راهنمای پیکربندی سوئیچ قابل برنامه ریزی

از طریق صفحه وب

برای مدل های :

2408H4SM+ /1608H4SM+ / 802H4SMI / 3200H4SM

Kdt.ir

تهیه و تنظیم :

شرکت کاوش داده پردازان

فهرست

مقدمه

این راهنما به طور عمده صفحه وب در سوئیچ را شرح می دهد. کاربر می تواند سوئیچ را به وسیله صفحه وب مدیریت کند. این راهنما برای عملکرد هر صفحه وب یک معرفی نامه ساده دارد. لطفا برای یادگیری عملکرد هر قسمت از تنظیمات سوئیچ به راهنمای کاربر آن قسمت مراجعه کنید. این راهنما به طور عمده موارد زیر را شامل می شود:

۱) مرور اجمالی و کلی به صفحات وب

۲) معرفی صفحات وب

-

۱) مرور اجمالی به صفحه وب

۱_ ۱مشخصه های دسترسی به وب

سوئیچ ویژگی هایی را برای دسترسی به وب برای کاربران فراهم می کند. کاربر میتواند به وسیله مرورگر وب به سوئیچ دسترسی یابد و سوئیچ را پیکربندی و مدیریت کند. مشخصه های اصلی دسترسی به وب عبارتند از:

- دسترسی آسان؛ کاربران به آسانی می تواند از هر جایی در شبکه از طریق IP Address به سوییچ دسترسی یابند .
- کاربران میتوانند از طریق FireFox و Chrome و Microsoft internet Explorer و سایر مرورگرها برای دسترسی به صفحات وب سوئیچ استفاده کنند. صفحه وب برای کاربران به شکل گرافیکی و جدولی ارائه شده است.
- سوئیچ تمام قابلیت های خود را در قالب یک صفحه وب کامل فراهم می کند، کاربران میتوانند اکثر عملیات سوئیچ را به وسیله این صفحات وب مدیریت و پیکربندی کنند.
- دسته بندی قابلیت های صفحات وب به صورت منظم و یکپارچه، کاربر برای پیدا کردن صفحه مرتبط جهت پیکربندی و مدیریت به راحتی می تواند اقدام کند.

۱_۲ سیستم مورد نیاز مرورگر وب

حداقل سیستم مورد نیاز برای ورود به صفحه مرورگر وب سوئیچ در جدول ۱ نشان داده شده است.

Hardware and Software	System Requirement
CPU	Pentium 586 above
RAM	128MB above
Resolution	800x600 above
Color	256 colors above
Browser	IE4.0 above or Chrome 22.3 above
Operating System	Microsoft®,Windows95®,Windows98®,WindowsNT®, Windows2000®,WindowsXP®,WindowsME®, WindowsVista®, Windows7®, Windows8®, Windows10®,MAC, Linux,Unix operating system

جدول شماره ۱

۱_۳ مرحله ی ورود به مرورگر وب

پیش از آنکه شما تنظیمات سویچ از طریق مرورگر وب را شروع کنید، به یکسری اطلاعات نیاز دارید.

لطفا به موارد زیر توجه کنید:

- از قبل یک IP آدرس بر روی سوئیچ پیکربندی شده است، به طور پیش فرض، IP آدرس در VLAN1 تنظیم شده است.IP آدرس در سوئیچ به صورت پیش فرض **192.168.0.1** می باشد.
- عدد Subnet Mask به صورت پیش فرض : **255.255.255.0** است.
- برای اتصال به سوئیچ یک کامپیوتر میزبان نیاز دارید با یک مرورگر نصب شده و به شبکه وصل شده باشد و کامپیوتر میزبان به وسیله سوئیچ بتواند پینگ کند.
- پس از انجام دو کار بالا کاربر در نوار آدرس مرورگر، IP آدرس سوئیچ را وارد کرده و دکمه اینتر (Enter) را برای ورود به صفحه وب ورودی سوئیچ فشار بدهد. همانطورکه در شکل(۱) نشان داده شده

است ،برای ورود به بخش تنظیمات می بایست از طریق کاربر مدیر اقدام کنید.نام کاربری و پسورد مدیر به صورت پیش فرض **admin** می باشد.

User: admin

pass: admin

نکته:

اگر سیستم برای مدیریت چند کاربر و کاربران خاصی فعال باشد، پسورد admin برای کاربران دیگر اثر نخواهد داشت یعنی دسترسی کاربران دیگر به وب با پسورد admin کار نمی کند، نام کاربری و پسورد کاربرانی که برای مدیریت دسترسی دارند، مورد تایید است.

شکل ۱

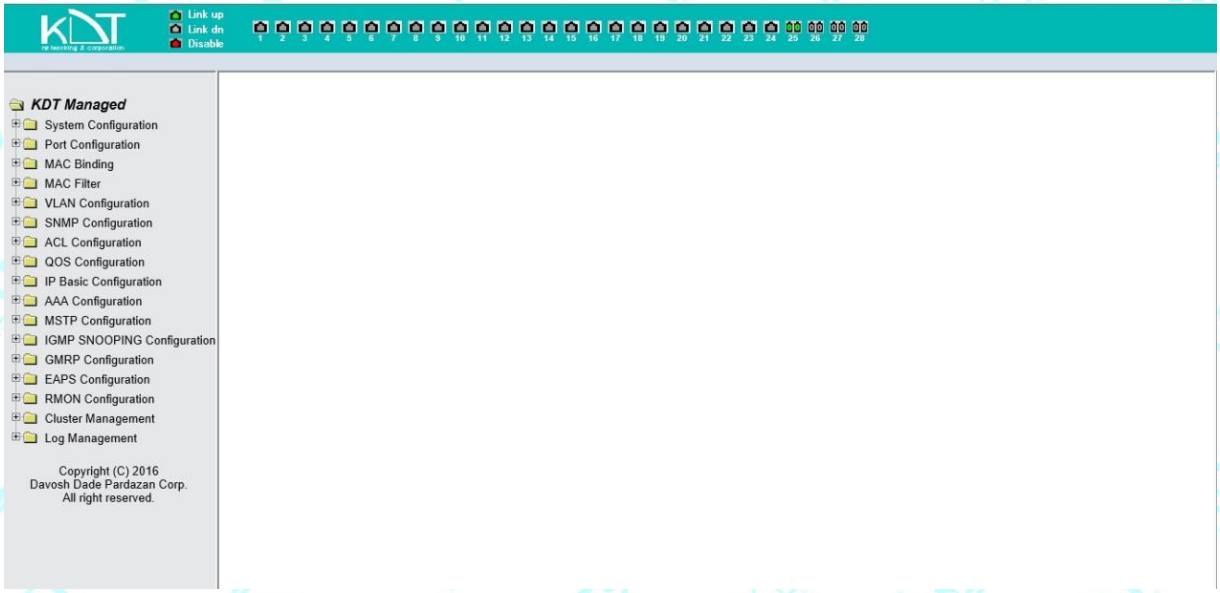
۱_۴ ساختار اصلی صفحه وب سویچ

ساختار اصلی صفحه وب سویچ در شکل ۲ مشاهده می کنید، صفحه وب سوئیچ از سه بخش کلی تشکیل شده است:

۱)عنوان صفحه

۲) صفحه منوی درختی

۳)صفحه اصلی



شکل ۲

۱_۴_۱ عنوان صفحه:

در بالای صفحه سمت چپ Logo (طرح) و وضعیت port (درگاه) قابل مشاهده می باشد.

در اینجا وضعیت پورتها با رنگ نمایش داده شده است

رنگ سبز نشان دهنده این است که port وصل است.

رنگ طوسی نشان دهنده این است که port وصل نیست.

رنگ قرمز نشان دهنده این است که port خاموش است. (تنظیمات مخصوص در شکل ۱۷نشان داده شده است)

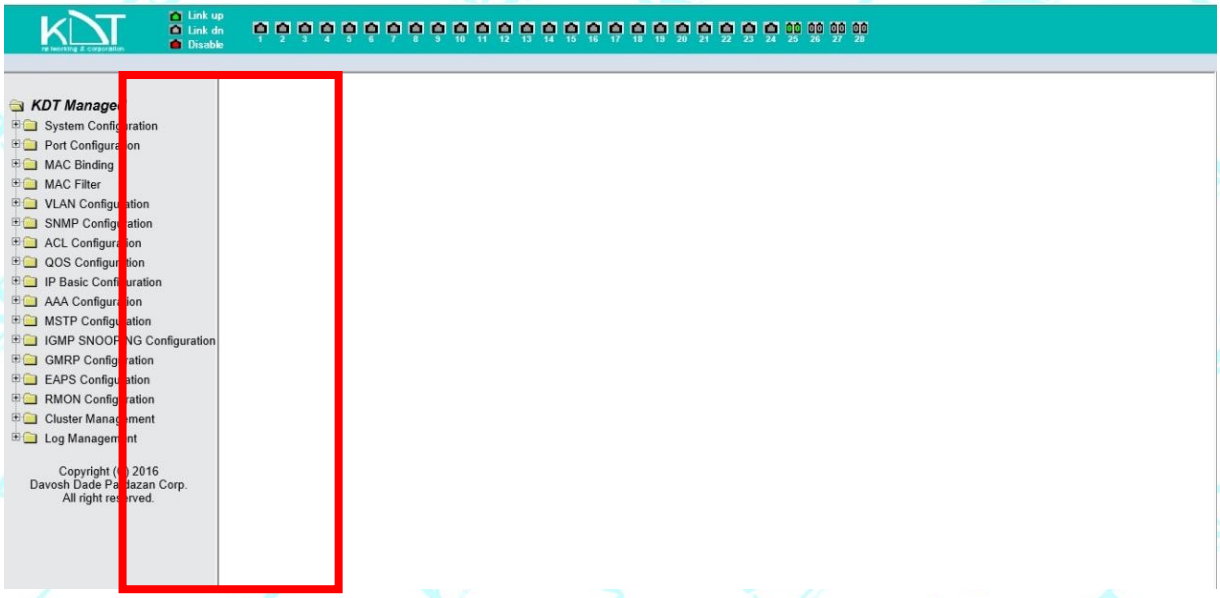
۱_۴_۲ صفحه اصلی:

برای نمایش صفحه ای که توسط کاربر از منوی درختی(navigation tree) انتخاب شده، استفاده می شود.

۱_۵ ساختار منوی درختی

شکل(۳)، ساختار منوی درختی را نشان میدهد. منوی درختی در سمت چپ هر صفحه واقع شده است و صفحهات وب را در یک منوی درختی به صورت گروه بندی نمایش می دهد و کاربر به راحتی می تواند صفحه وب مورد نظر خود را از داخل این گروه ها پیدا کند.

گروه ها به دو حالت مختلف نمایش داده میشود. حالت اول شاخه اصلی که دارای زیر شاخه های متعدد است که عنوان آنها به اختصار نمایش داده شده است و گروه دوم زیر شاخه های آنها می باشد که عنوان صفحهات را نمایش می دهند.



شکل(۳)

۱_۶ معرفی دکمه های صفحات

چندین دکمه متداول روی صفحه وجود دارند، نقش این دکمه ها در همه صفحات عموماً یکسان است،جدول(۲)، برای معرفی نقش این دکمه ها می باشد.

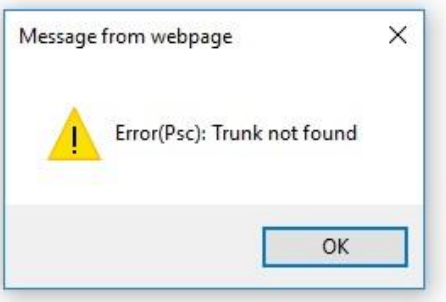
دکمه	کاربرد
Refresh	بروز رسانی صفحه
Apply	بررسی صحت موارد وارد شده و سپس ثبت تغییرات روی حافظه موقت دستگاه
Delete	پاک کردن موارد انتخاب شده
Help	باز کردن صفحه راهنمای مربوطه

جدول۲

۱_۷ پیام خطا

سوئیچ، وقتی درخواست های کاربر را پردازش میکند اگر آن تنظیمات مشکل داشته باشد، پیام خطای مربوطه را در یک پنجره نمایش میدهد.

شکل (۴)، یک پیام خطا را در قالب پنجره نشان می دهد.



شکل(۴)

۸_۱ فیلد انتخاب ورودی

(هر یک از خانه های جدول را که قابلیت انتخاب کردن دارد را فیلد گویند)

صفحاتی هستند که در چپ ترین ستون جدول قرار دارند و یک فیلد انتخاب ورودی دارند. همانطور که درشکل(۵) نمایش داده شده به وسیله این صفحات شما امکان دستیابی به ردیف های مختلف جدول را دارید.

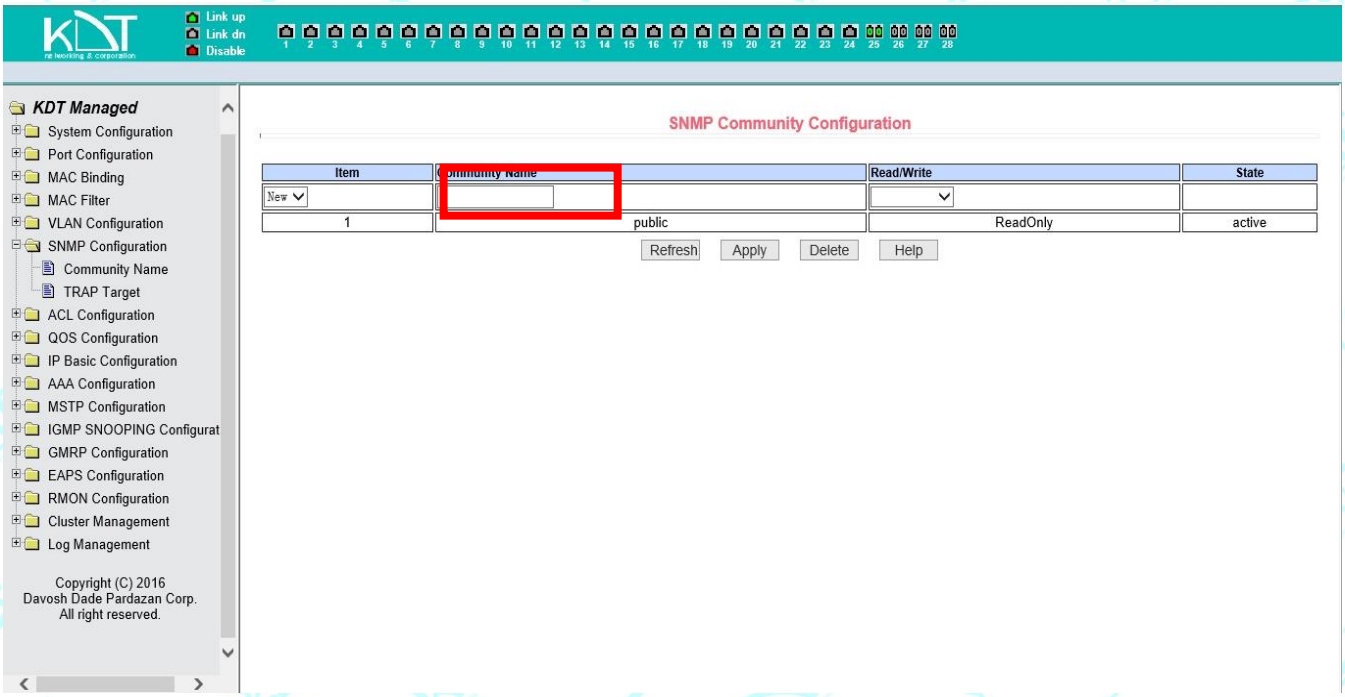
وقتی شما یک گزینه را در فیلد ورودی انتخاب میکنید اطلاعات مربوط آن ردیف در اولین سطر نمایش داده می شود. توجه داشته باشید که فقط ردیفی می تواند تصحیح شود که فعال باشد.

وقتی که وارد صفحه ای می شوید فیلد انتخابی گزینه جدید(NEW) را نشان میدهد و تمام ردیف هایش خالی می باشد.

اگر می خواهید یک ردیف جدید اضافه کنید گزینه New را از منوی کشویی در فیلد انتخاب ورودی انتخاب کنید و اطلاعات ردیف جدید را وارد کنید و دکمه اعمال کردن(Apply)را فشار دهید .

اگر می خواهید ردیف موجود را تصحیح کنید، شماره گزینه مناسب را از منوی کشویی در فیلد انتخاب ورودی انتخاب کنید و ردیف را آنگونه که نیاز است تصحیح کنید و دکمه اعمال کردن (Apply) را فشار دهید، تغییرات مربوطه راخواهید دید که در جدول نمایش می دهد.

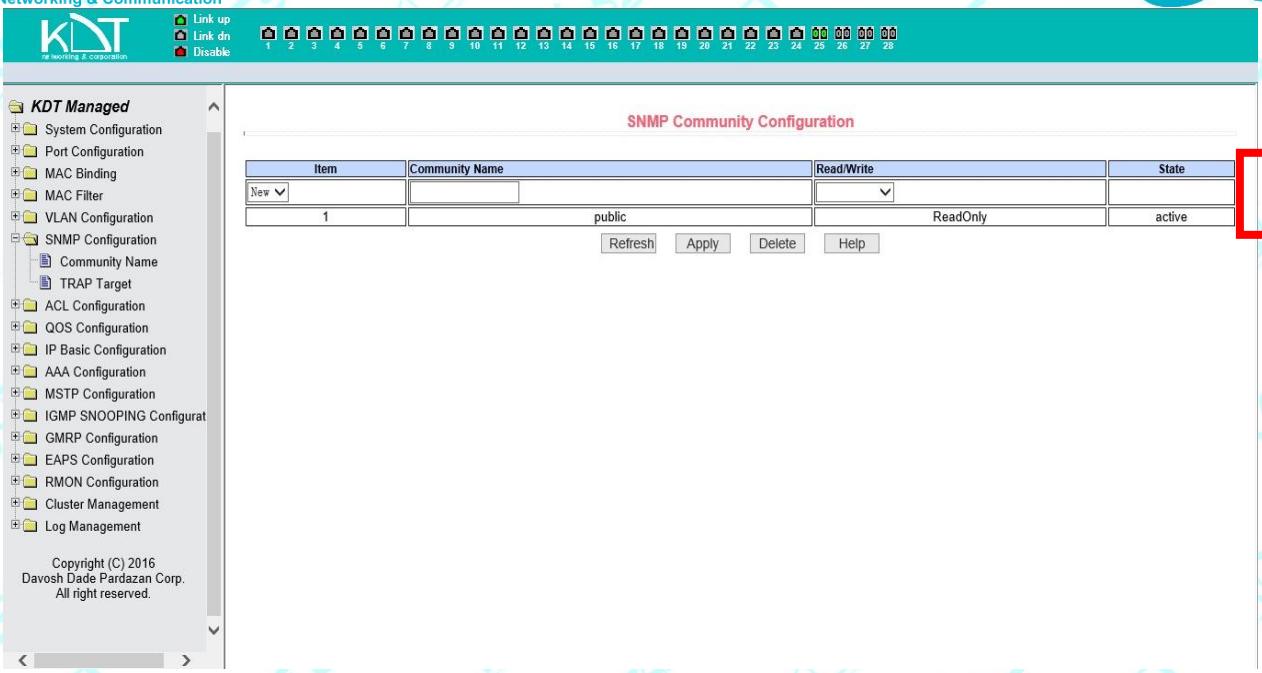
اگر میخواهید ردیفی را حذف کنید، گزینه مربوطه را از منوی کشویی در فیلد انتخاب ورودی انتخاب و دکمه حذف (delete) را فشار دهید. ردیف از جدول پاک خواهدشد.



شکل(۵)

۹_۱ وضعیت فیلد

داخل صفحات در راست ترین ستون جدول وضعیت فیلد وجود دارد و اطلاعات مربوطه را نمایش می دهند. همانطور که در شکل(۶) مشخص است موقیت وضعیت فیلد را میتوانید مشاهده کنید. از آنجا که وضعیت داده ها به صورت داخلی پردازش می شود، وضعیت فیلد فقط خواندنی است (غیر قابل ویرایش.) زمانی که تمام اطلاعات داده شده معتبر باشد وضعیت آن به طور خودکار فعال (active) نشان داده میشود.


Link up
Link dn
Disable
KDT Managed
System Configuration
Port Configuration
MAC Binding
MAC Filter
VLAN Configuration
SNMP Configuration
Community Name
TRAP Target
ACL Configuration
QOS Configuration
IP Basic Configuration
AAA Configuration
MSTP Configuration
IGMP SNOOPING Configurat
GMRP Configuration
EAPS Configuration
RMON Configuration
Cluster Management
Log Management
Copyright (C) 2016
Davosh Dade Pardazan Corp.
All right reserved.
SNMP Community Configuration
Item
Community Name
Read/Write
State
New
1
public
ReadOnly
active
Refresh
Apply
Delete
Help

شکل(۶)

۲) معرفی صفحات وب

صفحات وب سوئیچ در قالب گروه هایی سازمان دهی شده اند که هرکدام شامل یک یا چند صفحه وب میشوند. در اینجا ما به بررسی صفحات وب هر گروه می پردازیم.

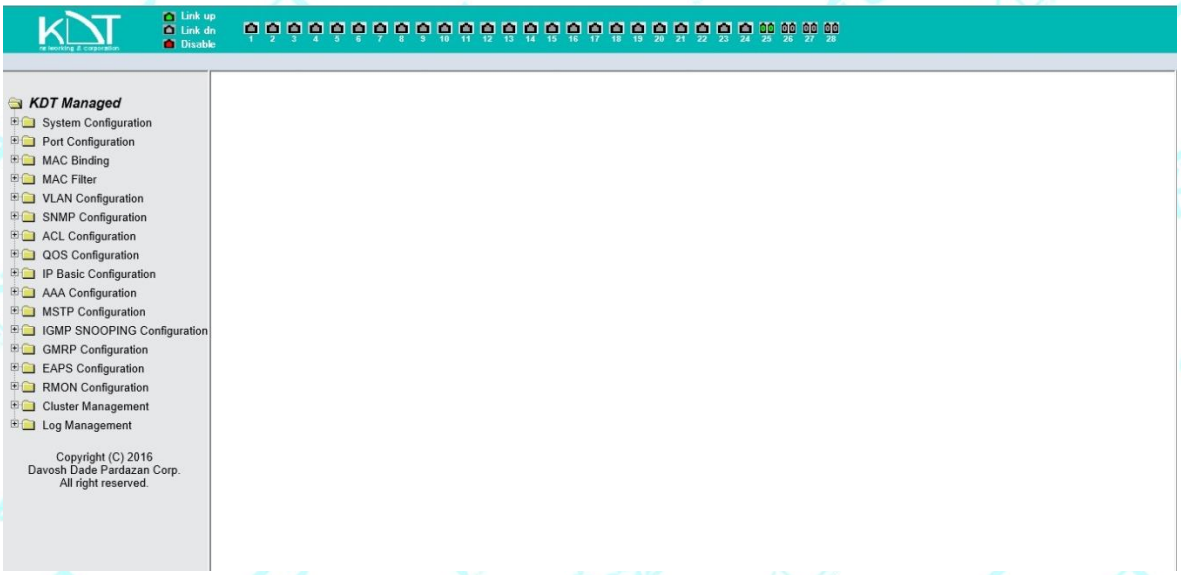
۲_۱ پنجره اجازه ورود به صفحه وب

شکل(۷) پنجره اجازه ورود برای زمانی که ابتدا کاربر می خواهد وارد صفحه وب شود را نشان می دهد. کاربر نام کاربری و رمز عبور را در قسمت مربوطه وارد می کند و سپس دکمه(ok) را برای ورود به صفحه وب در سوئیچ کلیک می کند. رمز عبور بسیار حساس است، رمز عبور کاربر مدیر می تواند تا ۶۱ حرف باشد، و رمز عبور و نام کاربری کاربران دیگر هم میتواند تا ۶۱ حرف باشد. نام کاربری پیش فرض سوئیچ همان admin است. رمز عبور کاربر مدیر هم به طور پیش فرض admin است.

شکل(۷)

۲_۲ صفحه اصلی

شکل(۸) صفحه اصلی وب سوئیچ را نشان می دهد. این صفحه بعد از آن که کاربر وارد به صفحه شد، نمایش داده خواهد شد.



شکل(۸)

۲_۳ پیکربندی سیستم

۲_۳_۱ صفحه اطلاعات پایه

شکل (۹) صفحه پیکربندی اطلاعات پایه را نشان می‌دهد که در آن کاربر می‌تواند اطلاعات اولیه را به دلخواه پیکربندی کند.

System Description:

شرح سیستم: نشان می دهد که این سویچ مربوط به چه خانواده ای از محصولات است.

System Object ID:

شماره شناسایی سیستم: نشانگر هویت سیستم در مدیریت شبکه است.

:System Version

نسخه سیستم: شماره مدل نرم افزار فعلی استفاده شده توسط سوئیچ را نشان می دهد.

:Num Network Interface

شماره رابط شبکه: شماره پورت های موجود در سوئیچ را نشان می دهد.

:System Start Time

زمان شروع سیستم: زمان آغاز فعالیت سویچ از زمانی که آخرین بار به برق متصل شده تا کنون را نشان می دهد.

ساعت سیستم، ساعت فعلی سیستم را نشان می دهد. کاربر می تواند ساعت فعلی سیستم را تغییر دهد و نیاز دارد که پارامترهای سال و ماه و روز وساعت و دقیقه و ثانیه راوارد کند.

:System Name

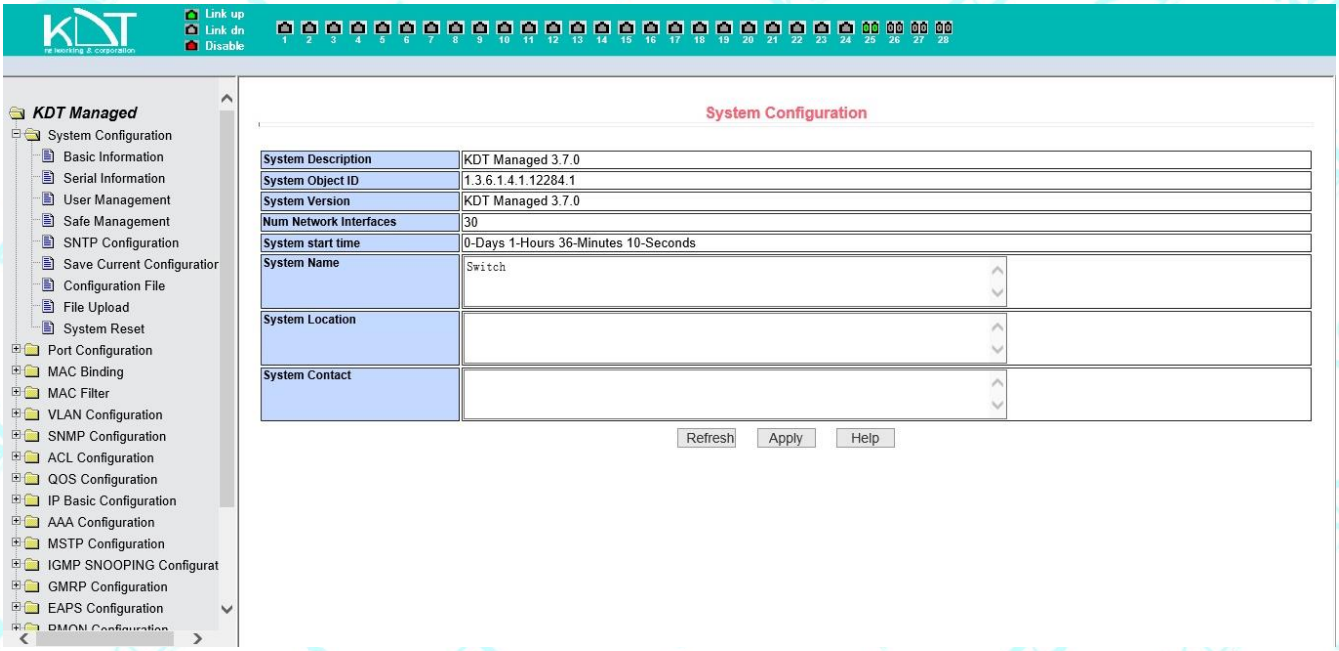
نام سیستم: نام سیستم سوئیچ را در شبکه نشان میدهد که کاربر نام سیستم را هم می تواند تغییر دهد.

:System Location

محل سیستم: محل فیزیکی سوئیچ را در شبکه نشان می دهد و کاربر می تواند نام محل سیستم را تغییر دهد.

:System Contact

سیستم مخاطب: نمایش لیست کسانی را که به سویچ میتوانند دسترسی داشته باشند را در اینجا وارد میکنیم.کاربرمی تواند اطلاعات مخاطب را هم تغییر دهد .

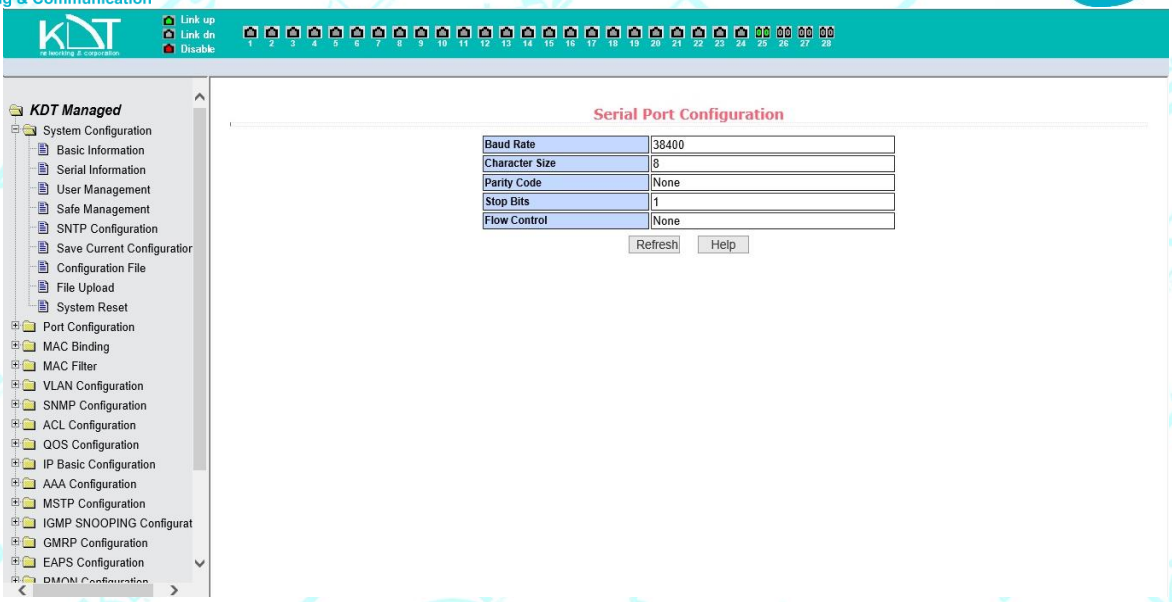


شکل(۹)

۲_۳_۲ صفحه پیکربندی Serial Port

شکل(۱۰) صفحه پیکربندی پورت سریال را نشان میدهد که نمایانگر سرعت ثانیه ای پورت سریال وسایر اطلاعات مربوط به آن است. هنگامی که کاربر میزبان به واسطه نرم افزار ترمینال (مانند Windows HyperTerminal , Putty) سوئیچ را میخواهد مدیریت کند، اطلاعات پورت ترمینال نرم افزار و پورت سریال باید با اطلاعات این صفحه یکسان باشد.

نکته: **38400**: baud Rate switch می باشد.

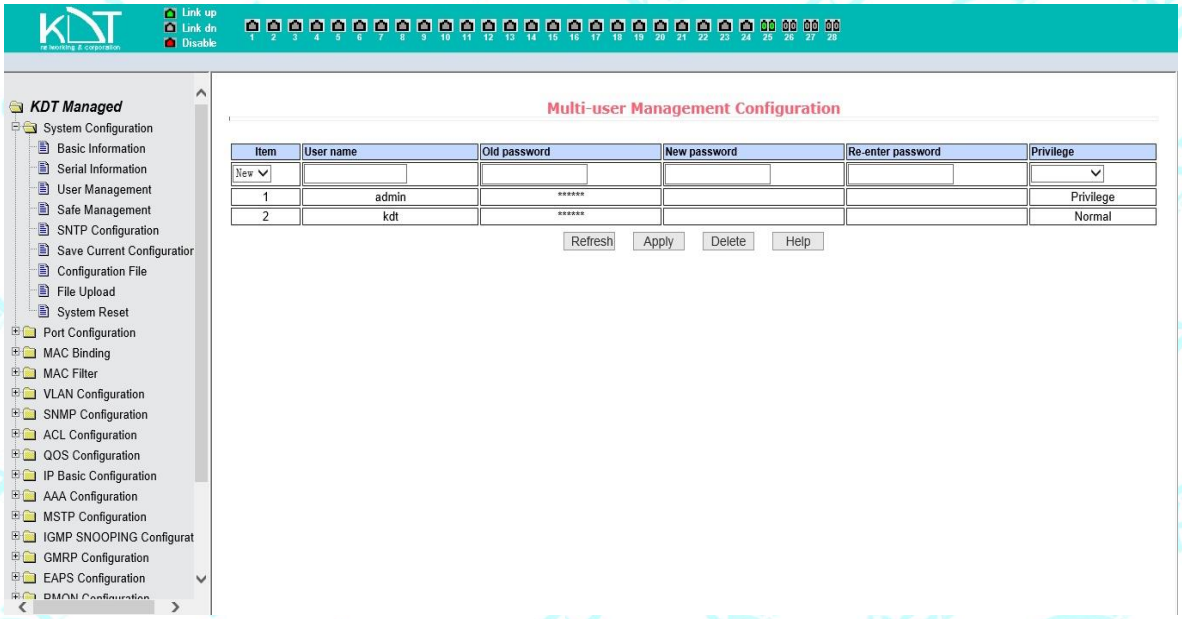


شکل(۱۰)

۳_۳_۲ صفحه پیکربندی مدیریت کاربران

شکل(۱۱) صفحه پیکربندی مدیریت کاربران را نشان میدهد. به وسیله این صفحه کاربر می تواند رمز کاربر سوئیچ را تغییر دهد. Telnet و Web از همان رمز کاربر admin استفاده می کند تا زمانی که کاربر دیگری فعال نباشد.

رمز ها مورد نفوذ پذیری هستند، و شما حداکثر تا ۶۱ حرف می توانید آن را تنظیم کنید. اگر می خواهید رمز عبور را تغییر دهید کاربر باید رمز عبور جدید را دوبار وارد کند. سپس روی کلید اعمال کردن(apply) کلیک می کند تا رمز عبور جدید فعال شود، حال کاربر به صفحه ورود مجدد نیاز دارد که بعد از اعمال کردن رمز عبور جدید پنجره ورود نمایان خواهد شد (درشکل ۷ نشان داده شده است). کاربر باید رمزجدید ورود به صفحه وب را وارد کند. در هر زمان به وسیله این صفحه کاربران می توانند کاربران دیگر را پیکربندی کنند. سوئیچ برای کاربران دیگر پیش فرض نشده است.



شکل(۱۱)

۴_۳_۲ صفحه پیکربندی امن

شکل(۱۲) صفحه پیکربندی امن را نشان می دهد. به واسطه پیکربندی این صفحه، مدیر می تواند مدیریت خدمات Telnet و Web و SNMP را کنترل کند.

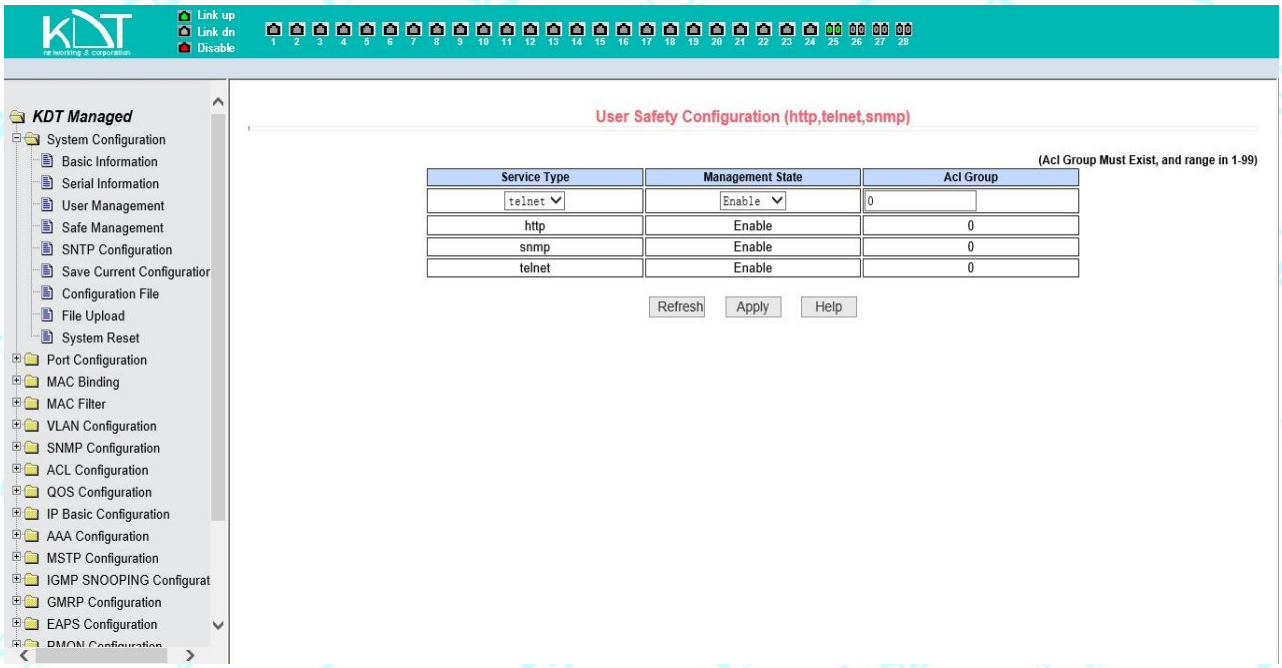
شما می توانید این خدمات را فعال یا غیر فعال کنید. این سرویس ها با IP استاندارد گروه ACL متصل می شوند.با پیاده سازی کنترل IP Address ، کاربر میزبان را برای دسترسی به این خدمات کنترل می کند.

به طور پیش فرض خدمات TELNET,WEB,SNMP در سوئیچ فعال است و عمل فیلترینگ انجام نمی شود، و تمام کاربران میزبان می توانند به سوییچ با این سه سرویس دسترسی یابد. اگر مدیر برای امنیت نخواهد یک یا تعدادی از این خدمات را برای بقیه کاربران فراهم کنند، می تواند یک یا چندتا از این خدمات را غیر فعال کند.

اگر مدیران فقط یک کاربر میزبان خاص را برای دسترسی به یک یا تعدادی از این سرویس ها بخواهند. یک یا چندتا از این خدمات می تواند فیلتر کردن ACL را انجام دهد. وقتی که یک سرویس نیاز دارد که فیلتر کردن ACL را انجام دهد، شما نیاز دارید که آن سرویس را فعال کنید و یک IP استاندارد گروه ACL را انتخاب کنید. (۱تا ۹۹) گروه ACL باید وجود داشته باشد.

اگر مدیر در این صفحه برای کنترل خدمات WEB مثل(مانند بستن سرویسWEB) موجب شود تا کاربران دیگر نتوانند ازصفحه WEB استفاده کنند، باید ذکر شود.

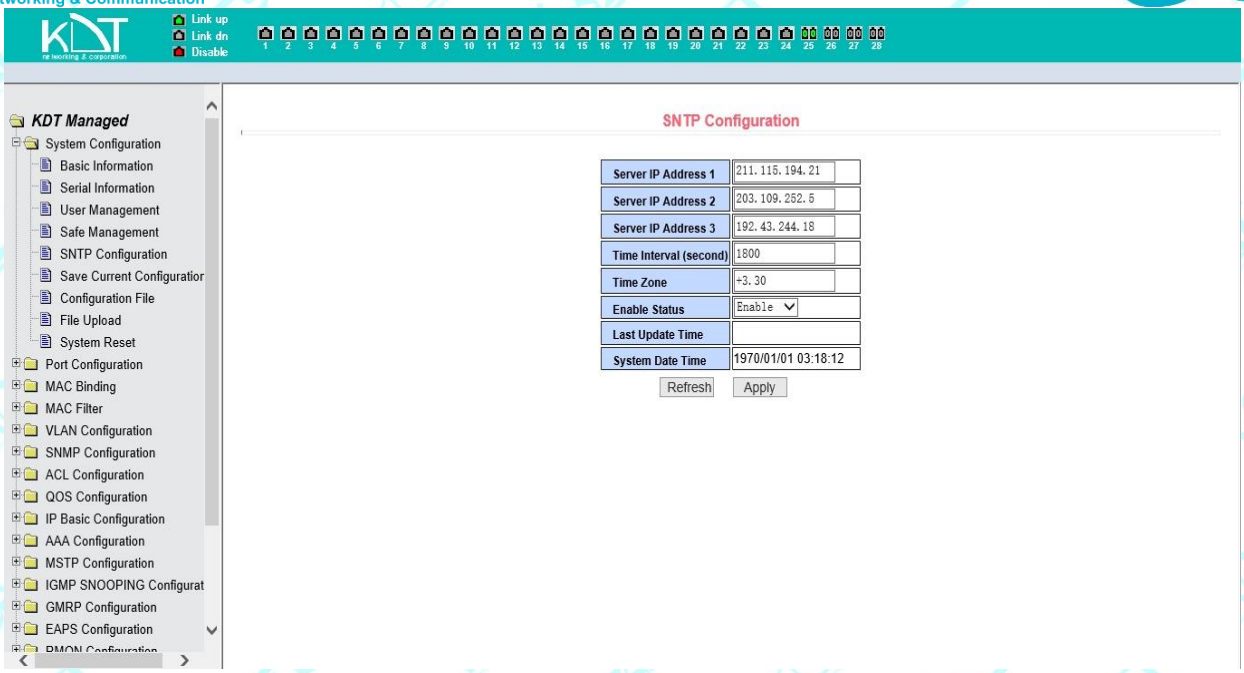
در این زمان از سایر راه ها برای ورود به سوئیچ استفاده می شود تا کنترل خدمات WEB را فعال کنند. طوری که کاربران بتوانند از صفحه وب استفاده کنند، (مانند باز کردن سرویسWEB).



شکل(۱۲)

۵_۳_۲ صفحه پیکربندی SNTP

شکل(۱۳)، صفحه پیکربندی SNTP را نشان می دهد. جایی که مدیر می تواند آدرس های IP سرور های تنظیم زمان در اینترنت وارد کند و یا ساعت سیستم را در صفحه به صورت دستی پیکربندی ببیند.

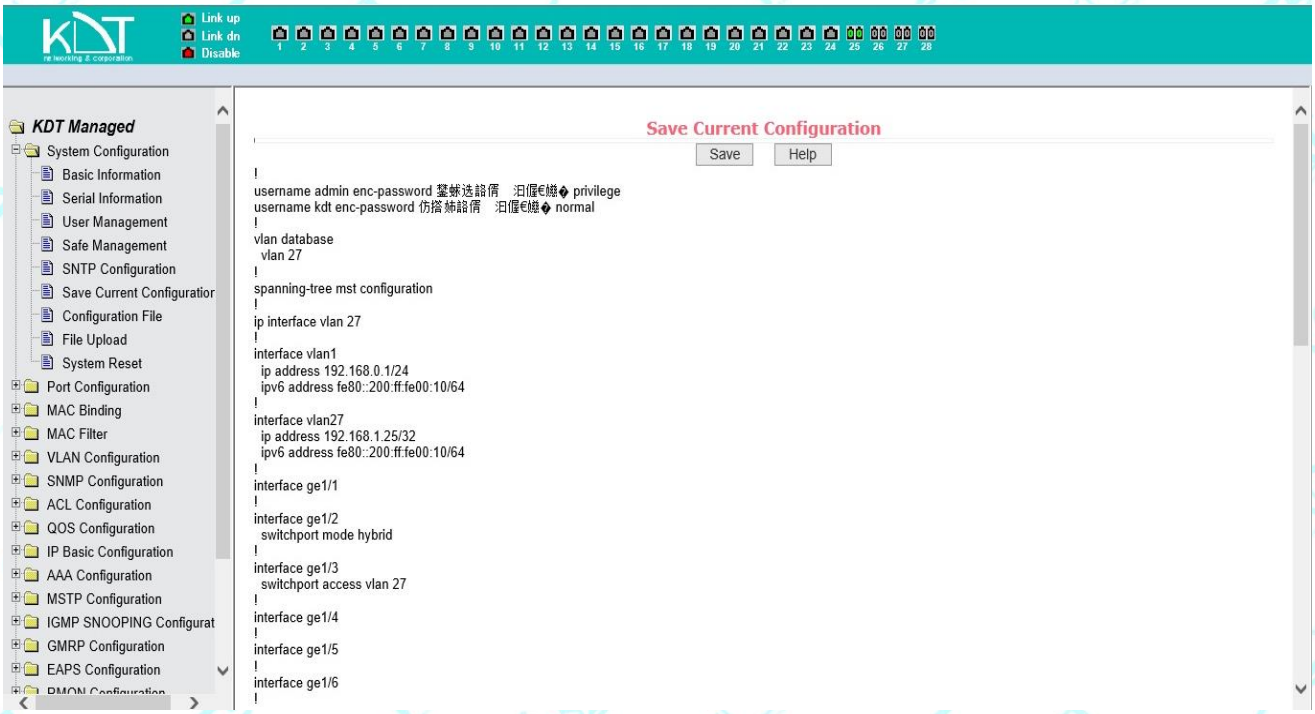


شکل(۱۳)

۶_۳_۲ صفحه پیکربندی ذخیره تنظیمات فعلی

شکل(۱۴)، صفحه پیکربندی تنظیمات فعلی را نشان می دهد. به وسیله این صفحه کاربر می تواند پیکربندی فعلی سوئیچ را ببیند. کلید ذخیره(save) پیکربندی فعلی سیستم رابه یک فایل پیکربندی ذخیره می کند. چون عمل ذخیره، ابتدا تراشه FLASH را پاک و سپس عمل ذخیره را انجام می دهد این عمل مقداری زمان معین می گیرد.

هنگامی که کاربر پیکربندی اش را انجام داد ومیخواهد که پیکربندی پس از راه اندازی مجدد سوئیچ از بین نرود، باید دکمه (Save) را در این صفحه، پیش ازخروج از صفحه وب، کلیک کند.

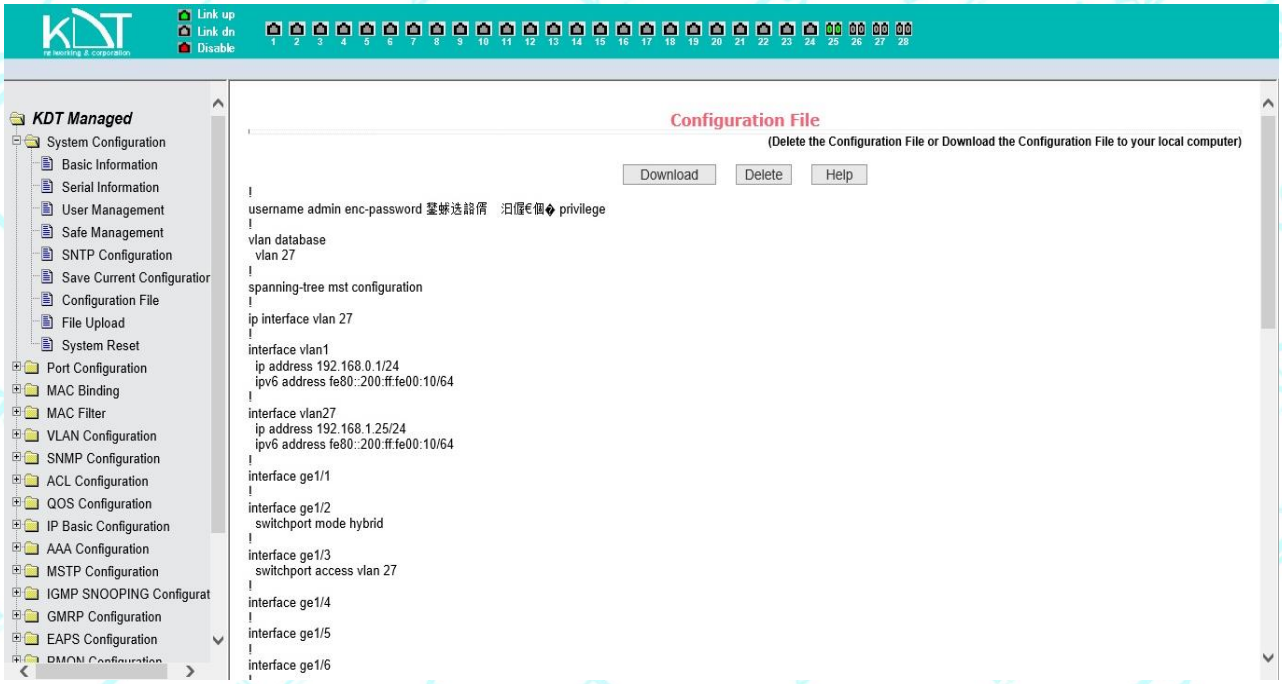


شکل(۱۴)

۷_۳_۲ صفحه پیکربندی فایل

شکل(۱۵)، صفحه پیکربندی فایل را نشان می دهد. این صفحه به کاربر اجازه می دهد که نخستین پیکربندی سیستم را ببینند. پیکربندی ابتدایی در واقع، فایل پیکربندی درFLASH است. وقتی هیچ فایل پیکربندی در FLASH نباشد سیستم با پیکربندی پیشفرض شروع شده است. کلید حذف(Delete) برای پاک کردن فایل پیکربندی درFLASH است.با کلیک کردن دکمه delete یک پنجره ظاهر می شود، این پنجره از کاربر می پرسد آیا حذف فایل پیکربندی را تایید میکنید؟ اگر تایید میکنید، دکمه okرا در پنجره را کلیک کنید و در غیر اینصورت دکمه(Cancel) را فشار دهید.

کلید(Download) برای دانلود فایل پیکربندی در کامپیوتر استفاده می شود. دکمه دانلود را کلیک کنید، یک پنجره ظاهر می شود، کاربر مسیر ذخیره و نام فایل پیکربندی را مشاهده می کند و ذخیره انجام می شود. فرمت فایل دانلود شده به صورت یک فایل cfg می باشد.



شکل(۱۵)

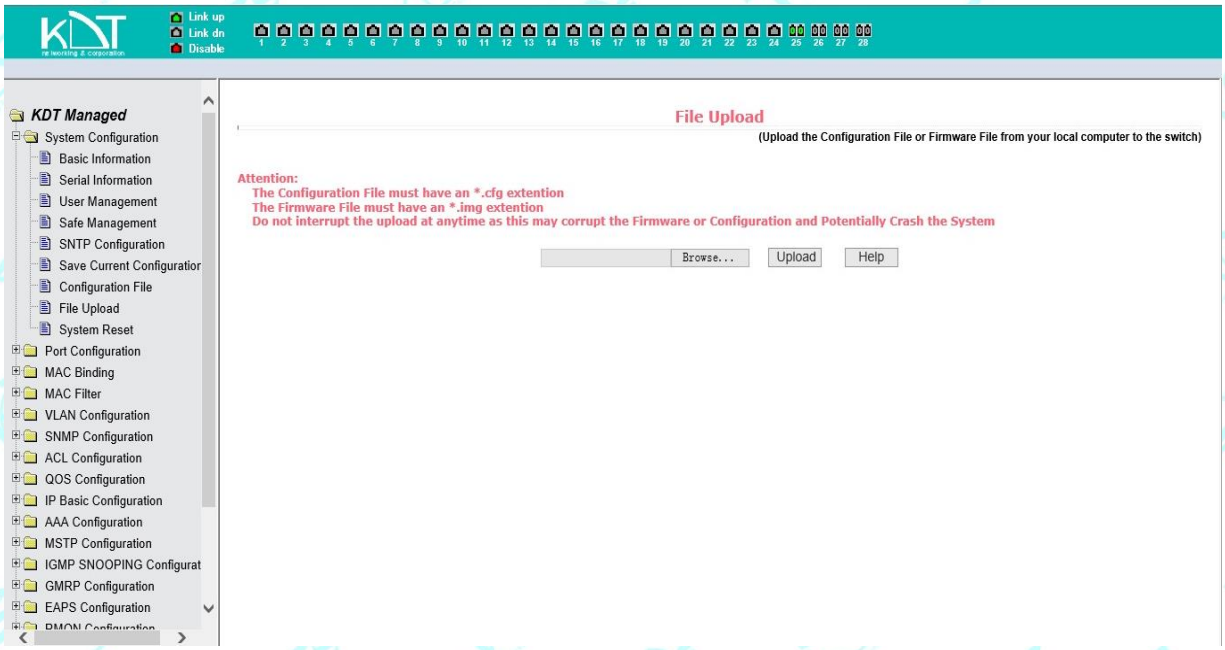
۸_۳_۲ صفحه بارگذاری فایل

شکل(۱۶)، صفحه بارگذاری فایل را نشان می دهد. به وسیله آن کاربر می تواند فایل پیکربندی ذخیره شده از قبل را در سوئیچ بارگذاری کند. دکمه مرور(Browse) را برای انتخاب مسیرفایل مورد نظر برای بارگذاری از کامپیوتر استفاده می شود.

دکمه(upload key) را برای انجام عملیات بارگذاری فایل پیکربندی بر روی سویچ استفاده می شود.

پسوند فایل پیکربندی باید cfg. باشد. فایل باید توسط سازنده فراهم شده باشد، و پسوند فایل سیستم عامل باید img. باشد.

روی صفحات دیگر یا جهت راه اندازی مجدد سوئیچ پیش از آنکه نتایج کامل بارگذاری صفحه نیامده، کلیک نکنید. در غیر این صورت با عدم موفقیت کامل بارگذاری فایل مواجه می شوید و باعث خرابی سیستم می شوید.

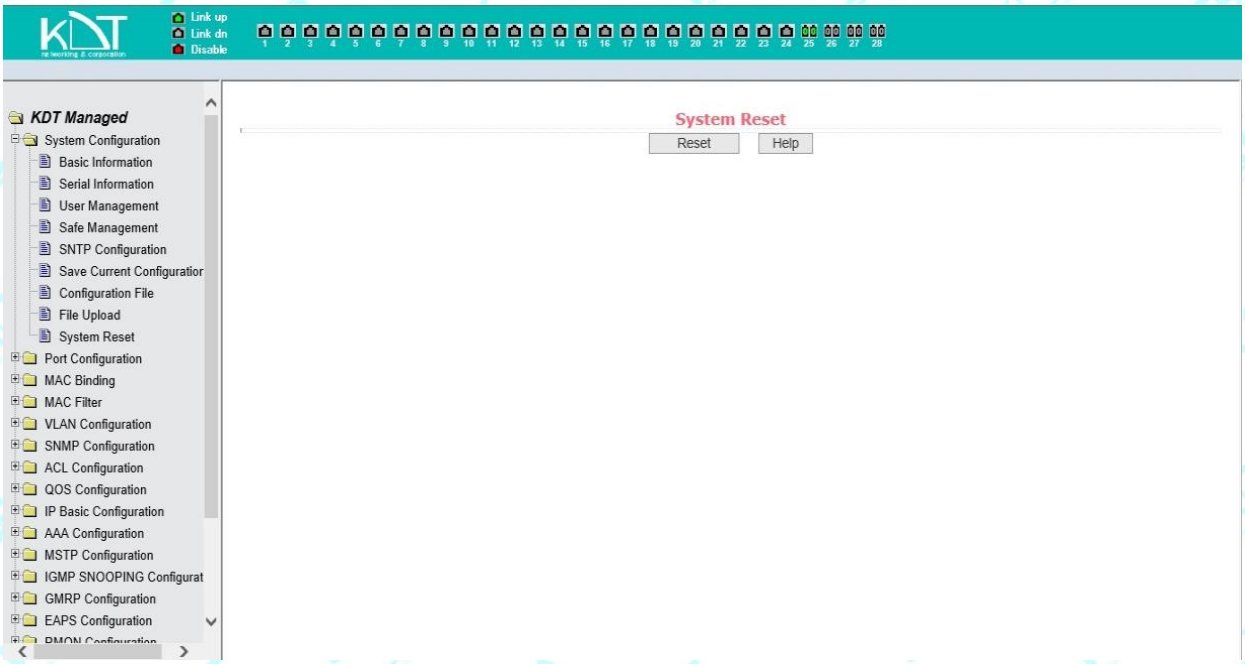


شکل(۱۶)

۹_۳_۲ راه اندازی مجدد سیستم

شکل(۱۷)، راه اندازی مجدد سیستم را نشان می دهد. به وسیله این صفحه کاربران می توانند سوئیچ را مجددا راه اندازی کنند. وقتی شما دکمه(restart) را کلیک میکنید یک پنجره ظاهر می شود و از شما سوال می پرسد که آیا کاربر برای راه اندازی مجدد سوئیچ مطمئن است؟

اگر موافقید دکمه ok و در غیر اینصورت دکمه cancel را فشار دهید. صفحات زمانی که در حال راه اندازی مجدد است، دیگر باز نمی شود.



شکل(۱۷)

۲_۴ ساختار درگاه یا Port

۱_۴_۲پیکربندی پورت/ صفحه نمایش پورت

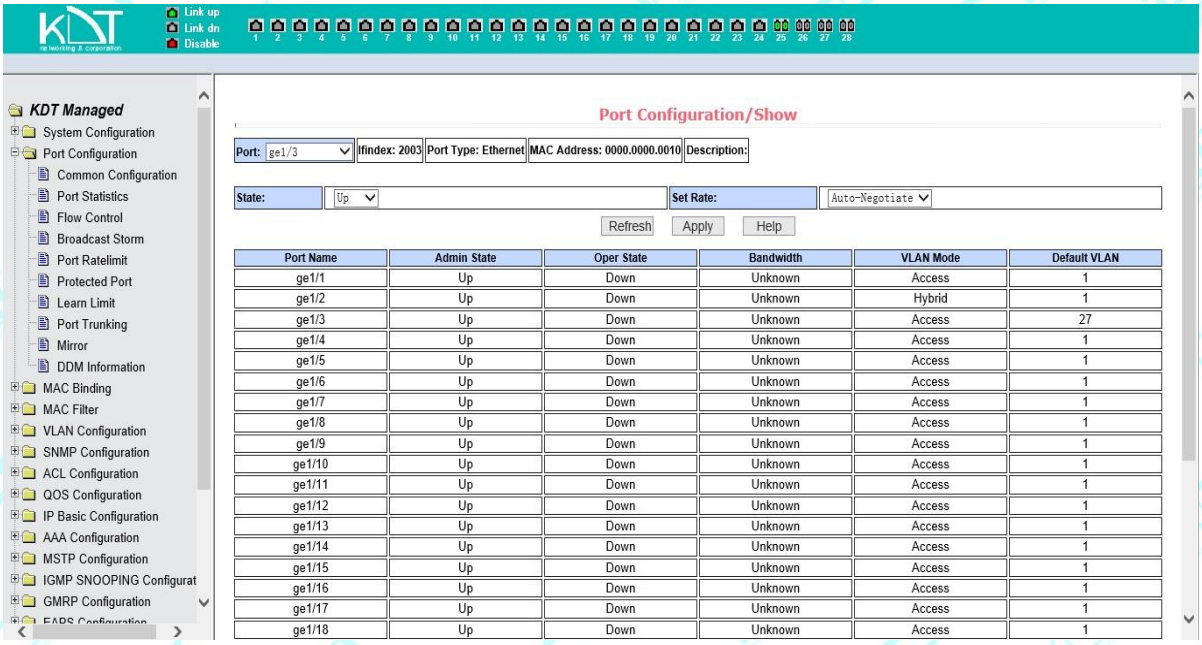
شکل(۱۸)، پیکربندی پورت/ صفحه نمایش پورت را نشان می دهد . کاربر به وسیله این صفحه می تواند پورت را فعال و غیر فعال کند، سرعت پورت را تنظیم کند، یا اطلاعات اصلی تمام پورت ها را ببینید.

برای تنظیم یک پورت خاص، شماره پورت دلخواه را از منوی کشویی برای تنظیم پورت انتخاب کنید.

موقعیت پورت به صورت پیش فرض در وضعیت up می باشد. شما می توانید از منوی کشویی برای غیر فعال کردن پورت، آن را در و ضعیت down بگذارید.

کاربر همچنین می تواند سرعت پورت را از منوی کشویی سرعت انتخاب و تنظیم کند.

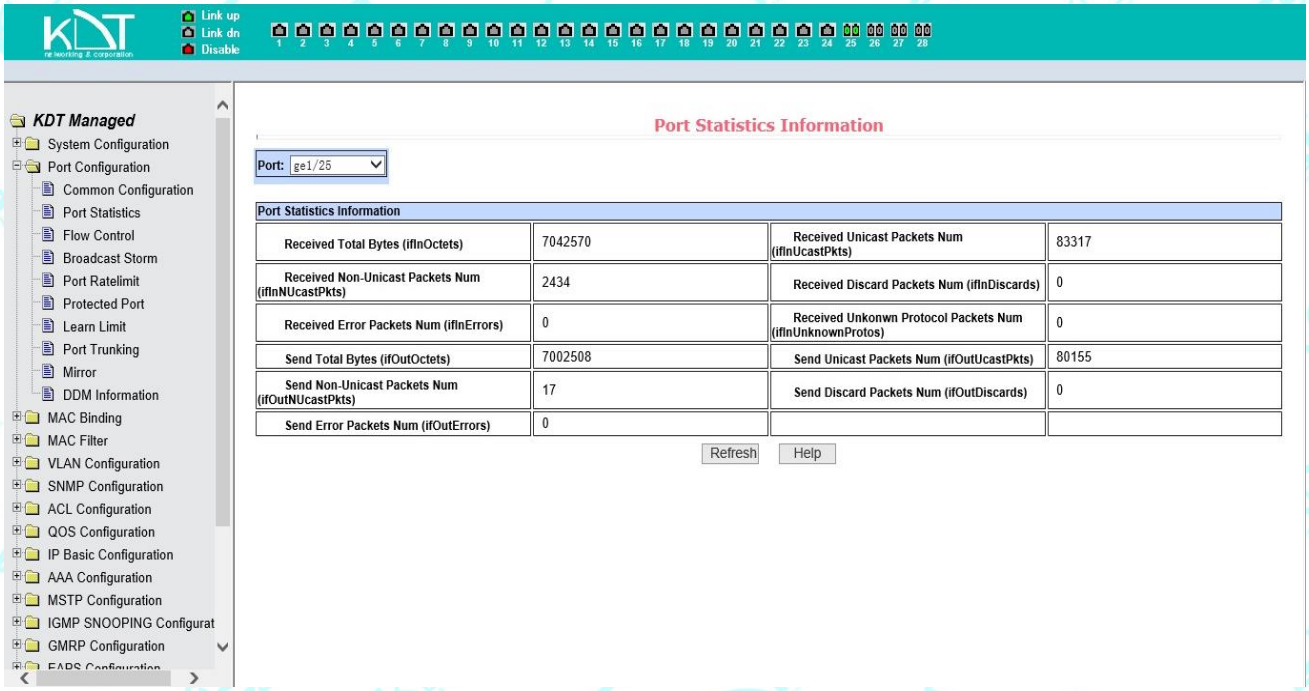
کاربر می تواند سایر اطلاعات اصلی برای تمام پورت ها را در این صفحه ببینند.



شکل(۱۸)

۲_۴_۲ صفحه اطلاعات آماری پورت

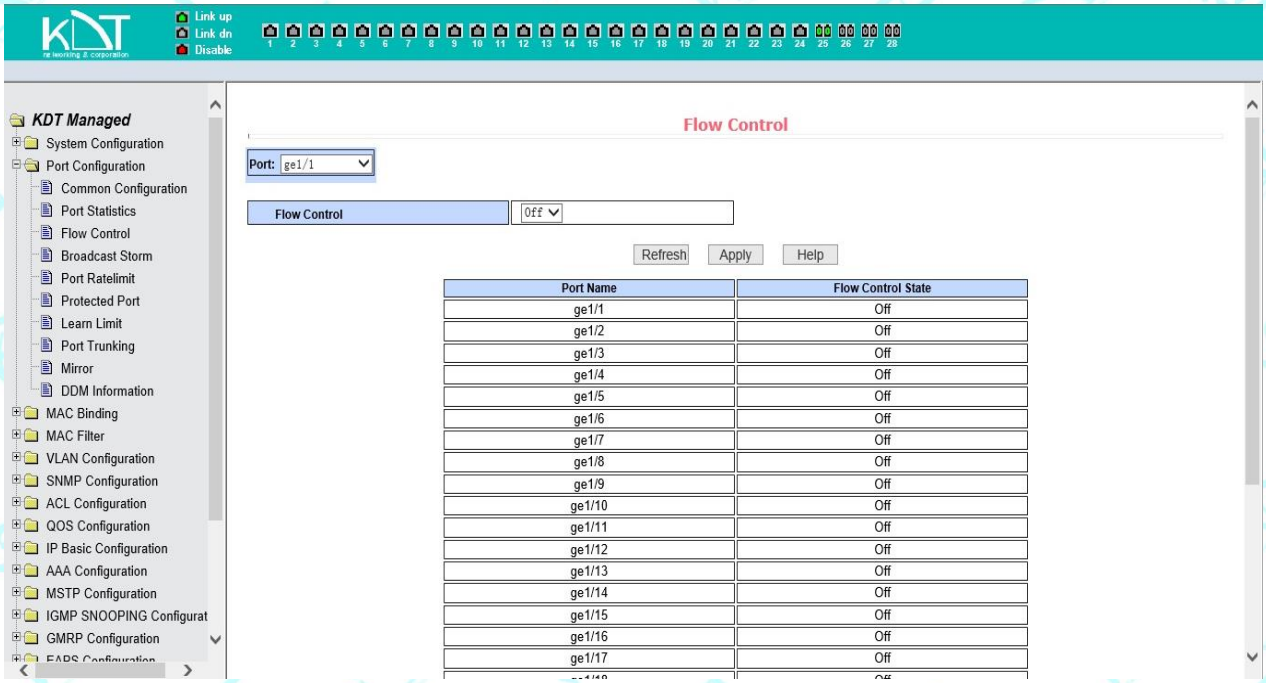
شکل(۱۹)، صفحه اطلاعات آماری پورت را نشان می دهد. برای دیدن اطلاعات یک پورت مشخص، یک پورت را از منوی کشویی برای مشاهده انتخاب کنید. کاربران می توانند آمارهای بسته های ارسال و دریافت پورت را به وسیله این صفحه ببینند.



شکل(۱۹)

۳_۴_۲ صفحه کنترل Flow (جریان)

شکل(۲۰)، صفحه کنترل جریان را نشان می دهد. کاربر می تواند از این صفحه برای باز یا بستن کنترل جریان هر پورت استفاده کند.در منوی کشویی گزینه های خاموش(off) یا روشن(on) برای فعال یا غیر فعال کردن کنترل جریان یک پورت استفاده میشود. در همین زمان به وسیله این صفحه شما میتوانید وضعیت کنترل جریان همه پورت ها را مشاهده کنید.



شکل(۲۰)

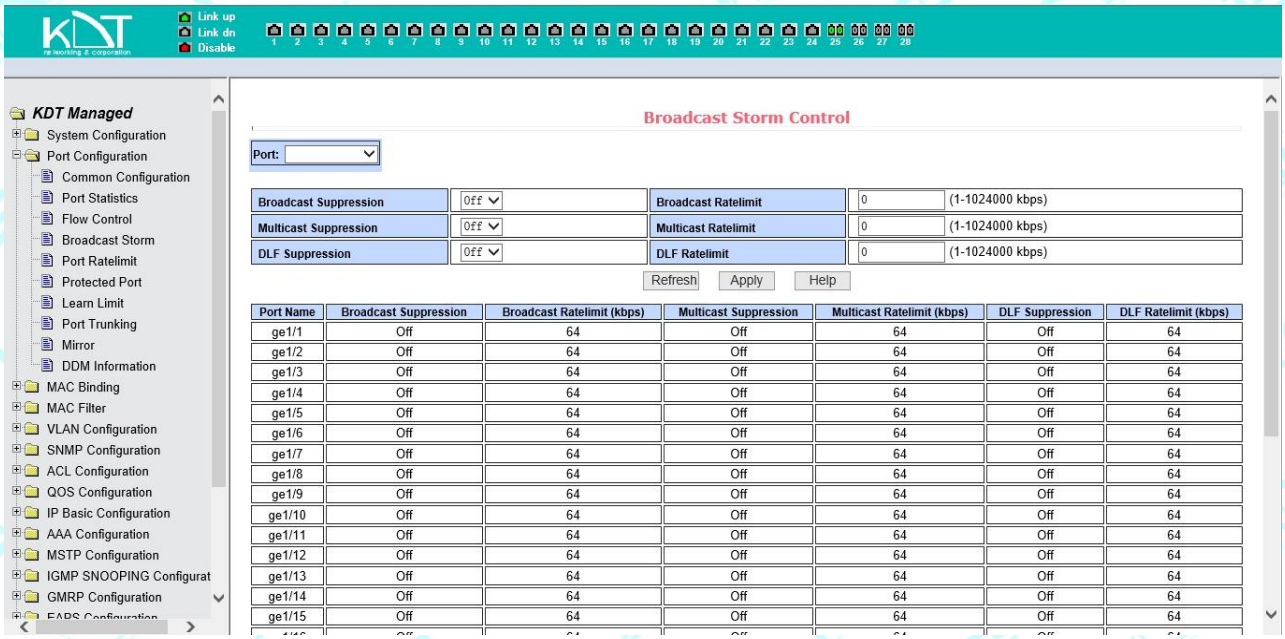
۴_۴_۲ صفحه کنترل (broadcast storm)

شکل(۲۱)، صفحه کنترل broadcast storm را نشان می دهد . این صفحه برای جلوگیری و کاهش بسته های broadcast ، بسته های multicast، وبسته ها DLF در port(درگاه) استفاده می شود.

برای پیکربندی پورت مورد نظر را از نوار کشویی پورت انتخاب کنید .on و off برای فعال و غیر فعال کردن توقیف و کاهش broadcast , multicast , DLF, در پورت می باشد. اصطلاح جلوگیری و کاهش برای محدود کردن سرعت در محدوده بین ۱تا ۱۰۲۴۰۰۰ در کیلو بایت، استفاده می شود.

محدوده سرعت در جلوگیری یا کاهش broadcast, DLF, multicast در یک پورت یکسان است.

به وسیله این صفحه شما می توانید وضعیت broadcast storm کل پورت ها را مشاهده کنید.



شکل(۲۱)

۵_۴_۲ صفحه محدوده سرعت پورت

شکل(۲۲)، صفحه محدوده سرعت پورت را نشان میدهد. این صفحه برای پیکربندی سرعتی که در آن پورت ها ارسال و دریافت می شوند، استفاده می شود .

ابتدا پورت مورد نظر را برای پیکربندی از نوار کشویی پورت انتخاب کنید.

Send Packets Rate Control (کنترل پهنای باند بسته ارسالی): برای, وارد کردن مقدار مورد نظر پهنای باند بسته های ارسالی است. این پهنای باند درمحدوده ۱تا ۱۰۲۴۰۰۰ در کیلوبایت استفاده می شود.

بعد از ورود مقادیر مورد نظر بر روی دکمه اعمال کردن (Apply) کلیک کنید.

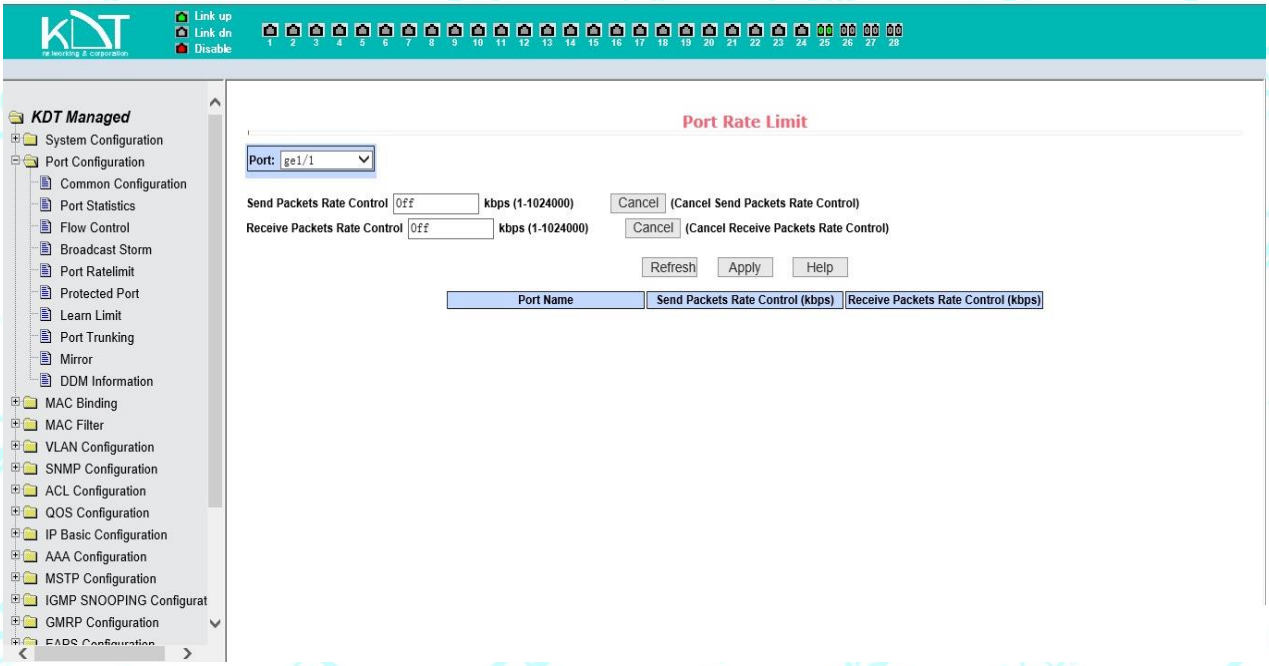
اگر پورتی بدون مقادیر (کنترل پهنای باند باشد)، نشان دهنده خاموش بودن آن است. کلید cancel مربوط به غیر فعال کردن (کنترل پهنای باند ارسالی) استفاده می شود.

Receive Packets Rate Control (کنترل پهنای باند بسته دریافتی) : برای وارد کردن مقدار مورد نظر پهنای باند بسته های دریافتی است. این پهنای باند در محدوده ۱ تا ۱۰۲۴۰۰۰ در کیلوبایت استفاده می شود.

بعد از ورود مقادیر موردنظر بر روی دکمه اعمال کردن(apply) کلیک کنید.

اگر پورتی بدون مقادیر (کنترل پهنای باند باشد)، نشان دهنده خاموش بودن آن است. کلید cancel مربوط به غیر فعال کردن (کنترل پهنای باند دریافتی) استفاده می شود.

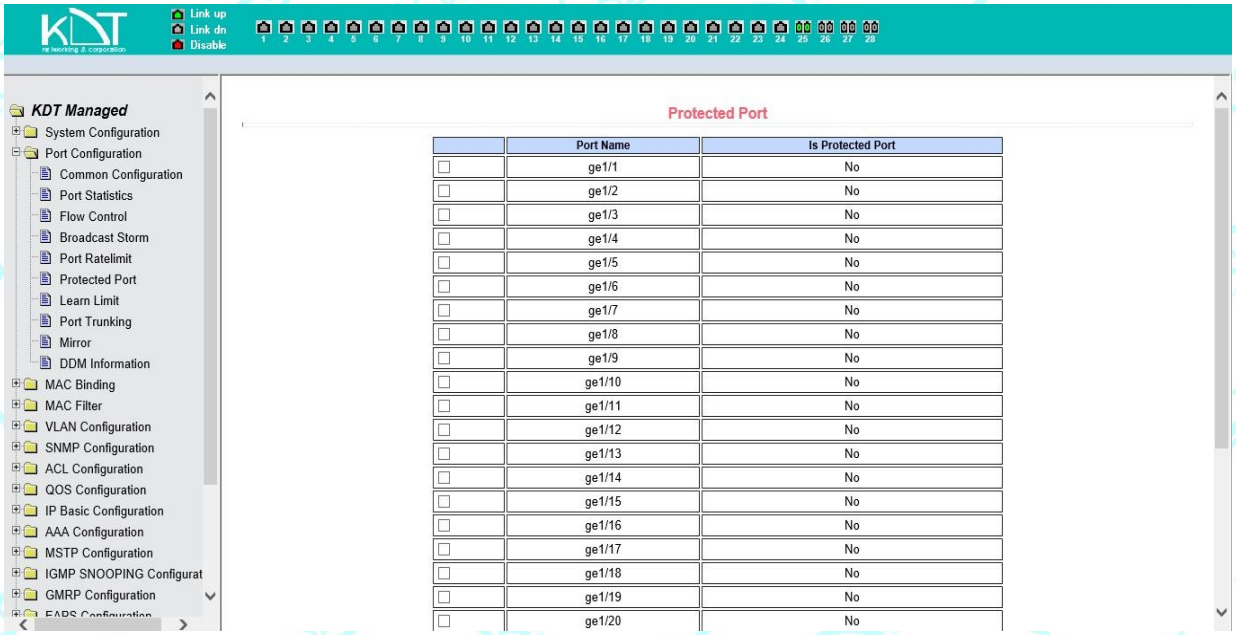
اگر پورتی با پهنای باند دلخواه پیکربندی شده باشد، در لیست نمایش داده خواهد شد.



شکل(۲۲)

۲_۴_۶ صفحه پورت محافظت شده

شکل(۲۳)، پورت محافظت شده را نشان می دهد. این صفحه برای پیکربندی محافظت از پورت استفاده می شود.

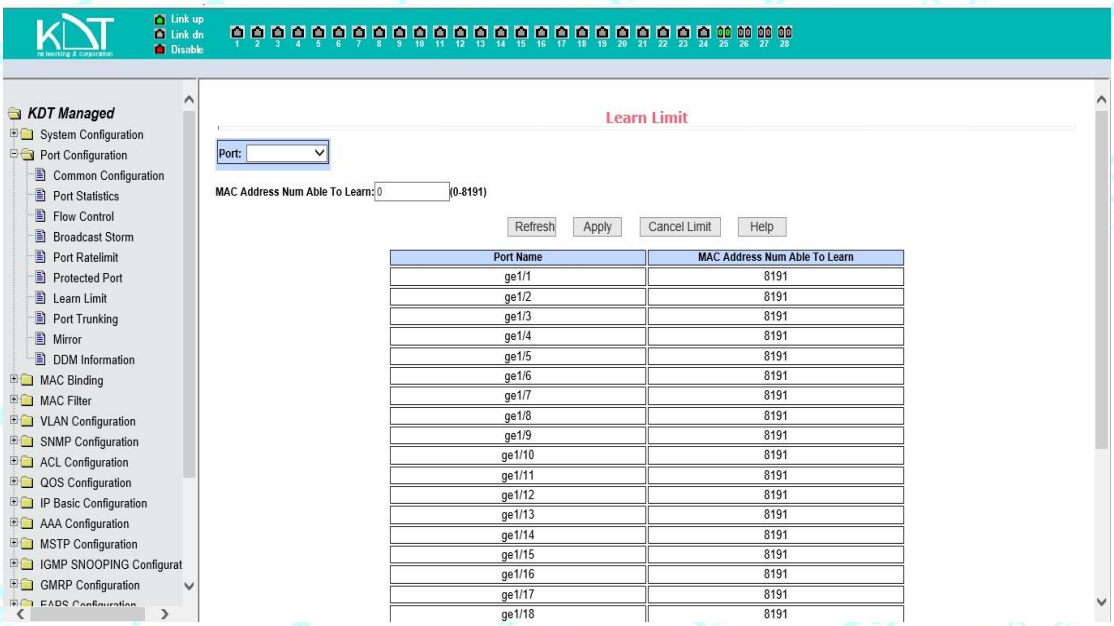


شکل(۲۳)

۲_۴_۷ صفحه محدود کردن پورت

شکل(۲۴)، صفحه محدوده کردن پورت را نشان می دهد. این صفحه برای تعیین کردن تعداد آدرس های MAC که پورت می تواند در برگیرد، استفاده می شود.

محدوده ی آن از ۱تا ۸۱۹۱ است. مقدار پیش فرض 8191 است، که همچنین بیشترین مقدار هم است.وقتی این عدد در ردیف هر پورت وارد شده باشد نشان میدهد که پورت با محدودیت های در برگیرندگی پیکر بندی نشده است. در جدول این صفحه لیست تعداد MAC دربرگیرنده برای تمام پورت ها را نشان می دهد.



شکل(۲۴)

۸_۴_۲ صفحه پیکربندی Port Trunking

شکل(۲۵)، صفحه پیکربندی Port Tunking را نشان می دهد. این صفحه به کاربر اجازه می دهد تا Port Trunking را پیکربندی کند. این صفحه چهار قسمت را شامل میشود:

Trunk Group ID: شماره گروه ترانک

Trunk Method: حالت ترانک

Able Config Port: پورت قابل تنظیم

Member Port: پورت های عضو گروه ترانک

برای ایجاد یا تغییر Port Trunk، کاربر نیاز دارد تا یک Trunk group ID از شماره ۱ تا ۸ انتخاب کند.

در کادر Trunk Group ID از لیست مربوطه یکی را به دلخواه انتخاب کنید. اطلاعات گروه Trunk در اعضای گروه پورت قابل مشاهده است.بعد از انتخاب شماره Trunk مورد نظر روی دکمه (creat trunk group)کلیک کنید.

اگر Trunk group را ایجاد کرده باشید ، درنوار نمایش Trunk Group ID ، داخل پرانتز مقابل شماره ترانک پیغام Created (ساخته شد) نمایش داده می شود. اگر Trunk group ایجاد نشده باشد، داخل پرانتز مقابل شماره ترانک، پیغام Uncreated(ساخته نشد) نمایش داده می شود.

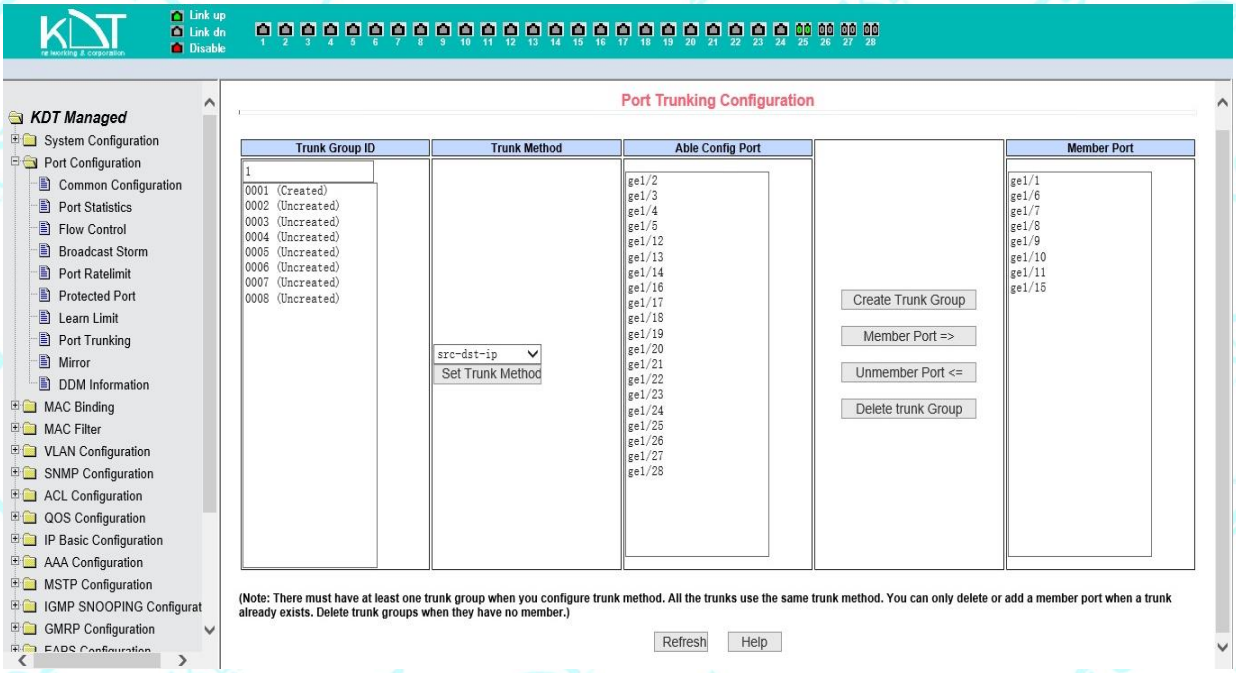
برای تنظیم (Trunk method)یک گزینه از نوار لیست کشویی انتخاب کرده و روی دکمه(Set Trunk method) کلیک کنید.سپس برای اضافه کردن یک Port Trunk ابتدا پورت مورد نظر را از لیست (Able Config Port) انتخاب و روی دکمه(member port) کلیک کنید. برای از میان بردن یک پورت از پورت های موجود در (group member port) ابتدا آن را از لیست انتخاب کرده و روی دکمه(Un member) کلیک کنید. برای پاک کردن کل trunk group ، روی دکمه (Delet trunk group) کلیک کنید،

شما می توانیداعضای پورت را در trunk Group موجود حذف یا اضافه کنید، در شرایطی که اعضا پورتی نداشته باشد ،trunk group را حذف کنید.

Trunk Method شش نوع حالت قابل انتخاب را فراهم می کند که عبارتند از:

۱. بر اساس مبدا MAC Address
۲. بر اساس مقصد MAC Address
۳. بر اساس مبدا و مقصد MAC Address
۴. بر اساس مبدا IP Address
۵. بر اساس مقصد IP Address
۶. بر اساس مبدا و مقصد IP Address

سوئیچ از هشت گروه Trunk Group پشتیبانی می کند و هر گروه هشت Trunk Port را پشتیبانی میکند. هر (trunk group) میتواند Trunk Port مخصوص به خود را پیکربندی کند.



شکل(۲۵)

۹_۴_۲ صفحه پیکربندی Port Mirror

شکل(۲۶)، صفحه پیکربندی Port Mirror را نشان می دهد. این صفحه به کاربراجازه می دهد که Port Mirror را پیکربندی کند.

Port Mirror یکی از روشهای آنالیز ترافیک شبکه است.

Port Mirror به واسطه آینه کردن پورت های ورودی و خروجی میتوان بسته های دیتا را کنترل و مانیتور کرد.

توجه داشته باشید که فقط یک Port Mirror می توان انتخاب کرد وInput Mirror و Output Mirror را میتوان به چند حالت انتخاب کرد.

این صفحه ۴ قسمت را شامل میشود:

۱. (Mirror port)نام آینه پورت

۲. (Able Config Mirrored Ports)پورت های قابل پیکربندی

۳. (Mirror Direction)مسیر آینه

۴. (Mirror Config Info)اطلاعات پیکربندی آینه

برای اجرای Port Mirror نام یک پورت را به طور کامل در فیلد Mirror port (جدول سمت راست) وارد کنید. فقط نام یک پورت را می توان وارد کرد. سپس پورتی که قرار است آینه شود را از قسمت(Able Config Mirrored Ports) انتخاب کنید.حال باید مسیری که قرار است به صورت آینه رصد شود را از قسمت Mirror Direction انتخاب کنید و در آخر روی دکمه اعمال کردن کلیک کنید تا عملیات آینه کردن اجرا شود. با اجرا شدن عملیات آینه در قسمت Mirror Config Info اطلاعات مربوط به Mirror Port نمایش داده می شود.

هنگامی که RECIEVE (دریافت) در Mirror Direction (مسیر آینه)انتخاب می شود، نشانگر این است بسته های دریافتی رسیده میشود.

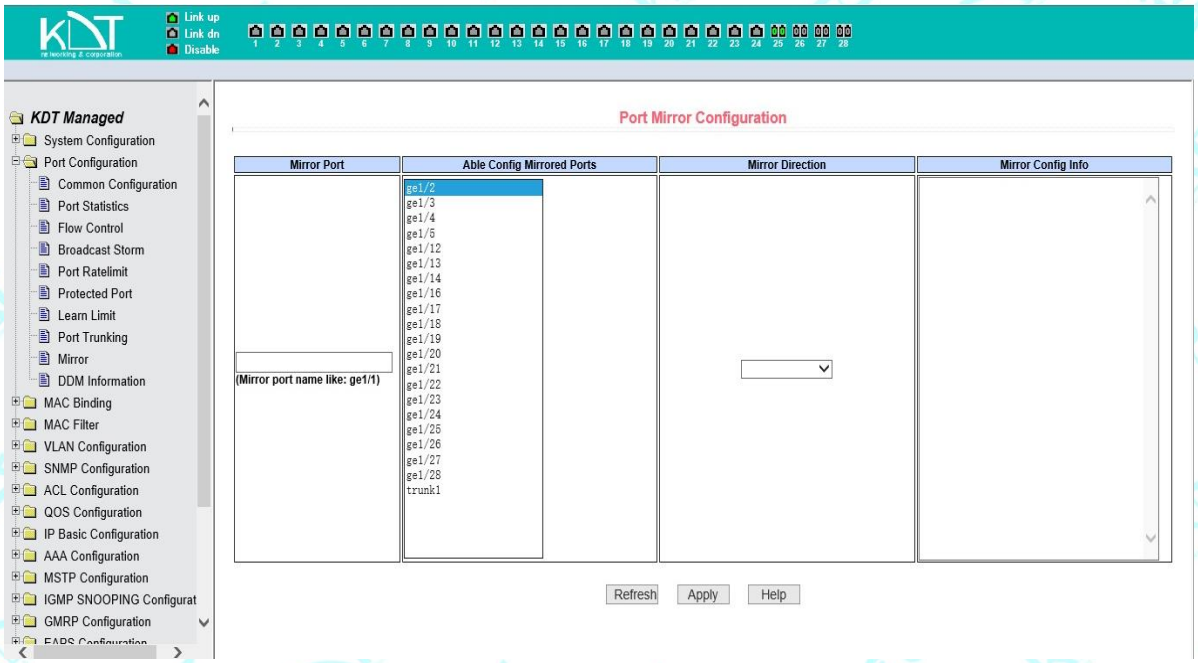
TRANSMIT (ارسال) نشانگر این است که بسته ها ارسال می شوند .

Both (جفت) نشان می دهند که تمام بسته ها در حال ارسال و دریافت هستند .

NOT_RECIEVE (دریافت نشود) بسته دریافتی کنسل شده است .

NOT_ TRANSMIT (ارسال نشود) نشان می دهد که بسته ارسالی کنسل شده است .

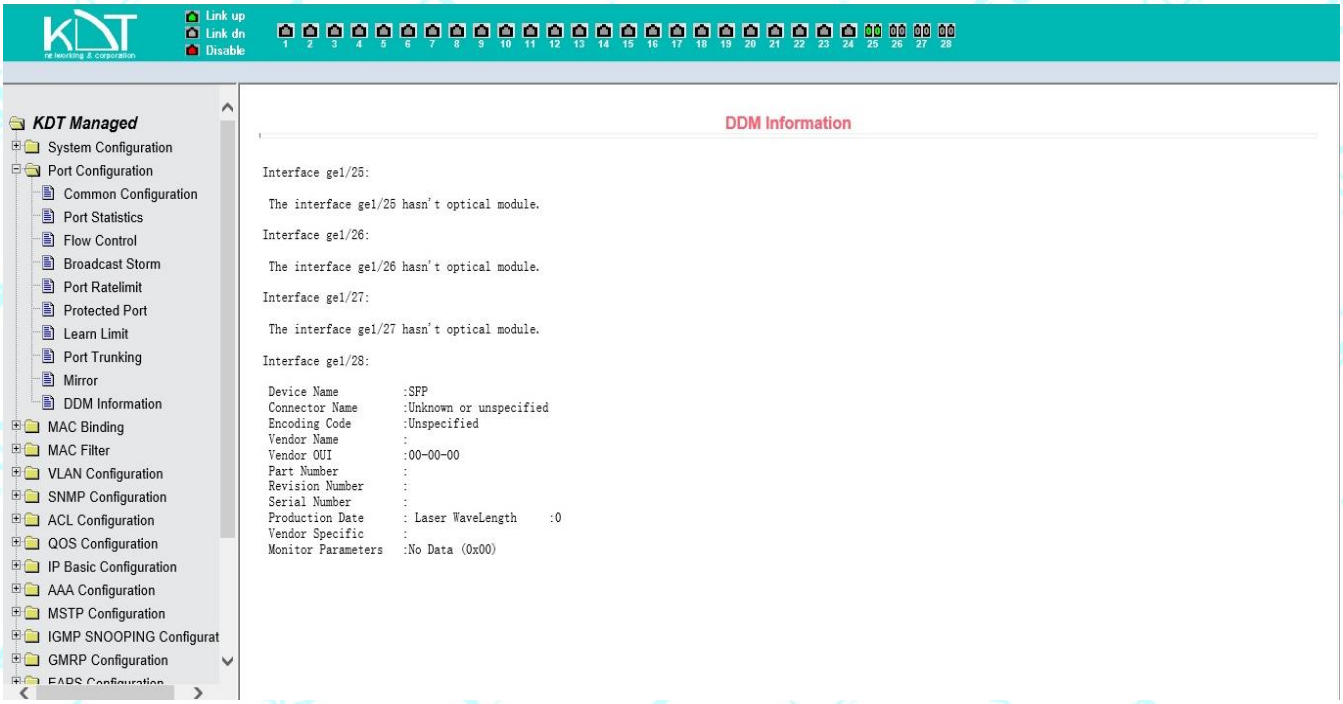
NEITHER نشان می دهد دریافت وارسال کنسل شده است، و برای همین Port Mirror کنسل میشود.


Link up
Link dn
Disable
KDT Managed
System Configuration
Port Configuration
Common Configuration
Port Statistics
Flow Control
Broadcast Storm
Port Ratelimit
Protected Port
Learn Limit
Port Trunking
Mirror
DDM Information
MAC Binding
MAC Filter
VLAN Configuration
SNMP Configuration
ACL Configuration
QOS Configuration
IP Basic Configuration
AAA Configuration
MSTP Configuration
IGMP SNOOPING Configurat
GMRP Configuration
Port Mirror Configuration
Mirror Port
Able Config Mirrored Ports
Mirror Direction
Mirror Config Info
(Mirror port name like: ge1/1)
ge1/2
ge1/3
ge1/4
ge1/5
ge1/12
ge1/13
ge1/14
ge1/16
ge1/17
ge1/18
ge1/19
ge1/20
ge1/21
ge1/22
ge1/23
ge1/24
ge1/25
ge1/26
ge1/27
ge1/28
trunk1
Refresh
Apply
Help

شکل(۲۶)

۲_۴_۱۰ صفحه مشخصات DDM

شکل(۱-۲۶) صفحه مشخصات Fiber Uplink را نشان می دهد.این صفحه برای مشاهده مشخصات فیبر نوری استفاده می شود.



شکل (۱-۲۶)

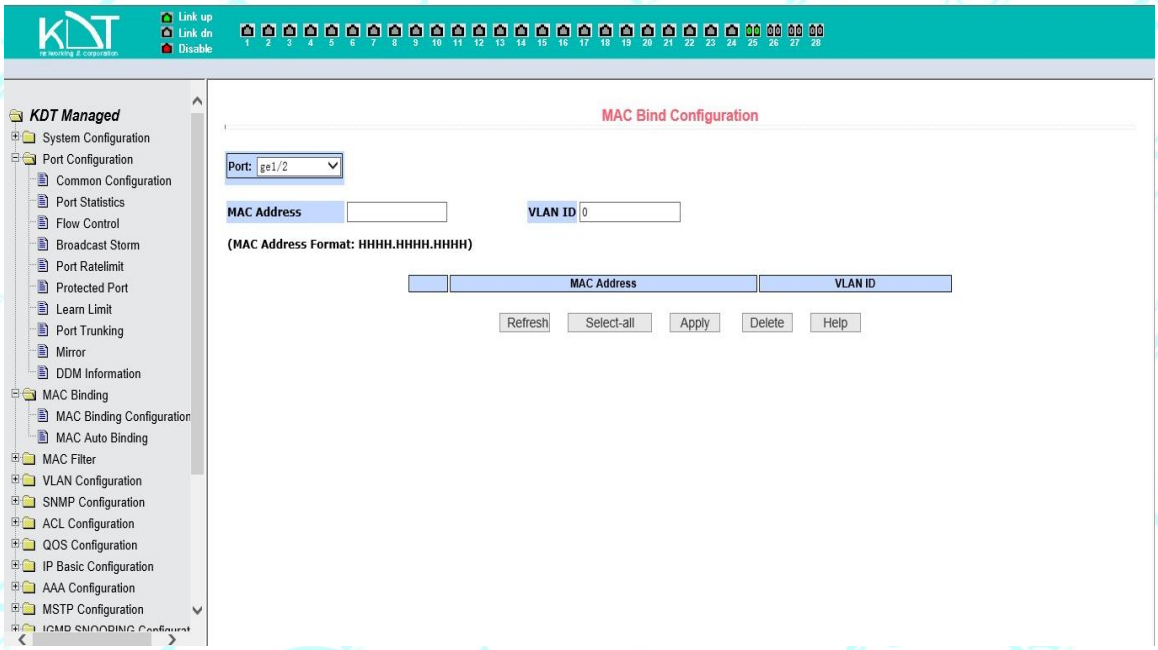
۲_۵ MAC Bind

۲_۵_۱ صفحه پیکربندی MAC Bind

شکل(۲۷)، صفحه پیکربندی MAC Bind را نشان می دهد. این صفحه برای پیوند دادن Port به Address MAC استفاده می شود.

قسمت MAC Address برای وارد کردن MAC Address مورد نظر استفاده میشود.

قسمت VLAN ID برای وارد کردن شماره VLAN که MAC Address به آن متعلق میشود ، استفاده می شود.



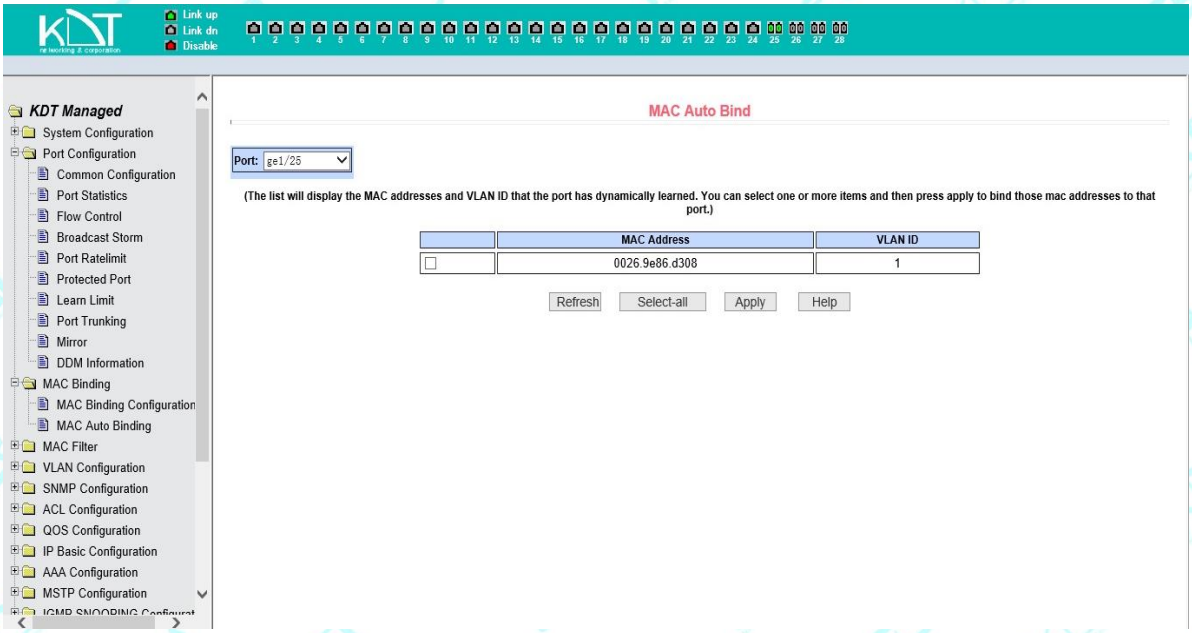
شکل(۲۷)

۲_۵_۲ صفحه خودکار MAC Bind

شکل(۲۸)، صفحه خودکار MAC Bind را نشان می دهد. این صفحه برای انجام پیوستن خودکار MAC Address به شماره Vlan که پورت در آن Vlan قرار گرفته استفاده می شود.

MAC Address و شماره VLAN در دو ردیف جدول آورده شده اند.

شما میتوانید موارد را از آنها انتخاب و آنها را خودکار درآورید.

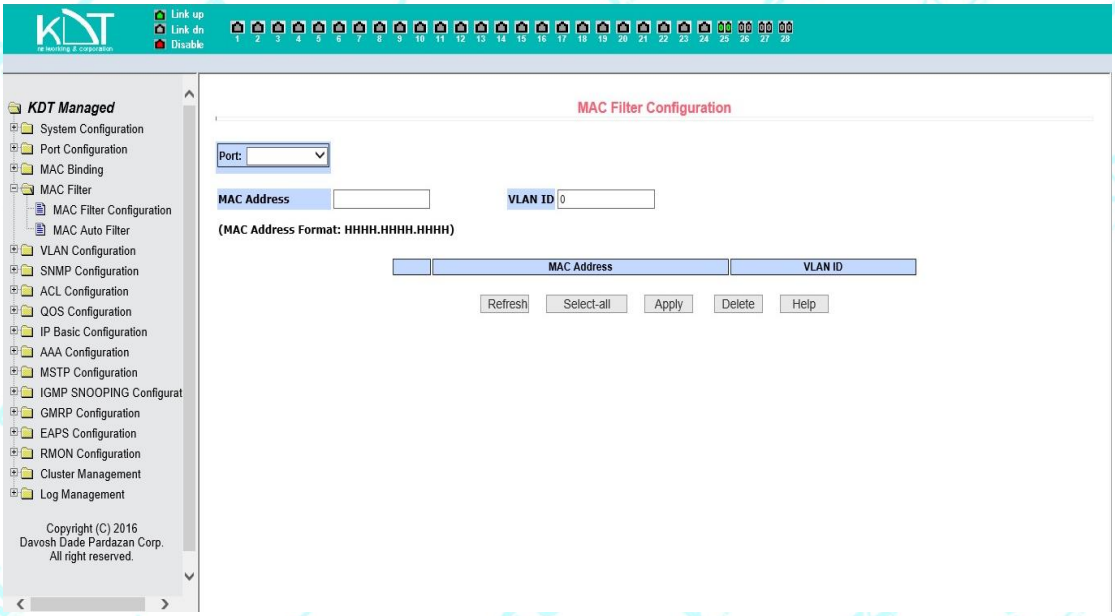


شکل(۲۸)

۶_۲ فیلترکردن MAC

۱_۶_۲صفحه پیکربندی فیلترکردن MAC

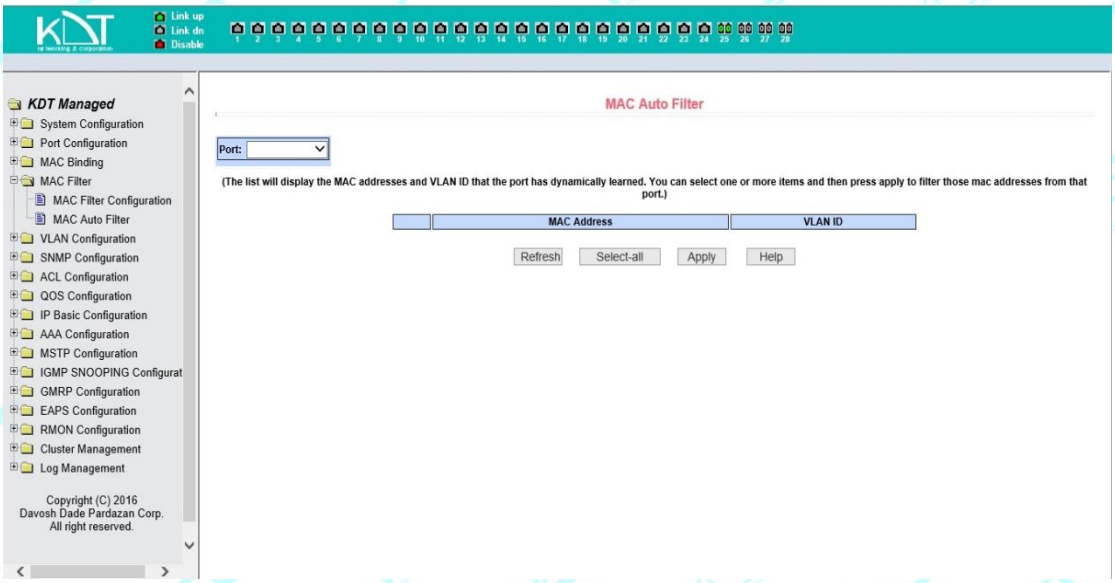
شکل(۲۹)، صفحه پیکربندی فیلترکردن MAC را نشان می دهد. این صفحه برای فیلترکردن Address MAC ها استفاده می شود.فیلد MAC Address روی صفحه، برای وارد کردن MAC Address مورد نظر جهت فیلتر کردن مورد استفاده قرار می گیرد. فیلد VLAN ID برای وارد کردن شماره VLAN که MAC Address در آن باید فیلتر شود مورد،استفاده قرار می گیرد.



شکل(۲۹)

۲_۶_۲ فیلترکردن خودکار MAC

شکل(۳۰)،صفحه فیلتر کردن خودکار MAC را نشان می دهد برای .فیلتر کردن MAC به طور خودکار نیاز است شما ابتدا پورت مورد نظر که قرار است MAC Address ها در آن فیلتر شوند را انتخاب کنید.سپس MAC Address ها به صورت خود کار در جدول نمایش داده میشوند که میتوانید آنها را انتخاب و در آخر روی دکمه اعمال کردن (Apply) کلیک کنید.



شکل(۳۰)

۲_۷ پیکربندی VLAN

۲_۷_۱ صفحه اطلاعات VLAN

شکل(۳۱)، صفحه اطلاعات VLAN فعلی را نشان می دهد. این صفحه فقط صفحه نمایشی است و قابلیت تنظیم ندارد و شما میتوانید VLAN های ساخته شده، وضعیت VLAN ها و پورت های عضو VLAN را مشاهده کنید.

در پنجره کشویی تمام vlan های ساخته شده رو میتوانید مشاهده و انتخاب کنید.، در جدول داخل صفحه، لیستVLAN ID را نشان میدهد که تا ۳۰ ردیف را می توانید مشاهده کنید، وهمچنین وضعیت و اعضای پورت هر VLAN نیز قابل مشاهده است.

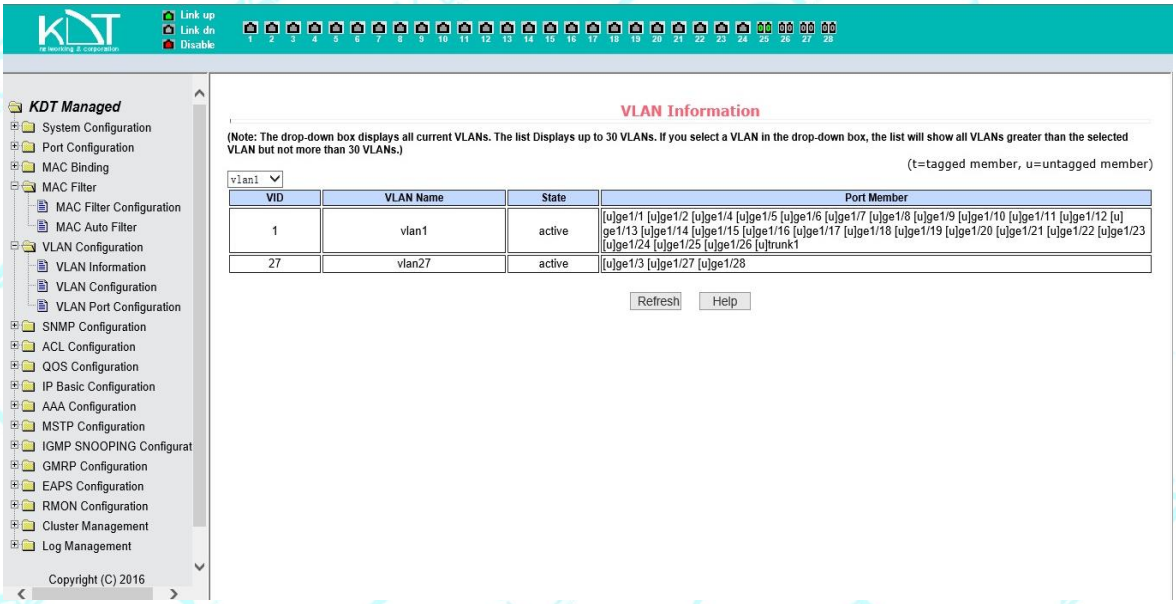
شما می توانید یک VLAN را از پنجره کشویی انتخاب کنید، و لیست اطلاعات آن را مشاهده کنید. اما اگر تمام vlan ها بیشتر از ۳۰ عدد نباشند، صرف نظر از منوی کشویی که کدامvlan را انتخاب می کند، لیست اطلاعات، تمام vlan ها را نمایش خواهد داد .

یک پورت نمی تواند عضوی از یک VLAN باشد، مگر یک عضو علامت دار یا غیر علامت دار از یک VLAN باشد.

پورت ها به دو صورت نشانه گذاری می شوند که عبارتند از:

tagged => t : یعنی پورت یک عضو علامت دار این VLAN می باشد.

untagged => u : یعنی پورت یک عضو غیر علامت دار این VLAN می باشد.



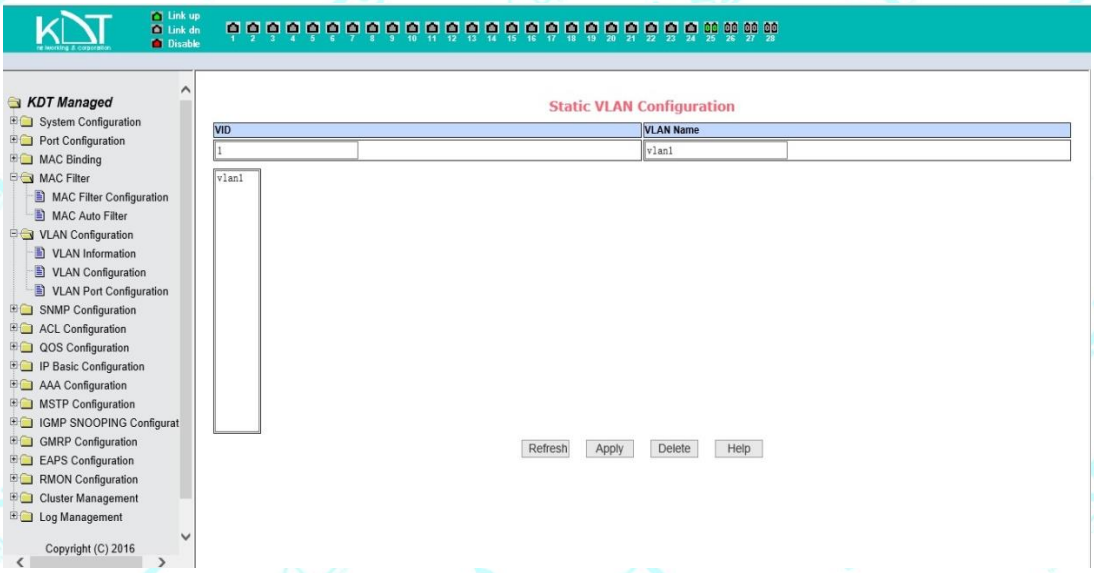
شکل(۳۱)

۲_۷_۲ صفحه سازماندهی VLAN

شکل(۳۲) صفحه پیکربندی شده VLAN را نشان میدهد. این صفحه به کاربران اجازه می دهد تا VLAN ایجاد کنند. اگر شما می خواهید که یک VLAN جدید بسازید، ابتدا در فیلد VID از دامنه ۲ تا ۴۰۹۴ یک عدد را وارد میکند .اسم VLAN توسط کاربر برطبق VLAN ID وارد میشود و برای تغییر نام می تواند از همین صفحه استفاده کند. بعد ساخت VLAN روی دکمه اعمال کردن (Apply) کلیک کنید

توسط لیست VID وVLAN Name و VLAN که توسط کاربر ایجاد شده را نمایش میدهد. سوئیچ به طور پیش فرض VLAN1 را می سازد ونمی تواند پاک شود.

اگر شما می خواهید یک VLAN را پاک کنید، کاربر نیاز دارد که بر روی VLANمربوط در لیست کلیک کند .VLAN در ردیف فعال نمایان خواهد شد. دکمه(Delete) را برای پاک کردن VLAN کلیک کنید . اطلاعات VLAN از لیست پاک خواهد شد.



شکل(۳۲)

۳_۷_۲ صفحه پیکربندی VLAN Port

شکل(۳۳)، صفحه پیکربندی VLAN Port را نشان می دهد. که برای پیکربندی VLAN بر روی پورت استفاده می شود و نتایج پیکربندی را نشان می دهد.

این صفحه شامل ۸ بخش است:

۱.PORT (درگاه)

۲.MODE (حالت)

۳.Current VLAN (تمام VLANهای فعلی)

۴.PortMember (پورت هایی که متعلق به VLAN است)

۵.Default VLAN (VLAN پیش فرض)

۶.Tagged (علامت دار)

۷.UnTagged (غیر علامت دار)

۸.UnMember (بدون عضو VLAN)

۱. قسمت port، برای انتخاب پورت مورد نظر جهت اتصال به یک VLAN استفاده می شود .

۲.قسمت mode؛ در اینجا حالت پورت در vlan را مشخص میکنیم که به صورت access یا hybrid یا trunk باشد.

حالت Access : وقتی پورتی در حالت access قرار می گیرد فقط میتواند عضو یک vlan باشد و به صورت untagged قرار بگیرد.

حالت Trunk : وقتی پورتی در حالت Trunk قرار می گیرد فقط میتواند عضو یک vlan باشد و به صورت untagged و هم به صورت tagged قرار بگیرد.

حالت Hybrid : وقتی پورتی در حالت Hybrid قرار می گیرد میتواند عضو چند vlan باشد و به صورت untagged و هم به صورت tagged قرار بگیرد.

۳. قسمت تمام VLANهای فعلی آن VLANهایی هستند که توسط کاربر ایجادشده اند. کاربران می توانند VLAN را از این لیست انتخاب کنند .

۴. قسمت پورت های متعلق به VLAN ، vlanهایی که آن پورت در آن وجود دارد را نشان می دهد.

علامت [P] نشانگر این است که VLAN،همان VLAN پیش فرض شده پورت است .

علامت [T]حاکی از این است که پورت یک عضو علامت دار شده(tagged member) از VLAN است.

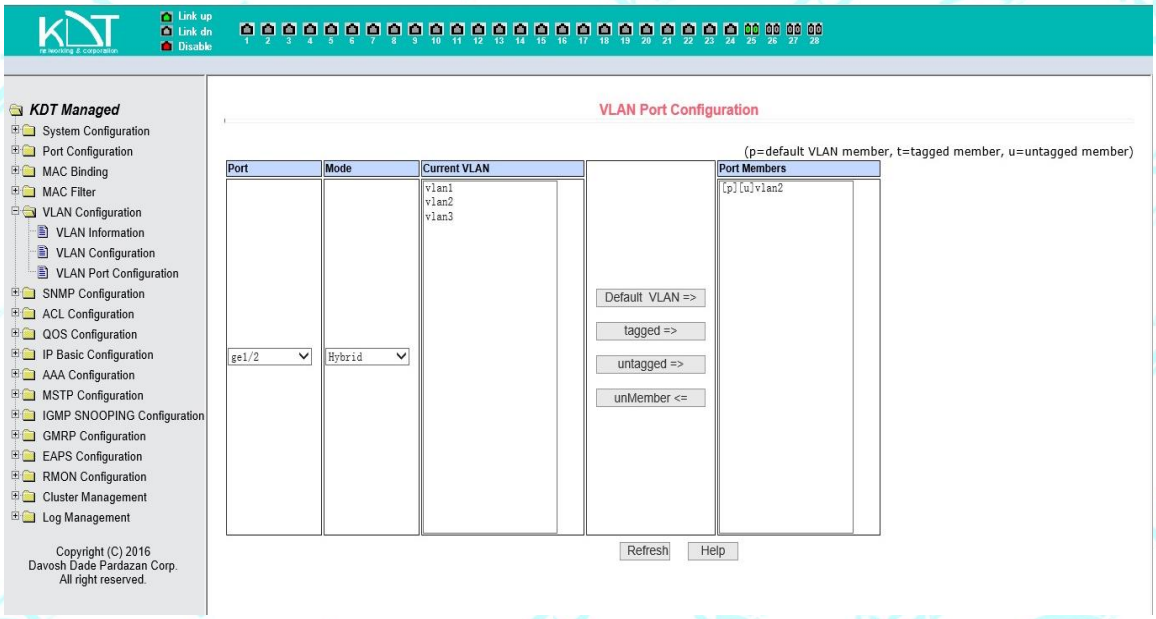
علامت [u] نشانگر آن است که پورت عضو علامت دار نشدهVLAN ,(Untaggedd member) است.

۵. با فشار دادن دکمه Default VLAN، VLAN پیش فرض پورت را پیکربندی میکنید، از قبل یک VLAN را از لیست Current VLANانتخاب کنید .

۶. با فشار دادن دکمه tagged ، برای پیکربندی پورت به عنوان یک عضو علامتدار(tagged member) ازVLAN های مشخص شده استفاده میشود،شما میتوانید یک یا چند VLAN را به طور همزمان ازلیست VLANهای موجود انتخاب کنید.

۷. با فشار دادن دکمه untagged، برای پیکربندی پورت به عنوان یک عضو غیرعلامت دار (untagged member) ، از VLANهای تعیین شده استفاده . شما میتوانید یک یا چند VLAN را به طور همزمان ازلیست VLANهای موجود انتخاب کنید.

۸. کلید (UnMember) برای برداشتن پورت از یک یا چند VLAN مشخص شده استفاده میشود. با انجام این عملیات VLAN ها از پورت مورد نظر پاک خواخد شد.فقط توجه داشته باشید که VLAN پیش فرض شده پاک نخواهد شد.



شکل(۳۳)

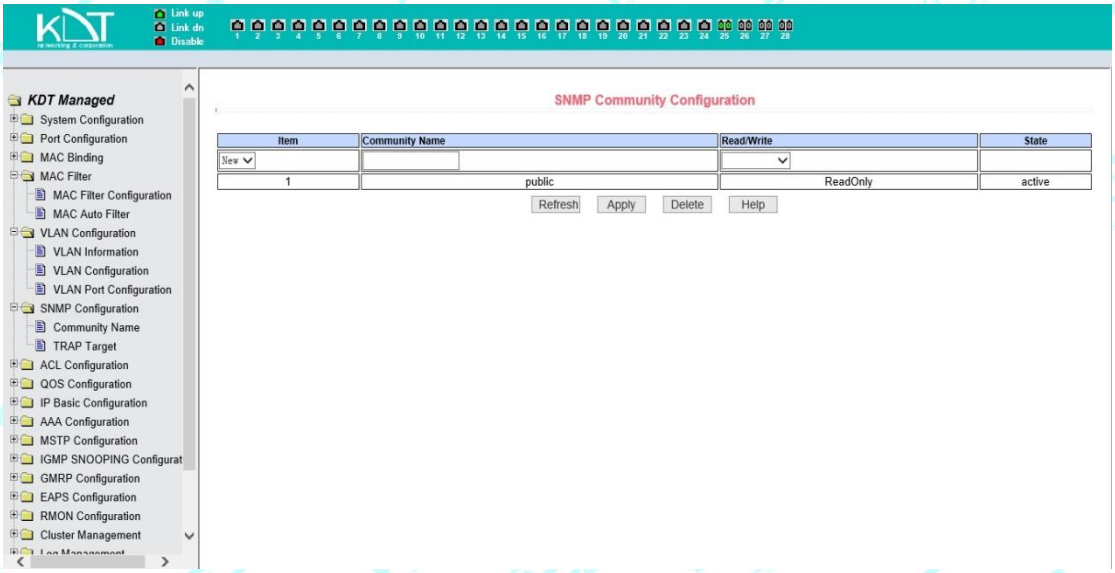
۸_۲ پیکربندی SNMP

۱_۸_۲ صفحه پیکربندی مجموعه SNMP

شکل(۳۴)، صفحه پیکربندی مجموعه SNMP را نشان می دهد.برای فعال سازی شما میتوانید یک نام به snmp بدهید و اجازه دسترسی به کاربر را فقط خواندنی و یا خواندن و نوشتن دهید.شما در کل میتوانید هشت snmp را بسازید.

بطور پیش فرض سوئیچ یک snmp با اسم public و سطح دسترسی فقط خواندنی دارد .

وقتی که نیاز است از طریق snmp سویچ را تنظیم کنید ، نیاز دارید که یک مجموعه خواندنی و نوشتنی را پیکربندی کنید .



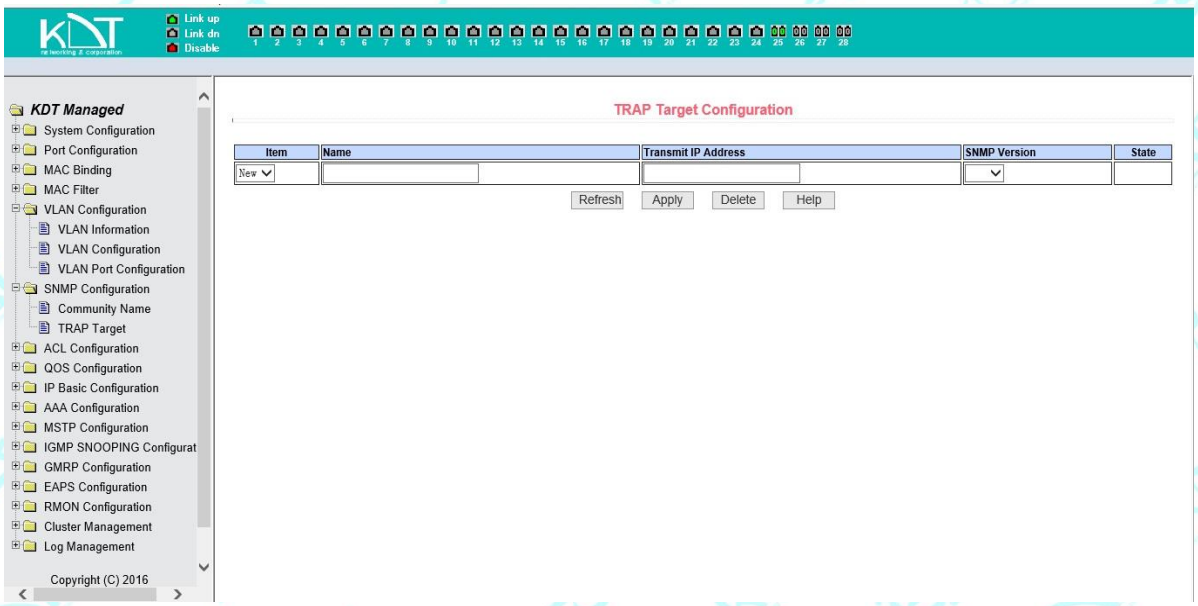
شکل(۳۴)

۲_۸_۲ صفحه پیکربندی TRAP Target

شکل(۳۵)، صفحه پیکربندی TRAP target را نشان می دهد ، کاربر اجازه میدهد آدرسIP را از ایستگاهی که پیام های TRAP و پارامترهایی از بسته پروتکلTRAP دریافت میکند، پیکربندی کند.

وقتی یک ورودی پیکربندی می شود، اسمی برای وارد کردن نام TRAP استفاده میشود .IP آدرس برای وارد کردن مقصد آدرس استفاده می شود. مدل نسخه SNMP برای انتخاب مدل بسته TRAP استفاده می شود .

اگر تنظیمات موفق باشد، وضعیت در ورودی به صورت فعال نمایش داده خواهد شد. اگر پیکربندی موفق شود عمل کرده SNMP TRAP اثر خواهد کرد. در صورتی که قطع یا وصل شدن اتصال، سوئیچ به صورت خودکار بسته TRAP را به آدرس مقصد می فرستد .



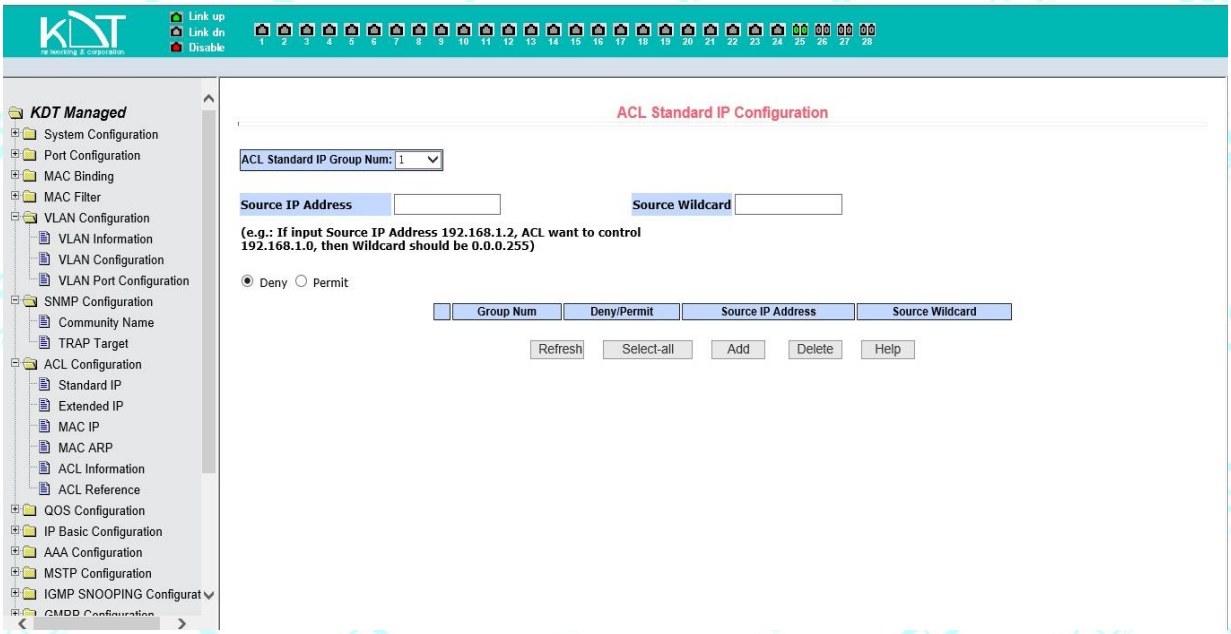
شکل(۳۵)

۹_۲ پیکربندی ACL

۱_۹_۲ صفحه پیکربندی ACL Standard IP

شکل(۳۶)، صفحه پیکربندی Access Control List Standard IP را نشان می دهد.

در این صفحه با دسته بندی IP های مختلف در ACL های گوناگون که میتوانند با اعدادی بین (بین ۱ تا ۹۹ یا ۱۳۰۰ تا ۱۹۹۹) گروه بندی شوند ، دستوراتی را به صورت مجاز یا غیرمجاز بودن آن IP وارد نمایید.توجه داشته باشید فیلدها را با IP و Source wildcard مربوطه تکمیل نمایید.



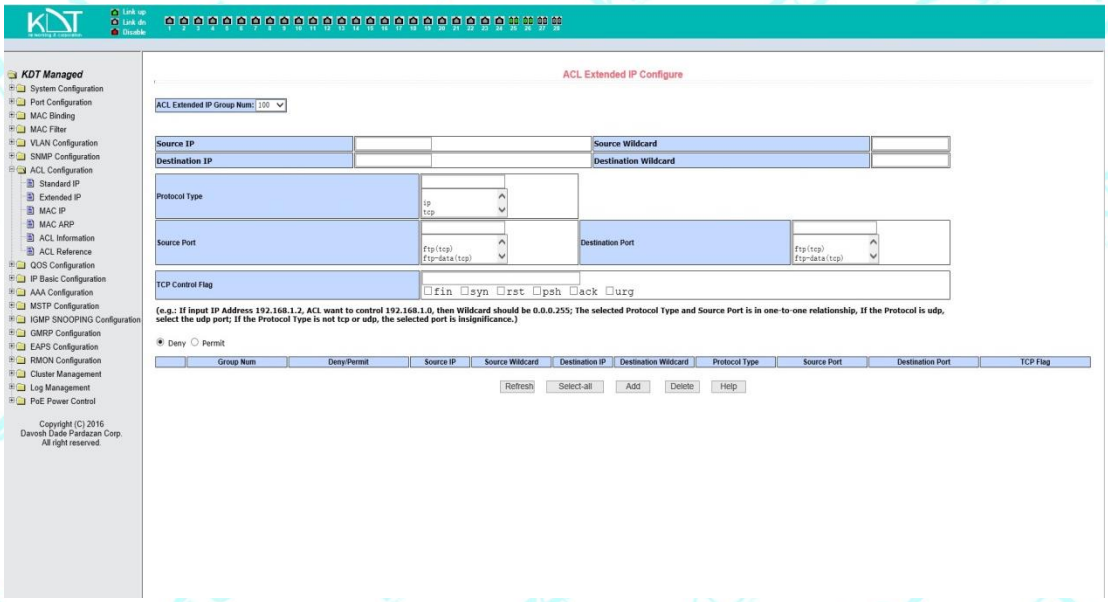
شکل(۳۶)

۲_۹_۲ صفحه پیکربندی ACL Extended IP

شکل(۳۷) صفحه پیکربندی ACL extended IP را نشان می دهد.

زمانی که کاربر یک دستور را اعمال میکند باید IP مبدا (Source IP) و IP مقصد (Destination IP) را تحت پوشش قرار دهد. کاربر می تواند برای ایجاد یک یا چند دستور، یک شماره گروه ACL، (بین ۲۰۰۰ تا ۲۶۹۹ یا ۱۰۰ تا ۱۹۹) را انتخاب کند.

برای IP مبدا پروتکل هایی مانند UPP , TCP , ICMP و... و برای IP مقصد فقط پروتکاهای UDP و TCP قابل انتخاب هستند.



شکل(۳۷)

وقتی یک کاربر یک دستور را شکل میدهد، هر دستور باید مانند فیلترینگ عمل کند ، به صورت اجازه دادن یا رد کردن.

وقتی کاربر یک دستور را در یک گروه دارای دستور ایجاد میکند، سیستم به طورخودکار به آن دستور، یک شماره به عنوان شماره دستور میدهد، و وقتی دستور دراین گروه پاک میشود سایر دستورات تغییر نمی کند و سیستم به طور خودکار یک دستور به این نوع گروه اختصاص می دهد. اگر شما می خواهید تمام دستورات گروه را پاک کنید،می توانید همه را انتخاب و سپس کلید Delete را کلیک کنید.

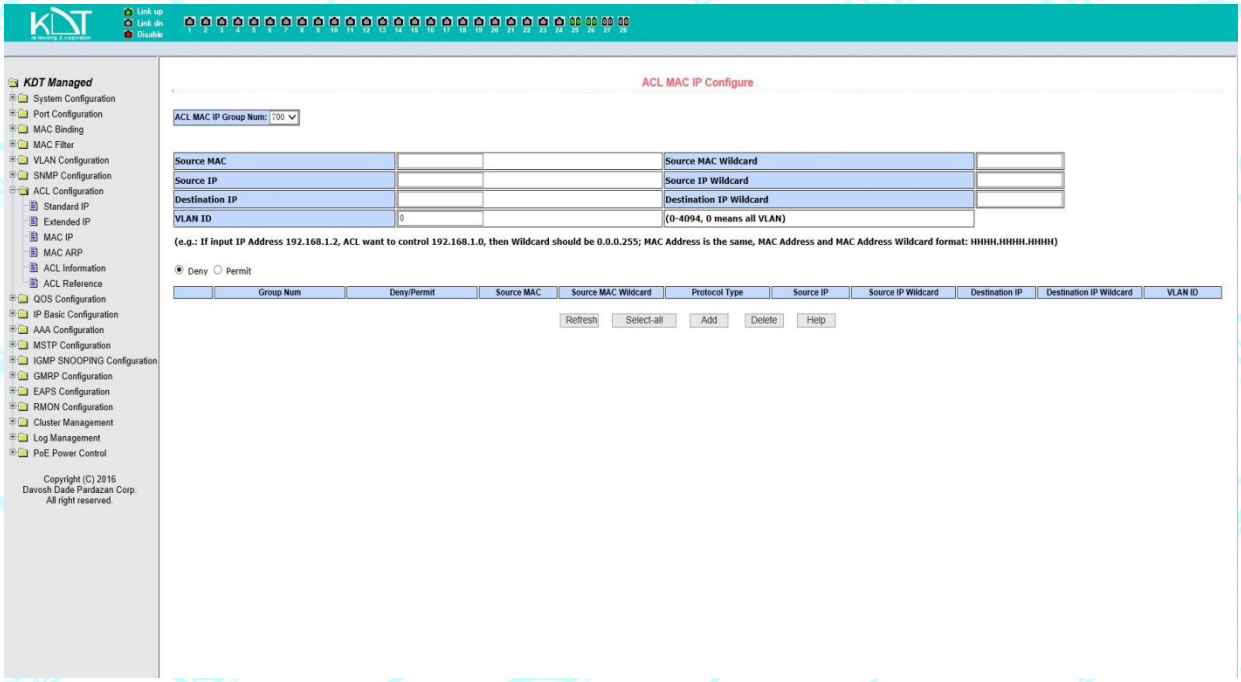
۳_۹_۲ صفحه پیکربندی ACL MAC IP

شکل(۳۸)، صفحه پیکربندی ACL MAC IP می دهد. شما می توانید از این صفحه برای ایجاد یک دستور برای آدرس های ACL MAC استفاده کنید.

کاربر می تواند یک شماره گروه ACL (در محدوده۷۰۰ تا ۷۹۹) برای ایجاد یک یا چند دستور در گروه انتخاب کند.

فیلد هایی که می توانند با مک آدرس فعال ، پر شوند عبارتند از : source ip address ,

destination ip address و vlan id



شکل(۳۸)

وقتی کاربر یک دستور را پیکربندی میکند، آدرس MAC ، منبع آدرس IP و مقصد IP آدرس ، نیاز دارند با آدرس منطبق شوند.در این صورت دستور می تواند با آدرسMAC و آدرس IP منطبق باشد. برای مثال: اگر دستور در محدوده آدرس های (۱۹۲,۱۶۸,۰,۰ تا ۱۹۲,۱۶۸,۰,۲۵۵) تطابق داشته باشد ،IP آدرس می تواند ۱۹۲,۱۶۸,۰,۱ و ماسک آن میتواند ۰,۰,۰,۲۵۵ باشد.

وقتی یک کاربر یک دستور را شکل میدهد، هر دستور باید مانند فیلترینگ عمل کند ، به صورت اجازه دادن یا رد کردن.

وقتی کاربر یک دستور را در یک گروه دارای دستور ایجاد میکند، سیستم به طورخودکار به آن دستور یک شماره به عنوان شماره دستور میدهد، و وقتی دستور دراین گروه پاک میشود سایر دستورات تغییر نمی کند

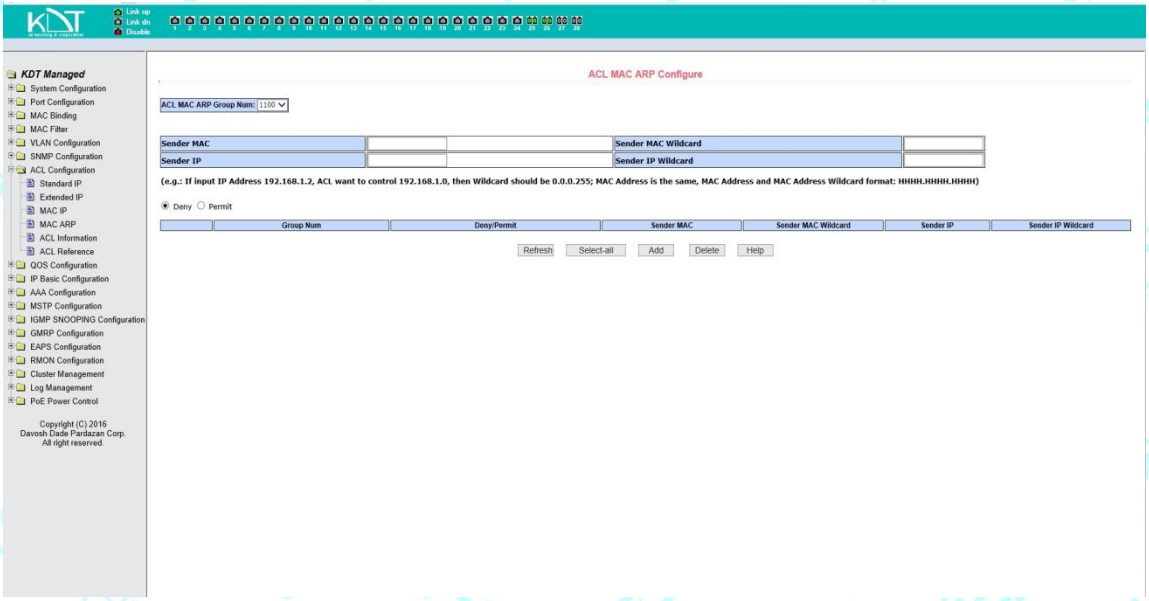
و سیستم به طور خودکار یک دستور به این نوع گروه اختصاص می دهد. اگر شما می خواهید تمام دستورات گروه را پاک کنید،می توانید همه را انتخاب و سپس کلید Delete را کلیک کنید .

وقتی یک کاربر یک دستور را شکل میدهد، VLA ID باید بین ۰ و ۴۰۹۴ انتخاب شود و عدد ۰ بیانگر همه ی آنها میباشد

۴_۹_۲ صفحه پیکربندی ACL MAC ARP

شکل(۳۹)، صفحه پیکربندی ACL MAC ARP را نشان می دهد. شما می توانید از این صفحه برای ایجاد یک دستور برای ACL MAC ARP استفاده کنید. کاربرمیتواند شماره گروه ACL برای ایجاد یک یا چند دستور در گروه انتخاب کند.

فیلد هایی که می توانند با دستور منطبق شوند عبارتند از نوع عملکرد ARP آدرس فرستنده ی MAC ،آدرسIP فرستنده.



شکل(۳۹)

وقتی کاربر یک دستور را شکل می دهد و آدرسIP و آدرسMAC ، با یک آدرس تطابق یافته با بیت فرستاده می شود.

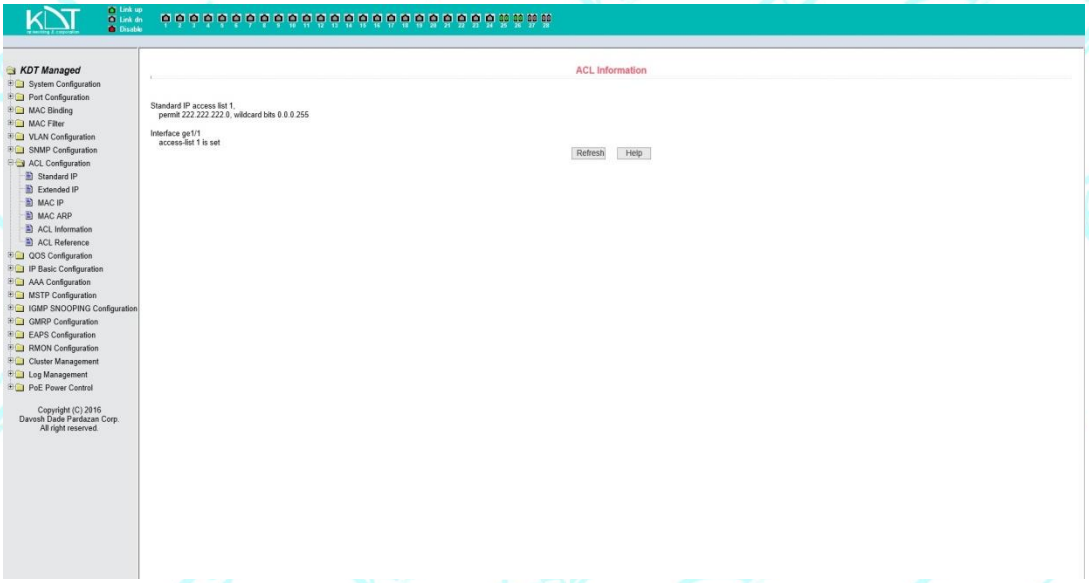
دستور می تواند با مجموعه ی IP آدرس و MAC آدرس منطبق باشد. برای مثال: اگر دستور در محدوده آدرس های (۱۹۲,۱۶۸,۰,۰ تا ۱۹۲,۱۶۸,۰,۲۵۵) تطابق داشته باشد ،IP آدرس می توانند ۱۹۲,۱۶۸,۰,۱ و ماسک آن ۰,۰,۰,۲۵۵ است.

وقتی یک کاربر یک دستور را شکل میدهد، هر دستور باید یک حالت فیلترینگ داشته باشد: اجازه دادن یا رد کردن.

وقتی کاربر یک دستور را در یک گروه دارای دستور ایجاد میکند، سیستم به طورخودکار به آن دستور یک شماره به عنوان شماره دستور میدهد، و وقتی دستور دراین گروه پاک میشود سایر دستورات تغییر نمی کند و سیستم به طور خودکار یک دستور به این نوع گروه اختصاص می دهد. اگر شما می خواهید تمام دستورات گروه را پاک کنید،می توانید همه را انتخاب و سپس کلید Delete را کلیک کنید .

۵_۹_۲ صفحه اطلاعات منبع ACL

شکل(۴۰)، صفحه اطلاعات منبع ACL را نشان می دهد که تمام دستورات و مرجع های پیکربندی شده در ACL فعلی را نشان می دهد .

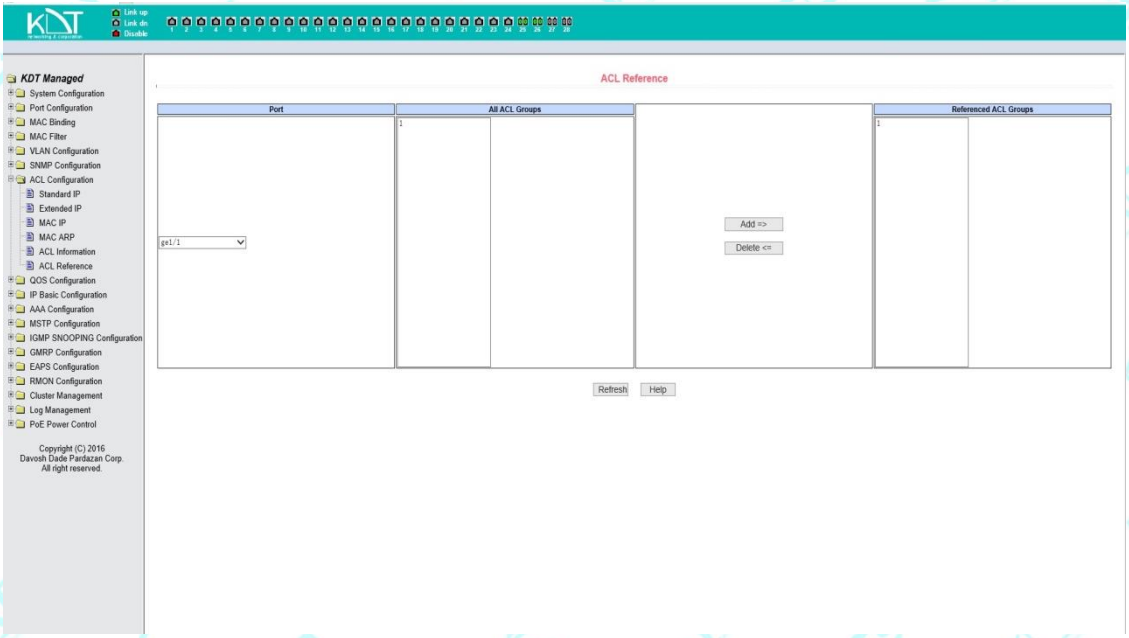


شکل(۴۰)

۶_۹_۲ صفحه پیکربندی منبع ACL

شکل(۴۱)، صفحه پیکربندی منبع ACL را نشان می دهد. شما می توانید از این صفحه برای انتخاب یک گروهِ ACL برای یک پورت استفاده کنید همچنین با انتخاب هر پورت میتوانید دستورات حاکم بر هر ACL را بر آن پورت (بر اساس نحوه ی دریافت پکت ها) اعمال نمایید.

هنگام انتخاب کردن یک گروه ACL روی پورت، شما می توانید Standard IP، Extension IP ، MAC ACL.IP ARP MAC را انتخاب کنید. گروهACL انتخاب شده باید وجود داشته باشد. لیست دستور گروه ACL را انتخاب کنید و کلید Add (اضافه کردن) را فشار دهید. هنگام پاک کردن یک گروهِ ACL، یک گروهِ ACL از لیست دستور گروه ها انتخاب و دکمه Delete را فشار دهید.



شکل(۴۱)

۲_۱۰ پیکربندی Qos

شکل(۴۲)، صفحه اعمال Qos را نشان می دهد.Qos فناوری که ترافیک داده هارا مدیریت می کند تا ازدست دادن داده، تاخیر و Jitter کاهش یابد. کاربر می تواند از این صفحه جهت پیکربندی نوع Qos هر پورت استفاده کنند. اما همچنین می تواند، اولویت پیش فرض کاربر راتغییر دهد. در لیست وضعیت Qos هر پورت و همچنین اولویت بندی کاربر را به صورت real-time نمایش می دهد.

انواع Qos:

No Qos:این حالت Qos غیر فعال می باشد.

Cos-based:

Dscp-based:

Dscpcos-based:


KDT Managed
System Configuration
Port Configuration
MAC Binding
MAC Filter
VLAN Configuration
SNMP Configuration
ACL Configuration
QOS Configuration
QOS Apply
QOS Schedule
IP Basic Configuration
AAA Configuration
MSTP Configuration
IGMP SNOOPING Configurat
GMRP Configuration
EAPS Configuration
RMON Configuration
Cluster Management
Log Management
PoE Power Control
Copyright (C) 2016
Davosh Dade Pardazan Corp.
All right reserved.
QOS Apply
Port:
QOS Type: NO QOS
User Priority: 0
Refresh
Apply
Port Name
QOS Type
User Priority
ge1/1 NO QOS 0
ge1/2 NO QOS 0
ge1/3 NO QOS 0
ge1/4 NO QOS 0
ge1/5 NO QOS 0
ge1/6 NO QOS 0
ge1/7 NO QOS 0
ge1/8 NO QOS 0
ge1/9 NO QOS 0
ge1/10 NO QOS 0
ge1/11 NO QOS 0
ge1/12 NO QOS 0
ge1/13 NO QOS 0
ge1/14 NO QOS 0
ge1/15 NO QOS 0
ge1/16 NO QOS 0
ge1/17 NO QOS 0
ge1/18 NO QOS 0
ge1/19 NO QOS 0
ge1/20 NO QOS 0
ge1/21 NO QOS 0
ge1/22 NO QOS 0
ge1/23 NO QOS 0
ge1/24 NO QOS 0
ge1/25 NO QOS 0
ge1/26 NO QOS 0
ge1/27 NO QOS 0
ge1/28 NO QOS 0

شکل(۴۲)

۲_۱۰_۲ صفحه برنامه Qos

شکل(۴۳)، صفحه برنامه ریزی Qos را نشان می دهد. کاربر می تواند از این صفحه برای پیکربندی برنامه ریزی نوع Qos هر پورت استفاده کند. همچنین می تواند اولویت صف را تغییر دهد. لیست نمایش برنامه ریزی هر پورت و مقدار سنگینی هر صف را به صورت real-time نمایش میدهد.

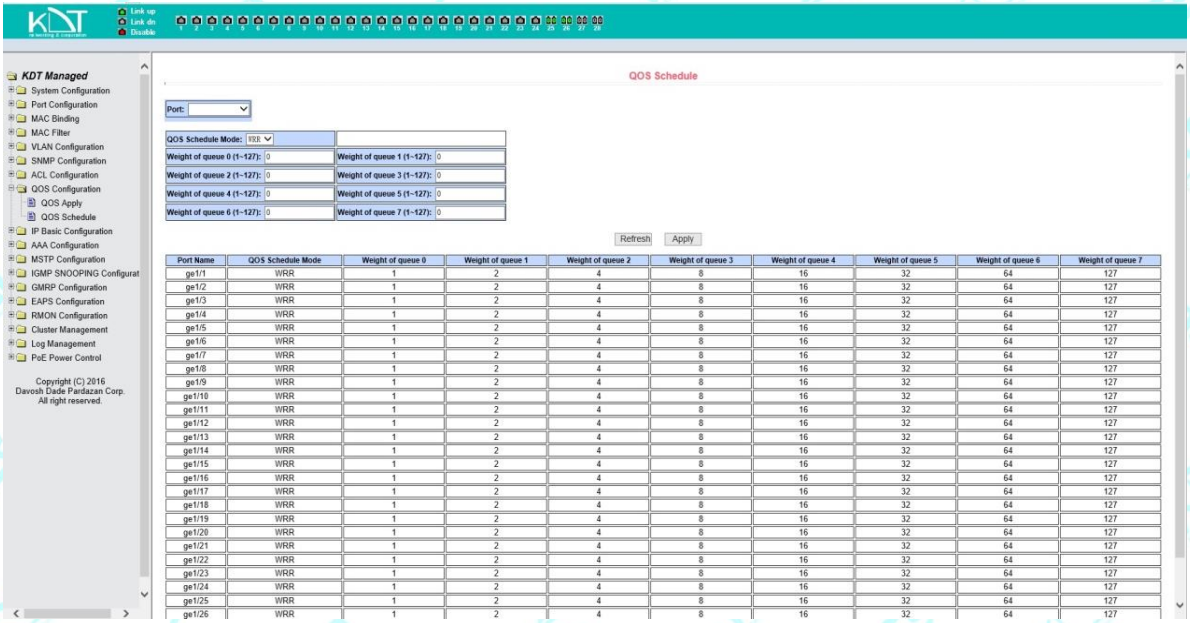
+

حالت های قابل برنامه ریزی Cos:

WRR:مخفف Weighted Round Robin می باشد. این روش ها تضمین میکند تمام صف ها در طول هر دوره خدمات رسانی شود.این الگوریتم برای چرخش سرویس در میان هشت صف استفاده می شود.چرخش براساس وزن هایی است که به هر صف اختصاص داده داده اید .

SP:مخفف Strict Priority می باشد.این روش خدمات برای ترافیک با اولویت بالا را تضمین می کند.این نرم افزار حداکثر وزن را برای هر صف تعیین میکند تا مکانیزم صف بندی را به عنوان چندین بسته در یک صف تا حدامکان به صفر برساند.

WFQ:مخفف weighted Fair Queuing می باشد.این روش دارای مزیت سرعت ،قابل اطمینان بودن و اجرای آسان است.



شکل(۴۳)

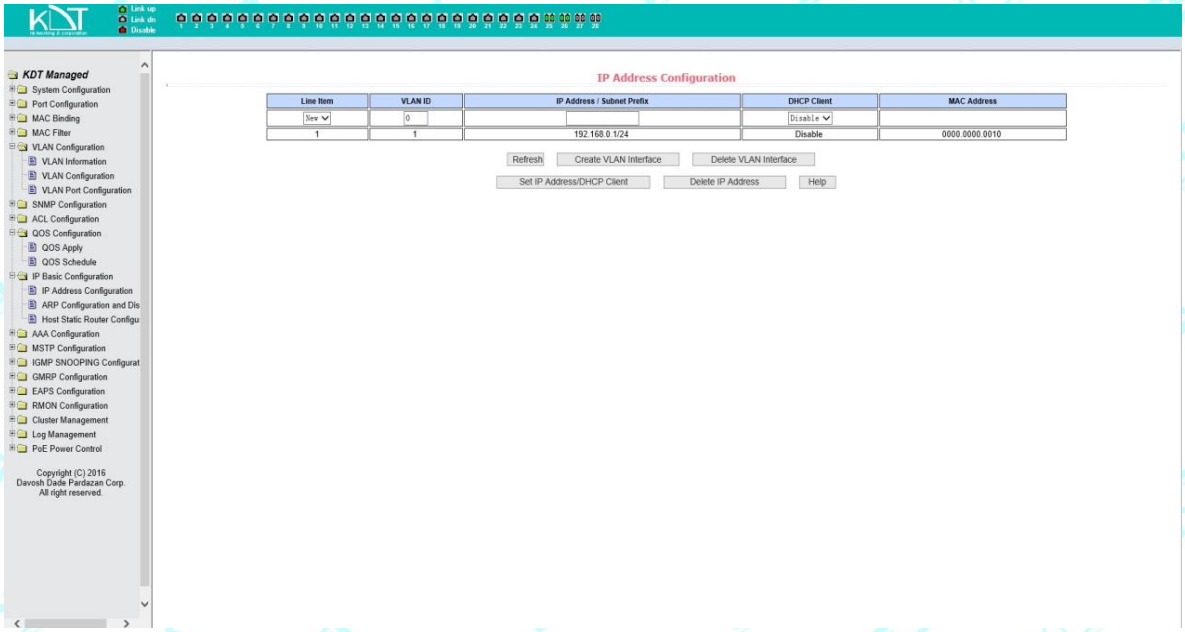
۲_۱۱ پیکربندی اصلی IP

۲_۱۱_۱ صفحه پیکربندی IP Address Configuration

شکل(۴۴)، صفحه پیکربندی IP Addressرا نشان می دهد. شما می توانید خط اتصال VLAN را پیکربندی کنید. یا آن را حذف کنید، همچنین می توانید خط اتصال IP آدرس را پیکربندی کنید، آن را پاک کنید و اطلاعات اتصال را ببینید.

تنها زمانی که VLAN (در همان لحظه) وجود دارد می تواند به عنوان یک رابط تنظیم گردد. فقط آدرس خود IP می تواند روی VLAN پیکربندی شده شکل بگیرد. سوئیچ به طور پیش فرض یک رابط VLAN1 دارد و این رابط نمی تواند پاک شود.

فقط یک IP برای یک VLAN می تواند ساخته شود.



شکل(۴۴)

۲_۱۱_۲ صفحه نمایش و پیکربندی ARP

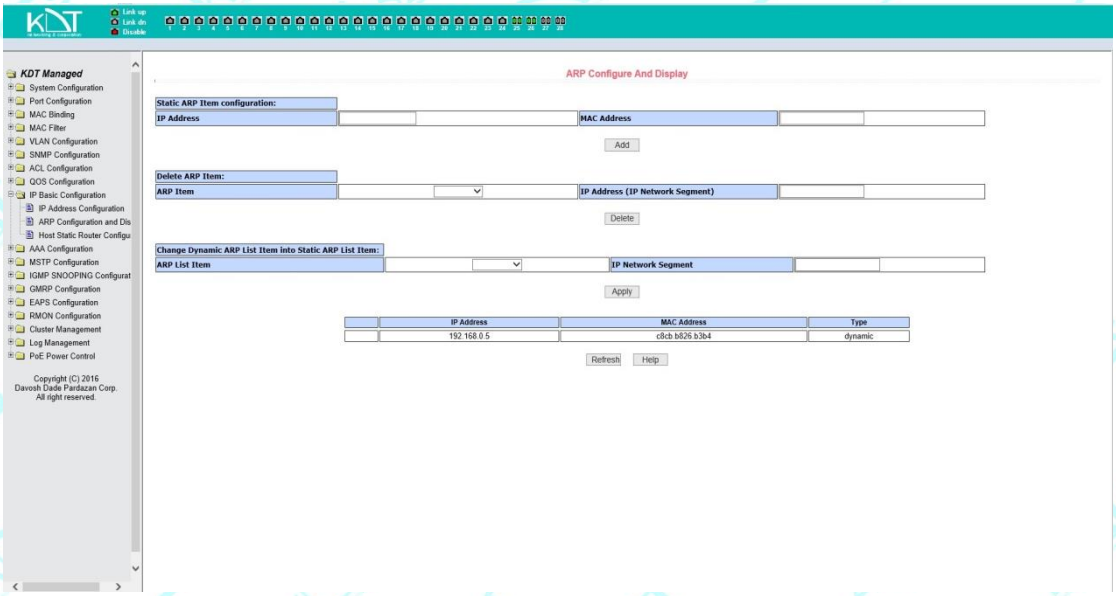
شکل(۴۵)، صفحه نمایش و پیکربندی ARP را نشان می دهد. این صفحه تمام اطلاعات جدول ARP متعلق به سوئیچ را نشان می دهد. شما می توانید از این صفحه برای پیکربندی ورودی های Static ARP، پاک کردن ورودی هایARP، و تبدیل ورودیهای dynamic ARP به ورودی های Static ARP استفاده کنید.

زمانی که شما یک ورودی Static ARP را پیکربندی می کنید، نیاز دارید که آدرسIP و آدرس MAC را وارد کنید، این آدرسMAC باید برای ارتباط با یک کامپیوتر باشد، سپس کلید اضافه کردن(Add) را کلیک کنید.

زمانی که یک کاربر ورودی ARP میکند، می توانید انتخاب کنید که یک ورودیARP را از یک IPآدرس، یک ورودیARP، از یک بخش شبکه، تمام ورودیهایARP، تمام ورودی های پویا(ARP dynamic) و تمام ورودی های ARP static پاک کنید. برای پاک کردن یک ورودی IP ARP، یا یک ورودی ARP از یک بخش شبکه، آدرس IP مخصوص یا قسمت IP ، را در جعبه داخلی وارد کنید و سپس کلید Delete را کلیک

کنید. زمانی که یک ورودی ARP پویا به ورودی ARP استاتیک تغییر می کند، شما می توانید ورودی پویای ARP را به ورودیARP استاتیک ، درقسمت شبکه، تغییر دهید.

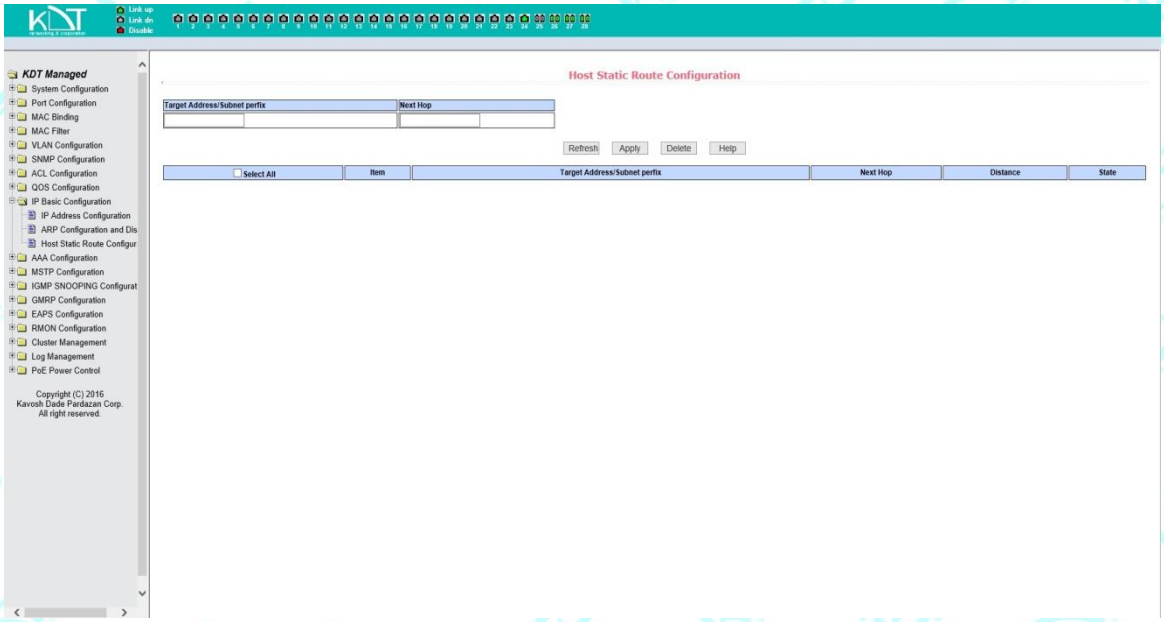
برای بخش شبکه، در جعبه داخلی، یک شبکه مشخص شده را وارد و سپس دکمه اعمال کردن(Apply) را کلیک کنید.



شکل(۴۵)

۳_۱۱_۲ صفحه پیکربندی Host static router

شکل(۴۶)، صفحه پیکربندی Host static router را نشان می دهد. کاربر می تواند Host static route سوئیچ را اضافه یا حذف کند. بطور پیش فرض، هیچ static route روی سوئیچ پیکر بندی نشده است. شما می توانید از این صفحه برای پیکربندیی route پیش فرض، که مقصد/ پیشوند (Subnet/destination) 0.0.0/0 است ، استفاده کنید .



شکل(۴۶)

۲_۱۲ پیکربندی AAA

۲_۱۲_۱ پیکربندی Tacacs +

شکل(۴۷)، صفحه پیکربندی Tacacs + را نشان می دهد. کاربر می تواند اطلاعات مربوط به Tacacs+ را پیکربندی کند. اطلاعات زیر می تواند تنظیم شود:

۱. فعال کردن عملکرد Tacacs +،

۲. پیکربندی IP آدرس سرور Tacacs +،

۳. (authentication type) نوع احراز هویت

۴. کلید رمز مشترک.

۱. پیش از استفاده عملکرد Tacacs+ باید آن را فعال کنید، که به طور پیشفرض پیکربندی شده است.

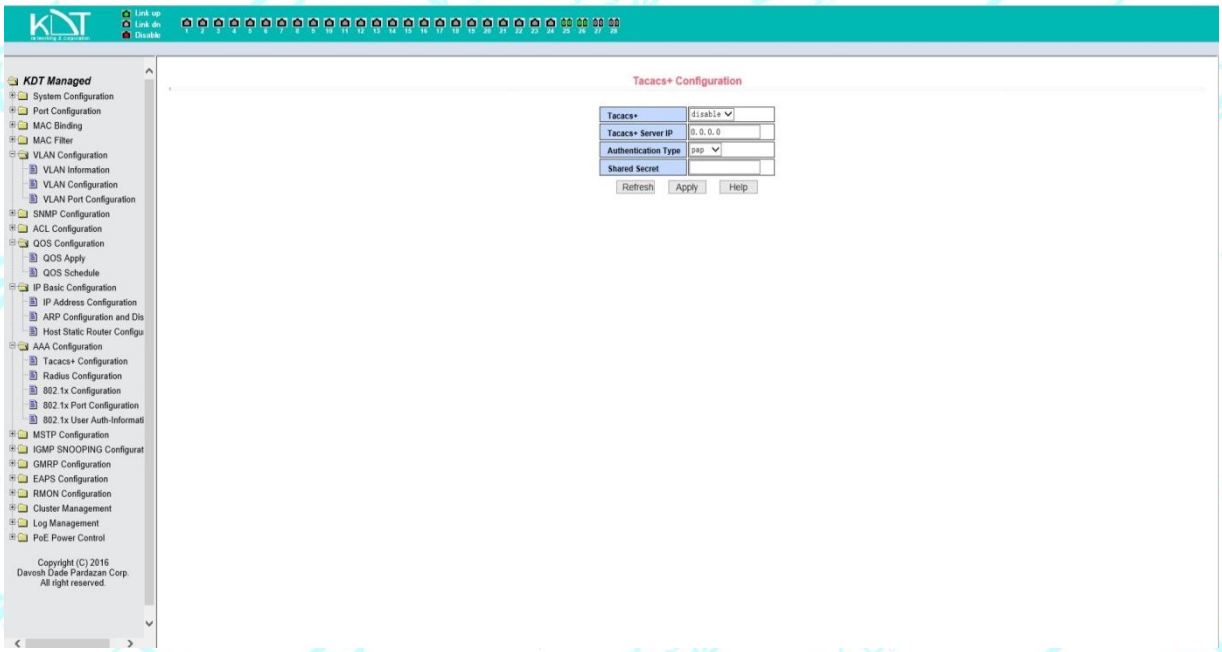
۲. آدرس IP برای سرور Tacacs+؛ که باید هنگام استفاده کردن ویژگی Tacacs+ تنظیم شود را پیکربندی کنید.

۳. نوع احراز هویت(authentication type)؛ دو نوع روش PAP و CHAP رابرای احراز هویت کاربر فراهم می آورد.

پیش فرض روی احراز هویت PAP میباشد. (روش PAP جهت احراز هویت کاربر)

۴. کلیدرمز مشترک؛ برای تنظیم بین سوئیچ و سرور +Tacacs با رمز مشترک رمزگذاری شده، استفاده می شود .

در authentication authorization این فیلد را باید تنظیم کرد وهمینطور به طوریکسان هم در تنظیمات +Tacacs .



شکل(۴۷)

۲_۱۲_۲ صفحه پیکربندی Radius

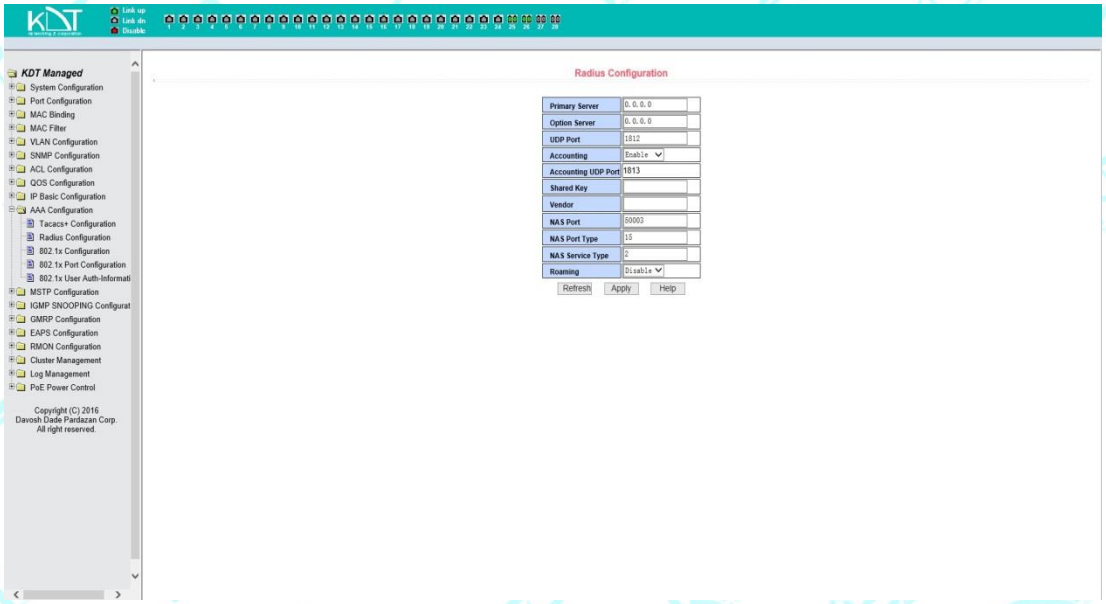
شکل(۴۸)، صفحه پیکربندی Radius را نشان می دهد. کاربر می تواند اطلاعات مربوط به Radius را پیکربندی کند و می تواند اطلاعات شامل زیر را تنظیم کند:

آدرس IP سرور radius ، این فیلد باید در authentication (احراز هویت) وbilling (از روشهای مدیریت شبکه) تنظیم شود.

- IP آدرس اختیاری سرور redius ، اگر یک سرور متناوب redius موجود باشد میتواند تنظیم شود.
- پورت احراز هویت UPD ؛ میزان پیش فرض ۱۸۱۲ است. کاربر معمولا نیازی به تغییر این فیلد ندارد.
- اگر برای شروع billing ، پیش فرض روی شروع است، در زمان شروع billing، انجام authentication و billing صورت میگیرد.
- پورت billing UPD ؛ میزان پیش فرض ۱۸۱۳ است . کاربر اصولا نیازی به تغییر این فیلد ندارد.

کلید اشتراک(Shared key)؛ برای تنظیم بین سوئیچ و (radius) سرور رمز گذاری شده با پسورد مشترک، استفاده می شود. این فیلد در authentication و billing باید با تنظیمات مشابه روی سرور (radius) تنظیم شود.

- اطلاعات مخصوص vender؛ کاربر اصولا نیازی به تغییر این فیلد ندارد.
- پورت NAS ؛ نوع پورت NAS ، نوع خدمات NAS ، کاربر عموماً نیاز به تغییر این سه مقدار ندارد.
- اگر عملیات رومینگ radius شروع یا خاموش کردید.



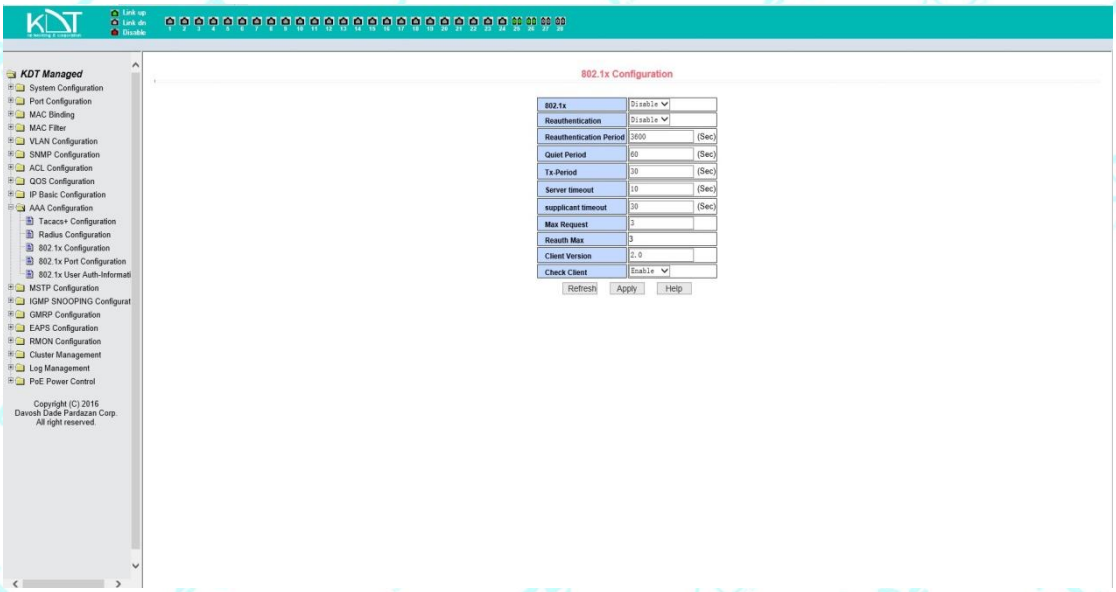
شکل(۴۸)

۳_۱۲_۲ صفحه پیکربندی 802.1X

شکل(۴۹)، صفحه پیکربندی 802.1X را نشان می دهد و اطلاعات مربوط به موارد زیر را به وسیله این صفحه پیکربندی کنید :

- اگر پروتکل 802.1X را شروع کردید، مطمئن شوید پروتکل802.1X را در زمان انجام accounting و authentication شروع میکنید .
- اگر سوییچ یک روش احراز هویت معمول (commom authentication method) یا تمدید یافته (extended authentication) باشد . اگر برای باز کردن عملکرد مجدد احراز هویت(reauthentiaction) ، پیشفرض باز نیست ، وقتی که احراز هویت و بیلینگ(billing) بر طبق وضعیت موجود برای تصمیم گیری انجام می گیرد ، تغییر دادن به عملکرد احراز هویت مجدد ، کاربررا مورد اطمینان تر می کند، زمانی که از billing و احراز هویت استفاده می کند. اما کمی ترافیک را در شبکه زیاد میکند .

- وقفه احراز هویت مجدد (internal reauthentication) را تنظیم کنید؛ فقط درموردی که عملکرد احراز هویت مجدد فعال شده است. پیش فرض ۳۶۰۰ ثانیه است. وقتی احراز هویت و بیلینگ بر طبق وضعیت موجود برای تنظیم مقدار انجام میگیرند، اما این مقدار خیلی نباید کم باشد.
- زمان سنج دوره Tx، کاربر اصولا نیاز به تغییر این فیلد ندارد.
- زمان سنج مهلت سرور(server timeout time)،کاربر اصولا نیاز به تغییر این فیلد ندارد.
- زمان سنج مهلت درخواست(suppicant timeout timer)، کاربر اصولا نیاز بهتغییر این فیلد ندارد.
- تعداد درخواست ها؛کاربر اصولا نیاز به تغییر این فیلد ندارد.
- نمایش بیشترین مقدار Reauth
- مدل client، شماره مدل client
- چک کردن client ؛ جهت چک کردن زمان سنجی بسته ترافیکی client ، پس ازگذراندن احراز هویت.



شکل(۴۹)

۴_۱۲_۲ صفحه پیکربندی پورت 802.1x

شکل(۵۰)، صفحه پیکربندی پورت 802.1x را نشان می دهد. شما می توانید وضعیت پورت 802.1x و بیشترین عددی که میزبان می تواند شکل بگیرد را درست کنید. همچنین می توانید پیکربندی هر پورت 802.1x را ببینید .

وضعیت پرت 802.1x چهار نوع است:

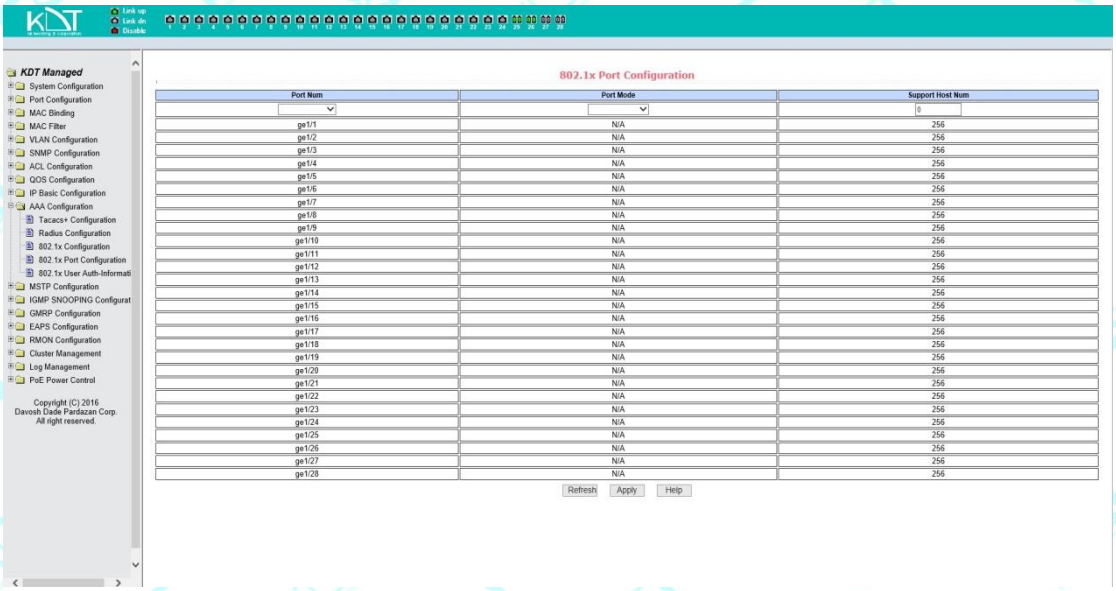
۱) وضعیت N/A

۲) ۲) وضعیت خودکار

۳) ۳)وضعیت اجباری Force-authorized

۴) وضعیت غیر اجباری Force-unauthorized

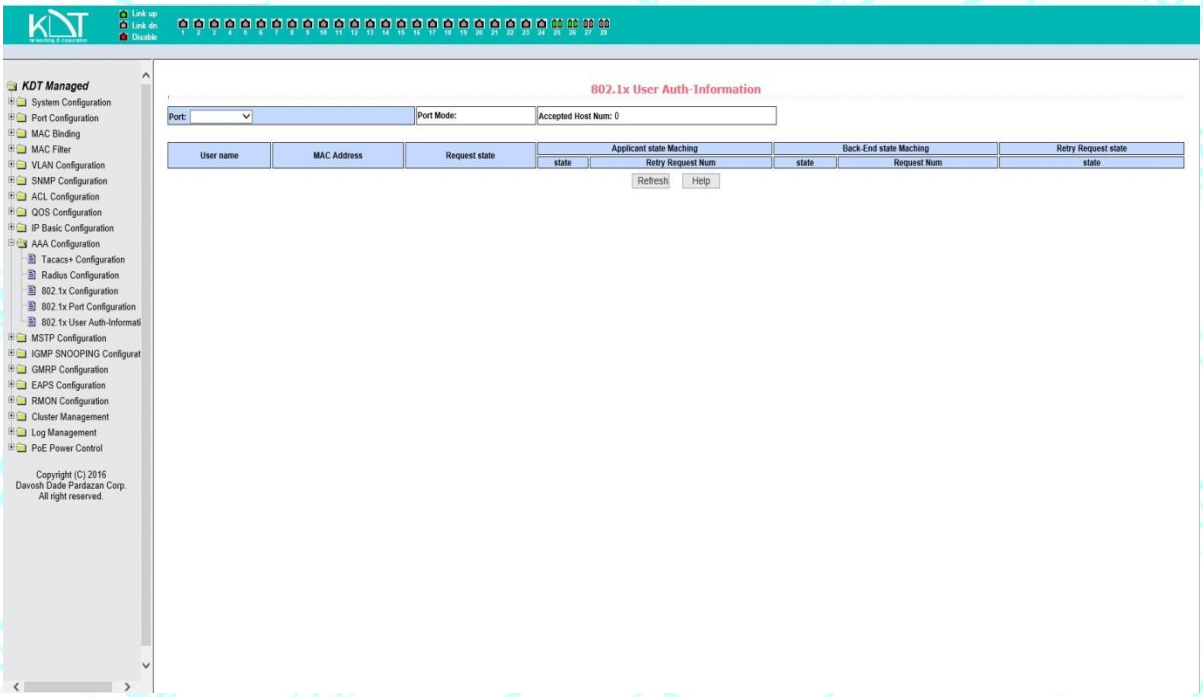
زمانی که یک پورت نیاز دارد تا احراز هویت 802.1x برای آن انجام شود، وضعیت پورت روی خودکار تنظیم می شود، اگر بدون انجام تایید بتواند به شبکه دست یابد، وضعیت پورت روی N/A تنظیم می شود. سایر دو وضعیت دیگر به ندرت در کاربرد عملی استفاده می شوند. احراز هویت ۸۰۲.۱× فعال می شود، بیشترین عدد Host که توسط پورت می تواند قابل دسترسی باشد ۲۵۶ است و کاربر می تواند آنرا برای پشتیبانی آن را ۲۵۶ تغییر دهد.



شکل(۵۰)

۵_۱۲_۲ صفحه اطلاعات کاربر 802.1x

شکل(۵۱)، صفحه اطلاعات معتبر کاربر 802.1x را نشان می دهد. شما می توانید وضعیت اطلاعات تمام کاربرانی را که به یک پورت دسترسی دارند را به وسیله این صفحه ببینید.

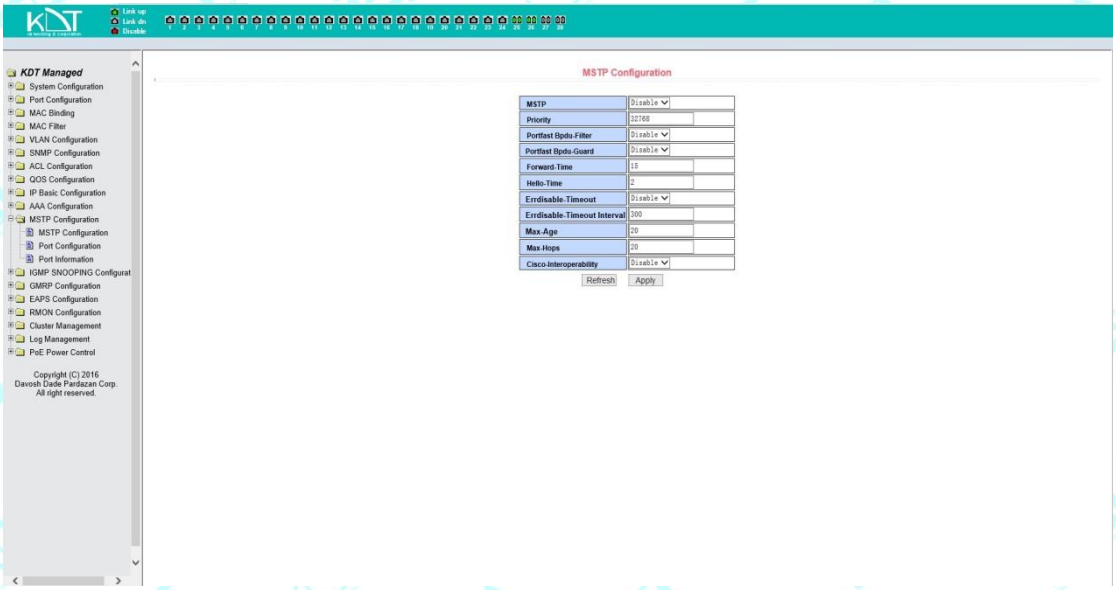

Link up
Link dn
Disable
KDT Managed
System Configuration
Port Configuration
MAC Binding
MAC Filter
VLAN Configuration
SNMP Configuration
ACL Configuration
QOS Configuration
IP Basic Configuration
AAA Configuration
Tacacs+ Configuration
Radius Configuration
802.1x Configuration
802.1x Port Configuration
802.1x User Auth-Informati
MSTP Configuration
IGMP SNOOPING Configurat
GMRP Configuration
EAPS Configuration
RMON Configuration
Cluster Management
Log Management
PoE Power Control
Copyright (C) 2016
Davosh Dade Pardazan Corp.
All right reserved.
802.1x User Auth-Information
Port:
Port Mode:
Accepted Host Num: 0
User name
MAC Address
Request state
Applicant state Maching
state
Retry Request Num
Back-End state Maching
state
Request Num
Retry Request state
state
Refresh
Help

شکل(۵۱)

۲_۱۳ پیکربندی MSTP

۲_۱۳_۱ صفحه پیکربندی عمومی MSTP

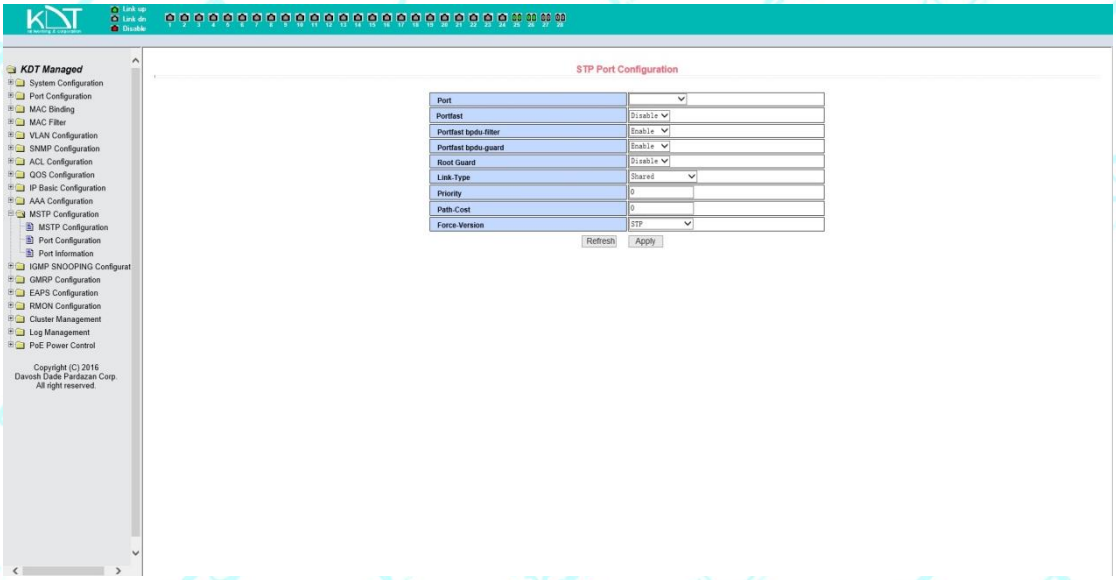
شکل(۵۲)، صفحه پیکربندی عمومیMSTP را نشان می دهد. شما می توانید پارامترهای عمومی MSTP را به وسیله این صفحه پیکربندی کنید.



شکل(۵۲)

۲_۱۳_۲ صفحه پیکربندی پورت MSTP

شکل(۵۳)، صفحه پیکربندی پورت MSTP را نشان می دهد. شما می توانید از این صفحه برای پیکربندی پارامترهای پورت MSTP استفاده کنید .



شکل(۵۳)

۳_۱۳_۲ صفحه اطلاعات پورت MSTP

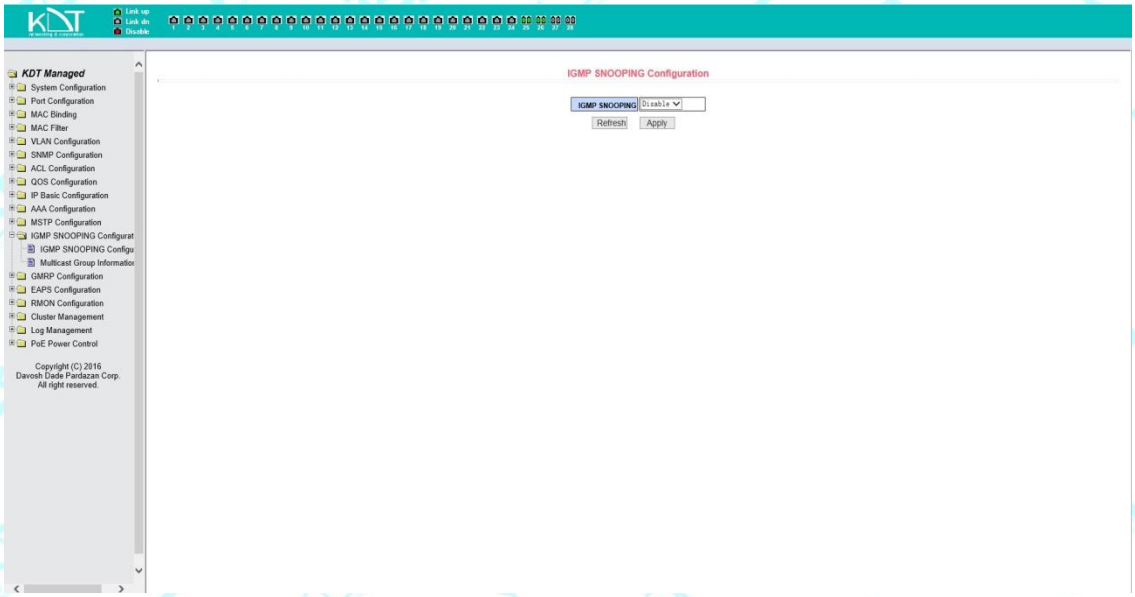
شکل(۵۴)، صفحه اطلاعات پورت MSTP را نشان می دهد. شما می توانیدوضعیت پورت MSTP را در این صفحه نگاه کنید.

شکل(۵۴)

۲_۱۴ پیکربندی IGMP SNOOPING

۲_۱۴_۱ صفحه پیکربندی عمومی IGMP SNOOPING

شکل(۵۵)، صفحه پیکربندی عمومی IGMP SNOOPING را نشان می دهد. شما می توانید IGMP SNOOPING را در این صفحه فعال کنید.



شکل(۵۵)

۲_۱۴_۲ صفحه اطلاعات گروه Multicast

شکل(۵۶)، صفحه اطلاعات گروه Multicast را نشان میدهد.

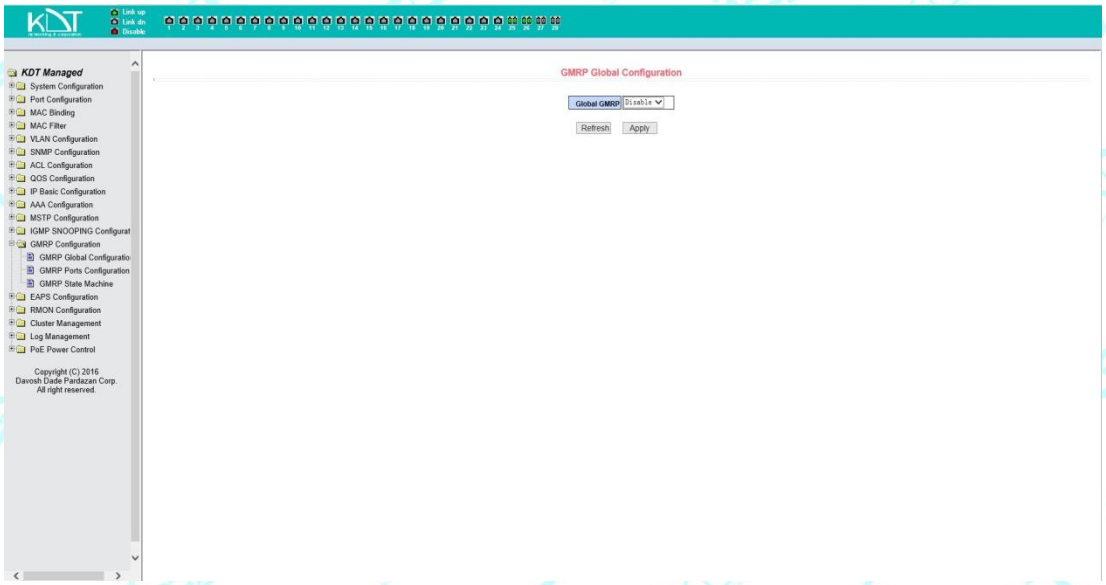
شما می توانیداطلاعات برنامه Multicast IGMP SNOOPING را از این صفحه ببینید.

شکل(۵۶)

۲_۱۵ پیکربندی GMRP

۲_۱۵_۱ صفحه پیکربندی عمومی GMRP

شکل(۵۷) صفحه پیکربندی عمومی GMRP می دهد. کاربر می تواند به وسیله این صفحه GMRP را فعال کند .



شکل(۵۷)

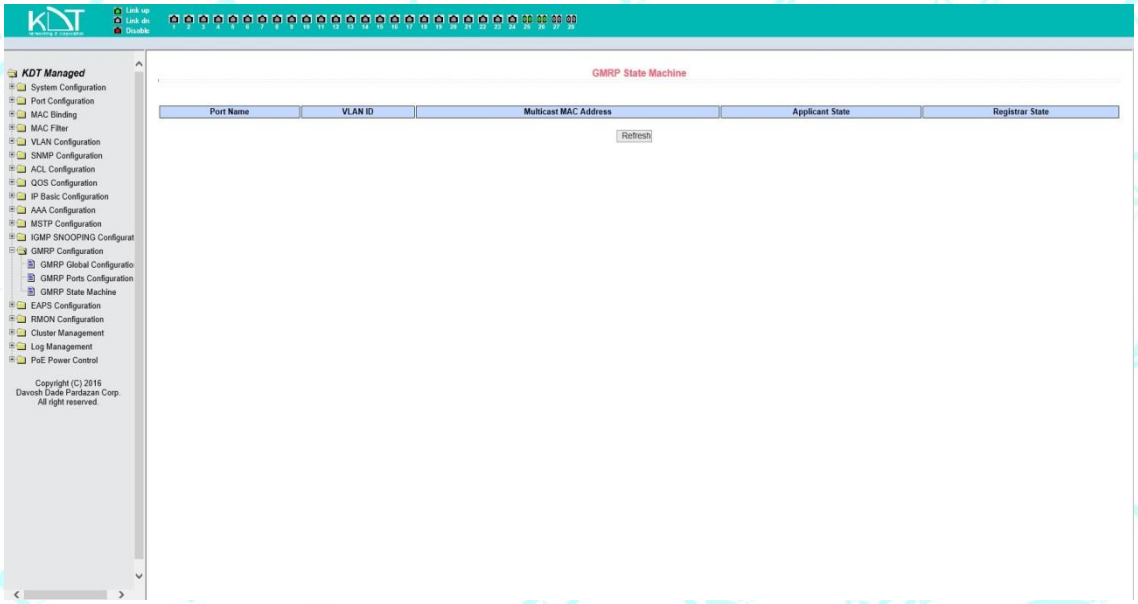
۲_۱۵_۲ صفحه پیکربندی پورت GMRP

شکل(۵۸)، صفحه پیکربندی پورت GMRP را نشان می دهد. کاربران میتوانند ازاین صفحه برای فعال کردن پورت GMRP استفاده کنند و اطلاعات پورت را ببینند .

شکل(۵۸)

۲_۱۵_۳ صفحه GRMP state Machine

شکل(۵۹)،GRMO state Machine را نشان می دهد. کاربران میتوانند اطلاعات state Machine GRMP از این صفحه ببینند.



شکل(۵۹)

۲_۱۶ پیکربندی EAPS

۲_۱۶_۱ صفحه پیکربندی EAPS

شکل(۶۰)، این صفحه برای ایجاد و پیکربندی اطلاعات EAPS استفاده می شود و همچنین می تواند برای حذف نمایش اطلاعات EAPS هم استفاده قرار گیرد.

EARS ring ID ، این ring ID مخصوص، در محدوده ۱ تا ۱۶ ، طبق منوی کشویی می تواند انتخاب شود . دو نوع بسازید، نه اینکه دوباره بسازید، اگر آن را نسازید، باید الگوی عبور و مدیر را بسازید، حالت مربوطه می تواند بر طبق نیازهای ویژه پیکربندی شود .

پورت یا درگاه اصلی، درگاه اصلی مثل: ge1/1 ` fe1/1 پورت متناسب، پورت دوم EAPS

کنترل Vlan، حلقه ERPS کنترل Vlan، مقدار از ۲_۴۰۹۴

محافظت vlan، حلقه محافظت vlan

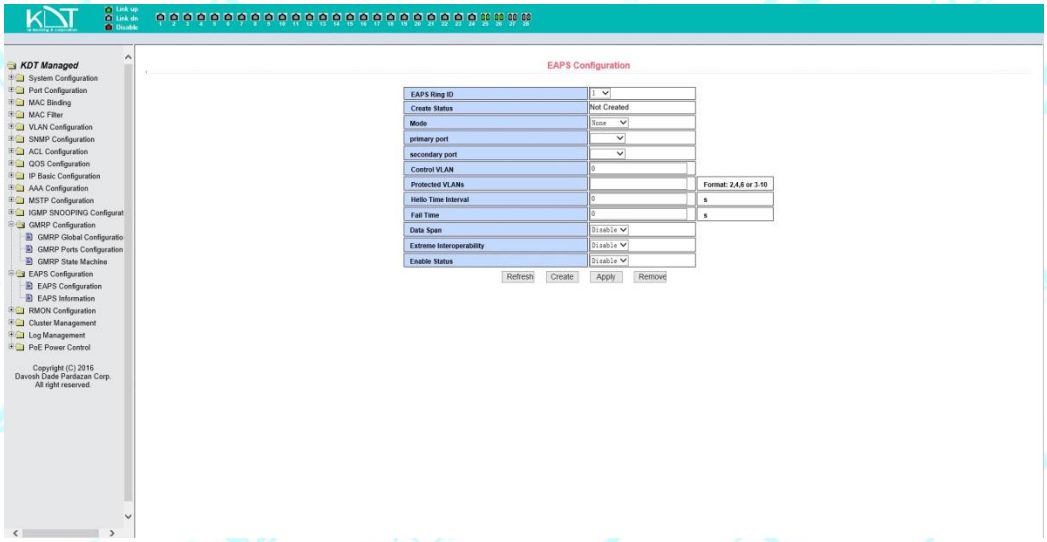
وقفه زمان سلام ، فرستادن پیام سلام برای وقفه زمان ، پیشفرض 1 ثانیه است .

زمان شکست ، تشخیص زمان خطا، پیشفرض 3 ثانیه است .

داده ارسال شده در سراسر حلقه ، در مورد حلقه های چندگانه، این عملکرد وقتی که داده نیاز دارد که در سراسر حلقه ارسال شود ، پیش فرض روشن نیست .

قابلیت همکاری زیاد، سازگاری با اکثر دستگاه های شبکه، پیش فرض روشن است.

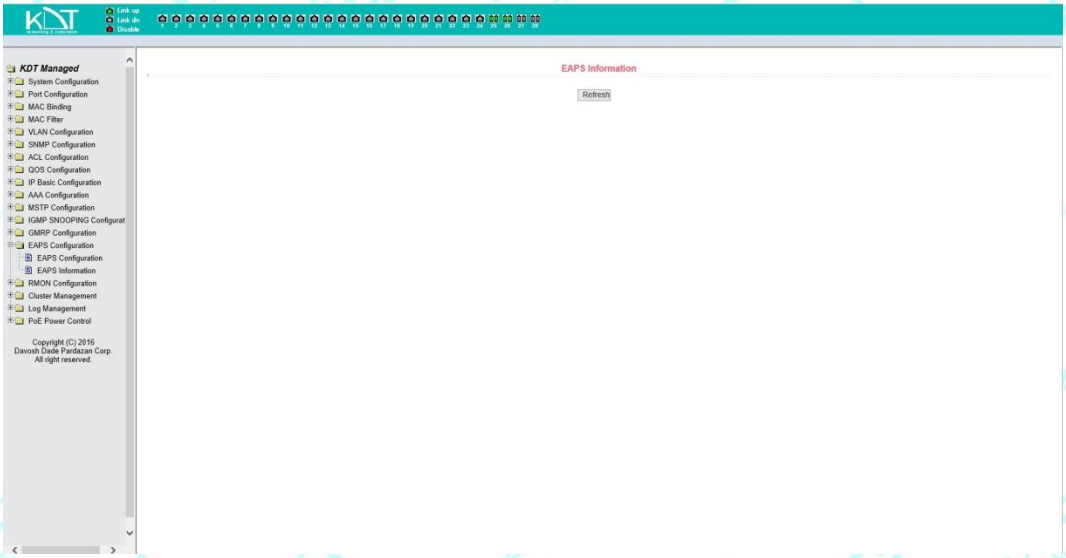
وضعیت فعال شده، آخرین حلقه EAPS فعال شده است.



شکل(۶۰)

۲_۱۶_۲ صفحه اطلاعات EAPS

شکل(۶۱)، صفحه اطلاعات EAPS نشان می دهد،کاربر می تواند اطلاعات پیکربندی EAPS از این صفحه ببیند.



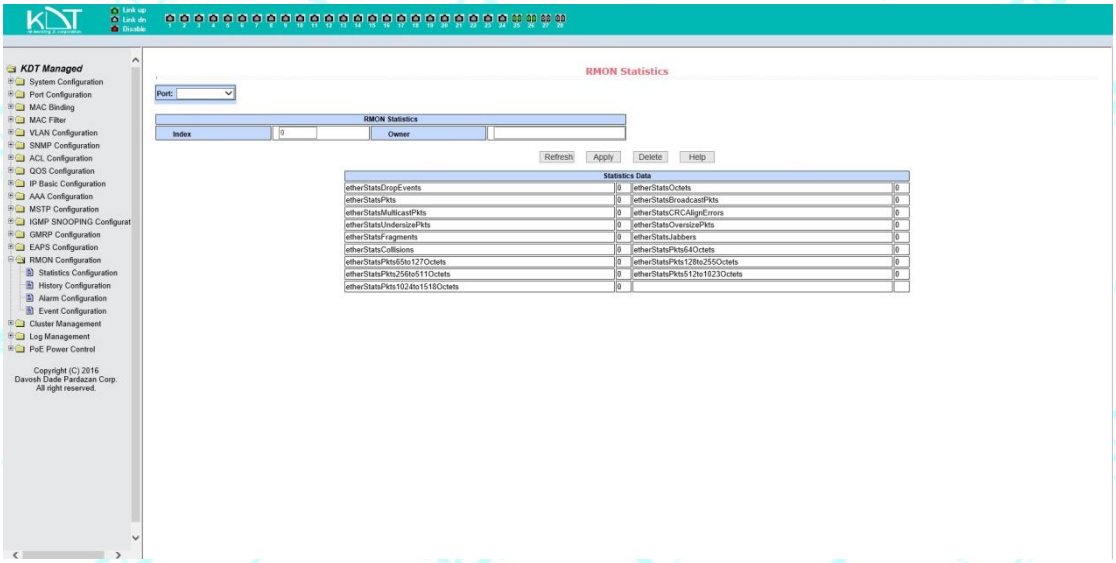
شکل(۶۱)

۲_۱۷ پیکربندی RMON

۲_۱۷_۱ صفحه پیکربندی گروه آمارهای RMON (statistics)

شکل(۶۲)، صفحه پیکربندی گروه آمارهای RMON نشان می دهد. کاربر می تواند گروه آمارهای RMON را به وسیله این صفحه پیکربندی کند. یک پورت را از لیست کشویی انتخاب و گروه آمارهای RMON را برای همان پورت پیکربندی کنید .

اگر شماره شاخص صفر است شماره شاخص درست (در محدوده ۰تا ۱۰۰) پر شده است و صاحب آن اختیاری است. شما می توانید برای پورت، گروه آمارهای RMON را پیکربندی کنید. جدول آمارها، پیکربندی موفق آمارهای پورت را نشان می دهد .



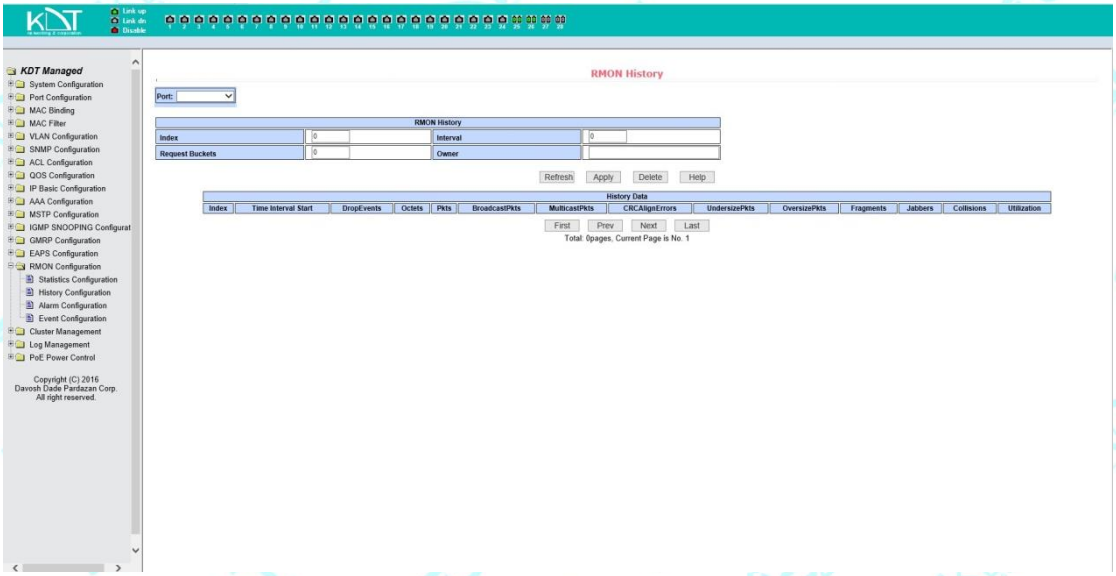
شکل(۶۲)

۲_۱۷_۲ صفحه پیکربندی گروه RMON history

شکل(۶۳)، صفحه پیکربندی گروه RMON history را نشان می دهد. کاربر می تواندگروه history RMON صفحه پیکربندی کند. یک پورت را از لیست کشویی انتخاب وگروه RMON history برای همان پورت پیکربندی کنید.

اگر شماره شاخص صفر است، شاخص درست(۰ تا ۱۰۰) ، وقفه و فاصله، bucket های درخواست و مالک ، اختیاری است.

شما می توانید برای پورت، گروه تاریخ RMON را پیکربندی کنید. وقفه ، به وقفه زمان برای جمع آوری داده، در ثانیه ها، در محدوده ۱تا ۳۶۰ اشاره دارد. درخواست بوکت ها، میزان اختصاص داده شده ی ذخیره است، نشان می دهد چند ذخیره انجام شده است. محدوده ۱ تا ۱۰۰ است. جدول آمارها ، داده های تاریخی به دست آمده از زمانیکه پیکربندی موفق بوده، را نشان می دهد.



شکل(۶۳)

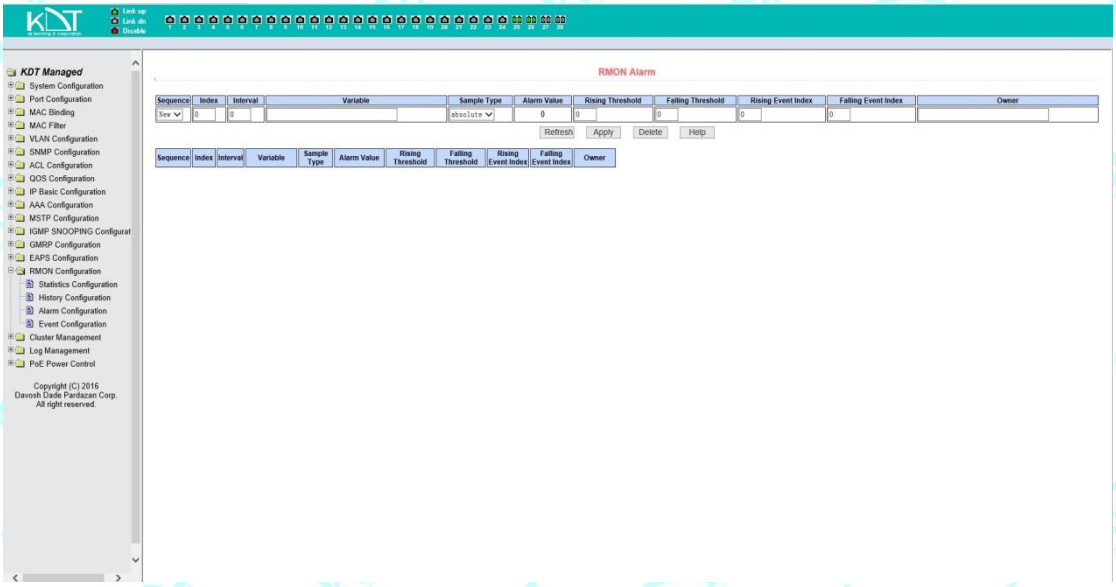
۳_۱۷_۲ صفحه پیکربندی گروه هشدار RMON

شکل(۶۴)، صفحه پیکربندی گروه هشدار RMON را نشان می دهد. کاربر میتواند گروه هشدار RMON تغییر دهد یا ایجاد کند .

یک گروه پیکر بندی شده هشدار را از لیست کشویی برای شکل گیری اطلاعاتش انتخاب کنید، و برای ایجاد آن New را انتخاب کنید، محدوده شاخص ۱ تا ۶۰ است، وقفه ۱ تا ۳۶۰۰ است، در چند ثانیه ، جسم مانیتورینگ(monitoring) در گروه MIB باید پر شود، تضاد می تواند منطبق انتخاب شود یا نشود، اما همچنان در آستانه پایین یا بالا باید پر شود ،شاخص اتفاق ، مالک اختیاری است.

میزان هشدار فقط خواندنی (غیر قابل ویرایش) و میزان نمونه را وقتی آخرین هشدارصادر شد را نشان میدهد.

شاخص اتفاق به شماره شاخص گروه اتفاقRMON اشاره دارد و باید جلوتر پیکربندی شود.

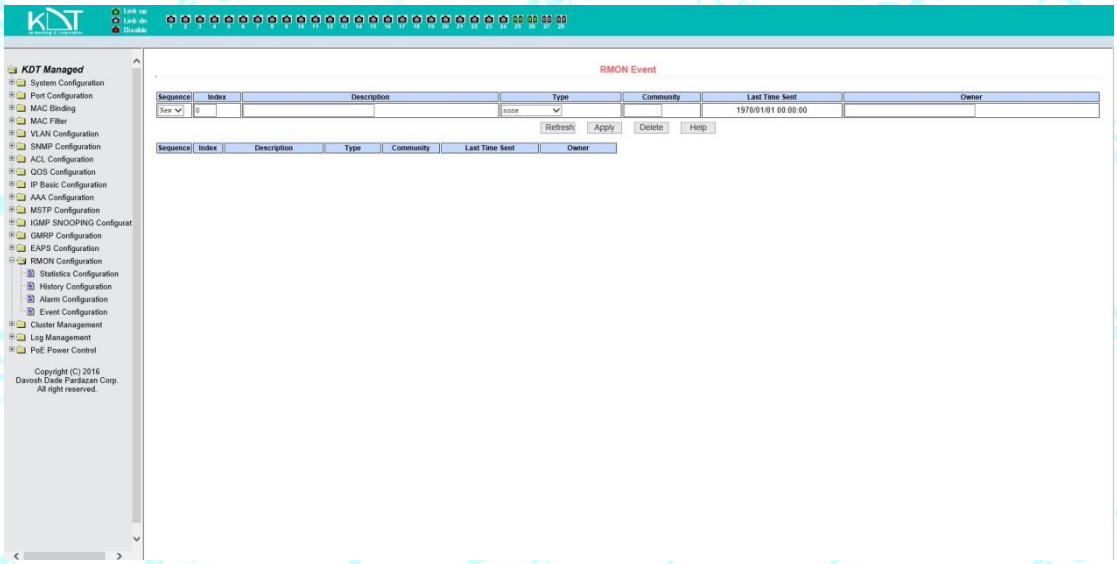


شکل(۶۴)

۴_۱۷_۲ صفحه پیکربندی گروه رویداد RMON

شکل(۶۵)، صفحه پیکربندی گروه رویداد RMON را نشان می دهد و جایی است که کاربر می تواند گروه های رویداد RMON را ایجاد یا تغییر دهد. گروه رویدادپیکربندی شده را از لیست کشویی برای پیکربندی اطلاعات انتخاب و New را برای ایجاد انتخاب کنید. محدوده شاخص از ۱ تا ۶۰ است. و تعریف یک رشته است. عملکرد می تواند انتخاب نشود(بدون عملکرد)، ورود ،SNMP_trap یا (log_and_trap).

اسم اشتراکی در دستگاه کار نمی کند، مالک اختیاری است، آخرین زمان ارسال فقط خواندنی است ، آخرین زمان که رویداد ارسال شد را نشان می دهد.



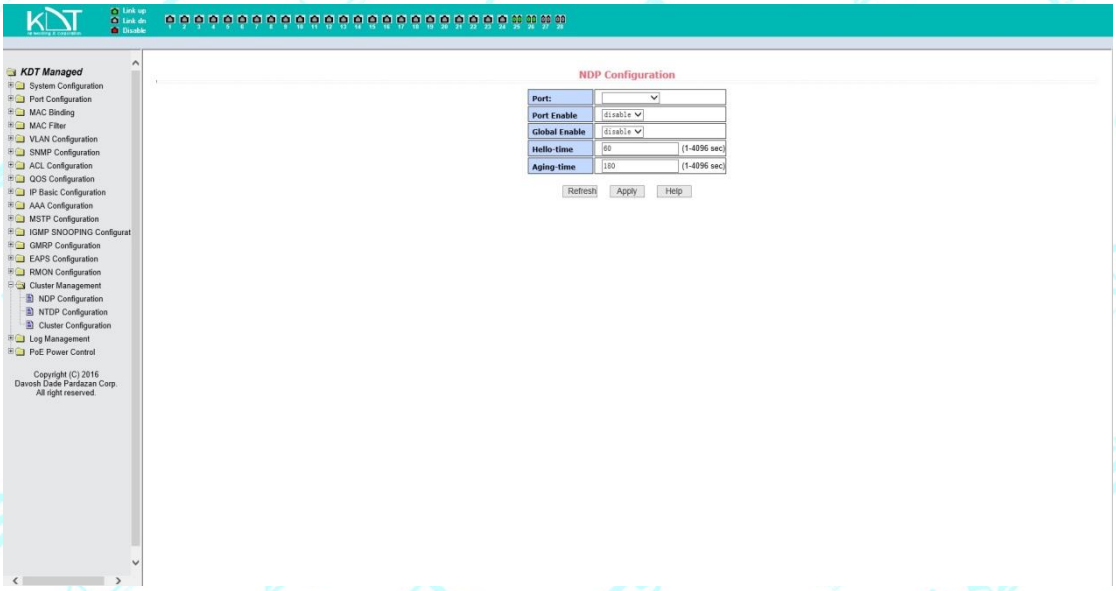
شکل(۶۵)

۲_۱۸ پیکربندی Cluster

۲_۱۸_۱ صفحه پیکربندی NDP

شکل(۶۶) صفحه پیکربندی NDP را نشان می دهد. جایی که کاربر می تواند NDP را پیکربندی کند. اطلاعاتی که می تواند تنظیم شوند شامل زیر است: انتخاب پورت،عملکرد پورت NDP، کارکرد جهانی NDP ، وقفه بسته های ارسالی NDP، زمان پیشین بسته های NDP دریافتی دستگاه ، انتخاب پورت، کتاب گونه ای که لازم است انتخاب کنید و عملکرد پورت NDP رافعال کنید .NPD باید به طور طبیعی کار کند و عملکرد جهانی NDP و پورت در یکزمان باید فعال شود.

زمان پیشین بسته های NDP توسط دستگاه به دستگاه دریافتی ارسال می شود. زمان موثر در محدوده ثانیه های ۱ تا ۴۰۹۶است. پیکربندی پیشفرض 180 ثانیه است. وقفه را ارسال بسته های NDP تشکیل می دهد. محدوده زمانی درست ثانیه های۱ تا ۴۰۹۶ است. پیش فرض 60 ثانیه است.



شکل(۶۶)

۲_۱۸_۲ صفحه پیکربندی NTDP

شکل(۶۷)، صفحه پیکربندی NTDP را نشان می دهند. جایی که کاربر می تواندNTDP را پیکربندی کند.

اطلاعاتی که می توانند تنظیم شوند شامل زیر است:

انتخاب پورت، فعال کردن عملکرد پورت NTDP، فعال کردن عملکرد جهانیNTDP، مجموعه محدوده توپولوژی، مجموعه وقفه های زمانی، زمان تاخیربسته ارسالی اولین پورت، تاخیر بسته های ارسالی سایر پورت ها .

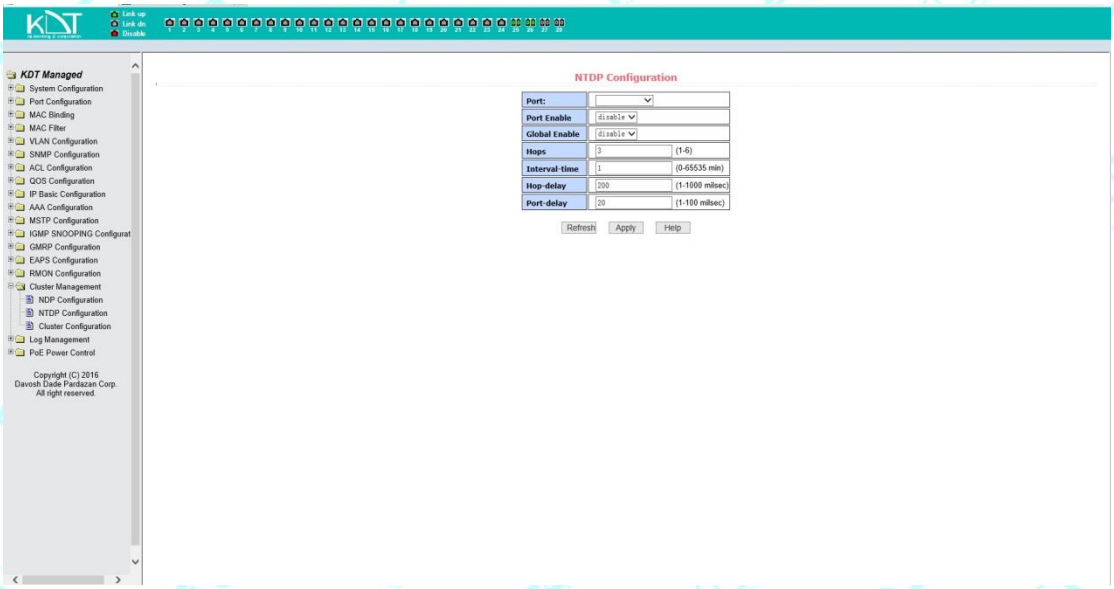
انتخاب پورت، پورت را به طور نیاز میتوانید انتخاب کنید و عملکرد پورت NTDPرا فعال کنید ،NTDP به طور معمول کار میکند شما همچنین عملکرد جهانی NTDP و عملکرد پورت آن را فعال کنید.

پیکربندی مجموع محدوده توپولوژی، محدوده موثر ۱تا ۶۰ است . ، در پیش فرض توپولوژی ، حداکثر تعداد دستگاه سه می باشد.

پیکربندی وقفه برای جمع آوری اطلاعات توپولوژی، محدوده موثر ۰ تا ۶۵۵۳۵ دقیقه است. پیکربندی پیشفرض یک دقیقه است.

زمان تاخیر را برای بسته های ارسالی اولین پورت پیکربندی کنید. محدوده موثر ۱ تا ۱۰۰ میلی ثانیه است. پیکربندی پیشفرض ۲۰۰ میلی ثانیه است.

زمان تاخیر را برای بسته های ارسالی اولین پورت پیکربندی کنید. محدوده موثر ۱ تا ۱۰۰میلی ثانیه است. پیکربندی پیشفرض ۲۰ میلی ثانیه است.



شکل(۶۷)

۳_۱۸_۲ صفحه پیکربندی cluster

شکل(۶۸)، صفحه پیکربندی cluster را نشان می دهد. کاربر می تواند cluster رابه وسیله این صفحه پیکربندی کند و جدول اعضای cluster را ببیند. اطلاعاتی که

میتوانند تنظیم شوند شامل: عملکرد های فعال cluster، پیکربندی مدیریت VLAN، آدرس مجموعه cluster ، وقفه برای ارسال بسته های دستی(handshake)، زمان موثر نگهداری برای دستگاه، اسم cluster ، روش پیوستن به cluster ، و حذف cluster است.

فعال کردن عملکرد cluster و فعال کردن عملکرد cluster برای عملکرد آن به طور معمول. برای این منظور اول باید عملکرد cluster را فعال کنید.

پیکربندی مدیریت VLAN با محدوده معتبر ۱ تا ۴۰۹۴، و پیش فرض بر VLAN1 پیکربندی محدوده IP آدرس اختصاصی استفاده شده توسط اعضای دستگاه ها درclusterمحدوده موثر آدرس IP ، 0.0.0.0 ~ 255.255.255.255 است.

محدوده موثر طول ماسک (0~32) است . وقفه(interval) برای ارسال بسته های دستی(handshake) ۱ تا ۲۵۵ ثانیه است و پیش فرض 10 ثانیه می باشد .

پیکربندی زمان موثر حافظه دستگاه در محدوده موثر ۱تا ۲۵۵ ثانیه است و پیکربندی پیش فرض ۶۰ ثانیه است .

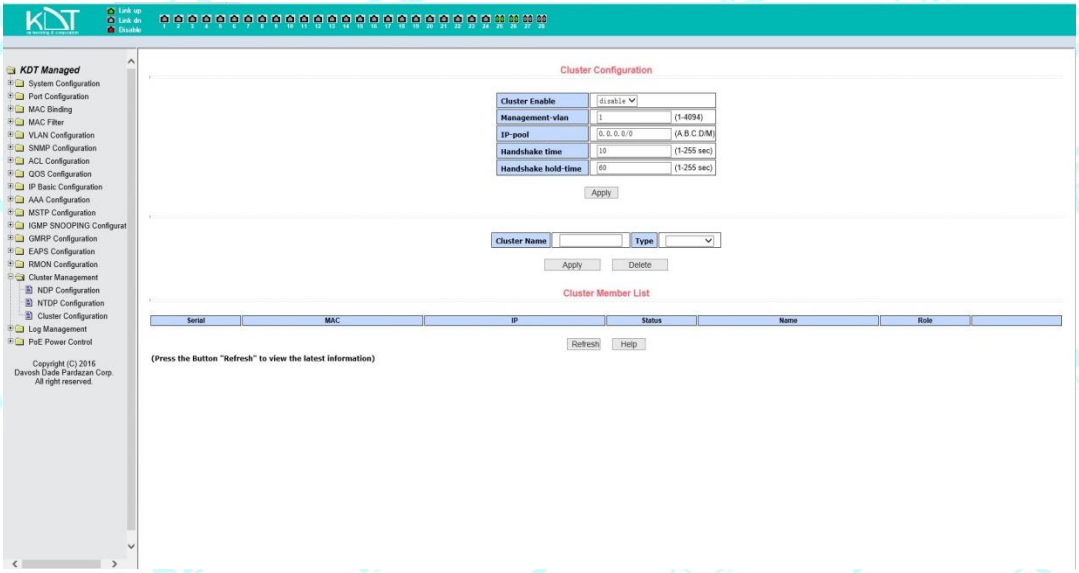
برای تشکیل یک cluster ، شما نیاز دارید نام cluster را درست کنید. برای پیوستن به cluster انتخاب کنید.

راه اتصال از هر دو روش خودکار و دستی (manual)است.

بعد از آنکه cluster تنظیم شد ، می تواند به طور خودکار به روش دستی(manual) سوئیچ شود: اما manual نمی تواند به Automatic سوئیچ شود.

(حالت) manual mode، می تواند نام cluster را عوض کند.

بعد از آنکه شما یک cluster را ساختید، می توانید دستگاه های عضو و دستگاه های خواهان عضو را درجدول اعضای cluster ببینید. شما می توانید یک دستگاه را اضافه یا یک دستگاه داوطلب را به اعضا، بسته به کار آن، اضافه کنید.

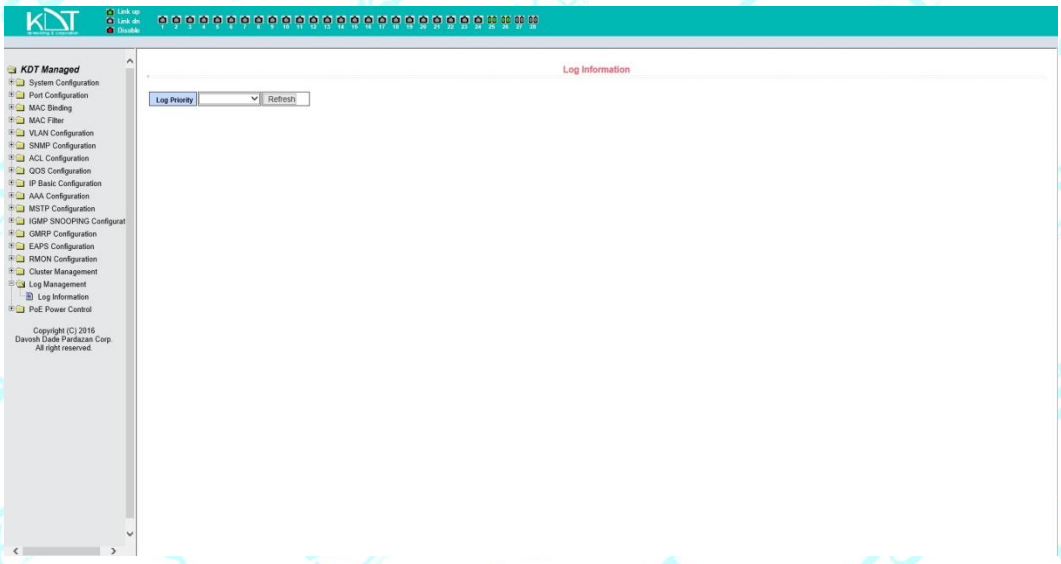


شکل(۶۸)

۲_۱۹ مدیریت ورود (log)

۲_۱۹_۱ اطلاعات ورود(log)

شکل(۷۱)، صفحه اطلاعات ورود(log) را نشان می دهد. کاربر به وسیله این صفحه می تواند log را ببینند. اولویت را از لیست کشویی انتخاب کنید، شما می توانید log آن مرحله را ببینید .Refresh را برای دیدن آخرین log کلیک کنید.



شکل(۷۱)

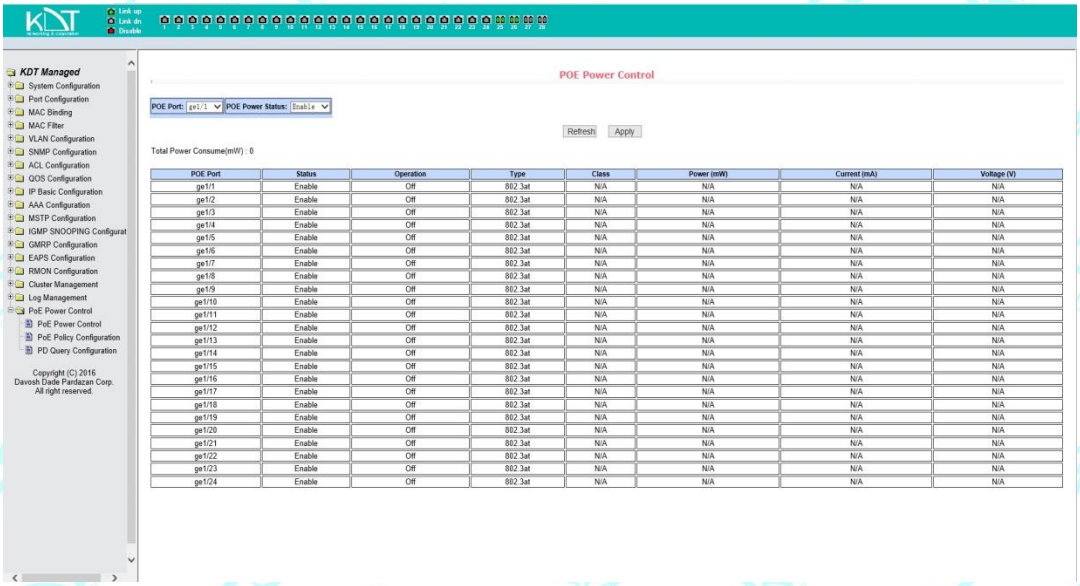
۲_۲۰ پیکربندی پورت POE

۲_۲۰_۱ پیکربندی

شکل(۷۲)، صفحه پیکربندی تولید POE پورت را نشان می دهد. شما می توانیدقدرت کلی دستگاه POE(برای به روز رسانی)، قدرت تنهایی پورت POE (برای بهروز رسانی)، روشن یا خاموش بودن POE؛ این صفحه به شما اجازه می دهد اطلاعات مربوط به دستگاه POE فعلی را ببینید.

پورت POE : شماره پورت تامین قدرت را انتخاب کنید.

وضعیت دستگاه POE: فعال یا غیرفعال سازی کنید.



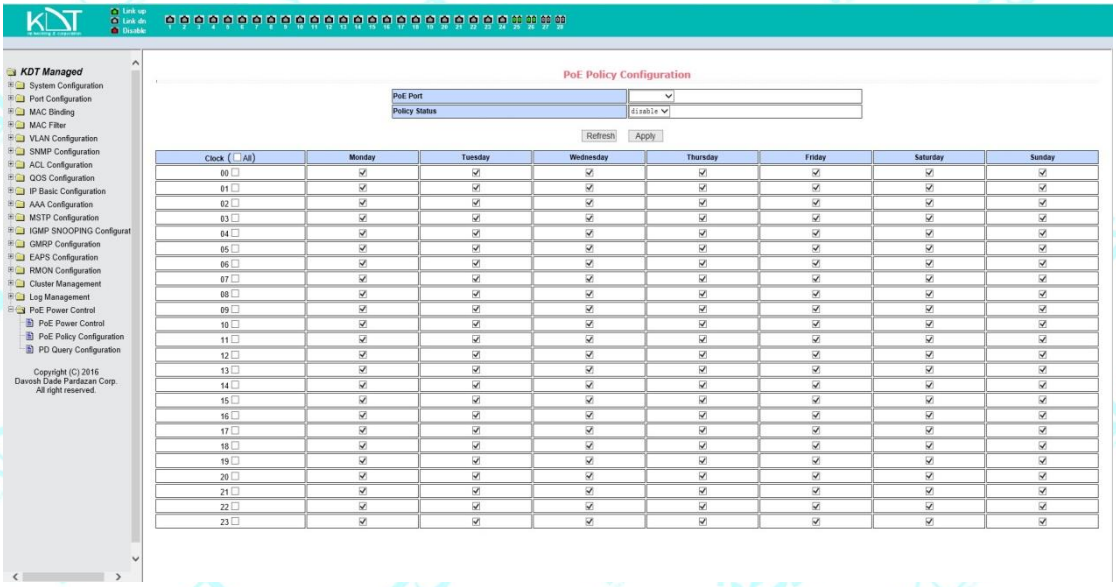
شکل(۷۲)

۲_۲۰_۲ پیکربندی برنامه POE

شکل(۷۳)، پیکربندی برنامه POE را نشان می دهد. به وسیله مدیریت برنامه ریزی، می توانید ذخیره قدرت POE را طبق نیازهای موجود فعال یا غیرفعال کنید، حالت کنترل ، حالت (هفته + ساعت) است.

کنترل پورت: برای انتخاب پورت ها که به مدیریت برنامه ریزی شده نیاز دارند، استفاده می شود.

(1_24)کنترل وضعیت وسیله: فعال یا غیرفعال



شکل(۷۳)

۲_۲۰_۳ بازیابی آنلاین POE (به روز رسانی شدن سیستم)

جهت خاموش یا روشن کردن دستگاه بازیابی آنلاینِ وضعیت بازیابی استفاده می شود، وقتی که دستگاه در حال شروع مجدد موجودی قدرت دستگاه است.