عبارت‌اند از: Source: مطابقت SMAC / SIP را فعال کنید. Destination: مطابقت DMAC / DIP را فعال کنید.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

Port Policing ۶.۲

پس از کلیک روی "Port Polcing" < "QoS Configure" ، صفحه‌ای که در ادامه مشاهده می‌کنید ظاهر می‌شود.



شکل ۶-۲ صفحه پیکربندی Port Policing

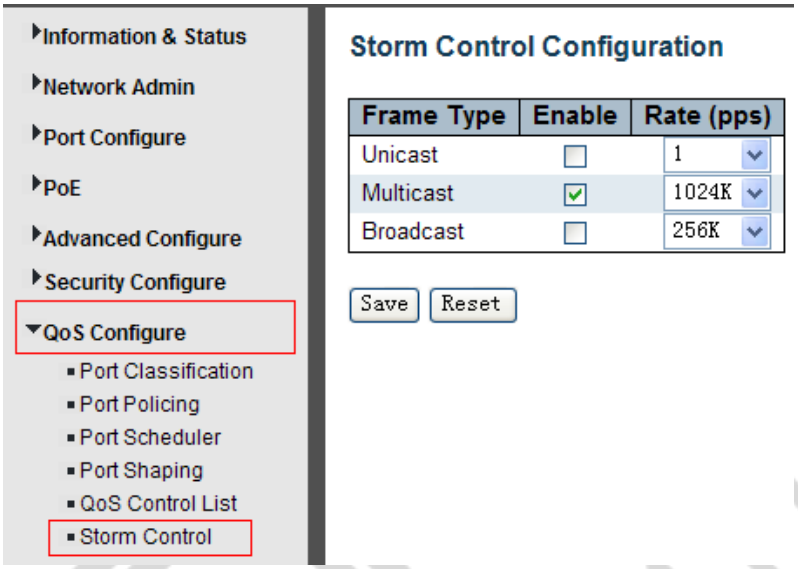
توضیحات پیکربندی:

Object	توضیحات
Enabled	، برای فعال سازی این Port Policing قسمت را تیک بزنید.
Rate	نرخ را برای policer کنترل می‌کند. مقدار پیش‌فرض ۵۰۰ است. هنگامی‌که " "kbps" "Unitیا " "fpsباشد ، این مقدار به ۱۰۰-۱۰۰۰۰۰۰ محدود می‌شود و وقتی " "Mbps" "Unitیا " "kfps باشد ، به ۱-۳۳۰۰ محدود می‌شود.
Unit	واحد اندازه گیری Policer Rate را به‌صورت Kbps ، Mbps، fps یا Kfps کنترل می‌کند. مقدار پیش‌فرض "kbps" است.
Flow Control	اگر کنترل جریان فعال باشد و پورت در حالت کنترل جریان باشد، به‌جای دور انداختن فریم‌ها، فریم‌های مکث ارسال می‌شوند.

برای ذخیره تنظیمات روی "Save" کلیک کنید.

Storm Control Configuration ۶.۳

پس از کلیک روی "Storm Control" <"QoS Configure" ، صفحه زیر ظاهر می‌شود.



شکل ۶-۳ صفحه پیکربندی Storm Control

توضیحات پیکربندی:

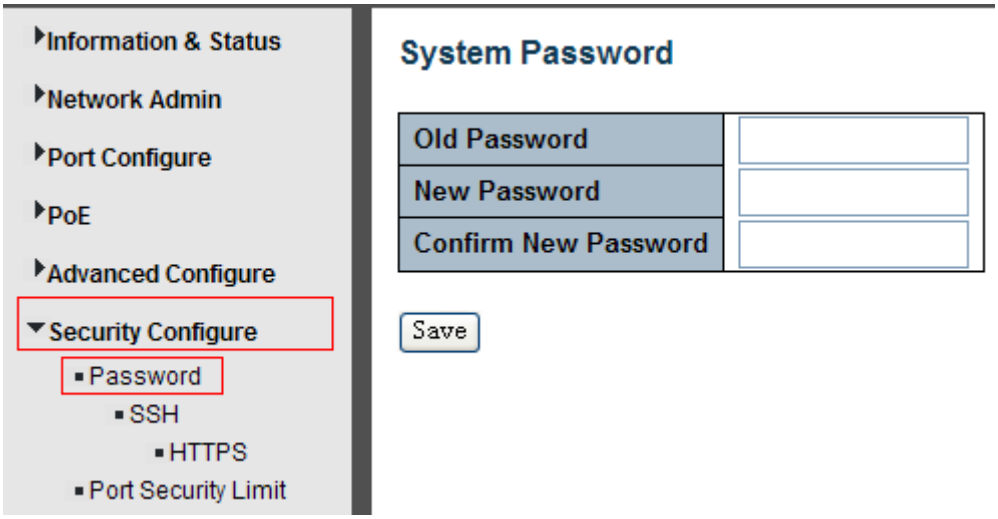
Object	توضیحات
Frame Type	این سوییچ از ۳ نوع Frame Type پشتیبانی می‌کند: Unicast ، Unknown Multicast و Broadcast.
Enable	تیک بزنید Storm Control برای فعال‌سازی.
Rate(pps)	واحد نرخ بسته‌های ثانیه (pps) است. مقادیر معتبر عبارت‌اند از: ۱ ، ۲ ، ۴ ، ۸ ، ۱۶ ، ۳۲ ، ۶۴ ، ۱۲۸ ، ۲۵۶ ، ۵۱۲ ، ۱K ، ۲K ، ۴K ، ۸K ، ۱۶K ، ۳۲K ، ۶۴K ، ۱۲۸K ، ۲۵۶K ، ۵۱۲K یا ۱۰۲۴K و...

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

Security Configure.۷

Password۷.۱

برای تغییر رمز ورود به سیستم سوییچ ، لطفاً روی "Password" > "Security Configure" کلیک کنید.



شکل ۷-۱ صفحه پیکربندی گذرواژه سیستم

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

۸۰۲.۱X ۷.۲

در دنیای ۸۰۲.۱X، کاربر Supplicant خوانده می‌شود، سوییچ، Authenticator و سرورRADIUS authentication server است. سوییچ به عنوان Man-in-the-middle عمل می‌کند ، درخواست‌ها و پاسخ‌ها را بین درخواست کننده و سرور احراز هویت هدایت می‌کند. فریم‌های ارسال شده بین درخواست کننده و سوییچ فریم‌های ویژه ۸۰۲.۱X است که به فریم‌های EAPOL (EAP over LANs) معروف است، فریم‌های EAPOL EU (RFC۳۷۴۸) PDUs را محصور می‌کند. فریم‌های ارسال شده بین سوییچ و سرورRADIUS، بسته‌های RADIUS هستند.

بسته‌های RADIUS همچنین EU PDU ها را به همراه سایر ویژگی‌های مانند آدرس IP سوییچ ، نام و شماره درگاه درخواست کننده روی سوییچ محصور می‌کند .EAP بسیار انعطاف‌پذیر است ، به این دلیل که روش‌های مختلف احراز هویت مانند MD۵-Challenge ، PEAP و TLS را امکان پذیر می‌کند. نکته مهم این است که احراز هویت (سوییچ) نیازی به دانستن اینکه متقاضی و سرور احراز هویت از کدام روش احراز هویت استفاده می‌کنند و یا چند فریم تبادل اطلاعات برای یک روش خاص مورد نیاز است ندارد. سوییچ به راحتی قسمت EAPفریم را در نوع مربوطه (EAPOL یا RADIUS) کپسولِ می‌کند و آن را به جلو هدایت می‌کند.

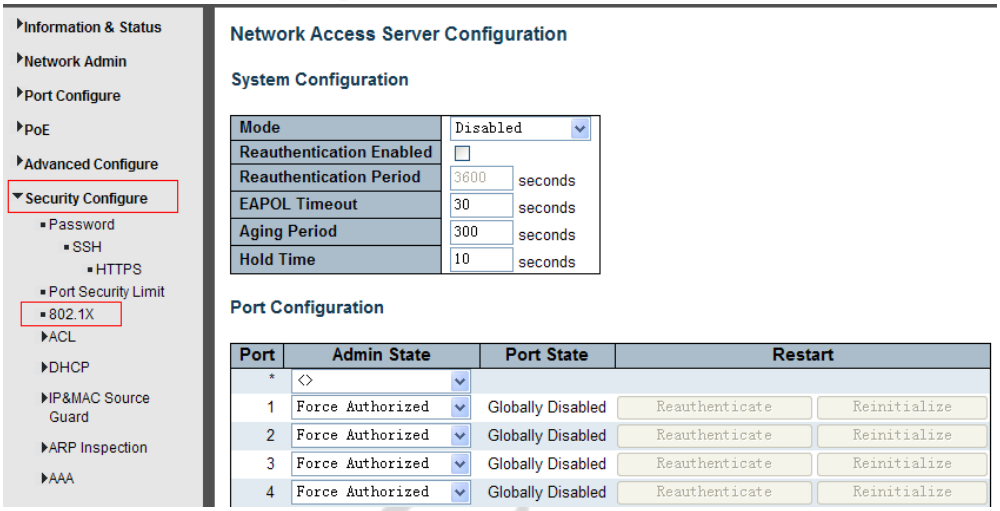
هنگامی‌که احراز هویت کامل شد ، سرور RADIUS بسته ویژه‌ای را ارسال می‌کند که حاوی نشانه موفقیت یا شکست است. سوییچ علاوه بر اینکه این تصمیم را به Supplicant ارسال می‌کند ، از آن برای باز کردن یا مسدود کردن ترافیک درگاه سوییچ متصل به Supplicant استفاده می‌کند.

استاندارد IEEE ۸۰۲.۱X یک پروتکل کنترل دسترسی و تأیید اعتبار مبتنی بر سرور را تعریف می‌کند که اتصال کلاینت‌های غیرمجاز را به اینترنت از طریق پورت‌های قابل دسترسی عمومی محدود می‌کند. سرور احراز هویت هر کلاینت متصل به پورت سوییچ را تأیید می‌کند قبل از اینکه خدمات ارائه شده توسط سوییچ یا LAN را ارائه دهد.

تا زمانی که کلاینت احراز هویت نشود ، کنترل دسترسی ۸۰۲.۱X فقط پروتکل احراز هویت قابل توسعه را از طریق ترافیک LAN (EAPOL) از طریق پورتی که کلاینت به آن متصل است ، مجاز می‌داند. پس از موفقیت در احراز هویت ، ترافیک عادی می‌تواند از طریق پورت عبور کند.

این سوییچ از احراز هویت مبتنی بر پورت ۸۰۲.۱X پشتیبانی می‌کند. در این صفحه ، کاربر می‌تواند ۸۰۲/۱ Xرا پیکربندی کند.

پس از کلیک روی "۸۰۲.۱X" > "Security Configure" ، صفحه‌ای که در ادامه مشاهده می‌کنید ظاهر می‌شود.



شکل ۲-۷ صفحه پیکربندی ۸۰۲.۱X

شرح پیکربندی:

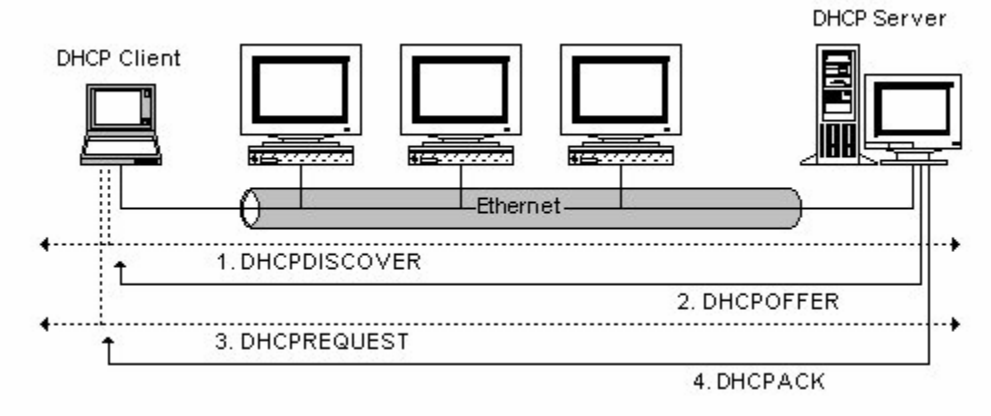
Object	توضیحات
System Configuration	در اینجا ، کاربر می‌تواند ۸۰۲.۱X یا احراز هویت مجدد را فعال یا غیرفعال کند ، همچنین Reauthentication Period / EAPOL Timeout / Aging Period / Hold Time را تنظیم کند
Port Configuration	برای انتخاب حالت مدیریت، روی منوی کشویی کلیک کنید. گزینه‌های موجود Mac based Auth. ، ۸۰۲.۱X ،Force Unauthorized ، Force Authorized

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

DHCP Snooping۷.۳

DHCP Overview۷.۳.۱

پروتکل DHCP به طور گسترده‌ای برای اختصاص پویا منابع شبکه قابل استفاده مجدد، مانند آدرس IP استفاده می‌شود. روند معمول DHCP برای به دست آوردن IP به شرح زیر است:



سرویس گیرنده DHCP پیام DISCOVER را به سرور DHCP ارسال می‌کند، اگر سرویس گیرنده در مدت زمان کوتاهی پاسخ را از سرور دریافت نکند، پیام DHCP DISCOVER مجدداً ارسال خواهد شد.

پس از دریافت پیام DHCP DISCOVER ، سرور DHCP منابع (برای مثال آدرس IP) را به سرویس گیرنده اختصاص می‌دهد و سپس پیام DHCP OFER را به سرویس گیرنده DHCP ارسال می‌کند.

بعد از دریافت پیامDHCP OFER ، سرویس گیرنده DHCP درخواست اجاره سرور را برای DHCP ارسال می‌کند و به سایر سرورها اطلاع می‌دهد که این سرور را برای اختصاص آدرس‌ها پذیرفته است.

پس از دریافت درخواستDHCP ، سرور بررسی خواهد کرد که آیا می‌توان منبعی را تخصیص داد یا خیر. در صورت تأیید، این پیام به DHCP ACKارسال خواهد شد؛ اگر خوب نباشد، پیام DHCP NAK ارسال خواهد شد. پس از دریافت پیامDHCP ACK ، استفاده از منبعی را که سرور اختصاص داده است شروع کنید. در صورت دریافتDHCP NAK ، سرویس گیرندهDHCP ، پیام DHCP DISCOVER را دوباره ارسال خواهد کرد.

About DHCP Snooping۷.۳.۲

آدرس‌های اختصاص داده‌شده به سرویس گیرنده‌های DHCP در درگاه‌های ناامن را می‌توان با دقت با استفاده از اتصال‌های دینامیکی ثبت شده در DHCP Snooping کنترل کرد. DHCP Snooping به شما امکان می‌دهد تا از شبکه در برابر سرورهای DHCP یا سایر دستگاه‌هایی که اطلاعات مربوط به پورت را به سرور DHCP ارسال می‌کنند، محافظت کند. این اطلاعات می‌تواند برای ردیابی آدرس IP به یک پورت فیزیکی مفید باشد.

نحوه استفاده از دستورات

ممکن است هنگام دریافت پیام‌های مخرب DHCP از یک منبع خارجی ، ترافیک شبکه مختل شود، DHCP snooping برای فیلتر کردن پیام‌های DHCP دریافت شده در یک رابط غیر ایمن از خارج از شبکه یا فایروال استفاده می‌کند، هنگامی‌که DHCP snooping در سطح Global فعال باشد و از طریق رابط VLAN فعال باشد ، پیام‌های DHCP دریافت شده از طریق دستگاهی که در DHCP snooping ذکر نشده است رها می‌شوند.

ورودی‌های جدول فقط برای رابط‌های معتبر شناخته می‌شوند. هنگامی‌که کلاینت آدرس IP را از سرور DHCP دریافت یا آزاد می‌کند ، ورودی به جدول DHCP snooping اضافه یا حذف می‌شود. هر ورودی شامل یک آدرس MAC ، آدرس IP ، زمان اجاره ، شناسه VLANو شناسه پورت است.

وقتی DHCP snooping فعال است ، پیام‌های DHCP که به یک رابط کاربری غیرقابل اعتماد وارد می‌شوند ، بر اساس ورودی‌های پویایی که از طریق DHCP snooping آموخته شده ، فیلتر می‌شوند.

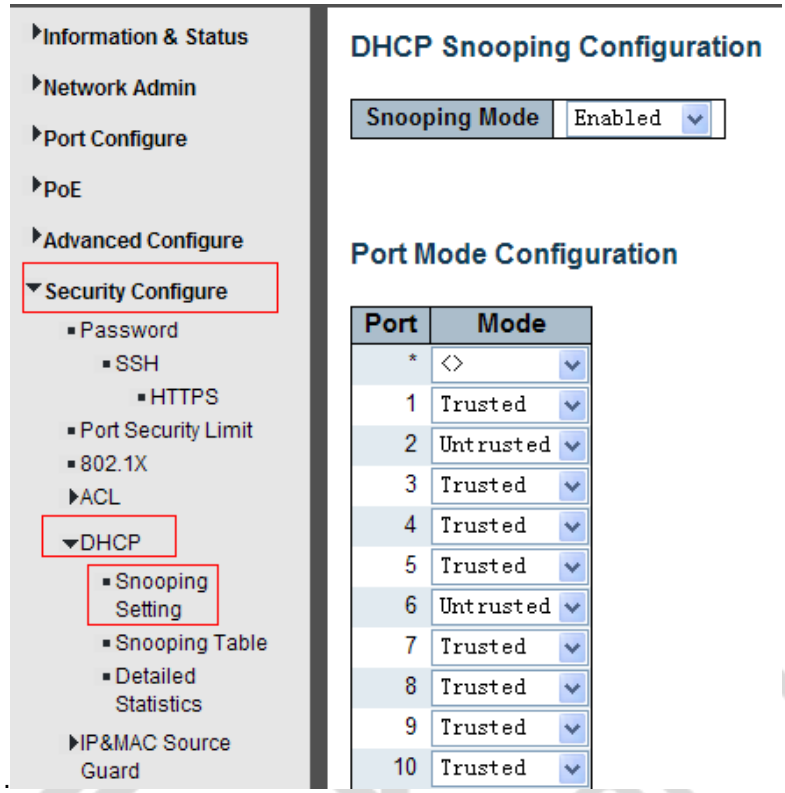
اگر بسته DHCP از کلاینت معیارهای فیلتر را تصویب کند ، فقط در همان VLAN به درگاه‌های قابل اطمینان ارسال می‌شود.

اگر بسته DHCP از سرور باشد ، در یک پورت مطمئن دریافت می‌شود ، به دو درگاه مطمئن و غیر قابل اعتماد در همان VLAN ارسال می‌شود.

اگر DHCP snooping در سطح Global غیرفعال باشد ، تمام binding های پویا از جدول bindings برداشته می‌شوند.

DHCP Snooping Configure۷.۳.۳

پس از کلیک بر روی "Snooping Setting" > "DHCP" > "Security Configure" ، صفحه زیر ظاهر می‌شود:



شکل ۷-۳ صفحه پیکربندیDHCP Snooping

شرح پیکربندی:

Object	توضیحات
DHCP Snooping Mode	بر روی منوی کشی کلیک کنیدDHCP Snooping برای فعال و یا غیرفعال کردن
Port Mode	حالت پورت DHCP Snooping را نشان می‌دهد. حالت‌های ممکن عبارت‌اند از: Trusted: درگاه را به عنوان منبع معتبر پیام‌های DHCP پیکربندی می‌کند. Untrusted: پورت را به عنوان منبع غیرقابل اعتماد پیام‌های DHCP پیکربندی می‌کند.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

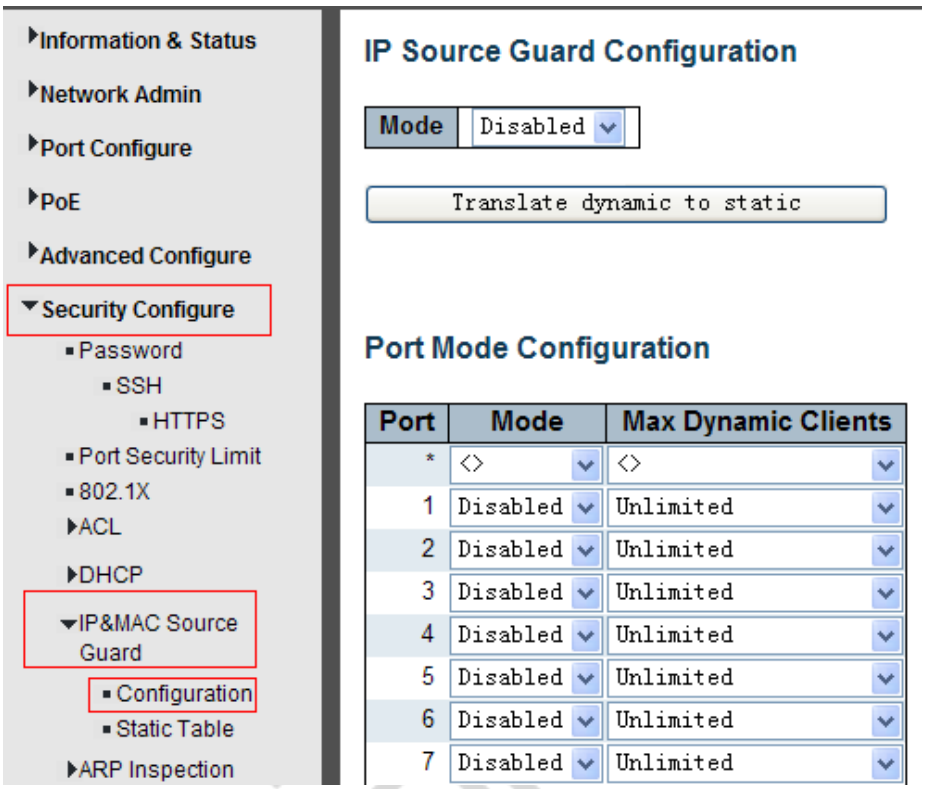
IP&MAC Source Guard۷.۴

IP & MAC Source Guard یک ویژگی ایمنی است که برای محدود کردن ترافیک IP در DHCP Snooping درگاه‌های غیرقابل اعتماد با فیلتر کردن ترافیک بر اساس DHCP Snooping Table یا پیکربندی دستی IP Source Bindings استفاده می‌شود. وقتی میزبان سعی در جعل و استفاده از آدرس IP میزبان دیگری دارد ، از حملات جعل IP جلوگیری می‌کند.

Port Configuration۷.۴.۱

در این صفحه ، کاربر می‌تواند IP & MAC Source Guard Port را تنظیم کند.

پس از کلیک بر روی "Configuration" > "IP & MAC Source Guard" > "Security Configure" ، صفحه زیر ظاهر می‌شود.



شکل ۴-۷ IP & MAC Guard- صفحه پیکربندی پورت

شرح پیکربندی:

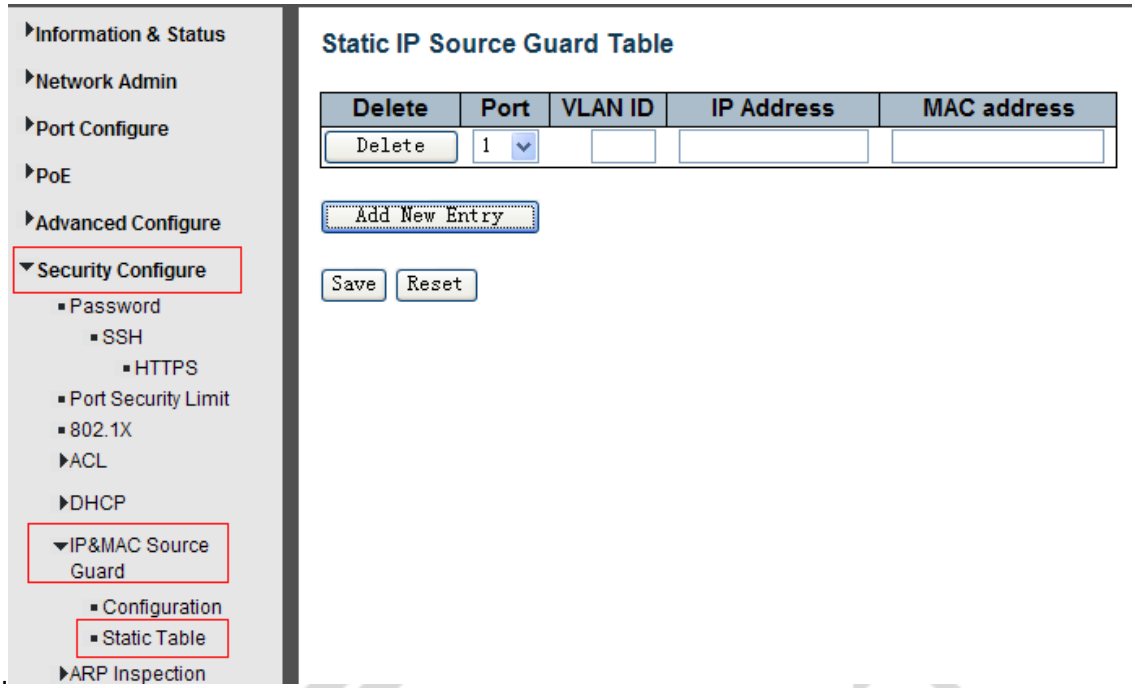
Object	توضیحات
Global Mode	برای فعال یا غیرفعال کردن عملکرد Global IP & MAC Source Guard ، روی منوی کشویی کلیک کنید
Port Mode	برای فعال یا غیرفعال کردن عملکرد IP & MAC Source Guard برای پورت مربوطه ، روی منوی کشویی کلیک کنید.
Max Dynamic Clients	برای انتخاب حداکثر کلاینت‌های پویا ، روی منوی کشویی کلیک کنید. گزینه‌های موجود: Unlimited ، ۰ ، ۱ ، ۲.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

Static Table۷.۴.۲

در این صفحه ، کاربر می‌تواند به‌صورت دستی Static Table of IP & MAC Guard را تنظیم کند تا عملکرد کنترل پورت را انجام دهد.

بعد از کلیک بر روی "Static Table" > "IP & MAC Source Guard" > "Security Configure" ، صفحه زیر ظاهر می‌شود:



شکل ۷-۵ صفحه پیکربندی جدول استاتیک

شرح پیکربندی:

Object	توضیحات
Port	برای انتخاب اینکه کدام پورت باید FIX شود روی منوی کشویی کلیک کنید.
VLAN	شناسه VLAN را که باید FIX شود را وارد کنید.
IP Address	IP آدرس را که باید FIX شود را وارد کنید.
MAC Address	MAC Address را که باید FIX شود وارد کنید.

برای ایجاد رکورد جدید ، روی دکمه "Add New Entry" کلیک کنید.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

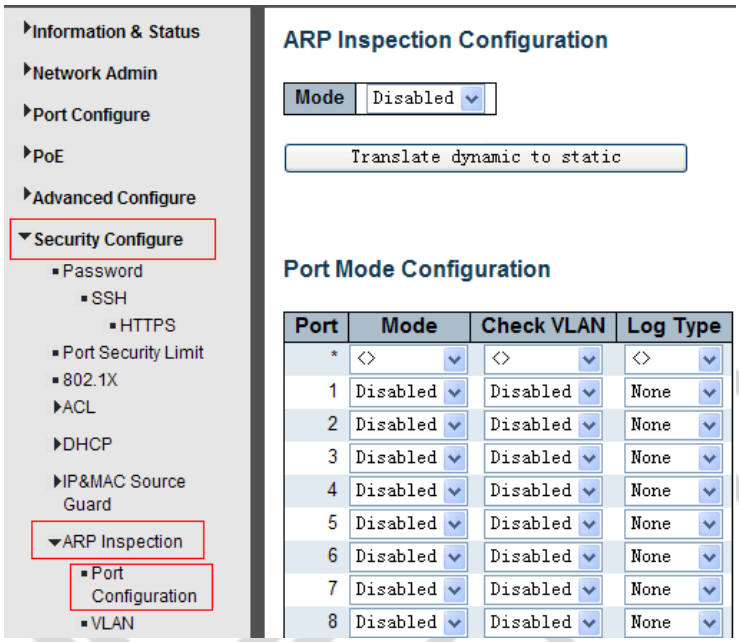
۷.۵ ARP Inspection

Dynamic ARP Inspection (DAI)یک ویژگی ایمنی است. با "poisoning" حافظه نهانگاه ARP می‌توان انواع مختلفی از حملات را علیه میزبان یا دستگاه‌های متصل به شبکه‌های لایه ۲ آغاز کرد. این ویژگی برای جلوگیری از چنین حملاتی استفاده می‌شود. فقط درخواست‌ها و پاسخ‌های معتبر ARP می‌توانند از طریق DUT انجام شوند. یک ARP پویا از بسته‌های ARP غیرقابل اعتماد مبتنی بر پایگاه داده DHCP Snoopingجلوگیری می‌کند. این صفحه پیکربندی مربوط به بازرسی ARP را فراهم می‌کند.

Port Configuration۷.۵.۱

در این صفحه می‌توانید پیکربندی پورت‌ها را ایجاد کنید.

پس از کلیک بر روی "Port Configuration" > "ARP Inspection" > "Security Configure" ، صفحه زیر ظاهر می‌شود.



شکل ۷-۶ صفحه پیکربندی پورت ARP Inspection

توضیحات پیکربندی:

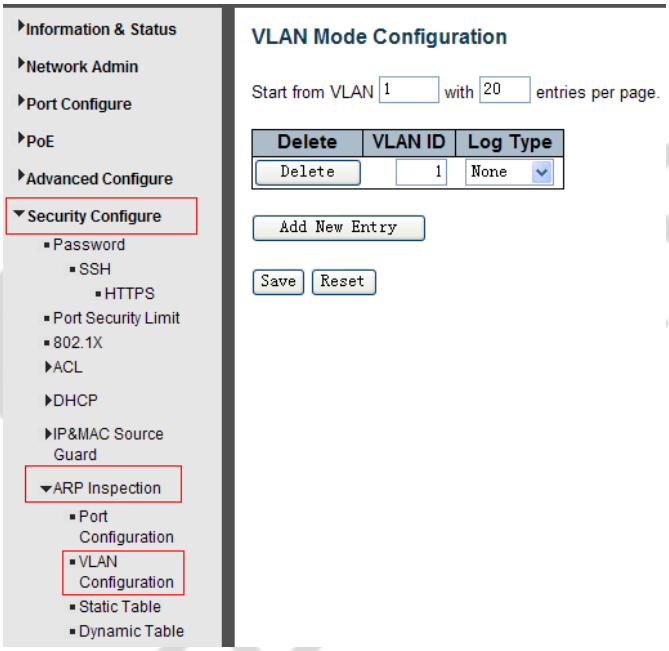
Object	توضیحات
Global Mode	برای فعال یا غیرفعال کردن Global ARP Inspection، روی منوی کشویی کلیک کنید.
Port Mode	برای فعال یا غیرفعال کردن ARP Inspection مبتنی بر پورت ، روی منوی کشویی کلیک کنید.
Check VLAN	اگر می‌خواهید پیکربندی VLAN را بررسی کنید، باید تنظیم "Check VLAN" را فعال کنید. تنظیمات پیش‌فرض "Check VLAN" غیرفعال است. هنگامی‌که تنظیم "Check VLAN" غیرفعال باشد ، نوع ورود به سیستم ARP بازبینی به تنظیمات پورت اشاره می‌کند. و تنظیم "بررسی "VLAN" فعال است ، نوع ورود به سیستم ARP به تنظیم VLAN اشاره دارد. تنظیمات ممکن "Check VLAN " عبارت‌اند از: Enabled : بررسی عملکرد VLAN را فعال می‌کند. Disabled: بررسی عملکرد VLAN را غیرفعال می‌کند.
Log Type	حالات Global Mode و Port Mode فقط در یک پورت داده‌شده فعال هستند و حالت "Check VLAN"غیرفعال است ، نوع ورود به سیستم ARP Inspection به تنظیمات پورت اشاره دارد. چهار نوع ورود به سیستم وجود دارد: None: چیزی ثبت نکنید

Deny: ورودهای تکذیب شده را ثبت کنید. Permit: ورودهای مجاز را ثبت کنید. ALL: همه ورودی‌ها را ثبت کنید.	

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

VLAN Configuration۷.۵.۲

پس از کلیک بر روی" VLAN Configuration" > "ARP Inspection" > "Security Configure" ، صفحه زیر ظاهر می‌شود



شکل ۷-۸ صفحه پیکربندی ARP Inspection VLAN

توضیحات پیکربندی:

Object	توضیحات
VLAN ID	شناسه این VLAN خاص را نشان می‌دهد
Log Type	برای فعال یا غیرفعال کردن بازرسی ARP مبتنی بر پورت ، روی منوی کشویی کلیک کنید. مشخص کنید بازرسی ARP در کدام VLAN فعال باشد. ابتدا باید تنظیمات پورت را در صفحه وب پیکربندی حالت Portفعال کنید. فقط وقتی حالت Global و حالت پورت در یک پورت داده‌شده فعال باشد ، بازرسی ARP در این پورت فعال می‌شود. ثانیاً ، می‌توانید VLAN را در صفحه وب پیکربندی حالت VLAN بررسی کنید. نوع ورود به سیستم را نیز می‌توان در هر تنظیم VLAN پیکربندی کرد. انواع احتمالی آن عبارت‌اند از: None: چیزی ثبت نکنید Deny: ورودهای تکذیب شده را ثبت کنید.

Permit: ورودهای مجاز را ثبت کنید. ALL: همه ورودی‌ها را ثبت کنید.	

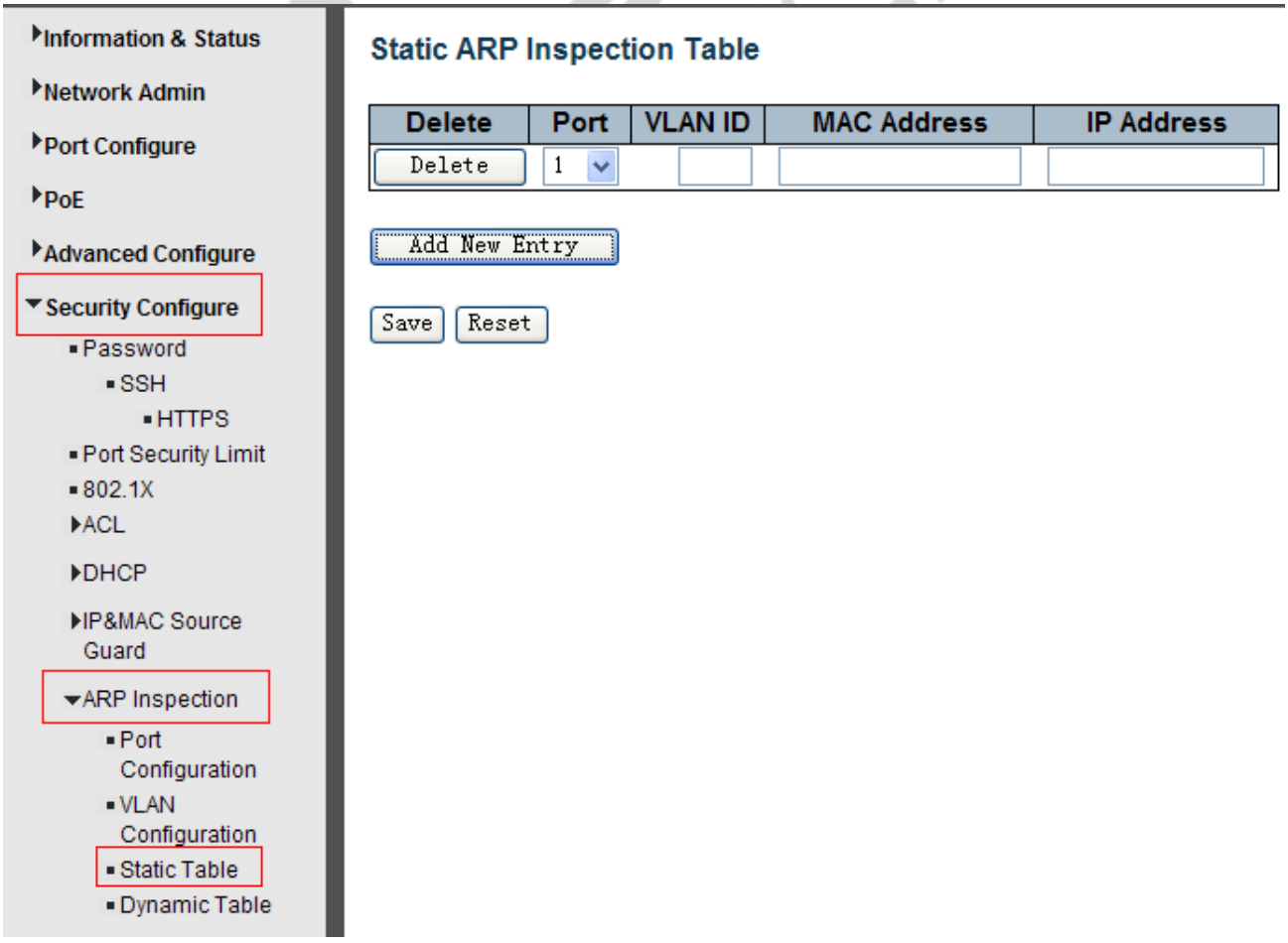
برای ایجاد رکورد جدید از پیکربندی VLAN ، روی دکمه "Add New Entry" کلیک کنید.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

Static Table۷.۵.۳

می‌توانید به‌صورت دستی ARP Inspection Static Table را برای کنترل پورت پیکربندی کنید.

پس از کلیک بر روی" Static Table " > " ARP Inspection" > "Security Configure" ، صفحه زیر ظاهر می‌شود.



شکل ۷-۹ صفحه پیکربندی جدول استاتیک

توضیحات پیکربندی:

Object	توضیحات
Port	برای انتخاب اینکه کدام درگاه باید ثبت شود ، روی منوی کشویی کلیک کنید.
VLAN	VLAN ID را که باید ثبت شود وارد کنید.
IP Address	IP آدرس را که باید ثبت شود وارد کنید.
MAC Address	مک آدرسی را که باید ثبت شود وارد کنید.

برای ایجاد رکورد جدید ، روی دکمه "Add New Entry" کلیک کنید.

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

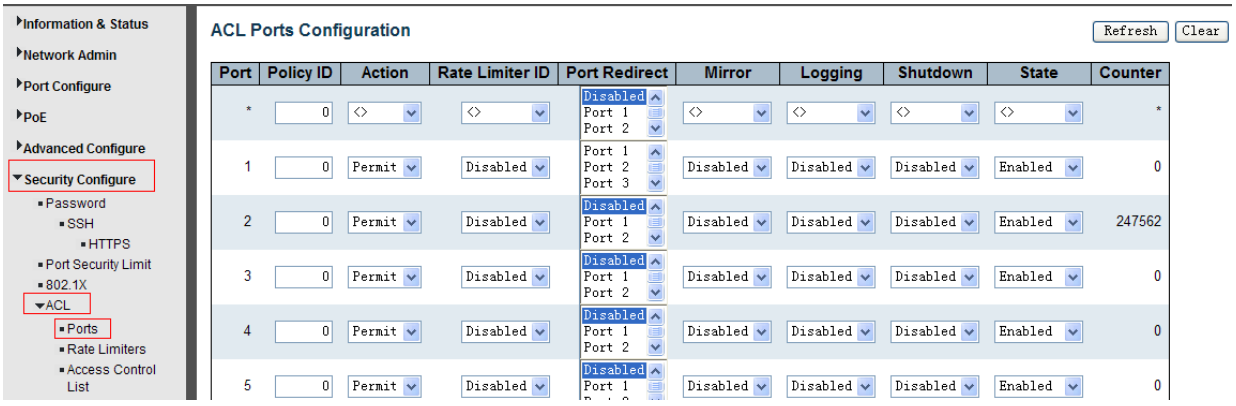
ACL۷.۶

ACL مخفف کلمه Access Control List است. این جدول فهرستی از ACE ها است که شامل ورودی‌های کنترل دسترسی است که مشخص می‌کند کاربران خاص یا گروه‌هایی که به اشیا خاص ترافیکی مانند فرآیند یا برنامه اجازه داده یا رد می‌شوند. هر شی ترافیکی قابل دسترسی حاوی شناسه ACL خود است. این امتیازات تعیین می‌کند که مجوز دسترسی خاص به اشیا ترافیکی وجود دارد یا خیر.

پیاده سازی ACL می‌تواند بسیار پیچیده باشد ، به عنوان مثال ، وقتی ACE ها برای شرایط مختلف اولویت بندی می‌شوند. در شبکه ، ACL به فهرستی از درگاه‌های سرویس یا سرویس‌های شبکه‌ای که در یک میزبان یا سرور در دسترس هستند، اشاره دارد که هرکدام از آنها فهرستی از میزبان‌ها یا سرورهای مجاز به استفاده از این سرویس را دارند. ACL به طور کلی می‌تواند برای کنترل ترافیک ورودی پیکربندی شود و در این زمینه ، آنها مشابه فایروال‌ها هستند.

ACL Ports Configure۷.۶.۱

پس از کلیک بر روی "Ports" > "ACL" > "Security Configure" ، صفحه زیر ظاهر می‌شود.



شکل ۷-۱۰ صفحه پیکربندی پورت‌های ACL

توضیحات پیکربندی:

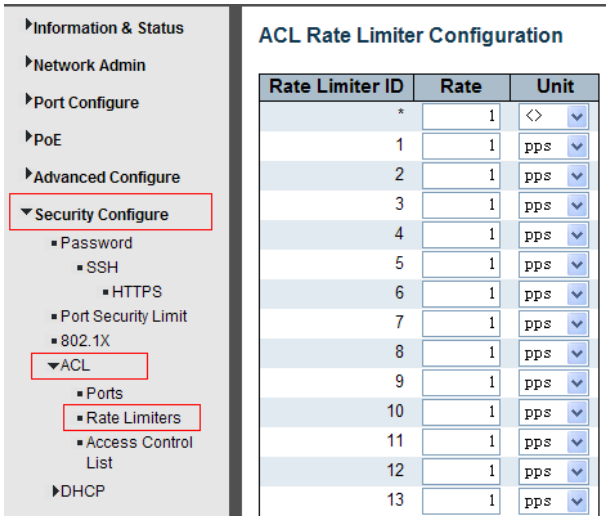
Object	توضیحات
Action	۲گزینه در دسترس وجود دارد: Permit: آن پورت خاص اجازه عبور داده‌ها را می‌دهد. Deny: آن درگاه خاص عبور داده‌ها را ممنوع می‌کند.
Rate Limiter ID	شناسه ثابت محدود کننده نرخ پورت ، لطفاً برای جزئیات بیشتر به "Rate Limiter Configuration" بروید.
Port Redirect	انتخاب کنید که کدام فریم‌های پورت هدایت شوند. مقادیر مجاز غیرفعال شده یا دارای شماره درگاهی خاص است و در صورت مجاز بودن اقدام به تنظیم آن نمی‌شود. مقدار پیش‌فرض "Disabled" است.
Mirror	عملکرد آینه این درگاه را مشخص کنید. مقادیر مجاز عبارت‌اند از: Enabled: فریم‌های دریافت شده در پورت منعکس شده است. Disabled: فریم‌های دریافت شده در پورت منعکس نشده‌اند. مقدار پیش‌فرض "Disabled" است.
Logging	فعال و غیرفعال سازی ورود به سیستم.
Shut Down	عملکرد خاموش کردن پورت این پورت را مشخص کنید، مقادیر مجاز عبارت‌اند از: Enabled: اگر فریمی روی پورت دریافت شود ، پورت غیرفعال می‌شود. Disabled: خاموش کردن پورت غیرفعال است. مقدار پیش‌فرض غیرفعال است." توجه: ویژگی خاموش کردن فقط زمانی کار می‌کند که طول بسته کمتر از ۱۵۱۸ باشد (بدون برچسب‌هایVLAN)
State	حالت پورت این پورت را مشخص کنید. مقادیر مجاز عبارت‌اند از: Enabled: برای باز کردن درگاه‌ها با تغییر در پیکربندی پورت فرار ماژول کاربرACL Disabled: برای بستن پورت‌ها با تغییر تنظیمات پورت فرار ماژول کاربرACL مقدار پیش‌فرض "Enabled" است.
Counter	تعداد فریم‌های منطبق با این قانون را می‌شمارد.

کلیک کنید."Save"برای ذخیره تنظیمات روی

Rate Limiter Configuration۷.۶.۲

می‌توانید در این صفحه پیکربندی محدود کننده نرخ ACL را ایجاد کنید.

پس از کلیک بر روی "Rate Limiter" > "ACL" > "Security Configure" ، صفحه زیر ظاهر می‌شود.



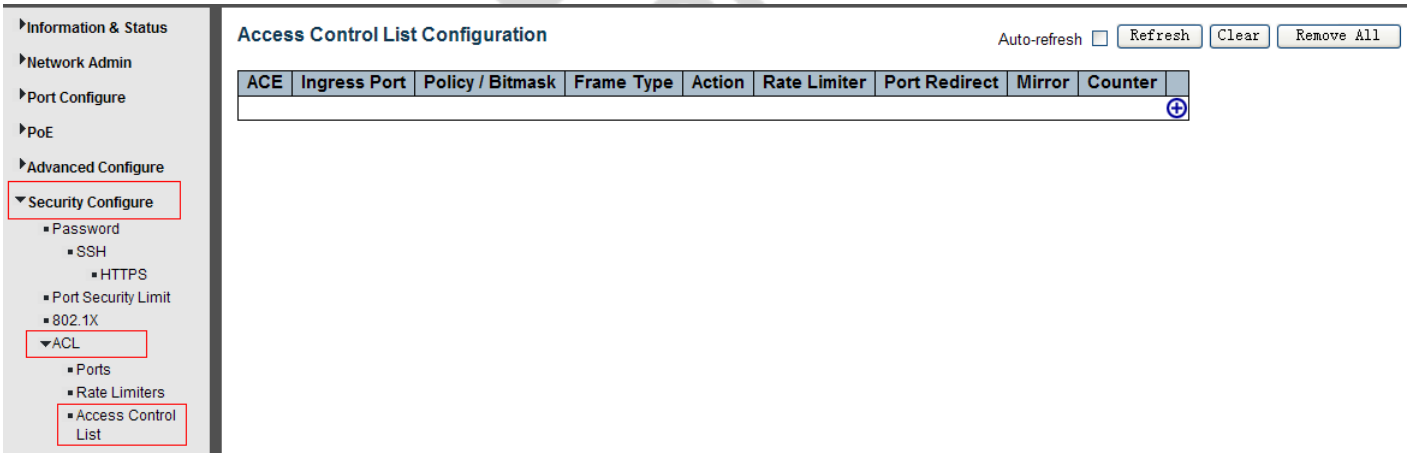
شکل ۷-۱۱ صفحه تنظیمات ACL Rate Limiters

پس از تنظیم پیکربندی لطفاً بر روی "Save" کلیک کرده تا تنظیمات ذخیره شوند.

۷.۶.۳پیکربندی لیست کنترل دسترسی

می‌توانید در این صفحه پیکربندی لیست کنترل دسترسی را ایجاد کنید.

پس از کلیک بر روی "Access Control List" > "ACL" >"Security Configure"، صفحه زیر ظاهر می‌شود.



شکل ۷-۱۲ صفحه کنترل پیکربندی لیست کنترل دسترسی

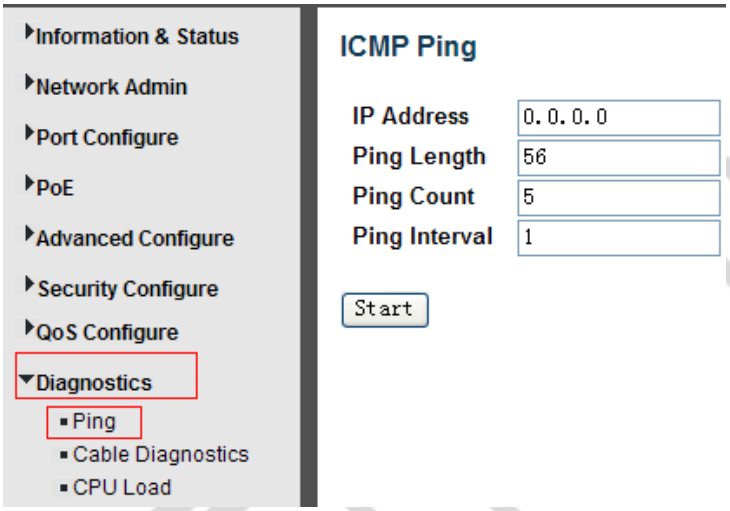
روی ⊕ کلیک کنید تا به لیست کنترل دسترسی هدایت شوید.

Diagnostics.۸

۸.۱تست پینگ

Ping یک برنامه کوچک است که می‌تواند بسته‌های ICMP Echo را به آدرس IP مشخص شده شما صادر کند. گره مقصد به بسته‌های ارسالی از سوییچ پاسخ می‌دهد. بنابراین تست پینگ برای عیب‌یابی مشکلات اتصال IP است.

پس از کلیک بر روی " Ping" <"Diagnostics"، صفحه زیر نمایش داده می‌شود.



شکل ۱-۸ صفحه تست پینگ

توضیحات پیکربندی:

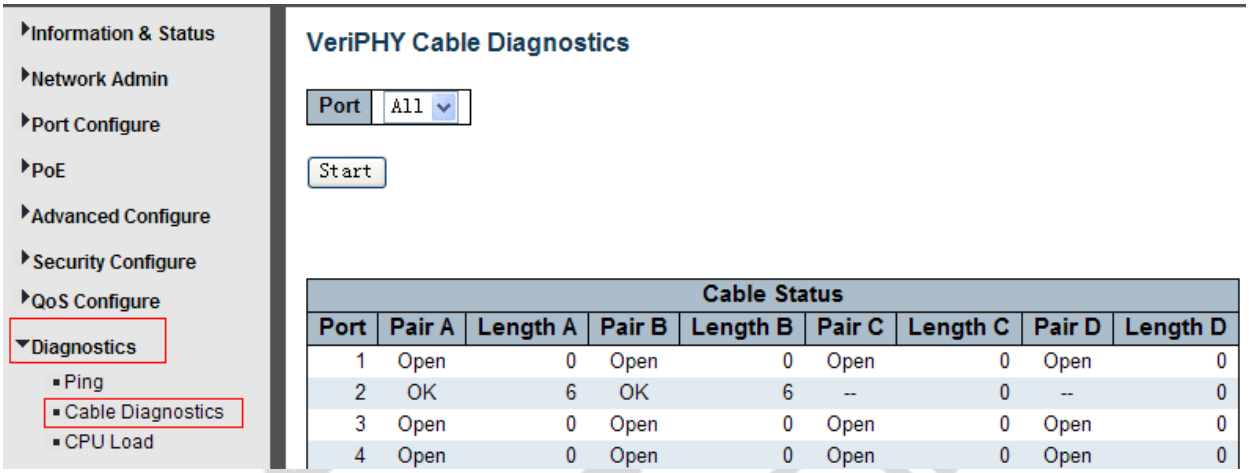
Object	توضیحات
IP Address	آدرس IP مقصد مورد نیاز برایPing
Ping Length	یک عدد بین ۱ و ۱۴۵۲ وارد کنید. پیش‌فرض: ۵۶
Ping Count	زمان ورود آدرس Ping IPv۴ یا آدرس (IPv۶ تعداد درخواست‌های echo برای ارسال) می‌توانید عددی بین ۱ تا ۶۰ وارد کنید.
Ping Interval	فاصله زمانی برای پینگ (ارسال بازه برای هر بسته ICMP)

روی "Start" کلیک کنید تا تست پینگ آغاز شود

Cable Diagnostics ۸.۲

Cable Diagnosticsآزمایش‌هایی را روی کابل‌های مسی ۱۰/۱۰۰/۱۰۰۰Base-T انجام می‌دهد. این عملکردها توانایی شناسایی طول کابل و شرایط عملیاتی و جدا کردن انواع خطاهای رایج را که می‌تواند در کابل کشی جفت پیچ خورده Cat۵ ایجاد شود ، دارند.

پس از کلیک بر روی"Cable Diagnostics" > "Diagnostics" ، صفحه دنبال شده ظاهر می‌شود.

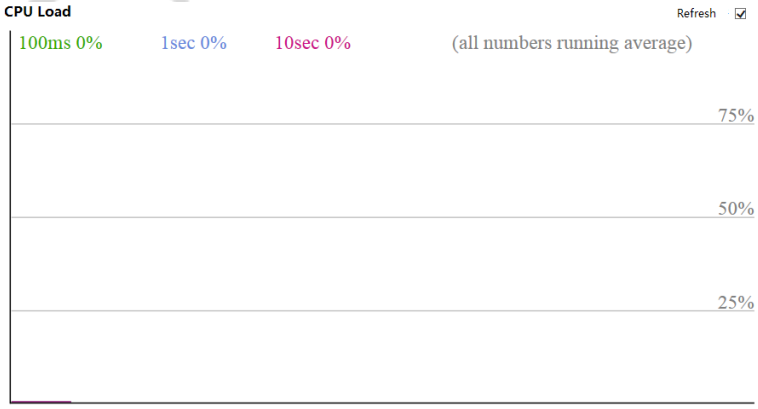


شکل ۸-۲ صفحه Cable Diagnostics

برای شروع تست "Cable Diagnostics" بر روی دکمه "Start" کلیک کنید.

۸.۳عملکرد CPU

این صفحه عملکرد CPU را نشان می‌دهد. پس از کلیک بر روی "CPU Load" > "Diagnostics"، صفحه زیر ظاهر می‌شود.

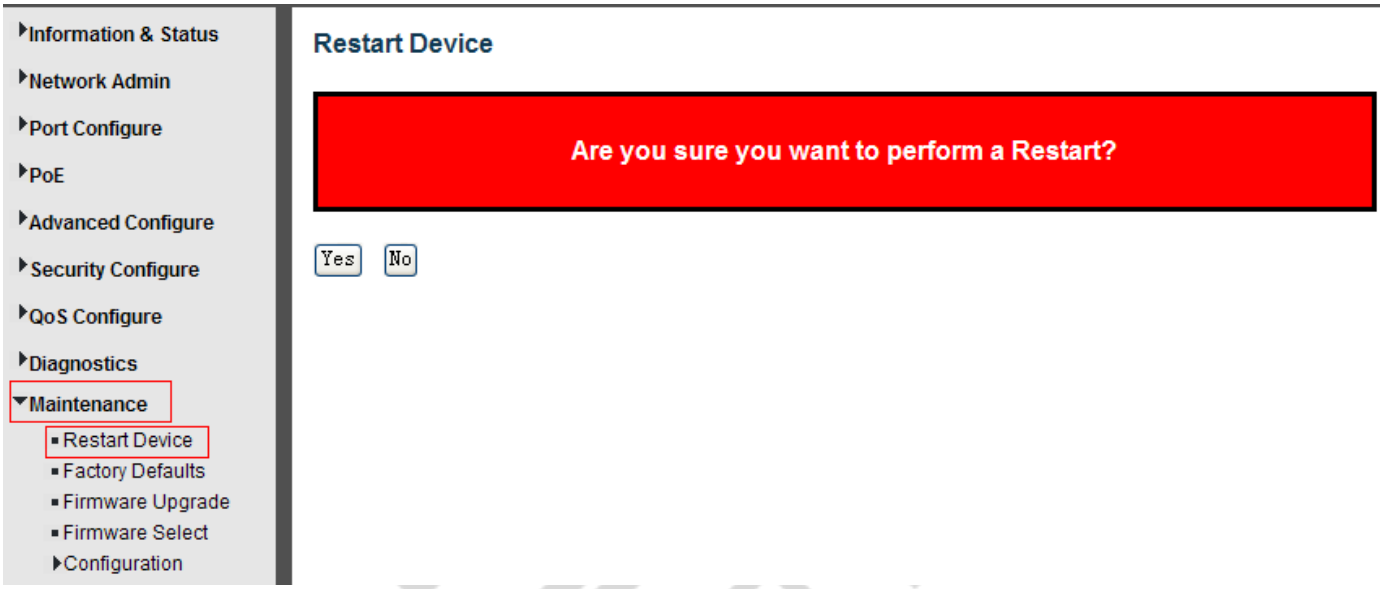


شکل ۸-۳ صفحه عملکرد پردازنده

۹. Maintenance

۹.۱راه‌اندازی مجدد دستگاه

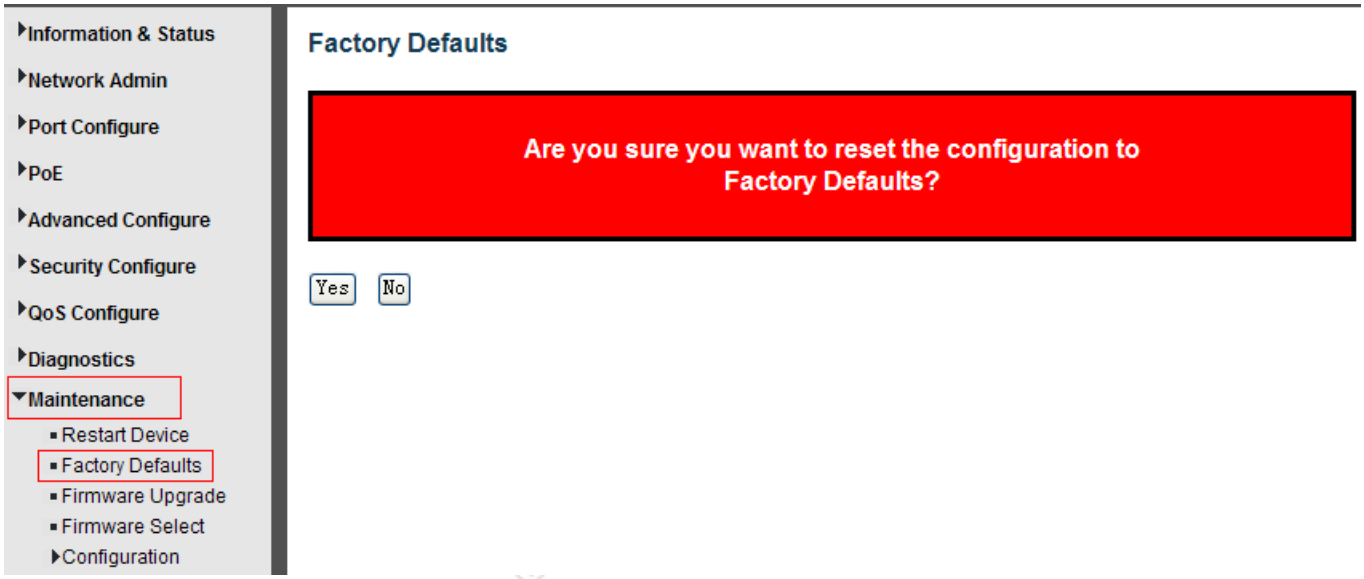
این صفحه برای راه‌اندازی مجدد سوییچ است. پس از کلیک بر روی"Restart Device" <"Maintenance"، صفحه زیر ظاهر می‌شود.



برای راه‌اندازی مجدد سوییچ روی "Yes" کلیک کنید.

۹.۲تنظیمات کارخانه

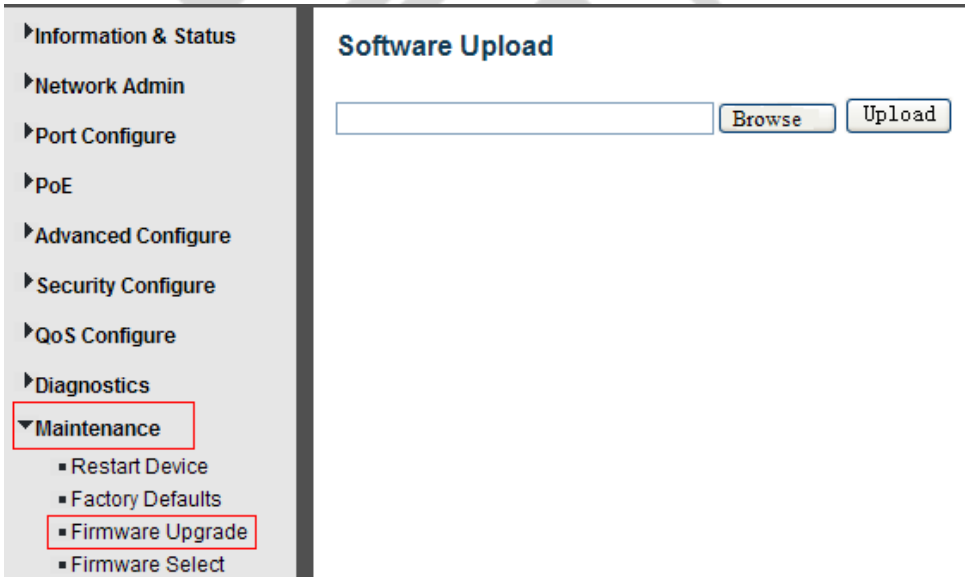
این صفحه برای انجام همه تنظیمات پیش‌فرض کارخانه است. پس از کلیک بر روی "Factory Defaults" < "Maintenance"، صفحه دنبال شده ظاهر می‌شود.



روی "Yes" کلیک کنید تا پیکربندی را به پیش‌فرض‌های کارخانه بازنشانی کنید.

۹.۳به‌روزرسانی سیستم‌عامل دستگاه

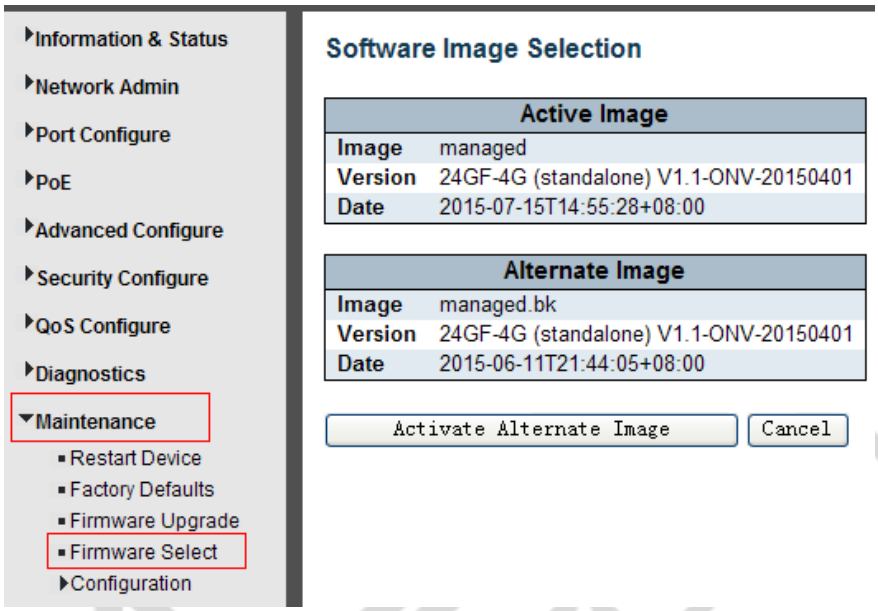
این صفحه برای به‌روزرسانی سیستم‌عامل دستگاه است. پس از کلیک بر روی"Maintenance">" Firmware Upgrade"، صفحه زیر ظاهر می‌شود.



روی "Browse" کلیک کنید تا Firmware مورد نیاز برای ارتقا را انتخاب کنید و سپس برای شروع به‌روزرسانی، "Upload" را کلیک کنید.

۹.۴ انتخاب Firmware

این صفحه برای انتخاب سیستم‌عامل دستگاه است. پس از کلیک بر روی "Maintenance" > "Firmware Select"، صفحه زیر ظاهر می‌شود.



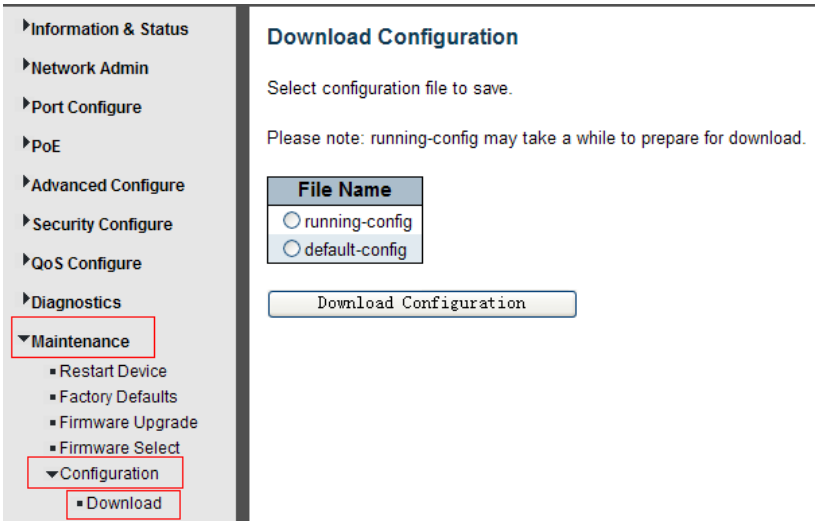
برای انتخاب میان‌افزار "Activate Alternate Image" را کلیک کنید.

۹.۵ انتخاب Firmware

در این صفحه، می‌توانید پرونده‌های پیکربندی را بارگیری، بارگذاری، فعال یا حذف کنید.

۹.۵.۱دانلود فایل پیکربندی

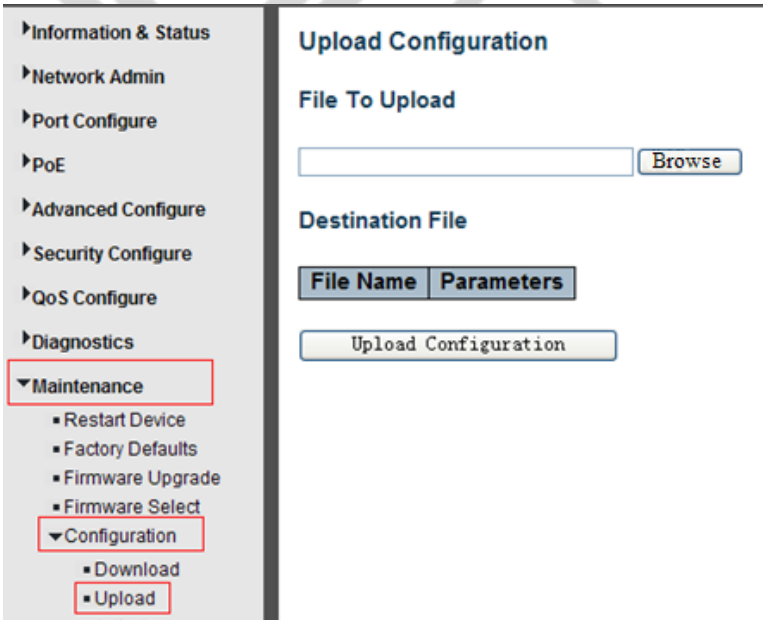
پس از کلیک بر روی "Download" > "Maintenance"، صفحه زیر ظاهر می‌شود.



یک فایل را انتخاب کنید و سپس روی دکمه "Download Configuration" کلیک کنید تا بارگیری شود.

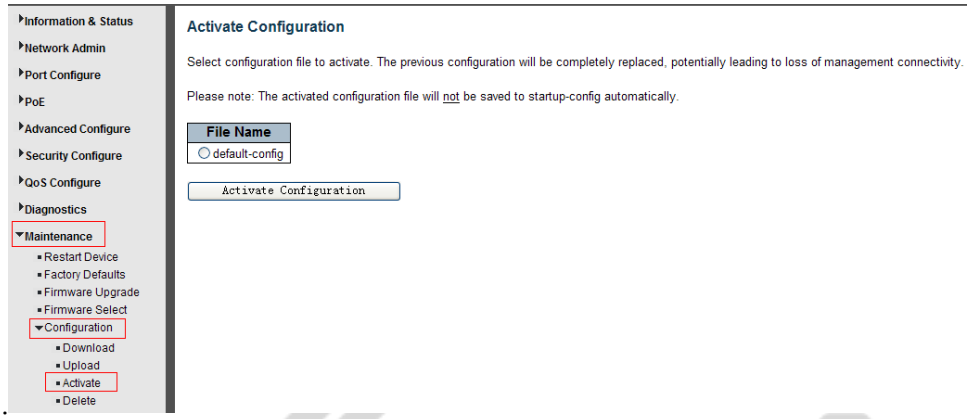
۹.۵.۲بارگذاری فایل پیکربندی

پس از کلیک بر روی" Upload " > "Maintenance" ، صفحه زیر ظاهر می‌شود. سپس کاربر می‌تواند پرونده پیکربندی را بارگذاری کند.



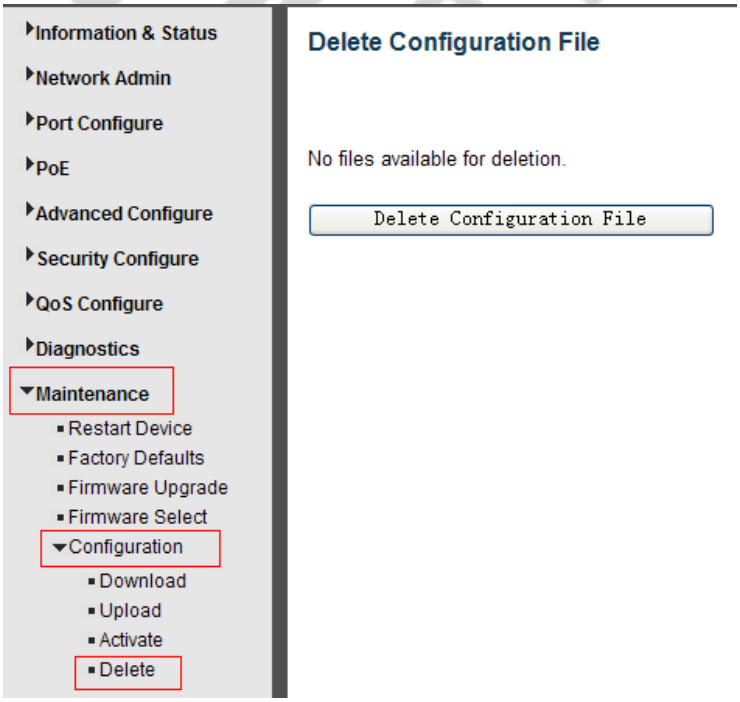
۹.۵.۳فعال‌سازی پیکربندی

پس از کلیک بر روی "Activate" <"Maintenance"، صفحه زیر ظاهر می‌شود. سپس می‌توانید پرونده پیکربندی را فعال کنید



۹.۵.۴حذف فایل پیکربندی

پس از کلیک بر روی" Delete " <"Maintenance" ، صفحه زیر ظاهر می‌شود. سپس می‌توانید پرونده پیکربندی را حذف کنید.



----------پایان----------