

Title: GWN78XX Switch Web Requirement

Summary:

This document is about the requirement of GWN78XX

**Document Number:** This document is about the requirement of the GWN78XX Switch

**Version:** 1.2.17

**Owner:** xhfang

**Reviewers:** qsding,jwli,lizhu,yaoliu,khlin,qjzou,

wliu,jluo,tyao,mymei,jhzhang,etc

目录

[1. 前言 9](#_Toc149138780)

[1.1 概述 9](#_Toc149138781)

[1.2 约定 10](#_Toc149138782)

[1.3 参考资料 11](#_Toc149138783)

[1.4 版本记录 12](#_Toc149138784)

[2. 管理 35](#_Toc149138785)

[2.1 支持管理的UI方式 35](#_Toc149138786)

[2.2 本地Web浏览器 36](#_Toc149138787)

[3. 登录/Login 37](#_Toc149138788)

[3.1 本地Web管理方式登录交换机 37](#_Toc149138789)

[3.2 Console口登录交换机 38](#_Toc149138790)

[3.3 Telnet方式登录交换机 39](#_Toc149138791)

[3.4 SSH方式登录交换机 39](#_Toc149138792)

[4. 全局配置 40](#_Toc149138793)

[4.1 搜索 40](#_Toc149138794)

[4.2 语言 40](#_Toc149138795)

[4.3 重启 40](#_Toc149138796)

[4.4 登录用户 40](#_Toc149138797)

[4.5 生效与保存 41](#_Toc149138798)

[4.6 新固件升级提示(FP2) 41](#_Toc149138799)

[4.7 云连接状态(FP1D) 42](#_Toc149138800)

[5. 概览/Dashboard(FP1B) 44](#_Toc149138801)

[5.1.1 接口信息/Port Info. 44](#_Toc149138802)

[5.1.2 日志/Log 47](#_Toc149138803)

[5.1.3 系统信息/System Info. 47](#_Toc149138804)

[6. 以太网业务/Switching 51](#_Toc149138805)

[6.1 端口基本配置/Port Basic Settings(FP1B) 51](#_Toc149138806)

[6.2 流量统计/Flow Statistics(FP1B) 54](#_Toc149138807)

[6.3 环路检测(FP2) 58](#_Toc149138808)

[6.4 端口自动恢复/Port Auto Recovery(FP1B) 62](#_Toc149138809)

[6.5 链路聚合/Aggregation Interface(FP1C) 64](#_Toc149138810)

[6.6 MAC表/MAC Table(FP1B) 69](#_Toc149138811)

[6.7 VLAN(FP1B) 75](#_Toc149138812)

[6.7.1 VLAN 75](#_Toc149138813)

[6.7.2 MAC VLAN (FP2) 85](#_Toc149138814)

[6.7.3 Protocol VLAN (FP2) 90](#_Toc149138815)

[6.7.4 Subnet VLAN (FP3) 【待评审】 92](#_Toc149138816)

[6.7.5 语音VLAN/Voice VLAN(FP1C) 93](#_Toc149138817)

[6.8 QinQ (FP2) 97](#_Toc149138818)

[6.9 VLAN交换 (FP2) 100](#_Toc149138819)

[6.10 GVRP (FP3) 102](#_Toc149138820)

[6.11 生成树/STP(FP1C) 109](#_Toc149138821)

[（四）兼容Cisco PVST(Per VLAN Spanning Tree) (FP2) 121](#_Toc149138822)

[（五）兼容Cisco PVST+(Per VLAN Spanning Tree Plus) (FP2) 123](#_Toc149138823)

[6.12 ERPS (FP3) 【待评审】 131](#_Toc149138824)

[7. IP业务/IP 146](#_Toc149138825)

[7.1 VLAN接口/VLAN Interface(FP1D) 146](#_Toc149138826)

[7.2 DHCP (FP1D) 158](#_Toc149138827)

[7.2.1 DHCP服务器/DHCP Server 166](#_Toc149138828)

[7.2.2 DHCP中继/DHCP Relay 176](#_Toc149138829)

[7.3 ARP表/ARP Table (FP1D) 179](#_Toc149138830)

[7.4 邻居发现/ND (FP1D) 182](#_Toc149138831)

[7.5 域名系统/DNS (FP1D) 187](#_Toc149138832)

[8. 路由业务/Routing 191](#_Toc149138833)

[8.1 路由表/Routing Table (FP1D) 192](#_Toc149138834)

[8.2 静态路由/Static Routing (FP1D) 194](#_Toc149138835)

[8.3 动态路由/Dynamic Routing(FP1D) 200](#_Toc149138836)

[8.3.1 RIP 200](#_Toc149138837)

[8.3.2 RIPng 209](#_Toc149138838)

[8.3.3 OSPF 213](#_Toc149138839)

[8.3.4 OSPFv3 232](#_Toc149138840)

[8.4 策略路由/Policy Routing (FP3) 240](#_Toc149138841)

[8.5 VRRP (FP3) 【待评审】 240](#_Toc149138842)

[9. 组播业务/Multicast 253](#_Toc149138843)

[9.1 IP组播 (FP3) 253](#_Toc149138844)

[9.2 IGMP (FP3) 255](#_Toc149138845)

[9.3 MLD (FP3) 255](#_Toc149138846)

[9.4 IGMP Snooping (FP1C) 255](#_Toc149138847)

[9.5 MLD Snooping(FP1C) 263](#_Toc149138848)

[9.6 MVR (FP3) 【待评审】 270](#_Toc149138849)

[10. QoS(FP1B) 275](#_Toc149138850)

[10.1 端口优先级/Port Priority 276](#_Toc149138851)

[10.2 优先级映射/Priority Mapping 278](#_Toc149138852)

[10.3 队列调度/Queue Scheduling 281](#_Toc149138853)

[10.4 队列整形/Queue Shaping 285](#_Toc149138854)

[10.5 端口限速/Rate Limit 286](#_Toc149138855)

[11. 安全业务/Security 288](#_Toc149138856)

[11.1 风暴控制/Storm Control(FP1B) 288](#_Toc149138857)

[11.2 端口安全/Port Security(FP1B) 290](#_Toc149138858)

[11.3 端口隔离/Port Isolation(FP1C) 294](#_Toc149138859)

[11.4 ACL(FP1B) 295](#_Toc149138860)

[11.5 IP源防护/IP Source Guard(FP1B) 326](#_Toc149138861)

[11.6 IPv6源防护/IP Source Guard(FP2) 330](#_Toc149138862)

[11.7 动态ARP检测/Dynamic ARP Inspection(DAI)(FP1C) 333](#_Toc149138863)

[11.8 攻击防范/Anti Attack(FP1B) 335](#_Toc149138864)

[11.9 RADIUS(FP1C) 341](#_Toc149138865)

[11.10 TACACS+(FP1C) 350](#_Toc149138866)

[11.11 AAA(FP1C) 354](#_Toc149138867)

[11.12 身份验证管理/802.1X(FP1C) 356](#_Toc149138868)

[11.13 DHCP Snooping(FP1C) 367](#_Toc149138869)

[11.14 DHCPv6 Snooping(FP2) 371](#_Toc149138870)

[12. PoE(FP1B) 377](#_Toc149138871)

[13. 维护 384](#_Toc149138872)

[13.1 升级/Upgrade 384](#_Toc149138873)

[13.2 诊断/Diagnostics(FP1B) 388](#_Toc149138874)

[13.2.1 日志/Log 388](#_Toc149138875)

[13.2.2 Ping 390](#_Toc149138876)

[13.2.3 Traceroute 391](#_Toc149138877)

[13.2.4 光模块/Fiber Module 392](#_Toc149138878)

[13.2.5 镜像/ Mirroring 393](#_Toc149138879)

[13.2.6 sFlow/sFlow (FP3) 【待评审】 401](#_Toc149138880)

[13.2.7 UDLD [TBD] 404](#_Toc149138881)

[13.2.8 线缆检测/Copper Test (FP1C) 404](#_Toc149138882)

[13.2.9 一键调试/OneClick Debug (FP1D) 405](#_Toc149138883)

[13.2.10 云连接状态检测 (FP1D) 406](#_Toc149138884)

[13.3 备份与恢复/Backup & Restore(FP1B) 408](#_Toc149138885)

[13.4 告警/Alert（适配Cloud端）(FP1D) 411](#_Toc149138886)

[13.5 SNMP(FP1C) 412](#_Toc149138887)

[13.6 RMON(FP1C) 421](#_Toc149138888)

[13.7 TR-069(FP3) 428](#_Toc149138889)

[13.8 LLDP & LLDP-MED(FP1C) 429](#_Toc149138890)

[13.9 节能管理/Energy Saving Management 448](#_Toc149138891)

[13.9.1 节能以太网/EEE(FP1D) 449](#_Toc149138892)

[14. 系统/System 451](#_Toc149138893)

[14.1 基础设置/Basic Settings 451](#_Toc149138894)

[14.2 登录服务/Login Service 453](#_Toc149138895)

[14.2.1 ~~管理IP地址/Management IP Address~~ (FP1B) 【去除，不再支持20221122】 453](#_Toc149138896)

[14.2.2 访问控制/Access Control 455](#_Toc149138897)

[14.3 用户管理(FP1B) 459](#_Toc149138898)

[14.4 时间策略/Time Policy (FP1D) 461](#_Toc149138899)

[14.5 1588v2 TC(FP2) 462](#_Toc149138900)

[15. 堆叠/Stack(FP3) 472](#_Toc149138901)

[16. LED指示灯(FP1C) 489](#_Toc149138902)

[17. 风扇/Fan(FP1D) 493](#_Toc149138903)

[18. 电源/Power Supply(FP1D) 495](#_Toc149138904)

# 前言

## 概述

GWN78XX系列交换机，是Grandstream第一代企业级交换机产品。GWN7800系列L2+交换机采用RTL83XX系列芯片，GWN7806(P)/10/20/30系列L3交换机采用RTL93XX系列芯片。本文档定义了交换机本地的软件功能需求和大致UI结构布局，作为后续产品开发任务需求指导。不包含GWN.Cloud的交换机集中管理需求。

目前支持的交换机型号如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 型号 | 接口 | 芯片 | 备注 |
| GWN7801 | 8x 10/100/1000 Base-T，2x 1G Fiber, 1x Console, 1x Reset Pinhole | RTL8380M | 二+层交换机 |
| GWN7801P | 8x 10/100/1000 Base-T with PoE/PoE+，2x 1G Fiber, 1x Console, 1x Reset Pinhole | RTL8380M | 二+层PoE交换机 |
| GWN7802 | 16x 10/100/1000 Base-T，4x 1G Fiber, 1x Console, 1x Reset Pinhole | RTL8382M | 二+层交换机 |
| GWN7802P | 16x 10/100/1000 Base-T with PoE/PoE+，4x 1G Fiber, 1x Console, 1x Reset Pinhole，1x Fan | RTL8382M | 二+层PoE交换机 |
| GWN7803 | 24x 10/100/1000 Base-T，4x 1G Fiber, 1x Console, 1x Reset Pinhole | RTL8382M | 二+层交换机 |
| GWN7803P | 24x 10/100/1000 Base-T with PoE/PoE+，4x 1G Fiber, 1x Console, 1x Reset Pinhole, 2x Fan | RTL8382M | 二+层PoE交换机 |
| GWN7806 | 48x 10/100/1000 Base-T，4x 10G Fiber，1x Console，1x Reset Pinhole, 3x Fan | RTL9311 | 二+层堆叠交换机 |
| GWN7806P | 48x 10/100/1000 Base-T with PoE/PoE+，4x 10G Fiber，1x Console，1x Reset Pinhole, 3x Fan | RTL9311 | 二+层PoE堆叠交换机 |
| GWN7811 | 8x 10/100/1000 Base-T, 2x 10G Fiber, 1x Console, 1x Reset Pinhole | RTL9301 | 三层交换机 |
| GWN7811P | 8x 10/100/1000 Base-T with PoE/PoE+, 2x 10G Fiber, 1x Console, 1x Reset Pinhole | RTL9301 | 三层PoE交换机 |
| GWN7812P | 16x 10/100/1000 Base-T with PoE/PoE+, 4x 10G Fiber, 1x Console, 1x Reset Pinhole，2x Fan | RTL9301 | 三层PoE交换机 |
| GWN7813 | 24x 10/100/1000 Base-T, 4x 10G Fiber, 1x Console, 1x Reset Pinhole，RPS | RTL9301 | 三层堆叠交换机 |
| GWN7813P | 24x 10/100/1000 Base-T with PoE/PoE+/PoE++(1-8), 4x 10G Fiber, 1x Console, 1x Reset Pinhole，3x Fan，RPS | RTL9301 | 三层PoE堆叠交换机 |
| GWN7816 | 48x 10/100/1000 Base-T, 6x 10G Fiber, 1x Console, 1x Reset Pinhole，3x Fan，热冗余电源 | RTL9311-CG | 三层堆叠交换机 |
| GWN7816P | 48x 10/100/1000 Base-T with PoE/PoE+/PoE++(1-8), 6x 10G Fiber, 1x Console, 1x Reset Pinhole，3x Fan，热冗余电源 | RTL9311-CG | 三层PoE堆叠交换机 |
| GWN7821P | 8x 2.5G Base-T with PoE/PoE+, 2x 10G Fiber, 1x Console, 1x Reset Pinhole | RTL9302C-CG | 三层PoE交换机 |
| GWN7823P | 12x 2.5G Base-T with PoE/PoE+, 12x 1G Base-T with PoE/PoE+, 6x 10G Fiber, 1x Console, 1x Reset Pinhole | RTL9313 | 三层PoE堆叠交换机 |
| GWN7832 | 12x 10G Fiber, 1x Console, 1x Reset Pinhole，2x Fan，RPS | RTL9313 | 三层汇聚型交换机 |
| GWN7831 | 4x 10/100/1000 Bast-T，24x 1G Fiber（1-4为Combo口），4x 10G Fiber，1x Console，1x Reset Pinhole，RPS | RTL9301 | 三层汇聚型交换机 |
| GWN7830 | 6x 1G Fiber，4x 10G Fiber，2x GbE，1x Console，1x Reset Pinhole | RTL9301 | 三层汇聚型交换机 |

注：RTL9300系列和RTL9310系列堆叠功能至多支持8个设备。~~RTL9300系列堆叠口固定，RTL9310系列堆叠口可配。~~

## 约定

1. 图形界面格式约定

|  |  |
| --- | --- |
| 格式 | 意义 |
| <> | 带尖括号“<>”表示按钮名，如“点击<确定>进行设置”。 |
| [] | 带方括号“[]”表示弹窗名、菜单名和数据表，如“弹出[设置向导]窗口”。 |
| / | 多级菜单用“/”隔开。如[安全/802.1X/启用802.1X认证]多级菜单表示[安全]菜单下的[802.1X]子菜单下的[启用802.1X]选项 |

1. 命令行格式约定

|  |  |
| --- | --- |
| 格式 | 意义 |
| {x|y|…} | 表示从多个选项中仅选取一个 |
| [x|y|…] | 表示从多个选项中选取一个或不选 |
| [x|y|…]\* | 表示从多个选项中选取一个、多个或不选 |
| \*xxxx | 表示此配置项为必填项，如“\*MIB  子树OID”表示MIB子树OID为必填项 |

1. 其他约定

*[蓝色加下划线倾斜字体]*为暂不支持的内容

(FP1B), (FP1C), (FP1D), (FP2), (FP3)为开发阶段需求划分

*XXXX*[采用修订方式]为阶段性需求评审后的需求变更

~~XXXX~~为删除的需求

[TBD]为待定需求

XXXX为差异需求说明

## 参考资料

|  |
| --- |
| 竞品，包括华为，华三，思科，NetGear，锐捷，优力普，希力等 |
|  |

## 版本记录

|  |  |  |  |
| --- | --- | --- | --- |
| 修订版本 | 修订日期 | 修订内容 | 修订人 |
| 1.2.17 | 2023.11.8 | 结合需求评审意见优化：   * 端口组的配置方案确定 * 镜像：开放普通业务数据收发配置 | xhfang |
| 1.2.16 | 2023.10.25-11.6 | 优化点：   * 流量统计改为端口统计 * 优化端口定时启用功能 * 堆叠 * 堆叠建立后，去除设备ID预设功能 * 堆叠建立后，无法修改堆叠配置，必须退出堆叠后才可修改，然后再重新加入堆叠 * 堆叠设置时，设备ID和堆叠口同时配置，设备重启后，堆叠口命名规则自动跟随设备ID变化同步更新 * 堆叠口2选1必填 * 风暴控制：IFG仅在Kbps单位下有效   FP2新增：   * 端口基本配置：新增[端口组](#_端口基本配置/Port_Basic_Settings(FP1B)) * 新增[RSPAN](#_13.2.5.4_RSPAN_(FP2)) * 联动RSPAN，优化[ACL规则高级设置](#_ACL(FP1B))镜像功能 * 升级：新增FTP/FTPS方式 * 1588v2 TC：开放PTP配置 | xhfang |
| 1.2.15 | 2023.09.21-10.25 | 优化点：   * RIP/RIPng：引入外部路由的度量值取值范围优化 * EEE：增加端口运行状态 * VLAN/端口设置 * 协议VLAN的索引选中后，一并显示协议类型值 * 协议VLAN的VLAN输入限制调整 * 端口环路检测：增加端口运行状态 * 端口优先级：补充出入方向说明 * VLAN交换：内外层VLAN无须是端口已加入的VLAN，去除此限制 * ARP/邻居发现：调整老化时间下限 * 【FP2新增】VLAN限速 * 新增VLAN绑定ACL，与端口绑定ACL互斥 * ACL规则高级设置新增限速设置 | xhfang |
| 1.2.14 | 2023.09.02-09.20 | 优化点：   * [堆叠](#_堆叠/Stack(FP3))：增加预留VLAN * [流量统计](#_流量统计/Flow_Statistics(FP1B))：新增私有MIB统计信息 * [VLAN/端口设置](#_VLAN)：QinQ端口不支持配置TPID * 语音VLAN：新增Untagged OUI模式，优化原OUI模式 * [VLAN交换](#_VLAN)： * 838x芯片的聚合组不支持VLAN交换 * 内外层VLAN有且仅有1个支持N to 1，端口下多组同步适用 * [VLAN接口](#_VLAN接口/VLAN_Interface(FP1D))： * IPv6默认网关为链路本地地址时，须支持配置出接口 * 补充VLAN接口获取IP的说明 * [协议VLAN](#_Protocol_VLAN_(FP2))：协议模板的协议值取值上限更新 * [DHCP服务器](#_DHCP服务器/DHCP_Server)：Option43新增2个业务选项 * [访问控制](#_访问控制/Access_Control)：优化Manager设置逻辑 | xhfang |
| 1.2.13 | 2023.08.24-09.01 | FP2新增小BUG需求点：   * [概览/端口信息](#_接口信息/Port_Info.)：增加邻居信息 * [概览/系统信息](#_系统信息/System_Info.)：新增管理VLAN显示，并调整管理IP和默认网关显示 * [端口基本配置](#_端口基本配置/Port_Basic_Settings(FP1B))：新增端口定时开启功能 * [VLAN接口](#_VLAN接口/VLAN_Interface(FP1D))：管理VLAN下支持配置默认网关   优化点：   * [端口基本配置](#_端口基本配置/Port_Basic_Settings(FP1B))：各型号聚合接口默认速率调整，去除Auto * VLAN接口/ARP/ND：补充删除VLAN接口的联动逻辑，当删除VLAN接口时，对应的邻居表项也同步删除 * [ARP](#_ARP表/ARP_Table_(FP1D))/[ND](#_邻居发现/ND__(FP1D))：邻居表老化时间下限调整 * [DHCP服务器](#_DHCP服务器/DHCP_Server)：补充option添加的判断逻 * [SNMP](#_SNMP(FP1C))：组的添加规则逻辑补充说明 * [夏令时](#_基础_设置/Basic_Settings)开关和模式合并优化 * 1588v2 TC：补充PTP TC仅支持管理VLAN的说明 * SSH/Telnet Client：补充规格上限 * 环路检测 * 增加报文类型设置 * 端口列表支持刷新 * 协议VLAN：补充无法删除的说明 * OSPF/接口设置：补充密钥输入限制 | xhfang |
| 1.2.12 | 2023.08.14 | 根据交互评审意见修改+优化：   * VLAN交换 * 内外层VLAN映射支持配置多组，规格与其他模块共享，上限由底层报错返回提示 * 内外层VLAN和映射后的内外层VLAN必须2选1配置 * DHCP Snooping的Remote ID和Circuit ID字符支持与名称/描述保持一致 * OSPF NBMA邻居配置上限优化 * GWN7816(P)电源指示灯 * 更新电源指示灯亮灯逻辑 * 补充电源供电逻辑 * 补充概览/系统信息的电源信息 * 补充更新各型号风扇策略 * GWN7806P风扇转速补充中转速选项 | xhfang |
| 1.2.11 | 2023.08.08 | 根据交互评审意见+BUG修改：   * 概览/系统信息：CPU使用率和内存使用率均增加历史详情控制图 * ACL规则高级设置 * 统计计数：统计单位分芯片平台更新 * 镜像 * 类型配置去除 * 镜像组补充只能选择空镜像组，否则提示“镜像组已绑定端口” * 镜像功能需提示“镜像功能需要前往“维护→诊断→镜像”配置观察口生效” * 优先级重定向优化为优先级映射 * 适配ACL规则的镜像功能，增加ACL镜像模块，与端口镜像合并显示与配置：仅入方向镜像显示绑定的ACL类型+ACL名称+规则ID，支持配置观察口（不包含ACL绑定的端口） * VLAN交换：838X平台不支持2 to 2，隐藏内层VLAN映射配置 * IP源防护/IPv6源防护：接口设置去除最大条目数配置 * LLDP-MED网络策略：VLAN取值范围优化 | xhfang |
| 1.2.10 | 2023.08.03 | 根据需求评审意见修改：   * 环路检测：暂仅支持shutdown动作 | xhfang |
| 1.2.9 | 2023.08.02 | FP2新增：   * 新增[VLAN交换](#_VLAN交换_(FP2)) * 新增[环路检测](#_环路检测(FP2)) * [VLAN IPv6接口](#_VLAN接口/VLAN_Interface(FP1D))：全球单播地址除手动配置外，增加网关优先级   优化：   * [OSPF](#_OSPF)：端口设置的简单认证密钥长度优化 * 名称/描述的字符支持更新，新增3项?/, * [路由通告](#_VLAN接口/VLAN_Interface(FP1D))：前缀长度取值范围优化 * [端口安全](#_端口安全/Port_Security(FP1B))：优化全局设置的速率说明 * SSH/Telnet Client：公钥校验支持 | xhfang |
| 1.2.8 | 2023.07.20 | * VLAN接口 * IPv6链路本地地址手动配置的前缀和编辑优化 * MTU取值范围更改，保证IPv6地址不丢失 * ACL：规则默认放行后，补充提示ACL创建后，系统默认规则丢弃且优先级最低 * 光模块信息 * 概览/接口信息：优化功率显示单位 * 诊断/光模块：优化功率显示单位并去除计算方式说明   FP3：   * 新增堆叠 | xhfang |
| 1.2.7 | 2023.07.07 | 优化：   * 名称/描述的字符支持与报错提示优化，具体详见[表](http://192.168.120.130:8888/Products/Files/doceditor.aspx?fileid=18176) * 端口基本配置 * 10Gbps SFP+端口支持自动检测功能 * GWN782X：2.5G电口不支持半双工 * 链路聚合：SFP+口使能自动检测后无法加入聚合组 * DHCP服务器：优化Option43配置 * 路由表：默认路由不再支持编辑和删除 * OSPF/OSPFv3 * 增加重启OSPF进程功能 * 路由器ID：补充修改生效的提示信息 * 接口设置：LSA传输延迟时间取值范围优化 * 每个VLAN接口最大支持5个邻居 * 1588v2 TC：仅支持电口 * SNMP * 视图：OID输入优化 | xhfang |
| 1.2.6 | 2023.06.26 | 根据需求评审意见修改+BUG建议优化：   * 概览 * ~~端口信息：Uplink口显示TBD~~ * 端口信息：PoE供电功率控制图优化时段和统计间隔 * 【新增】[端口基本配置](#_端口基本配置/Port_Basic_Settings(FP1B))：RTL93XX芯片平台，10G光口速率为10Gbps时增加DAC线选择 * 【优化】[协议VLAN](#_VLAN)：802.1p调整到端口设置与VLAN绑定 * 基本QinQ：TPID改为全类型端口支持配置 * 【新增】[VLAN IPv4接口](#_VLAN接口/VLAN_Interface(FP1D))：使用DHCP获取IP地址时增加网关优先级功能 * 【优化】[IGMP](#_IGMP_Snooping_(FP1C))/[MLD Snooping](#_MLD_Snooping(FP1C))：查询器的IP地址设置补充限制 * ACL * 【优化】规则数据行为默认放行 * 统计计数：83XX和93XX芯片平台做差异化处理 * Mirror/数据报文类型：83XX和93XX平台做差异化处理 * 优化3个高级设置的配置 * 【优化】[队列整形](#_队列整形/Queue_Shaping)：CBS支持型号更新 * 【优化】[端口限度](#_端口限速/Rate_Limit)：CBS优化 | xhfang |
| 1.2.5 | 2023.06.20 | FP2新增需求：   * 概览 * [系统信息](#_系统信息/System_Info.)：RTL9310平台新增双核CPU使用率显示 * ~~端口信息：增加Uplink口显示~~ * [端口信息](#_接口_信息/Port_Info.)：PoE端口补充历史供电功率显示，并以控制图形式展示 * [基本QinQ](#_VLAN) * [VLAN/端口成员](#_VLAN)：Trunk类型端口新增Trunk Allowed VLANs配置 * [语音VLAN](#_语音VLAN/Voice_VLAN(FP1C))：新增自动语音VLAN功能，即LLDP-MED相关联动设置 * 新增[IPv6SG](#_IPv6源防护/IP_Source_Guard(FP2)) * [ACL规则](#_ACL(FP1B))新增Statistic、Mirror、Priority Remapping * 告警：新增光模块温度告警与保护 * [夏令时](#_基础_设置/Basic_Settings)支持 * 新增[TR-069](#_TR-069(FP2_TBD))   优化：   * ACL：规则默认放行 | xhfang |
| 1.2.4 | 2023.06.15 | 根据需求优化和交互评审优化修改：   * 全局/搜索 * mDNS设备发现：补充支持发现的VLAN接口，默认所有接口参与发现 * 新固件升级提示 * 优化升级路径 * 提供一键下载升级功能 * 端口基本配置：GWN7831 Combo口自协商优先光口模式 * VLAN/端口设置：Access接收的帧类型默认值修改为All * MAC VLAN：优化为基于MAC绑定VLAN方式 * 协议VLAN * 优化协议模板配置 * 端口设置：开启协议VLAN功能后，指定协议模板与VLAN的映射关系 * VLAN接口 * Loopback接口默认值修改，包括IPv4和IPv6 * IPv6接口：全球单播地址静态配置的前缀取值范围优化 * DHCP服务器地址池个数规格调整为128个 * IPv6路由 * 默认/静态路由：链路本地地址作为下一跳地址，需要同时支持出接口配置 * 静态路由：前缀长度取值范围优化 * ARP和NDP邻居表规格调整为256 * DNS：域名后缀支持- * ACL名称配置支持空格（仅限中间） * 攻击防范：ICMP Ping和ICMPv6 Ping的配置说明优化 * DHCP Snooping：Circuit ID和Remote ID输入的特殊字符限制优化 * DHCPv6 Snooping：数据统计优化 * SSH/Telnet Client：补充公有key密钥校验支持 * 1588v2 TC：配置名称优化   RIP：   * 全局设置：增加全局RIP运行状态信息显示 * 接口设置 * 当接口无地址时，禁用编辑 * 接口列表，目的地址/掩码显示优化   RIPng：   * 全局设置：增加全局RIPng运行状态信息显示 * 接口设置 * 当接口无地址时，禁用编辑 * 接口列表，目的地址/前缀显示优化，且链路本地和全球单播地址均需显示   OSPF：   * 全局设置 * LSA定时器配置名称优化 * 始终通告默认路由的度量值和外部路由度量值取值范围优化 * 增加全局OSPF运行状态信息显示 * 接口设置 * 配置增加OSPF开关，开启后支持设置区域ID，区域ID设置既支持数字又支持IPv4地址 * 新增Fast Hello功能，Hello间隔和邻居失效时间优化 * 开销值取值范围调整 * 接口列表，增加接口地址和状态显示 * 接口增加OSPF运行详情信息显示 * 区域设置 * 区域ID以IPv4地址格式显示 * 区域不支持添加和删除（仅支持编辑），根据接口设置的区域ID自动生成和删除 * 邻居设置 * TAB名称优化为NBMA邻居 * 添加邻居增加Hello报文间隔、优先级 * 邻居列表，增加与邻居匹配的同网段接口地址（包括VLAN ID和IP地址）   OSPFv3：   * 全局设置 * 引入外部路由的度量值和度量类型暂不支持 * 增加全局OSPFv3运行状态信息显示 * 接口设置 * 配置增加OSPFv3开关，开启后支持设置区域ID，区域ID设置既支持数字又支持IPv4地址 * 邻居失效时间乘数去除 * 接口列表，增加接口地址和状态显示，且链路本地和全球单播地址均需显示 * 接口增加OSPFv3运行详情信息显示 * 区域设置 * 区域不支持添加和删除（仅支持编辑），根据接口设置的区域ID自动生成和删除 * 编辑时增加区域类型选择 | xhfang |
| 1.2.2 | 2023.05.12 | 根据交互评审和部分问题优化：   * [用户管理](#_用户管理(FP1B))：Monitor用户去除重启支持 * [AAA](#_AAA(FP1C))：方法1去除Empty，一个AAA里必须要有一个方法 * [静态路由](#_静态路由/Static_Routing_(FP1D))：静态路由表项去除Flags * [PVST](#_（四）兼容Cisco_PVST(Per_VLAN)：PVST端口设置优化 * [RIP](#_RIP)/[RIPng](#_RIPng) * 增加VLAN接口批量编辑个数上限 * 路由通告个数上限调整 * 增加批量添加/删除路由通告个数上限 * 增加邻居信息 * 去除路由表 * [OSPF](#_OSPF)：邻居信息列表去除计数器信息显示 * [OSPFv3](#_OSPFv3) * 区域设置，增加批量添加/删除个数上限 * 邻居信息，优化列表信息显示 | xhfang |
| 1.2.1 | 2023.04.28 | 根据需求评审意见优化：   * [MAC VLAN](#_MAC_VLAN_(FP2)) * 调整MAC-VLAN映射数量上限 * 掩码长度限制修改 * [Protocol VLAN](#_Protocol_VLAN_(FP2)) * 每个VLAN允许添加的协议模板上限修改 * 优化协议模板配置，改为协议索引、帧类型、协议类型值和802.1p优先级 * [GVRP](#_GVRP_(FP1D)[TBD]) * [PVST/PVST+](#_（四）兼容Cisco_PVST(Per_VLAN) * 确定采用方案一 * 当生成树模式选择PVST时，MST的实例和端口设置隐藏 * [DHCPv6 Snooping](#_DHCPv6_Snooping(FP2)) * [端口自动恢复](#_端口自动恢复)：增加选项DHCPv6速率超过限制 * [IP源防护](#_IP源防护/IP_Source_Guard(FP1B))： * 绑定表支持导入/导出 * 绑定表IP地址开放IPv6格式输入 * [PTP TC](#_PTP_TC(FP2)) * 默认模式修改为E2E TC * 端口列表去除端口状态信息显示   优化：   * [链路聚合/LACP端口设置](#_链路聚合/Aggregation_Interface(FP1C))：超时默认为慢 * [路由表](#_路由表/Routing_Table_(FP1D))/[静态路由](#_静态路由/Static_Routing_(FP1D))：表项增加Flags信息 * IGMP/MLD Snooping/组播端口：组播最大组数的取值0优化说明 * OSPF/OSPFv3： * OSPF/全局设置：默认路由通告优化 * OSPF/区域：NSSA类型的默认值改为Never，去除Candidate类型 * Database显示调整 * 去除路由表显示 * 邻居信息表显示调整 * RADIUS/TACACS+：服务器个数上限调整为4 * 用户管理：用户名去除特殊字符&的支持 * VLAN接口/静态路由/ARP表/ND表：型号规格更新 | xhfang |
| 1.2.0 | 2023.04.26 | FP2-6月版本新增：   * 新增1588v2 PTP TC * 新增MAC VLAN * 新增Protocol VLAN * 新增GVRP * 新增DHCPv6 Snooping * 新增PVST/PVST+ | xhfang |
| 1.1.12 | 2023.04.17 | 根据交互评审结果优化：   * 静态路由：网关接口设置优化 * 路由表： * 去除动态路由的老化时间 * 搜索条件增加路由协议筛选 * OSPF： * 配置/上限等优化 * 接口配置：密钥认证补充密钥配置 * 接口统计信息去除，改为邻居配置 | xhfang |
| 1.1.11 | 2023.04.13 | FP1D-6新增：   * [端口基本配置](#_端口基本配置/Port_Basic_Settings(FP1B))：GWN7831端口1-4补充工作模式 * [VLAN接口](#_VLAN接口/VLAN_Interface(FP1D))：IPv6接口全球单播地址：支持无状态DHCPv6获取地址 * [静态路由](#_静态路由/Static_Routing_(FP1D))：新增出接口配置 * [OSPF](#_OSPF)：接口新增邻居配置 * [诊断](#_云连接状态检测_(FP1D)) * 新增云连接状态检测 * 全局配置：新增云连接状态显示 * [访问控制](#_访问控制/Access_Control)：新增Manager二层发现 * [LED指示灯](#_LED指示灯(FP1C)) * 新增GWN7806(P)/16(P)/32/31/30的端口和电源指示灯需求 * GWN7816(P)的电源指示灯需求【TBD】 * 【GWN7813(P)】电源 * [电源](#_电源/Power_Supply(FP1D)_【待补充】)：补充电源使用逻辑 * [概览/系统信息](#_系统信息/System_Info.)：新增电源显示信息 * [PoE](#_PoE(FP1B))：新增GWN7813P电源PoE供电相关需求   优化：   * 端口基本配置 * 补充83xx平台jumbo帧的使用说明 * 链路聚合：补充聚合接口个数上限 * 生成树：MST实例上限补充说明 * VLAN接口： * 重新更新各平台接口数量限制 * 管理VLAN * 去除默认网关和生效网关 * 补充管理VLAN的IP地址冲突的提示 * ~~DHCP服务器：补充Option选项与类型的限制关系~~ * ARP表/ND表：接口显示优化 * 路由表：优化默认路由的协议显示 * 静态路由：优化掩码输入范围 * IGMP/MLD Snooping：查询器IP地址编辑时改为非必填，为空即表示使用VLAN接口IP地址 * 端口安全：优化列表安全MAC地址的词条显示 * Ping：接口改为非必填，且所有交换机均支持 * 光模块：补充Output/Input Power的计算方式说明 * 一键调试 * 支持保留最新文件，支持下载和删除，不再自动保存至PC * 因调试时间大大优化，去除“取消调试”功能 * 恢复出厂：补充启机时按reset键支持设备恢复出厂 | xhfang |
| 1.1.10 | 2023.03.15 | FP1D-5优化：   * [全局配置：新固件升级提示](#_固件版本提示(FP1D)) * [端口基本配置](#_端口基本配置/Port_Basic_Settings(FP1B))：端口编号变更，并补充命名规则 * [VLAN接口](#_VLAN接口/VLAN_Interface(FP1D))： * 补充接口IP地址冲突的Alert告警需求 * 优化IPv6 RA配置 * [调试/告警](#_告警/Alert(FP1D))：新增配合Cloud端的本地告警支持 | xhfang |
| 1.1.9 | 2023.03.10 | FP1D-5新增：   * [管理](#_支持管理的UI方式)：新增mDNS设备发现功能支持 * [全局配置](#_固件版本提示(FP1D))：新增固件版本提示 * [概览/系统信息](#_系统信息/System_Info.)：设备温度显示和高温告警 * [流量统计](#_流量统计/Flow_Statistics(FP1B))：Etherlike补充动态dTpPortIndiscards * [VLAN接口](#_VLAN接口/VLAN_Interface(FP1D))：管理VLAN下新增默认网关配置 * [系统/访问控制](#_访问控制/Access_Control)：新增Manager设置   本期优化：   * MAC地址、ARP等数量上限、PoE供电总功率等补充 * 概览/系统信息：补充默认网关显示逻辑 * [STP](#_生成树/STP(FP1C))：全局路径开销为长和短时，端口的路径开销取值范围补充 * [VLAN接口](#_VLAN接口/VLAN_Interface(FP1D))： * 一旦被DHCP服务器/中继选择，VLAN接口禁止编辑和删除 * 变更VLAN接口数量规格 * [DHCP](#_DHCP_(FP1D))： * DHC服务器的接口地址池和中继均只能选取静态IP地址配置的VLAN接口 * DHCP服务器的DHCP Option选项内容输入范围调整 * 地址分配逻辑变更，优化为接口地址池>中继，全局仅供给中继使用 * [ARP表](#_ARP表/ARP_Table_(FP1D))/[ND表](#_邻居发现/ND__(FP1D))：静态表项的接口不存在，显示— * [队列整形](#_队列整形/Queue_Shaping)/[端口限速](#_端口限速/Rate_Limit) * 补充CIR的最大值和默认值说明 * CBS的16整数倍限制去除 * 去除批量编辑功能 | xhfang |
| 1.1.8 | 2023.02.25 | FP1D-3/4优化：   * [端口基本配置](#_端口基本配置/Port_Basic_Settings(FP1B))：巨型帧默认值修改 * [VLAN接口](#_VLAN接口/VLAN_Interface(FP1D))：VLAN接口Up的判断条件修改 * [IPv6 RA](#_VLAN接口/VLAN_Interface(FP1D)) * 调整路由通告时间间隔的默认值 * 生存时间的0值表意修改 * 前缀支持至多添加8个 * 管理VLAN的IP获取说明优化 * OSPF/OSPFv3：路由器ID仅支持手动配置 * [一键调试](#_一键调试/Copper_Test_(FP1D))：设备重启，调试文件不保留 | xhfang |
| 1.1.7 | 2023.02.22 | FP1D-4新增：   * [VLAN接口](#_VLAN接口/VLAN_Interface(FP1D)) * 增加管理VLAN * 新增MTU设置 * 新增IPv6接口使能 * 新增IPv6 RA功能 * [动态路由](#_动态路由/Dynamic_Routing(FP1D)) * [路由表](#_路由表/Routing_Table_(FP1D))（仅L3支持） * [PoE++](#_PoE(FP1B))（仅GWN7813P/16P支持） * [一键调试](#_一键调试/Copper_Test_(FP1D)) * [Ping](#_Ping)：增加发包数和包长度   本期优化：   [VLAN接口](#_VLAN接口/VLAN_Interface(FP1D))   * 补充loopback接口和普通VLAN接口的状态判断逻辑 * IPv4 loopback接口的掩码前缀长度范围修改 * VLAN IPv6接口全球单播地址手动配置的前缀长度范围修改 * VLAN接口IPv4和IPv6共用情况说明，优化接口列表显示 * IPv6接口无状态自动配置，各接口均支持    [DHCP绑定表](#_DHCP服务器/DHCP_Server)   * 客户端名称新增特殊字符“-”支持    [ARP表](#_ARP表/ARP_Table_(FP1D))/[ND表](#_邻居发现/ND__(FP1D))   * 新增接口信息显示 * 补充添加表项的去重判断逻辑 * ND表的状态类型更新为2种    [DNS](#_域名系统/DNS__(FP1D))   * 静态域名主机名新增特殊字符“-”支持    路由相关   * 去除路由转发配置，底层默认开启 * 补充默认路由的配置逻辑 * 静态路由补充等价路由的配置支持    [IGMP Snooping](#_IGMP_Snooping_(FP1C))   * 组播地址表补充“源IP地址”表项显示（仅IGMPv3支持，IGMPv2显示“--”）    [优先级映射](#_优先级映射/Priority_Mapping)   * 优化文案显示    [队列整形](#_队列整形/Queue_Shaping)   * CBS范围调整    [端口限速](#_端口限速/Rate_Limit)   * CBS范围调整    [PoE](#_PoE(FP1B))   * 调整不同供电模式时的自定义限制取值范围和默认值    [线缆检测](#_线缆检测/Copper_Test_(FP1C))   * ​根据芯片手册的支持，更新检测结果和误差范围    [日期和时间](#_基础设置/Basic_Settings)   * 默认设置修改为自动同步NTP服务器 * 新增型号GWN7806(P)，补充相关模块说明 * 概述：新增GWN7806(P)型号端口规格和属性说明 * 概览/系统信息：风扇状态补充新增型号支持 * 端口基本配置：速率补充新增型号支持 * 静态路由：补充新增型号上限支持 * PoE：新增型号支持 * 风扇： * 补充新增型号支持 * 新增型号风扇降温逻辑与控制机制【Undo】 | xhfang |
| 1.1.6 | 2023.01.19 | FP1D-3新增：   * 新增动态路由 * RIP * RIPng * OSPF * OSPFv3 * 新增GWN7821P/23P/32交换机型号，相关修改涉及如下： * 概述：新增GWN782X/3X型号端口规格和属性说明 * 概览： * 端口信息：补充2.5G速率的说明 * 系统信息：风扇状态补充新增型号支持 * 端口基本配置：速率补充新增型号支持 * 语音VLAN：补充L3交换机OUI上限 * 静态路由：补充新增型号上限支持 * 动态路由：补充新增型号支持 * QoS： * 端口优先级：补充新增型号支持 * 队列调度：补充新增型号支持 * PoE： * 新增型号支持 * GWN7813P/16P：新增PoE++功能【Undo】 * 线缆检测：补充GWN7832不支持的说明 * 风扇： * 补充新增型号支持 * 新增型号风扇降温逻辑与控制机制【Undo】 * 新增电源：补充GWN781X/2X/3X的电源说明 * [队列调度](#_队列调度/Queue_Scheduling)：SP-WRR和SP-WFQ，权重范围变更 * [VLAN IPv6接口](#_VLAN接口/VLAN_Interface(FP1D))：链路本地地址优化 * [RMON](#_RMON(FP1C))： * 告警组：上升&下降阈值补充说明 * 告警组：owner必填 * [IGMP](#_IGMP_Snooping_(FP1C))/[MLD Snooping](#_MLD_Snooping(FP1C))：查询器单独设置，并新增状态和IP地址 * [概览/端口信息](#_接口信息/Port_Info.)：新增端口“异常关闭/ErrDisable”状态，并用红色标识 * [域名系统](#_域名系统/DNS__(FP1D))： * IPv6暂不支持 * 域名后缀和静态域名主机名字符长度优化 | xhfang |
| 1.1.5 | 2022.12.09 | FP1D更新：   * DHCP Server&Relay * 去除保留地址 * DHCP Server：新增全局地址池 * IP地址冲突检测改用免费ARP，不再使用Ping探测 * 将IPv4和IPv6的DHCP Server&Relay分开各自配置，本期暂不考虑DHCPv6相关 * 安全MAC地址表 * 端口安全：新增地址类型，补充动态和Sticky类型的安全MAC地址 * MAC表：安全MAC地址表同步显示 * 新增SSH/Telnet Client功能【仅在CLI中开放】 * 新增SSH远程访问功能 | xhfang |
| 1.1.4 | 2022.11.24 | FP1D更新：   * [VLAN接口](#_VLAN接口/VLAN_Interface(FP1D))优化： * 与管理VLAN部分合并 * 拆分成IPv4接口和IPv6接口 * IPv4接口支持DHCP和手动配置 * IPv6接口支持手动配置、有状态DHCPv6和无状态DHCPv6 * ARP表： * 去除一键清空静态ARP表项功能 * 邻居发现： * 去除一键清空静态邻居表项功能 * 邻居表新增状态显示 * [EEE](#_节能以太网/EEE(FP1D))： * 去除全局开关 * 端口EEE列表去除运行状态、远程EEE功能支持状态 * [静态路由](#_静态路由/Static_Routing_(FP1D))： * IPv4默认路由支持编辑和删除，仅支持编辑下一跳地址 * IPv4/IPv6直连路由：根据VLAN接口进行呈现，个数对应匹配 * 风扇： * 补充10分钟检测中温度持续上升的逻辑 * ​[升级](#_升级/Upgrade)： * ​开放启动时检测固件升级功能 * ​[端口优先级](#_端口优先级/Port_Priority)： * ​L2+交换机同步L3实现，基于接口进行端口优先级配置 * 文案优化：信任模式里的CoS改为802.1p * 信任模式开放IP优先级，并新增重标记IP优先级，且重标记DSCP/IP优先级互斥 * CoS变更为接口全局配置 | xhfang |
| 1.1.3 | 2022.11.07 | FP1D-2更新：   * [EEE节能以太网](#_节能以太网/EEE(FP1D))：去除端口LED指示灯控制功能 * LLDP/端口设置：802.3 EEE TLV，因芯片不支持去除 * [风扇](#_风扇/Fan(FP1D))： * 去除风扇描述 * 补充故障状态的说明   优化FP1A/B/C：   * 系统位置+系统联系人： * [系统](#_系统时间/Time_Settings)：时间设置改为基础设置，增加系统位置和系统联系人配置 * [概览/系统信息](#_系统信息/System_Info.)：增加系统位置和系统联系人，支持编辑，跳转至系统/基础设置进行修改 * [端口基本配置](#_端口基本配置/Port_Basic_Settings(FP1B))：光口速率默认Auto * [STP](#_生成树/STP(FP1C))：端口增加自动边缘功能 * [端口镜像](#_13.2.5.1_端口镜像/Port_Mirroring(FP1B))：镜像组配置去除开关 | xhfang |
| 1.1.2 | 2022.11.03 | FP1D-2新增：   * 新增风扇 * 新增13.8.1 节能以太网 * STP/端口设置：边缘端口增加自动边缘属性 * QoS/队列调度：L2+&L3均更改为支持基于接口的队列调度，且5种方式均支持 * 新增重启计划 | xhfang |
| 1.1.1 | 2022.10.31 | FP1D-1更新：   * [VLAN接口](#_VLAN接口/VLAN_Interface(FP1D)) * 优化VLAN接口数量添加上限 * IPv4优化掩码输入规范 * IPv6整体优化 * 管理VLAN相关IP信息同步显示在列表中，但不可编辑和删除 * [DHCP](#_DHCP_(FP1D)) * DHCP Server和DHCP Relay暂不支持IPv6 * DHCPv4的Ping探测报文数和超时暂不支持 * 优化DHCP Server和DHCP Relay基于VLAN接口同时配置时，优先生效本地DHCP服务器 * [ARP](#_ARP表/ARP_Table_(FP1D)) * 优化ARP表项删除功能 * [ND](#_邻居发现/ND__(FP1D)) * 优化ND表项删除功能 * [静态路由](#_静态路由/Static_Routing_(FP1D)) * 补充静态路由的上限说明 * 优化直连路由的掩码获取 | xhfang |
| 1.1.0 | 2022.10.26 | FP1D-1：   * 新增6.7 GVRP * 新增7.1 VLAN接口 * 新增7.2 DHCP * 新增7.3 ARP表 * 新增7.4 ND * 新增7.5 DNS * 新增8.1静态路由 * 新增14.4时间策略   FP1A/B/C优化：   * 端口基本配置： * Jumbo Frame默认值改为9000 * L2光口的速率模式，增加Auto选项 * 入站过滤：Access、Trunk端口不支持配置 * 流量统计：补充Etherlike和RMON的统计信息 * 端口自动恢复：触发机制默认全不选 * STP： * 【BUG 237606】STP关闭时，BPDU处理默认泛洪 * 【BUG 235991】生成树信息显示优化 * 攻击防范：默认全部关闭 * 【BUG 235748】不再支持HTTP访问，默认使用HTTPS访问，需做如下变更： * AAA/登录认证：去除“HTTP” * 访问控制：去除“开启HTTPS访问”，此阶段端口配置仍不开放 * 日志：修改RAM和Console日志打印的等级设置 * 管理IP地址：IPv4地址默认DHCP，一旦接在DHCP服务器下，则需使用DHCP获取的IP地址进行登录 * LED指示灯：补充产线升级的LED指示灯需求说明 | xhfang |
| 1.0.10 | 2022.09.05-21 | 更新   * [端口基本配置](#_端口基本配置/Port_Basic_Settings(FP1B))：【BUG 234792】MTU改为巨型帧/Jumbo Frame * [MAC表](#_MAC表/MAC_Table(FP1B))：补充针对全零MAC地址不学习的说明 * [VLAN/端口设置](#_VLAN)： * 【BUG 232981】Access端口允许接收的帧类型默认为Untag Only * 【BUG 236650】入站过滤功能，聚合接口支持 * [生成树](#_生成树/STP(FP1C))：【BUG 235090】增加MST域配置，包括域名、修订级别 * [IGMP/MLD Snooping / 全局配置](#_IGMP_Snooping_(FP1C))：未知组播报文，默认泛洪 * [IP源防护](#_IP源防护/IP_Source_Guard(FP1B))：【BUG 234627】四元绑定表支持分页 * [PoE](#_PoE(FP1B))： * 端口设置/供电模式：默认自动 * 端口设置：供电模式为“强制”时，支持自定义限值 * RMON：【BUG 236155】告警组列表支持刷新 * LLDP&LLDP-MED * LLDP全局配置/TLV间隔：取值改为5-32767 * LLDP-MED端口设置：补充的Extended Power via MDI TLV（即为PoE-PSE TLV）去除 * LED指示灯 * 系统灯：   + 1秒闪烁1次，3色统一   + 启机时在绿灯亮之前有一个红灯不可控 * PoE黄色灯，不再混色 | xhfang |
| 1.0.9 | 2022.09.02 | 更新   * 名称编辑限制最大长度为64字符，修改点涉及 * 概览/系统信息：设备名称 * VLAN：VLAN描述 * OUI：上限改为所有L2型号交换机均支持32个 * MLD Snooping查询器版本更新为MLDv1和MLDv2，默认MLDv1 * [队列调度](#_队列调度/Queue_Scheduling)：L2暂仅支持SP和WRR 2种类型 * [队列整形](#_队列整形/Queue_Shaping)：去除聚合接口支持 * [端口限速](#_端口限速/Rate_Limit)：去除聚合接口支持 * [攻击防范](#_攻击防范/Anti_Attack(FP1B))：TCP Blat和UDP Blat默认关闭 * [PoE](#_PoE(FP1B)) * 供电标准补充说明 * 供电策略修改 * 补充端口供电优先级和功率限值受LLDP端口Power via MDI TLV和LLDP-MED端口PoE/PSE TLV的协商而影响的说明 * [LLDP&LLDP-MED](#_LLDP_&_LLDP-MED(FP1C)) * 补充全局LLDP关闭后报文处理的说明 * LLDP端口设置：802.3 IEEE TLV新增Power via MDI TLV，并补充PoE端口供电优先级和功率限值受此TLV影响的说明 * LLDP-MED端口设置：~~新增Extended Power via MDI TLV，并~~补充PoE端口供电优先级和功率限值受此TLV影响的说明 * ​[访问控制](#_访问控制/Access_Control)：SSH默认开启 | xhfang |
| 1.0.8 | 2022.08.22~25 | 更新   * [端口基本配置](#_端口基本配置/Port_Basic_Settings(FP1B)) * 双工模式：补充当速率为1000Mbps时，不支持半双工 * [链路聚合](#_链路聚合/Aggregation_Interface(FP1C)) * 【BUG 234181】链路聚合列表中，针对单个聚合组，支持一键重置聚合组配置 * [MAC表](#_MAC表/MAC_Table(FP1B)) * 动态MAC地址表项：去除端口配置功能，仅保留老化时间配置 * [端口安全](#_端口安全/Port_Security(FP1B)) * 端口配置中，最大MAC数，上限改为256 * [ACL](#_ACL(FP1B)) * IPv4 ACL中，协议类型选项更新 * IPv6 ACL中，ICMP消息类型选项更新 * [镜像](#_13.2.5.1_端口镜像/Port_Mirroring(FP1B)) * 镜像组中，针对单个镜像组，支持一键重置镜像组配置 * [LLDP](#_LLDP_&_LLDP-MED(FP1C)) * LLDP-MED​端口设置： * TLV选项增加PoE-PSE TLV * Location TLV的配置更新 * 设备信息：优化本地设备信息、本地端口信息和邻居信息的说明 * [系统时间](#_系统时间/Time_Settings)：补充NTP服务器默认地址ntp.pool.org * [管理IP地址](#_管理IP地址/Management_IP_Address) * IPv6开关去除 * IPv6地址类型变更为3种，分别为：无状态自动配置、DHCP自动获取和静态IPv6，默认无状态自动配置 * [访问控制](#_访问控制/Access_Control) * ​Web闲置超时时间：上限改为1440分钟 | xhfang |
| 1.0.7 | 2022.08 | 更新   * [产品规格](#_概述) * 根据新要求，GWN7802/03(P)型号，光口数量从原来的2个变更为4个 * [链路聚合](#_链路聚合/Aggregation_Interface(FP1C)) * ​L3的成员接口，若端口速率不一致，无法加入同一聚合组 * 聚合组里的成员接口，最多支持添加8个 * 聚合接口设置   + - 速率选项更新     - 双工配置去除，默认自协商，但列表里需显示实际双工状态 * [VLAN/端口设置](#_VLAN) * 入栈过滤功能说明修改 * [语音VLAN](#_语音VLAN/Voice_VLAN(FP1C)) * 全局设置：增加CoS重标记功能，去除DSCP * 端口设置：Access和Dot1q-tunnel类型端口仅支持手动模式 * OUI   + - 个数限制补充：7801最多16个，其余型号最多32个     - 补充GS的OUI，共3个，无法编辑和删除     - OUI地址与掩码显示优化 * [生成树](#_生成树/STP(FP1C)) * 全局默认开启，且模式为RTSP * IGMP/MLD Snooping * 路由器端口：增加禁用端口配置，且与静态端口互斥 * MLD Snooping/VLAN设置：增加MLD Snooping查询器及其版本设置 * [端口安全](#_端口安全/Port_Security(FP1B)) * 全局增加端口MAC地址学习速率设置 * 端口列表增加实际端口MAC学习等数据，包括实际学习的MAC地址数、安全MAC地址数、相应的保护次数 * [DAI](#_动态ARP检测/Dynamic_ARP_Inspection(DAI)) * 端口数据统计表支持刷新和清空指定端口数据 * [攻击防范](#_攻击防范/Anti_Attack(FP1B)) * ICMP Ping：分开配置IPv4和IPv6 * [RADIUS](#_RADIUS(FP1C)) * 为与其他GWN设备/Cloud兼容，最大重传次数与重传超时时间配置调整 * [PoE](#_PoE(FP1B)) * 端口设置：去除最大供电功率设置 * 端口列表：PD等级优化说明 * [日志](#_日志/Log) * 补充RAM/Flash/Console日志显示等级与保存等说明 * [镜像](#_13.2.5.1_端口镜像/Port_Mirroring(FP1B)) * 默认支持4个镜像组 * 镜像端口出方向和入方向分开配置 * 观察端口不能重复加入镜像组 * [线缆检测](#_线缆检测/Copper_Test_(FP1C)) * 光口不支持 * 未接线缆时，可能也会有3-4米的长度显示 * [SNMP](#_SNMP(FP1C)) * 补充远程引擎ID、视图、组、团体、用户、通知的添加上限 * 本地引擎ID支持一键重置，且引擎字符数必须为偶数 * 远程云清字符数必须为偶数个 * [RMON](#_RMON(FP1C)) * 补充历史组、事件组、告警组的添加上限 * 事件组和历史组ID自动生成，不支持添加编辑 * [LLDP&LLDP-MED](#_LLDP_&_LLDP-MED(FP1C)) * ​LLDP功能关闭后，支持设置LLDP报文处理方式 * LLDP-MED/端口设置：支持添加不同应用的网络策略，但每类应用有且仅能添加1个 * 数据统计支持刷新和清空指定端口数据 | xhfang |
| 1.0.6 | 2022.07.20~07.30 | 更新FP1C：   * [链路聚合](#_链路聚合/Aggregation_Interface(FP1C))： * 补充链路聚合接口基本配置说明 * 聚合接口和成员接口的配置优先级 * 负载分担方式选项确认，并进行补充说明 * [语音VLAN：端口设置去除聚合接口](#_语音VLAN/Voice_VLAN(FP1C)) * [STP：补充全局开关与BPDU处理的联动逻辑](#_生成树/STP(FP1C)) * [组播：](#_IGMP_Snooping_(FP1C)) * 补充未知组播报文处理方法[全局]   IGMP Snooping：   * 补充组播转发模式 * 补充路由器端口配置   MLD Snooping：   * 补充组播转发模式 * 补充路由器端口配置 * [802.1X：用户认证模式选项及说明更新](#_身份验证管理/802.1X(FP1C)) * [线缆检测：补充检测注意事项](#_线缆检测/Copper_Test_(FP1C)) * [SNMP：团体-组选项更新](#_SNMP(FP1C)) * [LLDP&LLDP-MED：MED端口设置Location TLV设置更新](#_LLDP_&_LLDP-MED(FP1C)) * [LED指示灯：更新电口和光口故障时的指示灯颜色](#_LED指示灯(FP1C))   FP1B新增：   * [端口自动恢复：补充端口error-down状态表](#_端口自动恢复/Port_Auto_Recovery(FP1B))   FP1B-2/3/4根据交互评审意见优化   * [优先级映射：补充IP优先级与队列的映射](#_优先级映射/Priority_Mapping) * [队列整形：CBS仅L3支持](#_队列整形/Queue_Shaping) * [端口限速：CBS仅L3支持](#_端口限速/Rate_Limit) * [风暴控制：3类报文阈值设置单独开关补充](#_风暴控制/Storm_Control(FP1B)) * [ACL：](#_ACL(FP1B)) * 规则编号取值更新 * 数据行为补充shutdown选项 * 链路层ACL规则内的VLAN输入限制优化 * [IP源防护：](#_IP源防护/IP_Source_Guard(FP1B)) * IPSG绑定表单独配置显示 * 最大规则数改为最大条目数 * 端口配置补充校验类型 * [PoE：根据新方案更新需求](#_PoE(FP1B)) * [日志：](#_日志/Log) * 日志服务器上限补充 * 去除批量删除日志服务器设置 * 支持日志导出 * [Ping：L3补充接口选择](#_Ping) * [Traceroute：L3补充接口选择](#_Traceroute) * [镜像：去除批量删除镜像配置](#_13.2.5.1_端口镜像/Port_Mirroring(FP1B)) * [备份与恢复：](#_备份与恢复/Backup_&_Restore(FP1B)) * 去除备份服务器 * 去除保存触发备份功能 * 备份时提供运行/保存2类配置文件的选择 * 补充备份文件覆盖逻辑 * 上传备份文件恢复逻辑优化 * [基础设置：](#_系统时间/Time_Settings) * 去除设备名称设置 * 更新TAB为系统时间 * 夏令时TBD | xhfang |
| 1.0.5 | 2022.07.18 | FP1C：   * 新增6.4链路聚合 * 新增6.6.2语音VLAN * 新增6.8生成树 * 新增9.3 IGMP Snooping * 新增9.4 MLD Snooping * 新增11.3端口隔离 * 新增11.6 DAI * 新增11.8 RADIUS * 新增11.9 TACACS+ * 新增11.10 AAA * 新增11.11身份验证管理-802.1X * 新增11.12 DHCP Snooping * 新增13.2.7 Copper Test * 新增13.4 SNMP * 新增13.5 RMON * 新增13.6 LLDP&LLDP-MED   FP1B-1根据交互评审意见优化   * 概览： * 系统信息：补充IPv6本地地址； * 接口信息：接口类型补充百兆和千兆之分；接口速率显示；补充故障端口类型；电口图示补充PoE供电；光口无PoE供电信息，补充Fiber信息显示 * 端口基本配置：流量控制新增自协商选项（光口不支持） * 流量统计：补充端口速率显示 * 端口自动恢复：去除开关 * MAC地址表：动态MAC地址端口设置去除，合入端口安全处配置 * VLAN： * 基于VLAN设置端口补充端口链路类型显示 * 基于接口划分VLAN补充PVID显示 * 端口设置的Ingress Filtering所有链路类型的端口均支持配置   FP1B需求更新   * 更新12 PoE | xhfang |
| 1.0.4 | 2022.06.22 | 根据二审意见更新FP1B：   * 概览/接口信息：更新接口名称显示 * 端口基本配置：   速率默认值修改；  光口仅支持全双工模式；  MTU二层为全局，三层为接口配置；  去除速率抑制；   * 流量监管改为流量统计 * 端口自动恢复：触发机制支持更多场景 * VLAN：   VLAN&端口配置，去除Excluded，调整TPID   * VLAN接口：去除默认网关，仅管理VLAN支持 * MAC表：补充端口安全MAC表项 * 风暴控制：接口补充光口 * ACL：   更改时间策略与ACL的关联为基于接口，应用ACL与生效的时间策略→改回规则上  所有规则未匹配则Deny   * QoS：   端口优先级：二层为全局，三层为基于接口   * 队列调度：补充二层的全局队列调度 * 端口镜像：最多支持4组 * 管理IP地址更新 * 调整框架，并补充剩余功能 | xhfang |
| 1.0.3 | 2022.06.16 | 更新FP1B：   * 概览：去除部分信息，补充日志信息 * 端口配置：光口和电口配置有差别，进行备注区分，主要涉及速率、双工模式和速率抑制 * 流量监管：接口统计时间间隔为web刷新的时间设置，非底层 * 端口镜像：更新观察口的配置 * VLAN：更新VLAN上接口的配置，提供2种方式，基于VLAN设置接口和基于接口划分VLAN * MAC表：查看竞品大部分针对黑名单性质的MAC表项统称黑洞MAC地址表，故不作变更 * PoE：去除MCU PoE软件版本，因更换芯片方案，可能后续有变更，TBD * 风暴控制：补充IFG支持 * 端口安全：独立安全MAC地址表配置 * ACL：去除ACL编号配置，按MAC、IP进行分类配置；ACL应用也采用基于接口进行MAC和IP的关联 * 一键恢复配置功能：仅保留优先级映射表里的重置，其余地方统一去除 * 防范攻击：补充POD配置 * 用户管理：去除user类型用户 * 登录与密码：去除md5方式的登录密码支持，登录失败重试系数与重认证时间间隔内置，不可用户自定义 * 新增Diagnostics部分功能，包括日志、Ping、Traceroute和光模块，但UDLD和Copper Test TBD * 新增备份与恢复功能 | xhfang |
| 1.0.2 | 2022.06.02 | FP1B：   * 新增 概览：接口信息、系统信息 * 新增 端口管理：基本配置、流量监管、端口镜像、端口自动恢复 * 新增 VLAN：VLAN、接口配置、VLAN接口（从原IP接口优化） * 新增 MAC表 * 新增 PoE * 新增 风暴控制 * 新增 端口安全 * 新增 ACL * 新增 QoS：端口优先级、优先级映射、队列调度、流量整形、端口限速 * 新增 IP源防护 * 新增 攻击防范 * 新增 用户管理 | xhfang |
| 1.0.1 | 2022.02.24~03.01 | * 3登录：去除随机验证码 * 去除设置向导 * 6.1.2系统信息：去除管理IP，增加设备码，PN和SN待定；系统资源状态移至概览 * 7.1VLAN IP接口：IP地址增加输入限制与报错提示；VLAN IP接口IP地址增加DHCP支持，DHCP IP支持release和renew * 8.1基础设置：更新设备名称输入支持 * 8.2.1管理IP地址：移至FP2实现 * 8.3升级：优化升级确认弹窗；去除启动时检查升级； * 8.4时间策略：优化策略名称 | xhfang |
| 1.0.0 | 2022.01.21～29 | Initial Draft | xhfang |
|  |  |  |  |

# 管理

## 支持管理的UI方式

GWN78XX系列交换机支持Console口、本地Web浏览器、GWN云端管理(包括Web平台(Cloud&Manager)和App)、TR-069四种方式：

1. 本文档会在后续章节（4章-15章）中详细描述对Web UI的需求；
2. GWN.Cloud的大致功能基本和本地的Web保持一致（具体以Cloud需求为准），FP1阶段先利用映射方式（与路由器保持一致，采用SSH反向隧道方式）访问本地Web端页面进行管理，后续FP1D阶段再移步至Cloud云端进行集中管理；APP端管理根据Cloud计划进行支持；
3. 私有云GWN Manager，支持二层和三层发现协议进行对交换机的接管。
4. Console口管理：通过串口线连接Console口与PC，利用三方软件如SecureCRT登录交换机，采用命令进行管理。
5. TR-069平台，利用三方CPE管理平台对交换机进行管理。

GWN78XX交换机还支持mDNS协议(FP1D)。用于第三方Discovery工具发现局域网内的交换机设备，需要携带如下信息：

* 交换机状态
* 交换机名称
* 交换机型号
* 设备MAC地址
* 设备IP地址
* 设备固件版本号
* 设备制造商

支持所有VLAN接口参与发现过程，默认按照管理VLAN>VLAN ID从小到大的优先级参与。

## 本地Web浏览器

本地Web登录：

* 利用管理IP地址，远程打开Web管理平台入口
* 使用已授权的用户名和密码进行登录

# 登录/Login

交换机登录支持多种方式：

1. 本地Web管理方式登录交换机
2. Console口登录交换机
3. Telnet方式登录交换机
4. SSH方式登录交换机

## 本地Web管理方式登录交换机

进入Web管理页面前需要登录。用户可以使用已授权的用户名和密码登录Web管理平台，登录后显示[概览]界面。

* 用户名
* 密码

注：1.必须验证用户名和密码的正确性，否则需要提示“用户名或密码错误，剩余X次机会”

2.登录时，若密码输入错误达到5次，则需要进行登录限制。限制时间为15分钟，并提示用户“已锁定，请15分钟后再试”。

3.不同用户的登录错误次数不合并，各用户单独处理。

Admin用户首次登录Web管理平台：

设备出厂时，默认启用HTTP服务，且有缺省的登录用户，用户名为admin，密码为随机密码（附在设备机身贴纸上）、管理IP地址（192.168.0.254，附在设备机身贴纸上）。用户可以利用这些信息进行首次登录。

在PC浏览器中输入http://管理IP地址（默认管理IP地址为192.168.0.254），即可进入设备Web登录界面。输入用户名admin、随机密码，单击<登录>按钮即可登录Web管理平台。

注：1.PC必须与设备处于同一网段，否则无法打开默认管理IP地址。

2.若交换机接在了DHCP服务器下，则需要以DHCP获取到的IP进行登录。

Admin初次登录，需：

1.要求修改密码，提高安全性，并进行二次确认。

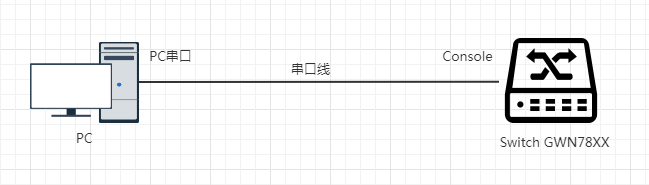
注：密码长度为8-32字符，输入内容不做限制

密码至少是数字、字母和特殊字符中的两者组合。

2.修改完初始密码后，进入本地Web。

## Console口登录交换机

使用串口线连接Console口与PC，如下图所示：



利用三方软件如SecureCRT登录到交换机，并使用授权的用户名与密码进行登录。

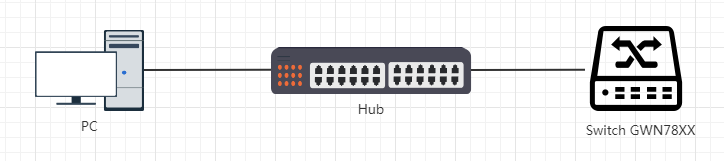
交换机提供的串口仅供日常版本上传、升级和维护使用。

## Telnet方式登录交换机

**前提：**

本地PC能Ping通交换机。并且，交换机需开启Telnet访问权限。

使用网线直接连接或者通过Hub连接，如下图所示：



利用三方软件如SecureCRT，使用Telnet方式连接交换机IP地址，登录到交换机，并使用授权的用户名与密码进行登录。

Telnet支持本地和远程用户登录，易于维护。

## SSH方式登录交换机

**前提：**

交换机需开启SSH访问权限。

利用三方软件如SecureCRT，使用SSH方式连接交换机IP地址和授权的用户名，登录到交换机，并使用对应的用户名与密码进行登录。

# 全局配置

全局配置主要有：搜索、语言、重启、登录用户(包括修改密码、退出登录)、生效与保存、固件版本提示。

## 搜索

支持搜索左侧导航栏、页面TAB、配置项名称。

## 语言

系统支持切换语言，暂仅支持中文、英文两种语言，缺省语言为English。

## 重启

支持重启交换机，需弹窗提示：

[若设备重启，所有未保存的配置信息都将丢失。确认重启？

<取消> <确定>]

## 登录用户

点击登录用户，支持修改密码、退出登录。

* + - 1. 修改密码

需要输入当前登录密码进行确认，校验通过后方可设置新密码。

新密码长度为8-32字符，输入内容不做限制，起码是数字、字母和特殊字符中的两者组合。

新密码需要二次确认，以确保密码无问题。

* + - 1. 退出登录

支持退出登录，返回登录页。

若有配置未保存就选择退出登录，需提示用户：

[退出后，若设备重启，所有未保存的配置信息都将丢失。确认退出？

<取消> <确定>]

## 生效与保存

配置页面下方提供<确定>按钮，点击后配置立即生效，供用户调试使用。

Web页全局提供<保存>按钮。当用户调试完成后，点击<保存>，可将所有配置写入保存。

点击<确定>后的配置，只要没有点击<保存>，可以通过设备重启的方式恢复至上一次保存的配置内容。（即没有保存，设备重启，配置信息会丢失）

注：可以在用户手动登出Web时，提示“退出后，若设备重启，所有未保存的配置信息都将丢失。确认退出？~~未保存本次配置信息，设备重启后会丢失~~”。

## 新固件升级提示(FP2)

~~前提：考虑官网服务器压力原因，不支持直接通过官网服务器下载升级，而且目前官网存放的是固件安装包的压缩包，无法直接下载升级。~~

设备需要支持检测GWN.Cloud上是否有新固件。

新增升级提示窗口。当检测到GWN.Cloud上有新固件时，以明显提示（如“NEW”字样或“小红点闪烁”等动效）告知用户有新固件可升级。可以显示可供升级的新固件版本号（仅显示GWN.Cloud上最新固件版本信息）。

支持一键跳转至[[*维护/升级*](#_升级/Upgrade)]页面。在此页面顶部提供当前版本号和新版本说明，需包括如下信息：

* 当前版本号
* 新固件版本号（仅显示GWN.Cloud上最新固件版本信息）
* 新固件在GWN.Cloud上的下载地址，打开以新页面形式直接下载最新固件~~的安装包（另一方式是直接定位到官网固件列表指定的产品，然后用户手动下载）~~，用户可通过自身需要上传固件或上传至自己搭建的固件服务器进行下载升级
* 新固件版本发布说明Release Note
* 新固件Release Note在官网的访问地址，打开以新页面形式直接显示官网Release Note PDF，方便用户查看新固件的功能更新点
* 支持一键升级，可通过提供的<一键升级>按钮，直接从GWN.Cloud上下载固件至设备本地进行更新升级

## 云连接状态(FP1D)

当且仅当交换机被Cloud/Manager接管时，在右上角显示“云”的图标，并显示连接状态{已连接|未连接}（可以考虑辅以不同的颜色表明连接状态），并支持快捷跳转至[*[维护/诊断/云连接状态检测]*](#_云连接状态检测_(FP1D))页面进行状态检测。

# 概览/Dashboard(FP1B)

### 接口信息/Port Info.

显示交换机接口信息，包括电口、光口和聚合接口。

建议以交换机实际接口图示形式显示所有接口：

1. 每个接口需要显示接口id，与实际对应；
2. 鼠标悬浮至每个接口，显示对应接口名称；
3. 需给出光口和电口的差异图示。
4. 需给出每个接口的状态图示，如已选中、LinkDown、Up、Shutdown、异常关闭/ErrDisable~~、故障~~；
5. 若电口开启PoE供电，还需在接口上加以PoE供电的显示；
6. 需给出一般接口和聚合接口的差异图示；
7. 需针对接口的速率做出区分，如≤百兆（＜100Mbps）使用浅绿色表示，千兆（1000Mbps）使用绿色表示，2.5G使用浅蓝色表示，万兆（10Gbps）使用蓝色表示；

**接口查看：**

选择某个接口（鼠标移至接口上显示接口id和速率）进行此接口的信息查看，具体包含如下信息：

**基本信息：**支持对接口进行配置，点击跳转至接口配置页面。

* 接口名称：默认显示接口id。
* 接口描述：根据实际设置显示接口的描述信息。
* 接口状态：显示接口状态，有
* Down：没有物理连线或线路故障
* Up：物理线路通畅
* Shutdown：接口被手动关闭
* ErrDisable：端口因发生异常如环路等自动关闭。此状态支持跳转至[*【端口自动恢复】*](#_端口自动恢复)进行设置
* ~~故障：接口发生故障~~
* 速率：显示接口实际速率，单位为Mbps。
* 双工模式：显示接口实际双工模式。
* MTU：显示接口实际最大传输单元。

**PoE供电**【仅PoE型号支持】**：**（仅电口）点击跳转至PoE/端口设置页面

* PoE供电状态：根据实际情况显示{Up|Down|Disable}
* 供电等级：根据实际PD设备受电情况显示
* 最大供电功率
* 当前供电功率
* 供电优先级

(FP2)供电功率控制图

以控制图形式显示端口最近24小时内的功率变化情况。记录时间间隔可选，有{10分钟 |30分钟 |1小时}，默认30分钟。

**Fiber信息：**（仅光口）点击跳转至诊断/光模块/指定光口详情页面

* 信号丢失
* 温度
* 输出功率(dBm)
* 输入功率(dBm)

**数据统计：**支持清空数据统计

* InOctets
* InUcastPkts
* InNUcastPkts
* InDiscards
* OutOctets
* OutUcastPkts
* OutNUcastPkts
* OutDiscards
* InMulticastPkts
* InBroadcastPkts
* OutMulticastPkts
* OutBroadcastPkts

**邻居信息：**显示端口直连的邻居信息(FP2)

* 主机名
* 设备标识：一般是设备MAC地址
* IP地址，包括IPv4地址和IPv6地址
* 制造商
* 当前速率，包括发送速率和接收速率，对应端口的接收速率和发送速率（单位需换算为Mbps）
* 当前流量：包括上传流量和下载流量，对应端口的接收流量和发送流量，涉及报文数和字节数（单位换算为MB）
* 连接时间：本次连上该端口的设备连接时间

一般情况下，一个邻居显示上述信息；若存在LLDP报文透传，则会出现一个端口下有多个邻居，此时显示邻居数量+第一个邻居信息，点击支持跳转至LLDP-邻居信息查看更多。

### 日志/Log

显示交换机日志信息。

将日志按照等级Emergency、Alert、Critical、Error、Warning、Notice、Information、Debug显示各自数量。每类日志支持查看详情，点击即跳转到[系统/调试/日志]，自动显示该等级下的所有日志。

### 系统信息/System Info.

系统信息主要显示系统基本信息、系统资源状态。

1. 系统基本信息

* 设备名称
* 系统位置
* 系统联系人

注：上述3项支持编辑，点击跳转至[*系统/基础设置*](#_基础_设置/Basic_Settings)进行修改。

* MAC地址
* 系统OID:1.3.6.1.4.1.42397
* 管理VLAN(FP2)和管理IP地址：管理IP地址显示包括IPv4的IP地址、IPv6的全球单播地址、链路本地地址
* 默认网关：显示包括IPv4默认网关、IPv6默认网关

注：默认网关显示实际生效值，与配置值(默认路由里配置的静态网关)、VLAN接口DHCP获取到的网关（采用网关优先级）的显示逻辑如下：网关使用优先级为：静态配置的网关>设置了优先级的网关(优先级从大到小)>VLAN接口上DHCP获取到的网关（VLAN ID从小到大，先到先得）。静态配置的网关网段与任一接口网段相同，则静态配置的网关生效，否则生效网关按照网关优先级配置进行选择，若优先级相同则以VLAN ID小的网关优先生效。

* PN序列号
* SN序列号
* 运行时长：以天/小时/分钟显示，不足1天的，天数不显示；小时同理
* 系统时间：当前系统时间，以年-月-日 时-分-秒表示
* 软件版本：随设备升级自动变更。当有新版本检测到时，进行提示“有新版本可升级”，并显示版本号，点击支持跳转至升级页面
* 硬件版本：固化在工厂分区中不可更改
* 引导程序

1. 系统资源状态

* CPU使用率【GWN7806(P)/16(P)/GWN7823P/32多核CPU显示平均值】

~~注：【GWN7806(P)/16(P)/GWN7823P/32】RTL9310平台为双核4个线程。需要显示总的CPU使用率，点击弹窗显示4个子CPU使用率。(FP2)~~

* 内存使用率

注：CPU使用率和内存使用率增加控制图以显示最近1分钟内的使用率变化情况，每5秒为一节点，显示此时间节点的时间（精确到秒）、CPU使用率和内存使用率。在控制图外显示当前系统时间的CPU使用率和内存使用率(FP2)

* 温度(FP1D)：不带风扇的设备温度（通过温传获取环温，作为设备温度）进行分段温度提示，正常温度时显示绿色，高温时使用红色，并进行高温告警；带风扇的设备，风扇高转速运行下温度仍然走高到临界点及以上的温度范围显示红色，并进行高温告警，此温度范围以下显示绿色，（具体温度详见下表）
* 风扇【L2仅GWN7802P/03P/06/06P型号支持，L3支持的型号有GWN7812P/13P/16/16P/32/31】(FP1D)：
* 风扇id
* 工作状态：正常Normal | 故障Failure | 停止Stop
* 风扇转速：可借助此判断是低转速、中转速(仅GWN7806P支持)还是高转速
* 【仅GWN7813(P)/32/31/23P】电源信息(FP1D)：
* 内置电源/RPS电源的使用状态：{未使用 | 故障 | 使用中 | 过压 | 欠压}
* 内置电源/RPS电源的LED指示灯状态

注：若RPS电源未接入则不显示其相关状态

* 【仅GWN7816(P)】电源信息(FP2):
* PSU1/2的使用状态：{未接入 | 使用中 | 故障}
* PSU1/2的LED指示灯状态
* PoE供电状态【仅PoE型号支持】：显示PoE供电状态，包括总消耗功率和剩余功率

GWN78XX交换机温度及高温告警温度临界点：

|  |  |  |
| --- | --- | --- |
| 型号 | 正常温度 | 高温及告警 |
| GWN7801/GWN7801P | ＜55℃ | ≥55℃ |
| GWN7802 | ＜55℃ | ≥55℃ |
| GWN7803 | ＜55℃ | ≥55℃ |
| GWN7802P | ＜76℃ | ≥76℃ |
| GWN7803P | ＜73℃ | ≥73℃ |
| GWN7806 |  |  |
| GWN7806P |  |  |
| GWN7811/GWN7811P |  |  |
| GWN7812P |  |  |
| GWN7813 |  |  |
| GWN7813P |  |  |
| GWN7832 |  |  |
| GWN7831 |  |  |
| GWN7830 |  |  |
| GWN7816 |  |  |
| GWN7816P |  |  |
|  |  |  |

# 以太网业务/Switching

## 端口基本配置/Port Basic Settings(FP1B)

接口配置模块主要用于配置接口，包括电口、光口和聚合接口。

支持端口组配置，支持批量端口快速配置。(FP2)

【配置参数】

* 接口：选择需要配置的交换机接口，包括电口、光口和聚合接口。支持多选（只能选择单一类型的接口）进行批量配置。

注：GWN780X/1X/2X/3X的端口，使用1/0/x表示。（x为端口序号）

端口编号命名规则：设备号/槽位号/端口号。对于单台没有运行堆叠的交换机，端口编号采用：1/槽位号/端口号（槽位号统一取值为0）。交换机加入堆叠后，接口编号采用：设备号/槽位号/端口号。槽位号与端口号的编号规则与单机状态下一致。

* 接口描述：【text文本框】用于配置此接口的信息描述，可以是使用用途描述等，最长128字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示
* 工作模式【仅GWN7831端口1/0/1-1/0/4】：【下拉框】虽然设备面板上有一个GE电口和一个GE光口，但设备内部只有一个转发接口，两者是光电复用关系，不能同时工作（一者使用时，另一者自动处于禁用状态）。根据实际设置接口的工作模式，有{自协商|电口模式|光口模式}，默认自协商。当选择“自协商”时，若电口和光口均有接入，则优先默认光口模式，若都没有接入则默认电口模式；接口的速率、双工和流控均采用默认值。
* 接口使能：【下拉框】设置是否使能接口，选项为{启用| 禁用}，默认启用。
* 定时启用(FP2)：【下拉框】当且仅当“接口使能”为“启用”时支持配置。选择接口启用的时间段，选项有{无|各个时间策略的名称|新增}，支持弹窗新建时间策略，具体配置详见[*系统→时间策略*](#_时间策略/Time_Policy)。默认无，即一直启用。
* 自动检测【仅93XX芯片平台的SFP+光口支持】：【开关】设置是否开启10G光口速率和DAC线的自动检测功能，默认开启，设备会自动根据接入的光模块和DAC线自适应速率和DAC线。此时，10G光口的速率和DAC线配置不可配置，只有关闭后才支持配置。
* 速率：【下拉框】设置接口的速率。当设置为Auto时，接口的速率由本接口和对端端口双方自动协商而定。
* 电口速率：GWN7800和GWN7810系列选项有{Auto| 10Mbps| 100Mbps| 1000Mbps}，默认Auto；GWN782X系列选项有{ Auto| 10Mbps| 100Mbps| 1000Mbps| 2.5Gbps}，默认Auto（其中2.5Gbps需要看是2.5电口还是1G电口，只有2.5G电口才有）；GWN7830/31选项有{Auto| 10Mbps| 100Mbps|1000Mbps}，默认Auto。
* 光口速率：GWN7800(除7806(P))系列选项有{Auto|100Mbps|1000Mbps}，默认Auto；GWN7806(P)/10/20/3X选项有{~~Auto|~~100Mbps|1000Mbps|10Gbps}，默认10Gbps（其中GWN783X需要看是1G SFP口还是10G SFP+口，只有10G SFP+口才有10Gbps选项）。注：10G光口不支持自协商。
* 聚合接口速率：GWN7800(除7806(P))系列聚合接口速率选项有{~~Auto|~~ 10Mbps| 100Mbps| 1000Mbps}，默认1000Mbps；GWN7806(P)/10/30/31系列聚合接口速率选项有{~~Auto|~~ 10Mbps| 100Mbps| 1000Mbps| 10Gbps}，默认1000Mbps；GWN7820系列聚合接口速率选项有{~~Auto|~~ 10Mbps| 100Mbps| 1000Mbps| 2.5Gbps| 10Gbps}，默认1000Mbps；GWN7832聚合接口速率选项有{~~100Mbps|1000Mbps|~~10Gbps}，默认10Gbps。注：10G光口不支持自协商。
* DAC线【仅93XX芯片平台的SFP+光口支持】：【下拉框】当且仅当SFP+光口速率设置为10Gbps时出现并支持配置。设置10G光口使用的DAC线使用，选项有{禁用| 0.5m| 1m| 3m| 5m}，默认禁用。
* 双工模式：【下拉框】设置接口的双工模式，电口选项有{自协商|全双工|半双工}，默认自协商。注：光口仅支持全双工模式；聚合接口仅支持自协商。
* 自协商：接口的双工状态由本接口和对端端口自协商而定。
* 全双工：支持接口收发数据包。
* 半双工：支持接口只能发送/接收数据包。注：当端口速率设置为2.5Gbps/1000Mbps时，半双工不支持

注：1. 聚合接口：GWN780X(除06(P))：自协商，GWN7806(P)/1X/2X/3X：自协商(加入10G口之后变成全双工)

2. 光口：GWN780X(除06(P))：全双工，GWN78(P)/1X/2X/3X：全双工

* 巨型帧/Jumbo Frame：【text文本框】设置接口的最大传输单元，取值范围为1518-10000，默认9216。

注：1.二层交换机，巨型帧作为全局设置；三层交换机，巨型帧每个端口支持单独配置。2.在计算报文长度时，不包括VLAN的4字节，暂仅针对GWN7801(P)/02(P)/03(P)。

* 流量控制：【单选】设置对接口进行流量控制，选项有{开启|关闭|自协商}，默认关闭。开启后，如果本地设备发生拥塞，将向对端设备发送消息，通知对端设备暂时停止发送报文；对端设备在接收到该消息后，将暂时停止向本地发送报文；反之亦然，从而避免报文丢失现象的发生。

注：光口不支持自协商模式。

当双工模式设置为“半双工”时，流量控制功能不生效。

接口列表：

* 列表显示接口名称、接口类型、接口描述、接口状态、速率（自动检测(实际速率) | 配置速率+DAC(实际速率)）、双工模式、MTU、流量控制开关状态。
* 支持编辑单个/批量/全部端口配置。

端口组配置：

添加端口组：至多添加32个

* 端口组ID：自动从1开始编号，至多32
* 描述：【text文本框】描述此端口组的用途等，最长128字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示
* 端口成员：【多选】显示交换机端口图，支持选择电口、光口和聚合口

端口组列表：

* 显示端口组ID、描述、端口成员信息
* 支持编辑
* 支持删除

端口组支持在多个模块使用，具体表现见下表：

|  |  |
| --- | --- |
| **模块** | **修改点** |
| 以太网业务 | |
| 端口基本设置 | 1.编辑增加端口组选择 |
| 环路检测 | 1.端口，编辑增加端口组选择 |
| 链路聚合 | 1.组，端口选择增加端口组  2.LCAP，编辑增加端口组选择 |
| ~~MAC地址表~~ | ~~1.静态MAC地址添加，端口选择增加端口组选择~~ |
| VLAN | 1.VLAN编辑，端口选择增加端口组选择  2.端口设置，编辑增加端口组选择  3.端口成员，编辑增加端口组选择  4.语音VLAN/OUI端口设置。编辑增加端口组选择 |
| 生成树 | 1.端口设置，编辑增加端口组选择  2.MST端口设置，编辑增加端口组选择  3.PVST端口设置，编辑增加端口组选择 |
| 组播业务 | |
| IGMP Snooping | 1.路由器端口，编辑端口增加端口组选择  2.组播地址，添加/编辑端口增加端口组选择  3.祖波端口，编辑增加端口组选择 |
| MLD Snooping | 1.路由器端口，编辑端口增加端口组选择  2.组播地址，添加/编辑端口增加端口组选择  3.祖波端口，编辑增加端口组选择 |
| PoE | |
| 接口设置 | 1.编辑增加端口组选择 |
| QoS | |
| 端口优先级 | 1.编辑增加端口组选择 |
| 队列调度 | 1.编辑增加端口组选择 |
| 队列整形 | 1.编辑增加端口组选择 |
| 端口限速 | 1.编辑增加端口组选择 |
| 安全业务 | |
| 风暴控制 | 1.端口，编辑增加端口组选择 |
| 端口安全 | 1.端口，编辑增加端口组选择  2.安全MAC地址，添加/编辑端口增加端口组选择 |
| 端口隔离 | 1.编辑增加端口组选择 |
| ACL | 1.绑定，编辑增加端口组选择 |
| IP源防护 | 1.端口防护，编辑增加端口组选择  2.四元绑定表，添加/编辑端口增加端口组选择 |
| IPv6源防护 | 1.端口防护，编辑增加端口组选择  2.四元绑定表，添加/编辑端口增加端口组选择 |
| DAI | 1.端口，编辑增加端口组选择 |
| 802.1X | 1.端口模式/端口，编辑增加端口组选择  2.端口，编辑增加端口组选择 |
| DHCP Snooping | 1.Option 82/Circuit ID，添加/编辑端口增加端口组选择  2.端口设置，编辑增加端口组选择 |
| DHCPv6 Snooping | 1.Option 18，添加/编辑端口增加端口组选择  2.端口设置，编辑增加端口组选择 |
| 维护 | |
| LLDP/LLDP-MED | 1.全局配置/端口设置，编辑增加端口组选择  2.LLDP MED端口设置，编辑增加端口组选择 |
| 节能管理 | 1.编辑增加端口组选择 |
| 系统 | |
| 1588v2 TC | 1.端口设置，编辑增加端口组选择 |

配置说明：

* 若存在端口组内端口之间配置无法一致，则底层报错处理或直接对部分端口做不生效处理，由开发视情况决定
* 一旦端口组配置生效，则端口处配置需同步更新

端口组的交互方式：

在列表左上角的<编辑>按钮后面增加端口和端口组选择，默认选择端口，则列表呈现所有端口，按当前实现使用；若选择某个端口组，则列表进行筛选，仅显示端口组内的端口，且默认勾选，支持批量编辑。

## 端口统计/Port Statistics(FP1B)

【功能概述】

支持接口的流量统计功能。通过流量监管，用户可以清晰查看到在指定时间间隔内，交换机各接口接收和发送的数据流量报文数。

【配置参数】

* 接口统计时间间隔 (秒)：【text文本框】设置接口统计数据流量信息的时间间隔，选项有{5s | 10s | 30s | 60s}，默认10s。设置后，Web页面将会每隔此时间间隔，刷新接口的数据流量信息。

流量统计表：

* 列表主要包含接口名称，各类统计信息如下：

注：不同芯片，端口统计信息有差异，建议直接以大文本框形式，从底层直接显示。

交互设计建议：建议主显示接收速率、接收的字节数、报文数、错误报文数，和发送速率、发送的字节数、报文数、错误报文数，详细的统计信息以“更多”的形式显示（包括但不限于下述信息）

（一）

* 速率：显示接口实际速率，包括接收和发送（单位：Mbps）
* InBytes：接收字节数
* InPkts：接收报文数
* InUnicastPkts：接收单播报文
* InMulticastPkets：接收组播报文
* InBroadcastPkts：接收广播报文
* InJumboPkts：接口接收的以太网帧长在1518字节到最大Jumbo帧长设定值之间且FCS正确的报文数目;对于其他设备，接口接收的VLAN帧长在1519字节到最大Jumbo帧长设定值之间且FCS正确的报文数目
* InDiscardPkts：接口在物理层检测时发现的丢弃报文数
* InPauseFrame：Pause帧。注：接口在未使能流量控制功能时不统计Pause帧统计
* InFrames：接口接收的802.3长度和实际数据长度不符的报文数
* InBandwidthUtil：输入带宽占用率
* InPeakRateAndTime：接口接收报文的最大速率和最大速率的发生时间
* In5MBitAndPktsRate：接口在前5分钟接收的比特速率和报文速率
* InTotalError：接口在物理层检测时发现的错误报文数
* InCrcError：大于63字节，小于1519字节且FCS错误的报文数
* InGiantsError：接口接收的超过Jumbo帧大小的报文数
* InRuntsError：接口接收的超小帧且CRC正确的报文数
* InFragmentsError：接口接收到的碎片报文数，碎片报文为接收长度小于64字节且CRC不正确的报文
* InAlignmentsError：接口接收的帧对齐错误的报文数
* InSymbolsError：接口接收的编码错误的报文数
* InIgnoredsError：接口接收的OpCode不是PAUSE的MAC控制帧的报文数
* OutBytes：发送字节数
* OutPkts：发送报文数
* OutUnicastPkts：发送单播报文数
* OutMulticastPkts：发送组播报文数
* OutBroadcastPkts：发送广播报文数
* OutJumboPkts：接口发出的VLAN帧长超过1517字节且FCS正确的报文数
* OutDiscardPkts：接口在物理层检测时发现的丢弃报文数
* OutPauseFrame：发送Pause帧的数目
* OutBandwidthUti：输出带宽占用率
* OutPeakRateAndTime：接口发送报文的最大速率和最大速率的发生时间
* Out5MbitAndPktsRate：接口在前5分钟发送的比特速率和报文速率

（二）Etherlike统计信息

* dot1dTpPortInDiscards
* dot3StatsFCSErrors
* dot3StatsSingleCollisionFrames
* dot3StatsMultipleCollisionFrames
* dot3StatsDeferredTransmissions
* dot3StatsLateCollisions
* dot3StatsExcessiveCollisions
* dot3StatsFrameTooLongs
* dot3StatsSymbolErrors
* dot3ControlInUnknownOpcodes
* dot3InPauseFrames

（三）RMON统计信息

* etherStatsDropEvents
* etherStatsOctets
* etherStatsPkts
* etherStatsBroadcastPkts
* etherStatsMulticastPkts
* etherStatsCRCAlignErrors
* etherStatsUnderSizePkts
* etherStatsOverSizePkts
* etherStatsFragments
* etherStatsjabbers
* etherStatsCollisions
* etherStatsPkts64Octets
* etherStatsPkts65to127Octets
* etherStatsPkts128to255Octets
* etherStatsPkts256to511Octets
* etherStatsPkts512to1023Octets
* etherStatsPkts1024to1518Octets

注：上述信息中，针对丢包Discards类数据统计，若有非0情况出现，建议做红色高亮提示，并伴随有syslog告警产生

（四）私有MIB统计信息(FP2)

* 根据各芯片支持，显示私有MIB的数据统计信息
* 支持清除单个/全部接口统计信息。

## 环路检测(FP2)

【功能概述】

环路检测技术（仅为单点环路检测技术）通过从接口周期性发送检测报文，检查该报文是否返回本设备（不要求收、发接口为同一接口），进而判断该接口、设备下挂网络或设备，或设备双接口间是否存在环路。在发现环路后，环路检测能向网管发送告警和记录日志，并能根据用户事先的配置对接口进行处理（默认shutdown接口），从而使接口处于受控状态，减小环路对本设备乃至整个网络的影响。

* 如果发现检测报文从发出去的接口接收到，则认为接口发生自环或该接口下挂的网络或设备中存在环路
* 如果发现检测报文被本设备上的其他接口接收到，则认为该接口所在的网络发生环路或设备发生自环

**检测报文：**环路检测技术通过周期性发送检测报文，并检测其是否返回本设备，以判断是否存在环路，这就要求：（1）当接口或网络发生环路，从该接口发送出去的检测报文必须能够回到本设备；（2）根据检测报文，系统能识别出是否本设备发送出去的检测报文，以及是本设备的哪个接口发送出去的检测报文。因此，环路检测技术发送的检测报文需要携带发送设备的MAC地址、发送报文的接口号，以便设备判断报文是否本设备发出以及从哪个接口发出；同时，还需要携带广播或组播类型的目的MAC地址，以保证接口或网络出现环路时，检测报文能够回送到本设备。支持同时发送Untagged和Tagged两种检测报文，则环路检测技术既可以基于VLAN进行检测，也可以基于接口进行检测。

**环路处理动作：**当系统检测到环路时，可以根据事先配置的处理动作对接口进行处理，使其处于某种受控状态，具体如下表所示：

|  |  |  |
| --- | --- | --- |
| 处理动作 | 描述 | 适用场景 |
| Trap | 只向网管发送Trap告警和记录日志 | 当用户仅需要告警环路，而不希望影响本接口流量的正常转发时。  该动作无法抑制网络风暴 |
| Block | 向网管发送Trap告警，同时阻塞接口，只允许BPDU报文通过 | 当用户需要接口在检测到环路后不允许数据报文通过，但又要保证某些BPDU协议报文（如LLDP等）的正常转发。  该动作可以抑制网络风暴 |
| Shutdown | 向网管发送Trap告警，同时关闭接口 | 当用户需要接口在检测到环路后彻底不参与任何计算或转发，以防止网络风暴。  该动作可抑制网络风暴 |
| No learing | 向网管发送Trap告警，同时禁止接口学习新MAC | 当用户需要接口在检测到环路后仍可以处理数据报文，但又要防止数据报文发送到错误的链路上。  该动作无法抑制网络风暴 |
| Quitvlan | 向网管发送Trap告警，同时将接口退出出现环路的VLAN | 当用户只希望解除VLAN内环路，不影响其他VLAN内的流量转发时。  该动作可抑制网络风暴 |

【暂仅支持Shutdown】

**受控接口自动恢复：**为及时在环路消失后将受控接口恢复到正常状态，环路检测技术支持环路状态自动恢复功能。系统在经过设置的恢复时间后会尝试在下一个恢复时间内恢复接口（详见6.4 端口自动恢复），若该恢复时间内没有收到受控接口发出的检测报文，则认为受控接口下的环路已经消除，将恢复该接口为正常状态。

注：更改受控接口的处理动作，该接口将自动恢复为正常状态，并根据更改后的配置重新进行环路检测及相应的处理。

【配置参数】

全局设置：

* 环路检测：【开关】设置是否再设备上开启环路检测功能，默认关闭。开启后，需设置检测报文的类型、环路检测时间间隔~~和端口恢复时间~~
* 检测报文类型：【text文本框】设置检测的报文协议号，16进制格式输入，取值范围为0x0000-0xFFFF（不区分大小写，系统会自动转为大写），默认0x8999

注：0x0000-0x05fff，0x0600-0x0601，0x0800-0x0806，0x0808，0x6559，0x8035，0x8037，0x809B，0x80D5，0x 80F3，0x8100，0x8137，0x 814C， 0x86DD， 0x880B， 0x 880C， 0x8847， 0x8848， 0x8863， 0x8864， 0x88BB， 0x88CC，0x8E88，0x9000，0x9100，0x9200这些不能输入，以底层返回报错形式提示

* 环路检测时间间隔 (秒)：【text文本框】设置环路检测发送检测报文的时间间隔，取值范围为1-1000，默认30秒
* ~~端口恢复时间 (秒)：【text文本框】设置当接口被Trap、Block、No learning或Quitvlan时的自动恢复时间，取值范围为1-1000，默认90秒。一般建议至少为环路检测时间间隔的3倍，若检测时间非常小，则建议在此基础上至少再增加10秒作为恢复时间~~

端口设置：

* 接口：选择交换机端口，包括电口、光口和聚合接口。可多选
* 环路检测：【开关】设置是否在接口上开启环路检测，默认关闭。开启后，一旦端口发生环路，则立即将该端口shutdown，自动恢复时间使用[*6.4端口自动恢复*](#_端口自动恢复/Port_Auto_Recovery(FP1B)_1)。

注：端口环路检测与STP环路保护的优先级为：STP环路保护>端口环路检测。

* ~~开启后，需选择接口在哪些VLAN下使能环路检测功能~~
* ~~VLAN：【单选，也可多选】从端口已加入的VLAN中选择需要进行环路检测的VLAN网络，默认PVID，可单选也可多选，至多8个~~
* ~~动作：【下拉框，单选】设置发生环路后，接口的处理动作，选项有{Trap |Block |Shutdown |No learning |Quitvlan}，默认shutdown~~

~~注：1.更改接口的处理动作，该接口将自动恢复为正常状态，并根据更改后的配置重新进行环路检测及相应的处理~~

~~2.Trap、Block、No learining和Quitvlan的端口自动恢复时间使用全局设置，Shutdown的端口。~~

端口列表：

* 显示端口、环路检测开关、~~检测VLAN、动作（~~状态~~）~~、恢复剩余时间
* 支持编辑单个/批量/全部端口配置
* 支持刷新

## 端口自动恢复/Port Auto Recovery(FP1B)

【功能概述】

当端口因MAC地址达到上限等原因被error down后，给予一种触发机制使端口重新使能正常工作，这就是端口自动恢复功能，down掉的接口经过延时时间后能够自动恢复。

【配置参数】

全局配置：

* 触发机制：【多选框】设置处于error disable状态的接口可以自动恢复为Up的触发功能，选项有[全部 | ARP报文检测 | STP BPDU保护 | DHCP速率超过限制 | DHCPv6速率超过限制(FP2)（搭配DHCPv6 Snooping增加） | 广播风暴控制 | 单播风暴控制 | 未知组播风暴控制 | UDLD | 端口自环(FP2) | BPDU环路(FP2) | ACL | 端口安全 ]\*，默认全不选。
* 延迟时间 (秒)：【text文本框】设置接口自动恢复为Up的延迟时间，取值范围为30-86400，默认30。

端口error-disable列表：

* 列表显示接口、errdisable原因（若未errdisable则显示--）、自动恢复的剩余时间。
* 支持手动强制恢复端口
* 列表支持刷新

## 链路聚合/Aggregation Interface(FP1C)

【功能概述】

以太网链路聚合，通过将多个物理接口捆绑为一个逻辑接口，可以在不进行硬件升级的条件下，达到增加链路带宽的目的。链路聚合技术主要有3个优势：（1）增加带宽；（2）提高可靠性；（3）负载分担。

**链路聚合组LAG**是指将若干条以太网链路捆绑在一起所形成的逻辑链路。每个聚合组唯一对应着一个逻辑接口，这个逻辑接口称之为链路聚合接口。链路聚合接口可以作为普通的以太网接口来使用，与普通以太网接口的差别在于：转发的时候链路聚合组需要从成员接口中选择一个或多个接口进行数据转发。

组成链路聚合接口的各个物理接口称为成员接口，成员接口对应的链路称为成员链路。

链路聚合组的成员接口存在活动接口和非活动接口两种。转发数据的接口称为活动接口，不转发数据的接口称为非活动接口。活动接口对应的链路称为活动链路，非活动接口对应的链路称为非活动链路。

**链路聚合模式：**根据是否启动链路聚合控制协议LACP，链路聚合分为手工模式和LACP模式。

（1）手工模式链路聚合

手工模式下，链路聚合的建立、成员接口的加入由手工配置，没有链路聚合控制协议LACP的参与。该模式下所有活动链路都参与数据的转发，平均分担流量。如果某条活动链路故障，链路聚合组自动在剩余的活动链路中平均分担流量。当需要在两个直连设备之间提供一个较大的链路带宽，而其中一端或两端设备都不支持LACP协议时，可以配置手工模式链路聚合。

（2）LACP模式链路聚合

聚合链路形成以后，LACP负责维护链路状态，在聚合条件发生变化时，自动调整链路聚合。

系统LACP优先级：为了区分两端设备优先级的高级而配置的参数。LACP模式下，两端设备所选择的活动接口必须一致，否则链路聚合组就无法建立。此时可以使其中一端具有更高的优先级，另一端根据高优先级的一端来选择活动接口即可。系统LACP优先级值越小优先级越高。

接口LACP优先级：为了区别同一个链路聚合组中的不同接口被选为活动接口的优先程度，优先级高的接口将优先被选为活动接口。接口LACP优先级值越小，优先级越高。

成员接口间M:N备份：LACP模式链路聚合由LACP确定聚合组中的活动和非活动链路，又称为M:N模式，即M条活动链路与N条备份链路的模式。这种模式提供了更高的链路可靠性，并且可以在M条链路中实现不同方式的负载均衡。

链路聚合模式比较见下表：

|  |  |  |
| --- | --- | --- |
| 维度 | 手工模式 | LACP模式 |
| 链路聚合组的建立方式 | 链路聚合组的建立、成员接口的加入由手工配置，没有链路聚合控制协议的参与 | 链路聚合组的建立基于LACP协议，LACP为交换数据的设备提供一种标准的协商方式，以供系统根据自身配置自动形成聚合链路并启动聚合链路收发数据。聚合链路形成以后，负责维护链路状态。在聚合条件发生变化时，自动调整或解散链路聚合。 |
| 设备是否需要支持LACP协议 | 不需要 | 需要 |
| 数据转发 | 正常情况下，所有链路都是活动链路。所有活动链路均参与数据转发。如果某条活动链路故障，链路聚合组自动在剩余的活动链路中分担流量 | 正常情况下，部分链路是活动链路。所有活动链路均参与数据转发。如果某条活动链路故障，链路聚合组自动在非活动链路中选择一条链路作为活动链路，参与数据转发的链路数目不变 |
| 是否支持跨设备的链路聚合 | 不支持 | 支持 |
| 检测故障 | 只能检测到同一聚合组内的成员链路有断路等有限故障，但是无法检测到链路断连、错连等故障 | 不仅能够检测到同一聚合组内的成员链路有断路等有限故障，还可以检测到链路故障、链路错连等故障 |

**链路聚合负载分担方式**

在使用链路聚合转发数据时，由于聚合组两端设备之间有多条物理链路，可能会产生同一数据流的第一个数据帧在一条物理链路上传输，而第二个数据帧在另外一条物理链路上传输的情况。这样一来同一数据流的第二个数据帧就有可能比第一个数据帧先到达对端设备，从而产生接收数据包乱序的情况。为了避免这种情况的发生，链路聚合组采用逐流负载分担的机制，把数据帧中的地址通过HASH算法生成HASH-KEY值，然后根据这个数值在链路聚合组转发表中寻找对应的出接口，不同的MAC或IP地址HASH得出的HASH-KEY值不同，从而出接口也就不同，这样既保证了同一数据流的帧在同一条物理链路转发，又实现了流量在聚合组内各物理链路上的负载分担。逐流负载分担能保证包的顺序，但不能保证带宽利用率。

用户可以根据流量模型设置不同的负载分担方式，流量中某个参数变化越频繁，选择对应负载分担方式的流量就越均衡。例如，在网络中，如果报文的IP地址变化较频繁，那么选择基于目的IP地址、源IP地址或源IP和目的IP地址的负载分担模式更有利于流量在各物理链路间合理的负载分担；如果报文的MAC地址变化较频繁，IP地址比较固定，那么选择基于目的MAC地址、源MAC地址或源MAC和目的MAC地址的负载分担模式更有利于流量在各物理链路间合理的负载分担。交换机可以基于报文的以下参数进行负载分担：（1）源MAC地址；（2）目的MAC地址；~~（3）源MAC和目的MAC地址；~~（4）源IP地址；（5）目的IP地址；~~（6）源IP和目的IP地址。~~

配置负载分担方式时，请注意：

（1）负载分担方式只在流量的出接口上生效，如果发现各入接口的流量不均衡，请修改上行出接口的负载分担方式；

（2）尽量将数据流通过负载分担在所有活动链路上传输，避免数据流尽在一条链路上传输，造成流量拥堵，影响业务正常运行。

【配置参数】

负载均衡分担方式：

* 负载均衡分担方式：【下拉框】选择合适的负载均衡方式，选项有{MAC地址|IP-MAC地址}，默认MAC地址。选择MAC地址，表示基于源或目的MAC地址进行数据报文负载分担；选择IP-MAC地址，表示基于源或目的IP地址-源或目的MAC地址进行数据报文负载分担。

创建链路聚合组：

* 链路聚合组：从LAG id中选择某个指定的链路聚合组。

注：83XX系列平台默认8个LAG，93XX系列平台根据根据端口数来限制，最大支持（端口数/2）个LAG。

* 名称：【text文本框】用于配置此链路聚合组的信息描述，可以是使用用途描述等，最长128字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示
* 类型：【下拉框】设置链路聚合组的类型，选项有{静态|LACP}，默认静态。静态时，LACP不使能；LACP时，LACP使能，自动调用开启全局LACP。
* 成员接口：【多选，最多8个】选择需要加入此链路聚合组的成员接口。

注：1.一个以太网接口只能加入一个链路聚合组，如果需要加入其它链路聚合组，必须先退出原来的链路聚合组。

2.当成员接口加入链路聚合组后，学习MAC地址或ARP地址按照链路聚合组来学习。

3.交换机的成员接口，若速率不一致，无法加入同一聚合组，需提示“端口速率不同，无法聚合”。

4.使能自动检测的10G SFP+口，无法加入聚合组，需报错提示。

5.已开启端口安全/镜像功能的端口，无法加入聚合组。

链路聚合组列表：

* 列表显示链路聚合组ID、名称、类型、链路状态、活动成员和非活动成员。
* 列表支持编辑
* 支持一键重置链路聚合配置

注：对于链路聚合接口的基本配置，需要前往[***端口基本配置***](#_端口基本配置/Port_Basic_Settings(FP1B))。

一旦物理接口加入聚合接口，其无法再配置，聚合接口的配置会优先于物理接口。

LACP：

* 系统优先级：【text文本框】设置LACP的系统优先级，取值范围为1-65535的整数，默认32768。

LACP端口设置：

* 端口：选择需要配置的交换机接口，包括电口和光口。支持多选进行批量配置。
* 端口优先级：【text文本框】设置端口的LACP协议优先级，取值范围为1-65535的整数，默认为1。端口的优先级取值越小，其LACP优先级越高。
* 超时：【下拉框】设置接收LACP报文超时时间，选项有{快|慢}，默认慢。快/short时，内定接收LACP协议报文的超时时间为3秒；慢/long时，内定接收LACP协议报文的超时时间是90秒。

LACP端口列表：

* 列表显示端口、端口优先级和超时。
* 支持编辑

## MAC表/MAC Table(FP1B)

【功能概述】

MAC地址表记录了交换机学习到的其他设备的MAC地址与接口的对应关系，以及接口所属VLAN等信息。设备在转发报文时，根据报文的目的MAC地址查询MAC地址表，如果MAC地址表中包含与报文目的MAC地址对应的表项，则直接通过该表项中的出接口转发该报文；如果MAC地址表中没有包含报文目的MAC地址对应的表项时，设备将采取广播方式在所属VLAN内除接收接口外的所有接口转发该报文。

MAC地址表中的表项分为：动态表项、静态表项和黑洞表项。不同MAC地址表的特点和作用：

|  |  |  |
| --- | --- | --- |
| MAC地址表类型 | 特点 | 作用 |
| 动态表项 | * 由接口通过报文中的源MAC地址学习获得，表项可老化 * 在系统重启后，动态表项会丢失 | * 通过查看动态MAC地址表项，可以判断两台相连设备之间是否有数据转发 * 通过查看指定动态MAC地址表项的个数，可以获取接口下通信的用户数 |
| 静态表项 | * 由用户手工配置，表项不可老化 * 在系统重启后，保存的表项不会丢失，只能手动删除 * 接口和MAC地址静态绑定后，其他接口收到源MAC是该MAC地址的报文将会被丢弃 * 一条静态MAC地址表项，只能绑定一个出接口 * 一个接口和MAC地址静态绑定后，不会影响该接口动态MAC地址表项的学习 * 静态MAC地址表项中指定的MAC地址，必须是单播MAC地址，不能是组播和广播MAC地址 * 静态MAC地址表项的优先级高于动态MAC地址表项，对静态MAC地址进行漂移时报文会被丢弃 * 已经存在的MAC地址类型是sticky等的MAC表项，不能将它配置为静态MAC地址表项 | 通过绑定静态MAC地址表项，可以保证合法用户的使用，防止其他用户使用该MAC进行攻击 |
| 黑洞表项 | * 由用户手工配合，表项不可老化 * 在系统重启后，保存的表项不会丢失 * 配置黑洞MAC地址后，源MAC地址或目的MAC地址是该MAC的报文将会被丢弃 | 通过配置黑洞MAC地址表项，可以过滤掉非法用户 |
| 端口安全表项 | * 由用户在端口安全里手动配置，表项不可老化 * 在系统重启后，保存的表项不会丢失 |  |

一般情况下，MAC地址表是根据设备收到的数据帧里的源MAC地址自动学习而建立的。如果MAC地址表中不存在该MAC地址表项，设备则将这个新MAC地址以及该MAC地址对应的接口和VLAN作为一个新的表项加入到MAC地址表中；如果MAC地址表中已经存在该MAC地址表项，设备将通过重置该表项的老化时间，对该表项进行更新。

动态MAC地址表项并非永远有效，每一条表项都有一个生存周期，到达生存周期仍得不到更新的表项将被删除，这个生存周期被称作老化时间。如果在达到生存周期前记录被更新，则该表项的老化时间将会重新计算。

由于MAC地址表的容量有限，当黑客伪造大量源MAC地址不同的报文发送到设备后，设备上的MAC地址表项资源可能会被耗尽。当MAC表被填满后，即使再收到正常的报文，也无法学习到报文中的源MAC地址，导致报文广播转发，浪费带宽资源。设备提供了2种方式对MAC地址学习进行控制：（1）基于接口关闭学习MAC能力；（2）基于接口限制MAC地址数。

注：默认非法的全零MAC地址不学习，直接将此类报文丢弃。

各型号设备MAC地址数量上限具体如下：

* GWN7801(P)/02(P)/03(P)：RTL8380系列平台，8K
* GWN7806(P)/16(P)/32/23P：RTL9310系列平台，32K
* GWN7811(P)/12P/13(P)/21P/31/30：RTL9300系列平台，16K

【配置参数】

**静态MAC地址表项**：

设备通过源MAC地址学习自动建立MAC地址表时，无法区分合法用户和非法用户的报文，带来了安全隐患。如果非法用户将攻击报文的源MAC地址伪装成合法用户的MAC地址，并从设备的其他接口进入，设备就会学习到错误的MAC地址表项，于是将本应转发给合法用户的报文转发给非法用户。为了提高安全性，网络管理员可手动在MAC地址表中加入特定MAC地址表项，将用户设备与接口绑定，从而防止非法用户骗取数据。

添加：

* MAC地址：设置待添加的静态MAC地址，必须是单播MAC地址，输入格式为HH:HH:HH:HH:HH:HH(其中，H为1-2位的十六进制数)，形如00:10:DC:28:A4:E9，不可设置为FFFF-FFFF-FFFF、组播地址和全零MAC地址，也不能为黑洞MAC地址。
* VLAN：【text文本框】设置静态MAC地址表项所属的VLAN，取值范围为1-4094
* 接口：【下拉框】设置MAC地址表项所属的接口，从交换机的接口（电口、光口和聚合接口）进行选择。

静态MAC地址表项列表：

* 列表显示MAC地址、VLAN、接口。
* 支持编辑静态MAC地址表项的所属VLAN和接口
* 支持删除单个静态MAC地址表项
* 支持清除静态MAC地址表项
* 列表支持分页显示

**黑洞MAC地址表项**：

为了防止黑客通过MAC地址攻击用户设备或网络，可将非信任用户的MAC地址配置为黑洞MAC地址，过滤掉非法MAC地址。当设备收到目的MAC或源MAC地址为黑洞MAC地址的报文，直接丢弃。

添加：

* MAC地址：设置待添加的黑洞MAC地址，输入格式为HH:HH:HH:HH:HH:HH(其中，H为1-2位的十六进制数)，例如00:10:DC:28:A4:E9，不可设置为FFFF-FFFF-FFFF、组播地址和全零MAC地址。
* VLAN：【text文本框】设置黑洞MAC地址表项所属的VLAN，取值范围为1-4094

黑洞MAC地址表项列表：

* 列表显示MAC地址、VLAN
* 支持编辑黑洞MAC地址所属的VLAN
* 支持删除单个黑洞MAC地址表项
* 支持清除黑洞MAC地址表项
* 列表支持分页显示

**动态MAC地址表项**：

默认情况下，设备的MAC地址学习功能都是开启的。在收到来自周边设备的数据帧时，会解析出数据帧的源MAC地址，然后与接收该数据帧的接口组合成一条MAC地址表项，添加到MAC地址表中。以后设备接收到去往该目的MAC地址的数据帧时，则直接查询MAC地址表就可以得到正确的发送接口，避免广播。若关闭MAC地址学习功能，设备在收到数据帧时将不会进行MAC地址的学习。另外之前学习到的动态表项不会立即删除，需要等待老化时间到达后老化删除，或手工执行删除MAC命令进行删除。

* ~~接口：选择进行MAC地址学习的交换机接口，包括电口、光口和聚合接口，可多选。~~
* ~~MAC地址学习功能：【开关】设置是否开启接口的MAC地址学习功能，默认开启。关闭后，需要指定接口所采取的的动作。~~
* ~~学习处理：【下拉框】当不开启接口的MAC学习，需要对接口采取一定的动作来对接收到的源MAC进行处理，选项有{丢弃|转发}，默认转发。~~
* ~~最大MAC地址学习数：【text文本框】设置接口上最多可以学习的MAC地址数量，取值范围为0-4096，0表示不限制MAC地址学习数量。默认为0。~~
* ~~报文处理：【下拉框】当MAC地址表项学习数量达到上限后，系统所采取的对源MAC地址报文的动作，选项有{丢弃|转发}，默认转发。~~
* ~~告警：【开关】当MAC地址学习数量达到上限后，是否发送告警消息。FP1暂不支持。~~

为了避免MAC地址表项爆炸式增长，需要合理配置动态MAC表项的老化时间，及时删除MAC地址表中的废弃MAC地址表项。老化时间越短，交换机对周边的网络变化越敏感，适合在网络拓扑变化比较频繁的环境；老化时间越长，交换机对周边的网络变化越不敏感，适合在网络拓扑比较稳定的环境。

* 老化时间 (秒)：【text文本框】设置动态MAC地址表项的老化时间，取值范围为0或60-1000000，默认300。设置为0，则表示不对动态MAC地址表项进行老化。

注：此为全局配置。

动态MAC地址表项列表：

* 列表显示VLAN、MAC地址、接口
* 支持清空动态MAC地址表项 [TBD]
* 支持刷新动态MAC地址表项
* 支持将指定的动态MAC地址表项添加为静态MAC地址表项
* 列表支持分页显示

**端口安全MAC地址表项：**（来源：端口安全）

* 列表显示地址类型、接口名称、VLAN、MAC地址
* 只读模式，不可编辑和删除

## VLAN(FP1B)

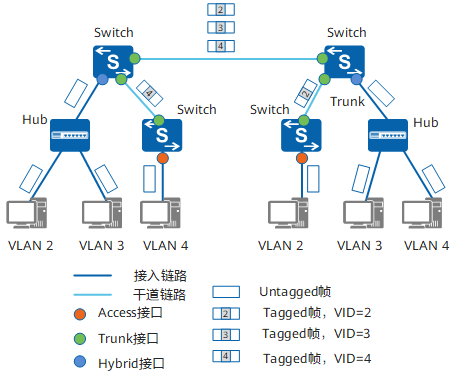
### VLAN

【功能概述】

交换机支持4094个VLAN。通过VLAN划分，可以将没有互通需求的主机进行二层隔离，限制广播域同时增强了网络的安全性。

基于接口的VLAN，按照设备接口来定义VLAN成员，将指定接口加入到指定VLAN中，处于同一VLAN的接口之间可以相互通信。一般情况下，基于端口划分VLAN适用于同一个交换机下。若是跨交换机，需要使用802.1Q VLAN。

**接口的链路类型**：交换机内部处理的数据帧一律都带有VLAN标签，而现网中交换机连接的设备有些只会收发Untagge帧，要与这些设备交互，就需要接口能够识别Untagged帧并在收发时给帧添加、剥除VLAN标签。同时，现网中属于同一个VLAN的用户可能会被连接在不同的交换机上，且跨越交换机的VLAN可能不止一个，如果需要用户间的互通，就需要交换机间的接口能够同时识别和发送多个VLAN的数据帧。根据接口连接对象以及对收发数据帧处理的不同，定义了4种接口链路类型：{Access | Trunk | Hybrid|QinQ}，以适应不同的连接和组网。



以太网链路包括接入链路（Access Link）和干道链路（Trunk Link）。接入链路用于连接交换机和用户终端（如用户主机、服务器、傻瓜交换机等），只可以承载1个VLAN的数据帧。干道链路用于交换机间互连或连接交换机与路由器，可以承载多个不同VLAN的数据帧。在接入链路上传输的帧都是Untagged帧，在干道链路上传输的数据帧必须都打上Tag。

* Access：接口发出去的报文不带Tag。一般用于和不能识别VLAN Tag的终端设备相连，或者不需要区分不同VLAN成员时使用。Access接口大部分情况只能收发Untagged帧，且只能为Untagged帧添加唯一VLAN的Tag。交换机内部只处理Tagged帧，所以Access接口需要给收到的数据帧添加VLAN Tag，也就必须配置缺省VLAN。配置缺省VLAN后，该Access接口也就加入了该VLAN。当Access接口收到带有Tag的帧，并且帧中VID与PVID相同时，Access接口也能接收并处理该帧。
* Trunk：接口发出去的报文，缺省VLAN内的报文不带Tag，其他VLAN内的报文都必须带Tag。一般用于连接交换机、路由器、AP以及可同时收发Tagged帧和Untagged帧的语音终端。它可以允许多个VLAN的帧带Tag通过，但只允许一个VLAN的帧从该类接口上发出时不带Tag（即剥除Tag）。
* Hybrid：接口发出去的报文可根据需要设置某些VLAN内的报文带Tag，某些VLAN内的报文不带Tag既可以用于连接不能识别Tag的用户终端和网络设备，也可以用于连接交换机、路由器以及可同时收发Tagged帧和Untagged帧的语音终端、AP。它可以允许多个VLAN的帧带Tag通过，且允许从该类接口发出的帧根据需要配置某些VLAN的帧带Tag（即不剥除Tag）、某些VLAN的帧不带Tag（即剥除Tag）。
* QinQ：QinQ接口也被称为Dot1q-tunnel接口。QinQ接口(802.1Q-in-802.1Q接口)使用QinQ协议，一般用于私网与公网之间的连接。它可以给帧加上双层Tag，即在原来Tag的基础上，给帧加上一个新的Tag，从而可以支持多大4094×4094个VLAN，满足网络对VLAN数量的需求。外层的Tag通常被称做公网Tag，用来标识公网的VLAN；内层Tag通常被称做私网Tag，用来标识私网的VLAN。

**缺省VLAN**：又称PVID(Port Default VLAN ID)。交换机处理的数据帧都带Tag，当交换机收到Untagged帧时，就需要给该帧添加Tag，添加什么Tag，由接口上的缺省VLAN决定。其具体作用是：

* 当接口接收数据帧时，如果接口收到一个Untagged帧，交换机会根据PVID给此数据帧添加等于PVID的Tag，然后再交给交换机内部处理；如果接口收到一个Tagged帧，交换机则不会再给该帧添加接口上PVID对应的Tag。
* 当接口发送数据帧时，如果发现此数据帧的Tag的VID值与PVID相同，则交换机会将Tag去掉，然后再从此接口发送出去，

每个接口都有一个缺省VLAN。缺省情况下，所有接口的缺省VLAN均为VLAN1，单用户可以根据需要进行配置：

* Access接口的缺省VLAN即为其允许通过的VLAN，修改接口允许通过的VLAN即可更改接口的缺省VLAN。
* Trunk和Hybrid接口可以允许多个VLAN通过，但是只能有一个缺省VLAN，修改接口允许通过的VLAN不会更改接口的缺省VLAN。
* 当删除某个VLAN时，如果该VLAN是某个接口的缺省VLAN，则对Access端口，缺省VLAN会恢复到VLAN1；对Trunk/Hybrid接口，缺省VLAN不会改变，即可以使用不存在的VLAN作为缺省VLAN。

**各类接口对数据帧的处理方式**：

|  |  |  |  |
| --- | --- | --- | --- |
| 接口类型 | 接收报文处理 | | 发送帧处理 |
| 报文不带Tag | 报文带Tag |
| Access | 接受该报文，并打上缺省的VLAN ID | * 当VLAN ID与缺省VLAN ID相同时，接收该报文 * 当VLAN ID与缺省VLAN ID不同时，丢弃该报文 | 先剥离帧的PVID Tag，然后再发送 |
| Trunk | 打上缺省的VLAN ID   * 当缺省VLAN ID在允许通过的VLAN ID列表里时，接收该报文 * 当缺省VLAN ID不在允许通过的VLAN ID列表里时，丢弃该报文 | * 当VLAN ID在接口允许通过的VLAN ID列表里时，接收该报文 * 当VLAN ID不在接口允许通过的VLAN ID列表里时，丢弃该报文 | * 当VLAN ID与缺省VLAN ID相同，且是该接口允许通过的VLAN ID时，去掉Tag，发送该报文 * 当VLAN ID与缺省VLAN ID不同，且是该接口允许通过的VLAN ID时，保持原有Tag，发送该报文 |
| Hybrid | 打上缺省的VLAN ID   * 当缺省VLAN ID在允许通过的VLAN ID列表里时，接收该报文 * 当缺省VLAN ID不在允许通过的VLAN ID列表里时，丢弃该报文 | * 当VLAN ID在接口允许通过的VLAN ID列表里时，接收该报文 * 当VLAN ID不在接口允许通过的VLAN ID列表里时，丢弃该报文 | 当VLAN ID是该接口允许通过的VLAN ID时，发送该报文。是否携带Tag由用户决定 |

【配置参数】

1. 创建VLAN：

* VLAN IDs：【text文本框】设置需要创建的VLAN ID，取值范围为2-4094。若只创建1个，则输入一个ID即可；若创建多个，则输入多个数字，以逗号分隔，形如创建5,6,7,8,11，可以输入“5-8,11”。
* VLAN描述：【text文本框】设置VLAN的描述，默认以VLANx(x为VLAN ID)表示，形如VLAN ID为2的描述为VLAN 2。允许输入64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示

VLAN列表：

* 列表显示VLAN ID、VLAN描述、Untag接口、Tagged接口。Untag接口和Tagged接口根据接口配置自动在VLAN列表里显示
* 列表默认有缺省VLAN1，VLAN描述为“default”，不可删除
* 支持对VLAN进行编辑，只允许修改VLAN描述
* 支持删除单个/批量/全部(除缺省VLAN1外)VLAN
* 列表支持分页显示

2. 接口配置：

支持对交换机接口（电口、光口、聚合接口）进行VLAN配置。既可以基于VLAN设置接口，也可以基于接口划分VLAN。

配置方式1：基于VLAN设置接口，即将接口加入到VLAN中，一般用于控制数据通信

* VLAN：在已创建的VLAN中选择某个VLAN
* 接口成员：显示所有交换机接口，包括电口、光口和聚合接口。选择接口进行配置其在VLAN中的功能，可多选。具体如下：
* 成员类型：【单选，可为空】设置接口在该VLAN下的配置，选项有{~~Excluded |~~ Tagged | Untagged}，在VLAN中默认无类型，即不在此VLAN中（仅在VLAN1中默认全为Untagged）。选择“Tagged”则表示该接口通过VLAN时需要打上Tag标记，选择“Untagged”则表示该接口将此VLAN ID设置为缺省VLAN，即PVID使用。根据接口链路类型，进行配置。
* 若接口为Access，则在一个VLAN中，只能选择Untagged，将该VLAN设为其PVID。
* 若接口为Trunk，则在一个VLAN中，可以将其打上Tag，即添加此VLAN为允许通过的VLAN，也可以将其设为Untagg，即设置此VLAN为其PVID。
* 若接口为Hybrid，则在一个VLAN中，可以将其打上Tag，即添加此VLAN为允许通过的VLAN，也可以将其设为Untagg，即设置此VLAN为其PVID。
* 若接口为Dot1q-tunnel(FP2)，则在一个VLAN中，只能选择Untagged，将该VLAN设为其PVID。

支持一键将接口全部设置为Untagged，也支持一键切换为Tagged，或者一键从VLAN中移除。

* ~~Forbidden：【勾选框】设置是否将接口设为Forbidden模式。~~

VLAN下的接口成员列表：

* 按照VLAN划分，显示每个VLAN下的所有接口名称、链路类型、成员类型
* 支持编辑接口成员和类型

配置方式2：基于接口划分VLAN，即根据接口用途选择指定的VLAN

* 接口：【单选】选择需要加入VLAN的交换机接口，包括电口、光口和聚合接口。
* 链路类型：显示接口的链路类型，不可配置。根据链路类型，进行接口成员属性和VLAN成员配置。
* 成员属性：【单选】设置接口在VLAN中的使用类型，选项有{~~Foridden|Excluded|~~Tagged|Untagged}，默认Tagged。Tagged表示该接口允许通过所选的VLAN，Untagged表示将设置所选VLAN为PVID。
* VLAN成员：【多选】显示所有已创建的VLAN，支持将VLAN加入到接口中。
* 若接口类型为Access：
* ~~可以设置成员属性为Forbidden，然后选择VLAN将其设为Forbidden VLAN。~~
* 可以设置成员属性为Untagged，将VLAN设为PVID。注：一个接口只能有一个PVID，重新选择的VLAN将会替换原来的Untagged VLAN。
* 若接口类型为Trunk：
* ~~可以设置成员属性为Forbidden，然后选择VLAN将其设为Forbidden VLAN。~~
* ~~可以设置成员属性为Tagged，然后选择VLAN（可单选也可多选）作为其允许通过的VLAN，将会打上Tag标记。~~
* Trunk允许通过的VLAN(FP2)：【text文本框】设置Trunk口可以通过的VLAN，不局限在已创建的VLAN中，可配置多个，默认1-4094。
* 可以设置成员属性为Untagged，然后选择VLAN（只能单选）设为PVID。注：一个接口只能有一个PVID，重新选择的VLAN将会替换原来的Untagged VLAN。
* 若接口为Hybrid：
* ~~可以设置成员属性为Forbidden，然后选择VLAN将其设为Forbidden VLAN。~~
* 可以设置成员属性为Tagged，然后选择VLAN（可单选也可多选）作为其允许通过的VLAN，将会打上Tag标记。
* 可以设置成员属性为Untagged，然后选择VLAN（只能单选）设为PVID。注：一个接口只能有一个PVID，重新选择的VLAN将会替换原来的Untagged VLAN。
* 若接口为Dot1q-tunnel(FP2)：
* ~~可以设置成员属性为Forbidden，然后选择VLAN将其设为Forbidden VLAN。~~
* 可以设置成员属性为Untagged，然后选择VLAN（只能单选）设为PVID。注：一个接口只能有一个PVID，重新选择的VLAN将会替换原来的Untagged VLAN。

接口成员列表：

* 显示接口名称、接口链路类型、Tagged VLAN、Trunk允许通过的VLAN、Untagged VLAN、PVID
* 支持编辑

3. 接口设置：

接口按照链路连接类型分类有4种，默认所有接口都是Trunk，默认PVID为1。

* 接口：选择需要配置的交换机接口（电口、光口和聚合接口），可多选。
* 链路类型：【下拉框】设置接口的链路类型，选项有{Access | Trunk | Hybrid | Dot1q-tunnel(FP2)}，默认Trunk。
* PVID：【text文本框】设置接口的PVID值，取值范围为1-4094的整数，默认为1。
* 允许接收的帧类型：【单选】选项有{All | Tag Only | Untag Olny}。根据接口链路类型，进行配置。
* 若接口为Access，则默认为All，不可配置。
* 若接口为Trunk，则默认为All，不可配置。
* 若接口为Hybrid，则默认为All，支持配置。
* 若接口为Dot1q-tunnel(FP2)，则默认为All，不可配置。
* 入站过滤/Ingress Filtering：【勾选框】Access和Trunk、Dot1q-tunnel类型的端口不支持此配置。设置是否开启接口的入站过滤功能，默认关闭。开启后，通过判断数据包所携带的vlan信息进行丢弃或转发的处理。
* TPID(FP2)：【下拉框】当且仅当链路类型为非QinQ时支持配置。配置Tag方式，选项有{0x8100 | 0x88a8 | 0x9100 | 0x9200}，默认0x8100。QinQ端口默认0x8100。
* VLAN交换(FP2)：【开关】当且仅当端口为物理端口（电口和光口）且链路类型为“Trunk”或“Hybrid”时支持配置。设置是否开启端口入方向（即接收数据报文时）的VLAN交换功能，默认关闭。开启后，需要配置接口映射VLAN，支持配置多组，由于规格与其他模块共享，故前端不做限制，由底层返回报错提示。
* \*外层VLAN：设置端口接收时的匹配报文外层VLAN，允许输入多个，至多32个（底层报错）~~，所有输入的VLAN必须是端口已加入的VLAN~~。
* 内层VLAN：设置端口接收时的匹配报文内层VLAN，允许输入多个，至多32个（底层报错）~~，所有输入的VLAN必须是端口已加入的VLAN~~。
* \*映射后的外层VLAN：设置端口接收时的报文转发后映射的外层VLAN，只能输入一个，且必须是端口已加入的VLAN。
* 映射后的内层VLAN：设置端口接收时的报文转发后映射的内层VLAN，只能输入一个，且必须是端口已加入的VLAN。

注：1.838X芯片仅支持1 to 1和N to 1，不支持2 to 2 VLAN映射，故不支持内层VLAN映射。

2.内外层VLAN有且仅有一组支持N to 1，即外层VLAN和内层VLAN至多只允许一个支持输入多个VLAN；多组之间也适用，即一个端口上配置多组时，内外层VLAN有且仅有一组支持N to 1。（相关报错由底层直接返回）

* 入方向：【开关】设置是否VLAN映射仅针对入方向生效，默认关闭，即端口默认接收会进行VLAN映射，反方向发送会进行VLAN逆映射。
* MAC VLAN功能：【开关】当且仅当链路类型为“Hybrid”时，支持配置。默认关闭
* 协议VLAN功能：【开关】当且仅当链路类型为“Hybrid”时，支持配置。默认关闭，开启后需要进行如下配置：为端口选择协议模板，并指定VLAN ID，至多8个协议模板全部配置
* 协议模板：【下拉框】选择协议索引，需要显示对应配置的协议类型值（只读）
* VLAN：【单选】设置端口上允许通过的指定协议模板划分的VLAN，取值范围为1-4094的整数
* 802.1p：【text文本框】设置协议在对应VLAN的802.1p优先级，用于当交换机阻塞时，优先发送优先级高的数据包。取值范围为0-7的整数，默认0
* IP子网VLAN功能(FP3)：【开关】当且仅当链路类型为“Hybrid”时，支持配置。默认关闭

接口列表：

* 列表显示接口名称、链路类型、PVID、允许接收的帧类型、Ingress Filtering开关状态、TPID、VLAN交换开关状态、MAC VLAN开关状态、协议VLAN（若关闭显示“禁用”，若开启则显示添加的协议模板数，点击可弹窗查看详细的协议模板与VLAN映射关系）、IP子网开关状态~~Tagged VLAN、Untagged VLAN、Tag方式~~
* 支持编辑单个/批量~~/全部~~接口
* ~~支持一键恢复接口的配置至初始状态~~

### MAC VLAN (FP2)

【需求来源】邮件《Bases para proyecto GWN76xx y GWN78xx en El Salvador》

【功能概述】

VLAN划分有多种方式，除了上述的基于接口以外，还有基于MAC地址、子网、网络层协议、匹配策略方式来划分。不同方式的比较如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| 划分方式 | 原理 | 优缺点 | 适用场景 |
| 基于接口 | 根据交换机的接口来划分VLAN。  网络管理员预先给交换机的每个接口配置不同的PVID，当一个数据帧进入交换机时，如果没有带VLAN标签，该数据帧就会被打上接口指定PVID的tag。然后数据帧将在指定PVID中传输 | 优点：定义成员简单  缺点：成员移动需重新配置VLAN | 适用于任何大小但位置比较固定的网络 |
| 基于MAC地址 | 根据数据帧的源MAC地址来划分VLAN。  网络管理员预先配置MAC地址和VLAN ID映射关系表，当交换机收到的是Untagged帧时，就依据该表给数据帧添加指定VLAN的Tag。然后数据帧将在指定VLAN中传输 | 优点：当用户的物理位置发生改变，不需要重新配置VLAN，提高了用户的安全性和接入的灵活性  缺点：需要预先定义网络中所有的成员 | 适用于位置经常移动但网卡不经常更换的小型网络，如移动PC |
| 基于子网【暂不支持】 | 根据数据帧中的源IP地址和子网掩码来划分VLAN。  网络管理员预先配置IP地址和VLAN ID的映射关系，当交换机收到的是Untagged帧，就依据该表给数据帧添加指定VLAN的Tag。然后数据帧将在指定VLAN中传输 | 优点：   * 当用户的物理位置发生改变，不需要重新配置VLAN * 可以减少网络通信量，可使广播域跨越多个交换机   缺点：网络中的用户分布需要有规律，且多个用户在同一个网段 | 适用于对安全需求不高、对移动性和简易管理需求较高的场景中。比如，一台PC配置多个IP分别访问不同网段的服务器，以及PC切换IP地址后要求VLAN自动切换等场景 |
| 基于协议 | 根据数据帧所属的协议（族）类型及封装格式来划分VLAN  网络管理员预先配置以太网帧中的协议域和VLAN ID的映射关系表，如果收到的是Untagged帧，就依据该表给数据帧添加指定VLAN的Tag。然后数据帧将在指定VLAN中传输 | 优点：将网络中提供的服务类型与VLAN相绑定，方便管理和维护  缺点：   * 需要对网络中所有的协议类型和VLAN ID的映射关系表进行初始配置 * 需要分析各种协议的格式并进行相应的切换，消耗交换机较多的资源，速度上稍具劣势 | 适用于需要同时运行多协议的网络 |
| 基于匹配策略（MAC地址、IP地址、接口）【暂不支持】 | 根据配置的策略划分VLAN，能实现多种组合的划分方式，包括接口、MAC地址、IP地址等  网络管理员预先配置策略，如果收到的是Untagged帧，且匹配配置的策略时，给数据帧添加指定的VLAN的Tag。然后数据帧将在指定VLAN中传输 | 优点：   * 安全性高，VLAN划分后，用户不能改变IP地址或MAC地址 * 网络管理人员可根据自己的管理模式或需求选择划分方式   缺点：针对每一条策略都需要手工配置 | 适用于需求比较复杂的环境 |

**VLAN划分方式的匹配优先级：**如果入方向Untagged帧同时匹配多种划分VLAN的方式，则优先级顺序从高到低依次为：基于匹配策略划分VLAN【暂不支持】 > 灵活QinQ【暂不支持】 或 基于MAC地址划分VLAN 或 基于子网划分VLAN > 基于协议划分VLAN > 基于接口划分VLAN（包含基本QinQ）。

其中，如果报文同时匹配了基于MAC地址划分VLAN和基于子网划分VLAN。缺省情况下，优先基于MAC地址划分VLAN，用户自己根据自己需求进行设置修改。基于接口划分VLAN的优先级虽然最低，但却是最常用的VLAN划分方式。

**MAC-Based VLAN** (FP2)

基于MAC地址划分VLAN不需要关注终端用户的物理位置，提高了终端用户的安全性和接入的灵活性。

基于MAC地址划分的VLAN只处理Untagged报文，对于Tagged报文处理方式和基于接口的VLAN一致。当接口收到的报文为Untagged报文时，接口会以报文的源MAC地址为根据去匹配MAC-VLAN映射表。如果匹配成功，则给报文添加表项中指定的VLAN ID并转发该报文；如果没有匹配到，则按其它匹配原则继续匹配；如果均匹配失败，则给报文添加端口的缺省VLAN ID并进行转发。

为了实现PC从任意交换机接入时，都会被划分到指定的VLAN，可以通过两种方式进行配置：

* 手动设置静态MAC VLAN
* 动态MAC VLAN：通过认证服务器来自动配置，即802.1X VLAN下发功能【暂不支持】。当802.1X用户通过认证后，交换机根据认证服务器提供的信息，动态创建MAC地址和VLAN的映射关系。用户下线时，自动删除该对应关系。该方式需要在认证服务器上配置MAC地址和VLAN的映射关系，具体需要结合802.1X功能。

基于MAC的VLAN划分功能仅在Hybrid端口上生效。且配置的MAC-VLAN映射表，MAC地址必须为单播地址，VLAN必须已存在。

【配置参数】

添加MAC-VLAN映射：至多添加128个映射关系

* MAC地址：【MAC格式的输入框】添加与所选VLAN关联的MAC地址，只能是单播MAC地址，不能设置全零、全F和组播地址
* 掩码长度：【text文本框】设置MAC地址掩码长度，取值范围是9-48的整数，默认48
* VLAN：【单选】从已添加的VLAN中选择
* 802.1p：【text文本框】设置MAC对应VLAN的802.1p优先级，用于当交换机阻塞时，优先发送优先级高的数据包。取值范围为0-7的整数，默认0

注：添加的每组MAC/掩码需做去重处理，包含相同与包含关系。

MAC-VLAN映射表：

* 显示MAC、掩码长度、VLAN、802.1p
* 支持编辑
* 支持删除单个/批量/全部
* ~~VLAN：【单选】从已添加的VLAN中选择~~
* ~~MAC组：每个VLAN支持添加多组MAC，包括MAC地址、掩码和802.1p优先级~~
* ~~MAC地址：【MAC格式的输入框】添加与所选VLAN关联的MAC地址，只能是单播MAC地址，不能设置全零、全F和组播地址~~
* ~~掩码长度：【text文本框】设置MAC地址掩码长度，取值范围是9-48的整数，默认48~~

~~注：需对每组MAC地址和掩码长度进行重复校验。当存在相同的MAC地址，但掩码长度不同时，以掩码长度最长的为准。完全相同则做去重处理。~~

* ~~802.1p：【text文本框】设置每组MAC对应VLAN的802.1p优先级，用于当交换机阻塞时，优先发送优先级高的数据包。取值范围为0-7的整数，默认0~~

~~MAC-VLAN映射表：~~

* ~~列表显示VLAN、添加的MAC组数~~

~~注：MAC-VLAN的映射数量，至多1024个，由ingress VLAN、MAC VLAN和Subnet VLAN共享，故当添加上限时，使用底层错误码上报返回即可~~

* ~~支持查看每个VLAN里的MAC信息，支持编辑和删除~~
* ~~支持编辑，以VLAN为索引~~
* ~~支持删除单个/批量/全部MAC-VLAN映射关系~~

端口设置：复用现有6.6.1 VLAN里的端口设置

### Protocol VLAN (FP2)

【需求来源】邮件《Bases para proyecto GWN76xx y GWN78xx en El Salvador》

【功能概述】

基于子网划分VLAN和基于协议划分统称为基于网络层划分VLAN，可减少手工配置VLAN的工作量，也可保证用户自由地增加、移动和修改。

协议VLAN技术是基于报文协议类型的VLAN分类技术，其可以将某一协议类型的空VLAN ID报文都划分到同一个VLAN。即交换机可以根据端口接收到的报文所属的协议（族）类型以及封装格式，将收到的不携带VLAN标记的报文，与用户设定的协议模板相匹配，匹配成功的自动分发到相应的VLAN中传输。

“协议类型+封装格式”称为协议模板，一个协议VLAN下可以绑定多个协议模板，不同的协议模板再用协议索引（protocol-index）来区分。所以，一个协议模板可以用“协议vlan-id + protocol-index”来唯一标识，然后通过配置将“协议vlan-id + protocol-index”和端口绑定。

基于协议的VLAN只处理Untagged报文，对于Tagged报文处理方式和基于接口的VLAN一致。当设备接口接收到Untagged帧时，设备先识别帧的协议模板，并去进行匹配协议VLAN。如果匹配成功，则给报文打上该协议VLAN的Tag；反之，给报文打上接口PVID的Tag。

基于协议的VLAN划分功能仅在Hybrid端口上生效。其将网络中提供的服务类型与VLAN相绑定，方便管理和维护。

【配置参数】

添加协议模板：受芯片限制，至多添加8个

* 协议索引：默认按照0-7的顺序依次显示
* 帧类型：【下拉框】设置划分VLAN报文的协议帧类型，选项有{Ethernet II | LLC | SNAP}，默认Ethernet II。
* 协议类型值：【text文本框】设置匹配Ethernet II封装格式的协议类型值，取值范围是0x600-0xfffe

协议模板列表：

* 列表显示协议索引、帧类型、协议类型值
* 支持编辑，以协议索引为索引
* 支持删除单个/批量/全部协议模板。若被端口绑定，则无法删除

~~添加协议VLAN：~~

* ~~VLAN：【单选】从已添加的VLAN中选择~~
* ~~协议模板：一个协议模板具有协议索引、协议帧类型、协议类型值、802.1p优先级。每个VLAN支持添加多个协议模板，至多8个~~
* ~~协议索引：默认按照0-7的顺序依次显示~~
* ~~帧类型：【下拉框】设置划分VLAN报文的协议帧类型，选项有{Ethernet II | LLC | SNAP}，默认Ethernet II。~~
* ~~协议类型值：【text文本框】设置匹配Ethernet II封装格式的协议类型值，取值范围是0x600-0xffff~~
* ~~802.1p：【text文本框】设置协议在对应VLAN的802.1p优先级，用于当交换机阻塞时，优先发送优先级高的数据包。取值范围为0-7的整数，默认0~~

~~协议VLAN列表：~~

* ~~列表显示VLAN、协议模板个数~~
* ~~支持查看每个VLAN里的协议模板信息，支持编辑和删除~~
* ~~支持编辑，以VLAN为索引~~
* ~~支持删除单个/批量/全部协议VLAN~~

端口设置：复用现有6.6.1 VLAN里的端口设置

### Subnet VLAN (FP3) 【待评审】

【需求来源】邮件《Bases para proyecto GWN76xx y GWN78xx en El Salvador》

【功能概述】

基于IP子网的VLAN是根据报文源IP地址及子网掩码来进行划分的。

基于IP子网的VLAN只处理Untagged报文，对于Tagged报文处理方式和基于接口的VLAN一样。当设备端口接收到Untagged报文后，会根据报文的源地址来确定报文所属的VLAN，然后将报文自动划分到指定VLAN中传输。

其主要用于将指定网段或IP地址发出的报文在指定的VLAN中传输。通过配置ACL和QoS策略实现。

基于IP子网的VLAN划分功能仅在Hybrid端口上生效。

【配置参数】

添加IP子网-VLAN映射：受芯片限制，至多添加12个

* IP地址：【text文本框】设置基于IP子网划分VLAN依据的源IP地址或网络地址，IPv4地址格式
* 掩码：【text文本框】设置IP子网的掩码，可以输入掩码长度，取值范围为0-32的整数，也可以输入IPv4地址格式的掩码
* VLAN【单选】从已添加的VLAN中选择
* 优先级：【text文本框】设置IP子网对应VLAN的优先级，用于当交换机阻塞时，优先发送优先级高的数据包。取值范围为0-7的整数，默认0

注：添加的每组IP子网/掩码需做去重处理，包含相同与包含关系。

IP子网-VLAN映射表：

* 显示IP地址/掩码长度、VLAN、优先级
* 支持编辑
* 支持删除单个/批量/全部

### 语音VLAN/Voice VLAN(FP1C)

【功能概述】

语音VLAN是为用户的语音数据流专门划分的VLAN。由于丢包和时延对通话质量的影响很大，用户对语音的质量比数据或者视频的质量更为敏感，因为在带宽有限的情况下就需要优先保证通话质量。通过配置语音VLAN，交换机可识别语音流，将语音流加入到Voice VLAN中传输，并对其进行有针对性的QoS保障，当网络发生拥塞时可以优先保证语音流的传输。

若要提高语音数据流的传输优先级，首先要能识别出语音数据流。识别出语音数据流后，再对语音数据流提升优先级后传输。Voice VLAN可以通过以下两种方式来实现对语音数据流的识别：

（1）通过收到报文的源MAC地址，即基于MAC地址的方式（手动模式）

设备可以根据进入接口的数据报文中的源MAC地址字段来判断该数据流是否为语音数据流。源MAC地址匹配系统设置的语音设备的组织唯一标识符OUI的报文被认为是语音数据流。用户需要预先设置OUI，适用于IP电话上送untagged语音报文的场景。

（2）通过报文携带的VLAN Tag，即基于VLAN的方式（自动模式）

若有大量IP电话接入交换机，配置IP电话的OUI会非常繁琐，可在交换机上配置基于VLAN来提升语音报文的优先级，此时设备会根据进入接口的报文的VLAN ID来判断该数据报文是否为语音报文。当VLAN ID匹配系统配置的Voice VLAN后，则认为是语音数据流。这种方式实现的前提是IP电话支持获取交换机上配置的Voice VLAN信息的功能，在大量IP电话接入的情况下，可以简化配置。

以上两种方案主要区别在于：当IP电话上送的是untagged语音报文时，必须配置OUI，才能把语音报文和数据报文区分开来；如果IP电话上送的是带Tag语音报文，则可配置基于VLAN的Voice VLAN，这样在大量IP电话接入的情况下，就不用配置繁琐的OUI，简化配置。

【配置参数】

* 语音VLAN模式：【单选】选择开启语音VLAN功能模式，选项有{关闭| 自动加入语音VLAN(FP2)| Tagged OUI模式| Untagged OUI模式}，默认关闭。
* 语音VLAN ID：【下拉框】从VLAN列表中选择一个VLAN作为语音VLAN。

注：缺省VLAN 1不能作为语音VLAN。

* CoS/802.1p：【text文本框】指定CoS/802.1p优先级，取值范围为0-7的整数，默认为6。值越大优先级越高。
* DSCP：【text文本框】当且仅当语音VLAN模式选择“自动语音VLAN”时支持配置，取值范围为0-63的整数，默认46。
* CoS重标记：【开关】当且仅当语音VLAN模式选择“Tagged OUI/Untagged OUI”时支持配置。设置是否将报文重定向，默认关闭。
* 老化时间 (分钟)：【text文本框】当且仅当语音VLAN模式选择“Tagged OUI/Untagged OUI”时支持配置。设置语音VLAN的老化时间，取值范围为30-65536的整数，默认为1440分钟。

注：老化时间只对OUI/自动模式下的端口有效。在自动模式下，系统会根据收到的语音报文的源MAC地址来决定是否把该报文的入端口加入语音VLAN。在将入端口加入语音VLAN后，系统会同时启动老化定时器。经过老化时间后，如果设备没有收到任何来自该入端口的语音报文，系统会自动把该端口从语音VLAN中删除。

OUI端口设置：当且仅当全局语音VLAN模式选择“Tagged OUI模式/Untagged OUI模式”时出现并支持配置。

* 端口：选择需要配置的交换机接口，包括电口、光口~~和聚合接口~~。支持多选进行批量配置。

注：1. Access和Dot1q-tunnel端口仅支持手动模式。Untagged OUI模式仅支持Hybrid端口。

2.语音VLAN和接口的缺省VLAN不能相同。

3.一个接口只能有一个VLAN被设置为语音VLAN。

* 状态： 【开关】设置是否开启端口的OUI语音VLAN功能，默认关闭。
* 模式：【下拉框】设置端口上语音VLAN的工作模式，选项有{手动|自动}，默认手动。设置为“手动”时，必须手工将端口加入到语音VLAN中，需要使用到LLDP功能；设置为“自动”时，会将报文中源MAC地址匹配到OUI的接口自动加入到语音VLAN中。

端口列表：

* 列表显示端口、状态和模式。
* 支持编辑

OUI：

* \*OUI地址：【text文本框】设置语音报文的MAC地址。输入格式为HH:HH:HH:HH:HH:HH(其中，H为1-2位的十六进制数)，不可设置为全零、组播地址和广播MAC地址。默认HH:HH:HH:00:00:00，后8位固定不可修改。
* 掩码：【text文本框】输入格式为HH:HH:HH:HH:HH:HH(其中，H为1-2位的十六进制数，且换算为二进制后只能以连续1开头，连续0结尾)。默认FF:FF:FF:00:00:00，后8位固定不可修改
* 描述：【text文本框】设置OUI的描述，最长64字符，

OUI列表：

OUI上限规定：L2/L3交换机最多32个

* 列表显示OUI地址、掩码和描述
* 默认显示如下表的OUI

|  |  |  |
| --- | --- | --- |
| OUI地址 | 掩码 | 描述 |
| 00:0B:82:00:00:00  C0:74:AD:00:00:00  EC:74:D7:00:00:00 | FF:FF:FF:00:00:00 | Grandstream |
| 00:03:6B:00:00:00 | FF:FF:FF:00:00:00 | Cisco |
| 00:01:E3:00:00:00 | FF:FF:FF:00:00:00 | Siemens |
| 00:06:B9:00:00:00 | FF:FF:FF:00:00:00 | NEC/Philips |
| 00:09:6E:00:00:00 | FF:FF:FF:00:00:00 | Avaya |

* 支持编辑
* 支持删除单个/批量和全部OUI(除却Grandstream OUI)

## QinQ (FP2)

【需求来源】邮件《5k GWN780x Brazil opportunity》

【功能概述】

QinQ（802.1Q-in-802.1Q）技术是一项扩展VLAN空间的技术，通过在802.1Q标签报文的基础上再增加一层802.1Q的Tag来达到扩展VLAN空间的功能，可以使私网LAN透传公网。在公网传输过程中，设备只根据外层VLAN Tag转发报文，并根据报文的外层VLAN Tag进行MAC地址学习，而用户的私网VLAN Tag将被当做报文的数据部分进行传输。

* 内层VLAN Tag：用户的私网VLAN Tag，Customer VLAN Tag（简称CVLAN）。设备依靠该Tag在私网中传送报文。
* 外层VLAN Tag：运营商分配给用户的公网VLAN Tag，Service VLAN Tag（简称SVLAN）。设备依靠该Tag在公网上传送QinQ报文。

**QinQ概念：**

（1）基本QinQ：基于端口方式实现。当端口配置了基本QinQ后，不论从该端口收到报文是否携带VLAN Tag，设备都会为该报文打上本端口缺省VLAN的Tag。如果收到的是带有VLAN Tag的报文，该报文就成为带双Tag的报文；反之，该报文就成为带有本端口缺省VLAN Tag的报文。

（2）灵活QinQ【暂不支持】：基于端口和VLAN相结合的方式实现，即端口对接收的报文，可以通过单层VLAN Tag转发，也可以通过双层VLAN Tag转发。它是对QinQ的一种更灵活的实现，又叫VLAN Stacking或QinQ Stacking。除了能实现所有基于QinQ的功能外，对于同一个接口接收的报文还可以根据不同的VLAN做不同的动作，可以实现：

* 基于VLAN ID的灵活QinQ，为具有不同内网VLAN ID的报文添加不同的外层VLAN Tag
* 基于802.1p优先级的灵活QinQ，根据报文的原有内层VLAN的802.1p优先级添加不同的外层VLAN Tag
* 基于流策略的灵活QinQ，根据QoS策略可以在添加外层VLAN Tag的同时对内层用户VLAN ID进行修改

二者之间的差别主要是：基本QinQ对进入二层QinQ接口的所有帧都加上相同的外层Tag；灵活QinQ对进入二层QinQ接口的帧，可以根据不同的内层Tag加上不同的外层Tag，对于用户VLAN的划分更加细致。

（3）QinQ Mapping：发生在报文从入接口接收进来之后，从出接口转发出去之前。接口在向外发送本地VLAN的帧时，将帧中的VLAN Tag替换成外部VLAN的VLAN Tag；在接收外部VLAN的帧时，将帧中的VLAN Tag替换成本地VLAN的VLAN Tag。一般部署在ME边缘设备上，对用户侧上送的报文进行映射操作，将用户报文携带的Tag映射用户指定的Tag后再接入公网。目前支持如下两种映射方式：

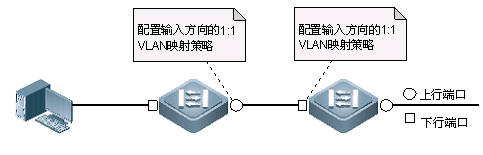
* 1 to 1的映射方式：当接口收到带有一层Tag的报文时，将报文中携带的一层Tag映射为用户指定的一层Tag
* 2 to 1的映射方式：当接口收到带有两层Tag的报文后，将报文中携带的外层Tag映射为用户指定的一层Tag，内层VLAN不变

（3）VLAN Mapping：也称为VLAN映射，主要功能是将用户报文中的私网VLAN Tag替换为公网的VLAN Tag，使其按照公网的网络规划进行传输。在报文被发送回用户私网时，再按照同样的规则将VLAN Tag恢复为原有的用户私网VLAN Tag，使报文正确到达目的地。VLAN Mapping支持以下两种映射关系：

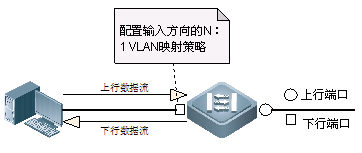
* 1 to 1 VLAN Mapping：将报文Tag的VID修改为另一个指定的Tag的VID，用不同的VLAN承载不同用户的相同业务，以区分不同用户
* 实现方式1：对于上行数据流，通过在下行端口上配置输入方向的VLAN映射策略，将原来的VLAN Tag映射为新的VLAN Tag；对于下行数据流，通过在下行端口上配置输出方向的VLAN映射策略，将报文的VLAN Tag映射到原来的VLAN Tag



* 实现方式2：对于上行数据流，通过在下行端口上配置输入方向的VLAN映射策略，将原来的VLAN Tag映射为新的VLAN Tag；对于下行数据流，通过在上行端口上配置输入方向的VLAN映射策略，将报文的VLAN Tag映射到原来的VLAN Tag



* N to 1 VLAN Mapping：将来自多个VLAN的报文Tag的VID修改为同一个Tag的VID，用一个VLAN承载原本由多个VLAN承载的不同用户的相同业务，以节约VLAN资源。其实现方式如下：
* 对于上行数据流，通过在下行端口上配置输入方向的VLAN映射策略，将原来的VLAN Tag映射为新的VLAN Tag；对于下行数据流的映射，当前不支持



**QinQ的封装方式：**

（1）基于接口的QinQ封装：进入一个接口的所有流量全部封装一个相同的外层VLAN Tag，封装方式不够灵活，用户业务区分不够细致，也称为QinQ二层隧道。

（2）基于流的QinQ封装：可以对接入接口的数据首先进行流分类，然后对于不同的数据流选择是否封装外层Tag、封装何种外层Tag，也称为二层灵活QinQ。

（2）在路由子接口上进行QinQ封装

**VLAN Tag的TPID值可调功能：**

标签协议表示TPID（Tag Protocol Identifier）是VLAN Tag中的一个字段，表示VLAN Tag的协议类型，IEEE 802.1Q协议规定该字段的取值为0x8100。

设备可以根据TPID值来识别报文中是否携带对应的VLAN Tag：当端口收到报文时，根据配置的TPID值与报文中相应的字段进行比较，如果二者一致，则表示报文中携带相应的VLAN Tag。另外，不同厂商的设备可能将QinQ报文外层VLAN Tag的TPID字段设为不同的值。为了和这些设备兼容，用户可以自行配置该TPID的值，使发送到公网中的QinQ报文携带的TPID值与其他厂商相同，就可以实现与其他厂商的设备互通。

由于TPID字段在以太网报文中所处位置与不带VLAN Tag的报文中协议类型字段所处位置相同，为避免网络中报文转发和接收造成混乱，不允许用户将TPID值设置为下述常用协议类型值：0x0806（ARP）、0x0200（PUP）、0x8035（RARP）、0x0800（IP）、0x86DD（IPv6）、0x8863/0x8864（PPPoE）、0x8847/0x8848（MPLS）、0x8137（IPX/SPX）、0x8000（IS-IS）、0x8809（LACP）、0x888E（802.1X）、0x88A7（集群）、0xFFFD/0xFFFE/0xFFFF（设备保留）。

【配置参数】

详见6.6.1 VLAN

## VLAN交换 (FP2)

【需求来源】邮件《5k GWN780x Brazil opportunity》

【功能概述】

VLAN Mapping通过修改报文携带的VLAN Tag来实现不同VLAN的相互映射。

**基本原理：**

交换机收到数据报文后，根据是否携带Tag做以下两种处理：

* 数据报文带Tag：根据配置的VLAN Mapping方式，决定替换单层、双层或双层中的外层Tag；然后进入MAC地址学习阶段，根据源MAC地址+映射后的VLAN ID刷新MAC地址表项；根据目的MAC+映射后VLAN ID查找MAC地址表项，如果没有找到，则在VLAN ID对应的VLAN内广播，否则从表项对应的接口转发。
* 数据报文不带Tag：根据配置的VLAN划分方式决定是否添加VLAN Tag，对于不能加入VLAN的数据报文上送CPU或丢弃，否则添加Tag；然后进入MAC地址学习阶段，按照二层转发流程进行转发。

**映射方式：**

设备支持基于VLAN和MQC方式实现VLAN Mapping，其中基于VLAN的VLAN Mapping包括以下映射方式：

* 1 to 1的映射方式：当部署VLAN Mapping功能设备上的接口收到带有单层VLAN Tag的报文时，将报文中携带的单层VLAN Tag映射为公网的VLAN Tag，包括1:1和N:1两种方式，其中1:1的方式是将指定的一个用户侧VLAN Tag标签，N:1的方式是将指定范围的多个用户侧VLAN Tag标签映射到一个网络侧VLAN Tag标签。
* 2 to 1的映射方式：当部署VLAN Mapping功能设备上的接口收到带有双层VLAN Tag的报文时，将报文中携带的外层VLAN Tag映射为公网的VLAN Tag，内层VLAN Tag作为数据透传。也包括1:1和N:1两种方式，其中1:1的方式是指将一个外层VLAN Tag映射到一个公网的VLAN Tag，内层VLAN Tag不变。N:1的方式是指通过多次配置命令将多个外层VLAN Tag映射到一个公网的VLAN Tag，内层VLAN Tag不变。
* 2 to 2的映射方式：当部署VLAN Mapping功能设备上的接口收到带有双层VLAN Tag的报文时，将报文中携带的双层VLAN Tag映射为公网的双层VLAN Tag。

基于MQC实现VLAN Mapping指的是通过MQC可以对分类后的报文实现VLAN Mapping。用户可以根据多种匹配规则对报文进行流分类，然后将流分类与VLAN Mapping的动作相关联，对匹配规则的报文重标记报文的VLAN ID值。基于MQC的VLAN Mapping能够针对业务类型提供差别服务。

【配置参数】

详见6.6.1 VLAN

838X芯片仅支持1 to 1和2 to 1，不支持2 to 2，93XX芯片3种均支持。

838X芯片的聚合组不支持VLAN交换。

## GVRP (FP3)

【功能概述】

GARP协议主要用于建立一种属性传递扩散的机制，以保证协议实体能够注册和注销该属性。GARP作为一个属性注册协议的载体，可以用来传播属性。将GARP协议报文的内容映射成不同的属性即可支持不同上层协议应用。

GVRP是GARP的一种应用，用于注册和注销VLAN。

GARP协议通过目的MAC地址区分不同的应用。

GVRP基于GARP机制，主要用于维护设备动态VLAN属性。通过GVRP协议，一台设备上的VLAN信息会迅速传播到整个交换网。GVRP实现动态分发、注册和传播VLAN属性，从而达到减少网络管理员的手工配置量及保证VLAN配置正确的目的。

应用实体：在设备上，每一个参与协议的端口可以视为一个应用实体。当GVRP在设备上启动的时候，每个启动GVRP的端口对应一个GVRP应用实体。

VLAN的注册和注销：GVRP协议可以实现VLAN属性的自动注册和注销。

* VLAN的注册：指将端口加入VLAN。
* VLAN的注销：指将端口退出VLAN。

GVRP协议通过声明和回收声明实现VLAN属性的注册和注销。

* 当端口接收到一个VLAN属性声明时，该端口将注册该声明中包含的VLAN信息（端口加入VLAN）。
* 当端口接收到一个VLAN属性的回收声明时，该端口将注销该声明中包含的VLAN信息（端口退出VLAN）。

消息类型：GARP应用实体之间的信息交换借助于消息的传递来完成，主要有三类消息起作用，分别为Join消息、Leave消息和LeaveAll消息。

* Join消息：当一个GARP应用实体希望其它设备注册自己的属性信息时，它将对外发送Join消息；当收到其它实体的Join消息或本设备静态配置了某些属性，需要其它GARP应用实体进行注册时，它也会向外发送Join消息。Join消息分为JoinEmpty和JoinIn两种，区别如下：
* JoinEmpty：声明一个本身没有注册的属性。
* JoinIn：声明一个本身已经注册的属性。
* Leave消息：当一个GARP应用实体希望其它设备注销自己的属性信息时，它将对外发送Leave消息；当收到其它实体的Leave消息注销某些属性或静态注销了某些属性后，它也会向外发送Leave消息。Leave消息分为LeaveEmpty和LeaveIn两种，区别如下：
* LeaveEmpty：注销一个本身没有注册的属性。
* LeaveIn：注销一个本身已经注册的属性。
* LeaveAll消息：每个应用实体启动后，将同时启动LeaveAll定时器，当该定时器超时后应用实体将对外发送LeaveAll消息。LeaveAll消息用来注销所有的属性，以使其它应用实体重新注册本实体上所有的属性信息，以此来周期性地清除网络中的垃圾属性。

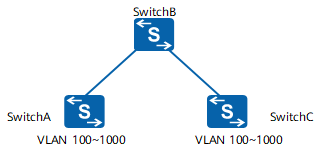
定时器：GARP协议中使用了4个定时器。

* Join定时器：用来控制Join消息（包括JoinIn和JoinEmpty）的发送。为了宝成Join消息能够可靠的传输到其他应用实体，发送第一个Join消息后将等待一个Join定时器的时间间隔，如果在一个Join定时器时间内收到JoinIn消息，则不发送第二个Join消息；如果没收到，则再发送一个Join消息。每个端口维护独立的Join定时器。
* Hold定时器：Hold定时器是用来控制Join消息（包括JoinIn和JoinEmpty）和Leave消息（包括LeaveIn和LeaveEmpty）的发送。当在应用实体上配置属性或应用实体接收到消息时不会立刻将该消息传播到其它设备，而是在等待一个Hold定时器后再发送消息，设备将此Hold定时器时间段内接收到的消息尽可能封装成最少数量的报文，这样可以减少报文的发送量。如果没有Hold定时器的话，每来一个消息就发送一个，造成网络上报文量太大，既不利于网络的稳定，也不利于充分利用每个报文的数据容量。每个端口维护独立的Hold定时器，Hold定时器的值要小于等于Join定时器值的一半。
* Leave定时器：用来控制属性注销。每个应用实体接收到Leave或LeaveAll消息后会启动Leave定时器，如果在Leave定时器超时之前没有接收到该属性的Join消息，属性才会被注销。因为网络中如果有一个实体因为不存在某个属性而发送了Leave消息，并不代表所有的实体都不存在该属性了，因为不能立刻注销属性，而是要等待其他实体的消息。每个端口维护独立的Leave定时器。
* LeaveAll定时器：每个GARP应用实体启动后，将同时启动LeaveAll定时器，当该定时器超时后GARP应用实体将对外发送LeaveAll定时器，开始新的一轮循环。接收到LeaveAll消息的实体将重新启动所有的定时器，包括LeaveAll定时器。在自己的LeaveAll定时器重新超时之后才会再次发送LeaveAll消息，这样就避免了短时间内发送多个LeaveAll消息。如果不同设备的LeaveAll定时器同时超时，就会同时发送多个LeaveAll消息，增加不必要的报文数量，为了避免不同设备同时发生LeaveAll定时器超时，实际定时器运行的值是大于LeaveAll定时器的值，小于1.5倍LeaveAll定时器值的一个随机值。一次LeaveAll事件相当于全网所有属性的一次Leave。由于LeaveAll影响范围很广，所以建议LeaveAll定时器的值不能太小，至少应该大于Leave定时器的值。每个设备只在全局维护一个LeaveAll定时器。

注册模式：手工配置的VLAN称为静态VLAN，通过GVRP协议创建的VLAN称为动态VLAN。GVRP有三种注册模式，不同的模式对静态VLAN和动态VLAN的处理方式也不同。

* Normal模式：允许动态VLAN在端口上进行注册，同时会发送静态VLAN和动态VLAN的声明消息。
* Fixed模式：不允许动态VLAN在端口上注册，只发送静态VLAN的声明消息。
* Forbidden模式：不允许动态VLAN在端口上进行注册，同时删除端口上除VLAN1外的所有VLAN，只发送VLAN1的声明消息。

GVRP特性使得不同设备上的VLAN信息可以由协议动态维护和更新，用户只需要对少数设备进行VLAN配置即可应用到整个交换网络，无需耗费大量时间进行拓扑分析和配置管理。如下图所示，所有设备都使能GVRP功能，设备之间相连的端口均为Trunk端口，并允许所有VLAN通过。只需在SwitchA和SwitchC上分别手工配置静态VLAN100~VLAN1000，设备SwitchB就可以通过GVRP协议学习到这些VLAN，最后各设备上都存在VLAN100~VLAN1000。



【配置参数】

首先，需要前往端口，配置端口为Trunk，并配置允许通过的VLAN，使其加入VLAN。必须确保要通信的交换机上端口加入的VLAN一致。

注：1.如果端口切换到其他类型（Access、Hybrid），则端口下的GVRP配置自动清除。

2.STP/RSTP/MSTP协议的实例0的阻塞接口能阻塞GVRP协议报文，MSTP的其他实例以及其他环网协议的阻塞接口均不能阻塞GVRP协议报文。为确保GVRP正常运行并防止GVRP协议成环，建议不要在环网协议的阻塞接口上使能GVRP功能。

全局配置：

* GVRP：【开关】设置是否开启GVRP功能，默认关闭。
* 定时器：默认暂仅支持Join、Leave、LeaveAll这3个定时器，并且作为全局设置，内部写定设置值，不能编辑。
* Join定时器：默认20毫秒。
* Leave定时器：默认60毫秒。
* LeaveAll定时器：默认1000毫秒。

端口设置：

* 接口：选择需要配置的交换机接口，包括电口、光口和聚合接口。支持多选进行批量配置。

注：只能选择Trunk接口进行GVRP设置。

* GVRP：【开关】设置是否开启端口的GVRP功能，默认关闭。
* VLAN创建：【开关】设置是否开启GVRP动态VLAN创建，默认开启。
* 注册模式：【下拉框】设置端口的GVRP注册模式，选项有{Normal模式|Fixed模式|Forbidden模式}，默认Normal模式。

端口列表：

* 列表显示端口、GVRP设置、VLAN创建设置、注册模式
* 支持编辑

VLAN成员：

* 列表显示VLAN、指定VLAN的静态成员端口、通过GVRP注册到指定VLAN的端口、VLAN类型（静态|动态，静态为本地配置的VLAN，动态为通过GVRP生成的VLAN）

数据统计：

* 刷新时间 (秒)：【text文本框】设置接口统计数据信息的时间间隔，选项有{5秒|10秒|30秒}，默认10秒。设置后，Web页面将会每隔此时间间隔，刷新接口的数据统计信息。

数据表：

* 列表显示端口名称，各类统计信息如下：
* 接收：
* JoinEmpty：接收JoinEmpty的消息次数
* Empty：接收Empty的消息次数
* LeaveEmpty：接收LeaveEmpty的消息次数
* JoinIn：接收JoinIn的消息次数
* LeaveIn：接收LeaveIn的消息次数
* LeaveAll：接收LeaveAll的消息次数
* 发送：
* JoinEmpty：发送JoinEmpty的消息次数
* Empty：发送Empty的消息次数
* LeaveEmpty：发送LeaveEmpty的消息次数
* JoinIn：发送JoinIn的消息次数
* LeaveIn：发送LeaveIn的消息次数
* LeaveAll：发送LeaveAll的消息次数
* 错误：
* Invalid Protocol ID：接收报文中协议ID非法次数
* Invalid Attribute：接收报文中属性非法次数
* Invalud Event：接收报文中属性描述的事件非法次数

## 生成树/STP(FP1C)

【功能概述】

**（一）STP**

STP是局域网中的破环协议，运行该协议的设备通过彼此交互信息来发现网络中的环路，并有选择地对某些端口进行阻塞，最终将环形网络结构修剪成无环路的树形图形结构，达到破除环路的目的。如果当前活动的路径发生故障，STP还可以激活冗余备份链路，恢复网络连通性。

**STP基本概念：**

（1）一个根桥：树形的网络结构必须有树根，引入根桥概念。对于一个STP网络，根桥在全网中只有一个，它是整个网络的逻辑中心，但不一定是物理中心。根桥会根据网络拓扑的变化而动态变化。网络收敛后，根桥会按照一定的时间间隔产生并向外发送配置BPDU，其他设备收到该配置BPDU后，如果优先级比自己的配置BPDU高，则非根桥设备会根据收到的配置BPDU中携带的信息更新自己STP端口存储的配置BPDU信息，否则会丢弃该配置BPDU。

（2）两种度量：生成树的生成计算有两大基本度量依据：ID和路径开销。

* ID：又分为BID（Bridge ID）和PID（Port ID）
* BID：桥ID，由16位的桥优先级与桥MAC地址构成。BID桥优先级占据高16位，其余的低48位是MAC地址。在STP网络中，桥ID最小的设备会被选举为根桥。
* PID：端口ID，由两部分构成，高4位是端口优先级，低12位是端口号。PID在某些情况下对选择指定端口有作用。
* 路径开销：端口变量，是STP协议用于选择链路的参考值。STP协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树形网络结构。在一个STP网络中，某端口到根桥的路径开销就是所经过的各个桥上的各端口的路径开销累加而成，这个值叫做根路径开销。

（3）三要素选举：从环形网络拓扑结构到树形结构，总体来说有三个要素：根桥、根端口和指定端口。

* 根桥RB：网桥ID最小的桥，通过交互配置BPDU协议报文选出最小的BID。
* 根端口RP：去往根桥路径开销最小的端口，根端口负责向根桥方向转发数据，这个端口的选择标准是依据根路径开销判定。在一个运行STP协议的设备上根端口有且只有一个，根桥上没有根端口。
* 指定端口DP

|  |  |  |
| --- | --- | --- |
| 分类 | 指定桥 | 指定端口 |
| 对于一台设备而言 | 与本机直接相连并且负责向本机转发配置消息的设备 | 指定桥向本机转发配置消息的端口 |
| 对于一个局域网而言 | 负责向本网段转发配置消息的设备 | 指定桥向本网段转发配置消息的端口 |

一旦根桥、根端口、指定端口选举成功，则整个树形拓扑建立完毕。在拓扑稳定后，只有根端口和指定端口转发流量，其他的非根非指定端口都处于阻塞状态，只能接受STP协议报文而不转发用户流量。

（4）四个比较原则

STP选举有四个比较原则，构成消息优先级向量：{根桥ID，根开销路径，发送设备BID，发送端口PID}。配置BPDU中携带本端口的主要信息见下表

|  |  |
| --- | --- |
| 字段内容 | 简要说明 |
| 根桥ID | 每个STP网络中有且仅有一个根。 |
| 根路径开销 | 发送配置BPDU的端口到根桥的距离，决定了到根桥的路径开销。 |
| 发送设备BID | 发送配置BPDU的设备的BID。 |
| 发送端口PID | 发送配置BPDU的端口的PID。 |

STP网络中的其他设备收到配置BPDU消息后，将比较上述4个字段，四个基本比较原则如下：

* 最小BID：用来选举根桥。运行STP协议的设备之间根据上表根桥ID字段选择最小的BID。
* 最小根路径开销：用来在非根桥上选择根端口。在根桥上，每个端口到根桥的根路径开销都是0。
* 最小发送者BID：当一台运行STP协议的设备要在两个以上根路径开销相等的端口之中选择根端口时，通过STP协议计算，将选择接收到的配置消息中发送者BID较小的那个端口。
* 最小PID：用于在根路径开销相同的情况下，不阻塞最小PID的端口，而是阻塞PID值较大的端口。

（5）五种端口状态

STP端口状态：

|  |  |  |
| --- | --- | --- |
| 端口状态 | 目的 | 说明 |
| Forwarding | 端口既转发用户流量也处理BPDU报文 | 只有根端口或指定端口才能进入Forwarding状态 |
| Learning | 设备会根据收到的用户流量构建MAC地址表，但不转发用户流量 | 过渡状态，增加Learning状态防止临时环路 |
| Listening | 确定端口角色，将选举出根桥、根端口和指定端口 | 过渡状态 |
| Blocking | 端口仅仅接收并处理BPDU，不转发用户流量 | 阻塞端口的最终状态 |
| Disabled | 端口不见不处理BPDU报文，也不转发用户流量 | 端口状态为Down |

对于STP，影响端口状态和端口收敛有以下3个参数：

* Hello Time：运行STP协议的设备发送配置消息BPDU的时间间隔，用于设备检测链路是否存在故障。设备每隔Hello Time时间会向周围的设备发送BPDU报文，以确认链路是否存在故障。当网络拓扑稳定后，该计时器的修改只有在根桥修改后才有效。新的根桥会在发出的BPDU报文中填充相应的字段以向其他非根桥传递该计时器修改的信息。但当拓扑变化之后，TCN BPDU的发送不受这个计时器的管理。
* Forward Delay：设备状态迁移的延迟时间。链路故障会引发网络重新进行生成树的计算，生成树的结构将发生相应的变化。不过重新计算得到的新配置消息无法立刻传遍整个网络，如果新选出的根端口和指定端口立刻就开始数据转发的话，可能会造成临时环路。STP采用一种状态迁移机制，新选出的根端口和指定端口要经过2倍的Forward Delay延时后才能进入转发状态，这个延时保证了新的配置消息传遍整个网络，从而防止了临时环路的产生。Forward Delay Timer指一个端口处于Listening和Learning状态的各自持续时间，默认是15秒，即Listening状态持续15秒，随后Learning状态再持续15秒。这两个状态下的端口会处于Blocking状态，这正是STP用于避免临时环路的关键。
* Max Age：端口的BPDU报文老化时间，可在根桥上通过命令人为改动老化时间。其通过配置BPDU报文的传输，可保证Max Age在整网中一致。运行STP协议的网络中非根桥设备收到配置BPDU报文后，报文中的Message Age和Max Age会进行比较。
* 如果Message Age小于等于Max Age，则该非根桥设备继续转发配置BPDU报文。
* 如果Message Age大于Max age，则该配置BPDU报文将被老化。该非根桥设备直接丢弃该配置BPDU，可认为网络直径过大，导致根桥连接失败。

如果配置BPDU是根桥发出的，则Message Age为0，否则，Message Age是从根桥发送到当前桥接收到BPDU的总时间，包括传输延时等。

**STP报文格式：**BPDU协议报文

配置BPDU报文是一种心跳报文，只要端口使能STP，配置BPDU就会按照Hello Time定时器规定的时间间隔从指定端口发出。

TCN BPDU是在设备检测到网络拓扑发生变化时才发出。

配置BPDU：即BPDU报文。在初始化过程中，每个桥都主动发送配置BPDU。在网络拓扑稳定以后，每台设备的指定端口都会周期性地发送配置BPDU。配置BPDU的长度至少要35字符，包含了桥ID、路径开销和端口ID等参数。只有当发送者的BID或端口的PID两个字段中至少有一个和本桥接收端口不同，BPDU报文才会被处理，否则丢弃，这样避免了处理和本端口信息一致的BPDU报文。配置BPDU在以下3种情况下会产生：

* 只要端口使能STP，则配置BPDU就会按照Hello Time定时器规定的时间间隔从指定端口发出
* 当根端口收到配置BPDU时，如果优先级比自己的配置BPDU高，则会根据收到的配置BPDU中携带的信息更新自己STP端口存储的配置BPDU信息并从指定接口向下游发送，否则会丢弃该配置BPDU。
* 当指定端口收到比自己查的配置BPDU时，会立刻向下游设备发送自己的BPDU。

TCN BPDU：只有协议号、版本和类型，类型字段固定0x80，长度只有4字节。在下游拓扑发生变化时向上游发送拓扑变化通知，知道根节点。TCN BPDU在以下2种情况下会产生：

* 端口状态变为Forwarding状态
* 指定端口收到TCN BPDU，复制TCN BPDU并发往根桥

STP不足：（1）Listening、Learning和Blocking状态都不转发用户流量；（2）端口扮演角色，根端口和指定端口可以都处于Listening状态，也可能都处于Forwarding状态；（3）STP算法被动，依赖定时器等待的方式判断拓扑变化，收敛速度慢。

**（二）RTSP**

**RSTP对STP的改进：**

（1）通过端口角色的增补，简化生成树协议的理解与部署

RSTP的端口角色有4种：根端口、指定端口、Alternate端口和Backup端口。其中，根端口和指定端口的作用同STP，Alternate端口和Backup端口描述如下：

* 从配置BPDU报文发送角度来看：Alternate端口是由于学习到其他网桥发送的配置BPDU报文而阻塞的端口；Backup端口是由于学习到自己发送的BPDU报文而阻塞的端口。
* 从用户流量角度来看：Alternate端口提供了从指定桥到根的另一条可切换路径，作为根端口的备份端口；Backup端口作为指定端口的备份，提供了另一条从根桥到相应网桥的备份通路。

给一个RSTP域内所有端口分配角色的过程就是整个拓扑收敛的过程。

（2）端口状态的重新划分

RSTP的状态规范把原来的5种状态缩减为3种。根据端口是否转发用户流量和学习MAC地址来划分。

* 如果不转发用户流量也不学习MAC地址，那么端口状态就是Discarding状态
* 如果不转发用户流量但学习MAC地址，那么端口状态就是Learning状态
* 如果既转发流量又学习MAC地址，那么端口状态就是Forwarding状态

|  |  |  |
| --- | --- | --- |
| STP端口状态 | RSTP端口状态 | 端口在拓扑中的角色 |
| Forwarding | Forwarding | 包括根端口、指定端口 |
| Learning | Learning | 包括根端口、指定端口 |
| Listening | Discarding | 包括根端口、指定端口 |
| Blocking | Discarding | 包括Alternate端口、Backup端口 |
| Disabled | Discarding | 包括Disabled端口 |

（3）配置BPDU格式的改变，充分利用了STP协议报文中的Flag字段，明确了端口角色---RST BPDU

（4）配置BPDU的处理发生变化

* 拓扑稳定后，配置BPDU报文的发送方式：拓扑稳定后，根桥按照Hello Timer规定的时间间隔发送配置BPDU。其他非根桥设备在收到上游设备发送过来的配置BPDU后，才会触发发出配置BPDU，此方式使得STP协议计算复杂且缓慢。RSTP对此进行了改进，即在拓扑稳定后，无论非根桥设备是否接收到根桥传来的配置BPDU报文，非根桥设备仍然按照Hello Timer规定的时间间隔发送配置BPDU，该行为完全由每台设备自主进行。
* 更短的BPDU超时计时：如果一个端口在超时时间（超时时间=Hello Time\*3\*Timer Factro）内没有收到上游设备发送过来的配置BPDU，那么该设备认为与此邻居之间的协商失败，无需等待一个Max Age、
* 处理次等BPDU：当一个端口收到上游的指定桥发来的RST BPDU报文时，该端口会将自身存储的RST BPDU与收到的RST BPDU进行比较。如果该端口存储的RST BPDU的优先级高于收到的RST BPDU，那么该端口会直接丢弃收到的RST BPDU，立即回应自身存储的RST BPDU。当上游设备收到下游设备回应的RST BPDU后，上游设备会根据收到的RST BPDU报文中相应的字段立即更新自己存储的RST BPDU。

（5）快速收敛

* Proposal/Agreement机制（P/A机制）：当一个端口被选举成为指定端口之后，此端口会先进入Discarding状态，再通过Proposal/Agreement机制快速进入Forward状态。此机制必须在点对点全双工链路上使用。
* 根端口快速切换机制：如果RSTP网络中一个根端口失效，那么网络中最优的Alternate端口将成为根端口并直接进入Forwarding状态。通过这个Alternate端口连接的网段上必然有个指定端口可以通往根桥。
* 边缘端口的引入：如果某一个指定端口位于整个网络的边缘，即不再与其他交换设备连接，而是直接与终端设备直连，这种端口叫做边缘端口。边缘端口不参与RSTP运算，可以由Disable直接转到Forwarding状态，且不经历时延，就像在端口上将STP禁用。但一旦边缘端口收到配置BPDU，就丧失了边缘端口属性，成为普通STP端口，并重新进行生成树计算，从而引起网络震荡。

（6）保护功能

* BPDU保护：交换机上通常将直接与用户终端（如PC）或文件服务器等非交换设备相连的端口配置为边缘端口。正常情况下，边缘端口不会收到RST BPDU，但如果有人伪造RST BPDU恶意攻击交换机，当边缘端口收到RST BPDU时，交换机会自动将边缘端口设置为非边缘端口，并重新进行生成树计算。当攻击者发送的RST BPDU报文中的桥优先级高于现有网络中根桥优先级时会改变当前网络拓扑，可能会导致业务流量终端。交换机开启BPDU保护后，如果边缘端口收到RST BPDU，边缘端口将被error-down，但是边缘端口属性不变，同时通知网管系统。
* 根保护【FP1C暂不支持】：由于错误配置或恶意攻击，网路中合法根桥有可能会疏导优先级更高的RST BPDU，使得合法根桥失去根地位，从而引起网络拓扑结构的错误变动，导致原来应该通过高速链路的流量被牵引到低速链路上，造成网络拥塞。启动根保护的指定端口，其端口角色只能保持为指定端口。一旦启用根保护功能的指定端口收到优先级更高的RST BPDU时，端口状态将进入Discarding状态，不在转发报文。经过一段时间（通常为2倍的Forward Delay），如果端口一直没有再收到优先级较高的RST BPDU，端口会自动恢复到正常的Forwarding状态。
* 环路保护：根端口和其他阻塞端口状态依靠不断接受来自上游交换设备的RST BPDU来维持。一旦由于链路拥塞或单向链路故障导致这些端口收不到来自上游交换设备的RST BPDU时，交换设备会重新选择根端口。原先的根端口会转变为指定端口，而原先的阻塞端口会迁移到转发状态，从而造成交换网络中可能产生环路。启动环路保护后，如果根端口或Alternate端口长时间收不到来自上游设备的BPDU报文时，将向网管发出通知信息（此时根端口会进入Discarding状态，角色切换为指定端口），而Alternate端口则会一直保持在阻塞状态（角色也会切换为指定端口），不转发报文，从而不会在网络中形成环路。直到链路不再拥塞或单向链路故障恢复，端口重新收到BPDU报文进行协商，并恢复到链路拥塞或者单向链路故障前的角色和状态。
* 防TC-BPDU攻击：交换设备在接收到TC BPDU报文后，会执行MAC地址表项和ARP表项的删除操作。如果有人伪造TC BPDU报文恶意攻击交换设备时，交换设备短时间内会收到很多TC BPDU报文，频繁地删除操作会给设备造成很大的负担，给网络的稳定带来很大隐患。启用防TC-BPDU保护后，在单位时间内，交换设备处理TC BPDU报文的次数可配置。如果在单位时间内，交换设备在收到TC BPDU报文数量大于配置的阈值，那么设备只会处理阈值指定的次数。对于其他超出阈值的TC BPDU报文，定时器到期后设备只对其统一处理一次，这样可以避免删除MAC地址表项和ARP表项，从而达到保护设备的目的。

**（三）MSTP：**

MSTP把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立。每棵生成树叫做一个多生成树实例MSTI，每个域叫做一个MST域。

生成树实例就是多个VLAN的一个集合。通过将多个VLAN捆绑到一个实例，可以节省通信开销和资源占用率。MSTP各个实例拓扑的计算相互独立，在这些实例上可以实现负载均衡。可以把多个相同拓扑结构的VLAN映射到一个实例里，这些VLAN在端口上的转发状态取决于端口在对应MSTP实例的状态。

MSTP的网络层次：MSTP网络中包含1个或多个MST域，每个MST域中包含一个或多个MSTI。组成MSTI的是运行STP/RSTP/MSTP的交换设备，MSTI是所有运行STP/RSTP/MSTP的交换设备经MSTP协议计算后形成的树状网络。

MST域（MST Region）：多生成树域，由交换网络中的多台交换设备以及它们之间的网段所构成。同一个MST域的设备具有下列特点：（1）都启动MSTP；（2）具有相同的域名；（3）具有相同的VLAN到生成树实例映射配置；（4）具有相同的MSTP修订级别配置。一个局域网可以存在多个MST域，各MST域之间在物理上直接或间接相连。用户可以通过MSTP配置命令把多态交换设备划分在同一个MST域内。

VLAN映射表：MST域的属性，描述了VLAN和MSTI之间的映射关系。

CST：公共生成树是连接交换网络内所有MST域的一棵生成树。如果把每个MST域看作是一个节点，CST就是这些节点通过STP或RSTP协议计算生成的一棵生成树。

IST：内部生成树是各MST域内的一棵生成树。IST是一个特殊的MSTI，MSTI的ID为0，通常称为MSTI0。IST是CIST在MST域中的一个片段。

SST：构成单生成树有2种情况：（1）运行STP或RSTP的交换设备只能属于一个生成树；（2）MST域中只有一个交换设备，这个交换设备构成单生成树。

CIST：公共和内部生成树是通过STP或RSTP协议计算生成的，连接一个交换网络内所有交换设备的单生成树。

域根：分为IST域根和MSTI域根。一个MST域内可以生成多棵生成树，每棵生成树都称为一个MSTI。MSTI域根是每个多生成树实例的树根。

总根：是CIST的根桥。

主桥（Master Bridge）即IST Master，是域内距离总根最近的交换设备。如果总根在MST域中，则总根为该域的主桥。

端口角色：根端口、指定端口、Alternate端口、Backup端口和边缘端口。除边缘端口外，其他端口角色都参与MSTP的计算过程，同一端口在不同生成树实例中可以担任不同的角色。

|  |  |
| --- | --- |
| 端口角色 | 说明 |
| 根端口 | 在非根桥上，离根桥最近的端口是本交换设备的根端。根交换设备没有根端口。根端口负责向树根方向转发数据。 |
| 指定端口 | 对一台交换设备而言，指定端口是向下游交换设备转发BPDU报文的端口。 |
| Alternate端口 | * 从配置BPDU报文发送角度来看，Alternate端口是由于学习到其他网桥发送的配置BPDU报文而阻塞的端口 * 从用户流量角度来看，Alternate端口提供了从指定桥到根的另一条可切换路径，作为根端口的备份端口 |
| Backup端口 | * 从配置BPDU报文发送角度来看，Backup端口是由于学习到自己发送的配置BPDU报文而阻塞的端口 * 从用户流量角度来看，Backup端口作为指定端口的备份，提供了另外一条从根节点到叶节点的备份通路。 |
| Master端口 | Master端口是MST域和总根相连的所有路径中最短路径上的端口，它是交换设备上连接MST域到总根的端口  Master端口是域中的报文去往总根的必经之路  Master端口是特殊域边缘端口，Master端口在CIST上的角色是根端口，在其他各实例上的角色都是Master端口 |
| 域边缘端口 | 域边缘端口是指位于MST域的边缘并连接其它MST域或SST域的端口 |
| 边缘端口 | 指定端口处于整个域的边缘，不再与任何交换设备连接 |

MSTP端口状态：

|  |  |
| --- | --- |
| 端口状态 | 说明 |
| Forwarding | 端口既转发用户流量又处理BPDU报文 |
| Learning | 过渡状态。交换设备根据收到的的用户流量，构建MAC地址表，但不转发用户流量。端口处理BPDU报文 |
| Discarding | 端口只接收BPDU报文 |

MSTP报文： MST BPDU

|  |  |  |
| --- | --- | --- |
| 版本 | 类型 | 名称 |
| 0 | 0x00 | 配置BPDU |
| 0 | 0x80 | TCN BPDU |
| 2 | 0x20 | RST BPDU |
| 3 | 0x02 | MST BPDU |

**MSTP拓扑计算：**

MSTP可以将整个二层网络划分为多个MST域，各个域之间通过计算生成CST。域内则通过计算生成多棵生成树，每棵生成树都被称为一个多生成熟实例。其中，实例0被称为IST，其他的多生成树实例为MSTI。

优先级向量：MSTI和CIST都是根据优先级向量来计算的，这个优先级向量信息都包含在MST BPDU中。各交换设备互相交换MST BPDU来生成MSTI和CIST。

参与CIST计算的优先级向量为（根交换设备ID，外部路径开销，域根ID，内部路径开销，指定交换设备ID，指定端口ID，接收端口ID）；参与MSTI计算的优先级向量为（域根ID，内部路径开销，指定交换设备ID，指定端口ID，接收端口ID）。向量优先级从左到右依次递减。

比较原则：同一向量比较，值最小的向量优先级最高。比较原则按照优先级从高到低进行比较，若同一向量相同，则网次低优先级向量进行比较。如果端口接收到的BPDU内包含的配置消息优于端口上保存的配置消息，则端口上原来保存的配置消息被新收到的配置消息替代。端口同时更新交换设备的全局配置消息；反之，新收到的BPDU被丢弃。

CIST计算：经过比较配置消息后，在整个网络中选择一个优先级最高的交换设备作为CIST的树根。在每个MST域内MSTP通过计算生成IST；同时MSTP将每个MST域作为单台交换设备对待，通过计算在MST域间生成CST。CST和MST构成了整个交换设备网络的CIST。

MSTI计算：在MST域内，MSTP根据VLAN和生成树实例的映射关系，针对不同的VLAN生成不同的生成树实例。（1）每个MSTI独立进行计算，互不干扰；（2）每个MSTI的生成树计算方法与STP基本相同；（3）每个MSTI的生成树可以有不同的根，不同的拓扑；（4）每个MSTI在自己的生成树内发送BPDU；（5）每个MSTI的拓扑通过命令配置决定；（6）每个端口在不同MSTI上的生成树参数可以不同；（7）每个端口在不同MSTI上的角色、状态可以不同。

在运行STP协议的网络中，一个VLAN报文将沿着如下路径进行转发：（1）在MST域内，沿着其对应的MSTI转发；（2）在MST域间，沿着CST转发。

### （四）兼容Cisco PVST(Per VLAN Spanning Tree) (FP2)

**PVST工作原理：**

STP和RTSP在局域网内的所有网桥都共享一棵生成树，不能按VLAN阻塞冗余链路，所有VLAN的报文都沿着一棵生成树进行转发。而PVST可以在每个VLAN内都拥有一棵生成树，能够有效地提高链路带宽的利用率。PVST可以简单理解为在每个VLAN上运行一个STP或RTSP，不同VLAN之间的生成树完全独立。故，PVST协议无法与STP/RSTP的设备进行互通。

运行PVST的交换机可以与运行Rapid PVST或PVST的三方设备互通。当运行PVST的交换机互联，或运行PVST的交换机与运行Rapid PVST的三方设备互通时，GWN78XX交换机支持像RTSP一样快速收敛。

**PVST的协议报文：**

PVST的BPDU与RTSP的BPDU存在3点不同：（1）报文的目的MAC地址改变，变为私有MAC地址01:00:0C:CC:CC:CD；（2）报文携带VLAN标签，确定该协议报文归属的VLAN；（3）报文配置消息固定格式链路头字段添加Organization code和PID字段。

根据端口类型的不同，PVST发送的BPDU格式也有所差别：

* Access端口：PVST将根据该VLAN的状态发送RTSP格式的BPDU
* Trunk端口和Hybrid端口：PVST将在缺省VLAN内根据该VLAN的状态发送RTSP格式的BPDU，而对于其他本端口允许通过的VLAN，则发送PVST格式的BPDU

**PVST工作原理：**

PVST借助MSTP的实例和VLAN映射关系模型，将MSTP每个实例映射一个VLAN。PVST中每个VLAN独立运行RTSP，独立运算，并允许以每个VLAN为基础开启或关闭生成树。每个VLAN内的生成树实例都有单独的网络拓扑结构，相互之间没有影响。这样既可以消除VLAN内的冗余链路，还可以实现不同VLAN间负载分担。

PVST在缺省VLAN上通过RTSP报文进行拓扑运算；在其他VLAN上通过带VLAN Tag的PVST报文进行拓扑运算。

PVST的端口角色和端口状态与RTSP相同，能够实现快速收敛。

**快速收敛机制：**

快速收敛机制包括边缘端口机制、根端口快速切换机制、指定端口快速切换机制，其中指定端口快速切换机制也称为P/A（Proposal/Aggrement，请求/回应）机制。

（1）边缘端口机制：当端口直接与用户中断相连，而没有连接到其他网桥或局域网网段上时，该端口即为边缘端口。边缘端口连接的是终端，当网络拓扑变化时，边缘端口不会产生临时环路，所以边缘端口可以略过两个Forward Delay的时间，直接进入Forwarding状态，无需任何延时。由于网桥无法自动判断端口是否直接与终端相连，所以用户需要手工将与终端连接的端口设置为边缘端口。

（2）根端口快速切换机制：当旧的根端口进入阻塞状态，网桥会选择优先级最高的替换端口作为新的根端口。如果当前新根端口连接的对端网桥的指定端口处于Forwarding状态，则新根端口可以立刻进入Forwarding状态，期间不需要延时。

（3）P/A机制：指定端口可以通过与对端网桥进行一次握手，即可快速进入转发状态，期间不需要任何定时器。P/A机制的前提条件是：握手必须在点到点链路上进行。有点到点链路作为前提，P/A机制可以实现网络拓扑的逐链路收敛，而不需要像STP要被动等待20秒的时间以确保全网实现收敛。

PVST的P/A机制与RTSP相同。当新链路连接或故障链路恢复时，链路两端的端口初始都为指定端口并处于阻塞状态。当指定端口处于Discarding状态和Learning状态，其所发送的BPDU中Proposal位将被置位，端口角色为指定端口。收到Proposal置位的BPDU后，网桥会判断接收端口是否为根端口。如果是，网桥会启动同步过程。同步过程指网桥阻塞除边缘端口之外的所有端口，在本网桥层面消除环路产生的可能。

### （五）兼容Cisco PVST+(Per VLAN Spanning Tree Plus) (FP2)

**PVST+工作原理：**

PVST+协议相对于PVST协议的改进是：提供了与标准STP协议互通的能力。

**PVST+报文处理方式：**

根据端口类型的不同，PVST+发送的BPDU格式也有所差别：

* Access端口：在所有VLAN内，只发送标准的STP格式的BPDU
* Trunk端口和Hybrid端口：在缺省VLAN内发送标准的BPDU（目的MAC地址为01:80:C2:00:00:00），而在其他允许通过的VLAN中发送PVST格式的BPDU

**（六）兼容Cisco Rapid PVST+(Rapid Per VLAN Spanning Tree Plus)【暂不支持】**

**Rapid PVST+工作原理：**

相对于PVST+协议，采用RTSP的机制，支持快速迁移特性。

**Rapid PVST+报文处理方式：**其报文处理机制与PVST+相同。

Rapid PVST+的端口角色有4种：根端口、指定端口、备用端口、备份端口和禁用端口。端口状态有4种：Blocking、Learning、Forwarding和Disabled。

【配置参数】

1. 全局设置：

* 生成树：【开关】设置是否启用生成树功能，默认关闭。当关闭时，需配置BPDU报文处理方式。
* BPDU处理：【单选】当关闭生成树时，交换设备收到BPDU报文的处理方式，选项有{丢弃|泛洪}，默认丢弃。
* 模式：【单选】选择生成树的工作模式，选项有{STP | RSTP | MSTP | PVST}，默认RSTP。
* 路径开销：【单选】设置配置路径开销的计算方案，选项有{短|长}，默认短。
* 桥优先级：【text文本框】当模式选择”PVST“时，基于VLAN设置，此处需隐藏。设置交换机的桥优先级。值越小，优先级越高。取值范围为0-61440的整数，以4096为步长，默认为32768。
* 最大跳数：【text文本框】当模式选择”PVST“时，不支持配置，需隐藏。设置每秒BPDU报文被转发的最大次数，其限制了生成树的规模。取值范围为1-40的整数，默认20。仅针对MSTP生效。
* Hello Time (s)/联络时间：【text文本框】当模式选择”PVST“时，基于VLAN设置，此处需隐藏。设置交换设备发送BPDU的时间间隔，用于检测链路是否存在故障。取值范围为1-10的整数，默认2秒。
* Max Age (s) /最大老化时间：【text文本框】当模式选择”PVST“时，基于VLAN设置，此处需隐藏。设置交换设备端口上的BPDU在设备上保存的最大时长，其根据此时间判断从上游交换设备收到的BPDU是否超时。取值范围为6-40的整数，默认20秒。
* Forward Delay (s)/转发延迟时间：【text文本框】当模式选择”PVST“时，基于VLAN设置，此处需隐藏。在网络拓扑改变后，设置交换设备的端口状态迁移的延迟时间。取值范围为4-30的整数，默认15秒。

注：3个时间配置时，必须满足如下关系：（Hello Time+1）\*2≤Max Age≤（Forward Time-1）\*2

生成树状态信息：（当模式选择“PVST”时不显示）

显示桥ID、根桥ID、根端口、根路径开销、拓扑变更次数以及最后一次变更的时间。

2. 端口设置：~~配置交换机端口的CIST参数。~~

* 接口：选择需要配置的交换机接口，包括电口、光口和聚合接口。支持多选进行批量配置。
* 生成树使能：【开关】设置是否开启接口的生成树功能，默认开启。
* 优先级：【text文本框】优先级是确定该端口是否会被选择根端口的重要依据。同等条件下优先级高的端口将被选为根端口。值越小，优先级越高。取值范围为0-240的整数，以16为步长，默认128。
* 路径开销：【text文本框】设置端口在指定生成树上的端口路径开销。全局 长路径开销的取值范围为0-200000000的整数，全局 短路径开销的取值范围为0-65535的整数，默认为0，表示自动进行路径开销计算。
* 边缘端口：【下拉框】设置是否将当前接口设置为边缘端口，选项有{自动|开启|关闭}，默认自动。

注：STP模式，不支持自动边缘功能，“自动”模式下始终呈现关闭状态。

* BPDU保护：【开关】设置是否开启交换设备边缘端口的BPDU保护功能，默认关闭。开启后，当边缘端口收到BPDU报文时，自动error-dwon。
* BPDU过滤：【开关】设置边缘端口是否开启BPDU过滤功能，默认关闭。开启后，边缘端口不处理、不发送BPDU报文。
* 点对点链路：【下拉框】当 全局 模式选择”PVST“时不支持配置。这个端口的点对点链路状态。以点对点链路相连的两个端口，如果为根端口或者指定端口，则可以快速迁移到转发状态，从而减少不必要的转发延迟时间。选项有{自动|开启|禁用}，默认自动。

端口列表：

* 列表显示每个端口的配置信息，有生成树设置、优先级、路径开销、边缘端口设置、BPDU保护设置、BPDU过滤设置、点对点链路设置
* 列表显示每个端口的状态，有端口状态、角色、指定桥ID、指定端口ID、指定路径开销、操作边缘、操作点对点
* 端口状态有Disabled、Listening、Learning、Forwarding、Blocking和Discarding。
* 端口角色有Root Port(根端口)、Designated Port(指定端口)、Alternate Port、Backup Port、Master Port和Disabled Port。
* 支持编辑端口设置

3. MSTP域（当且仅当模式选择“PVST”时隐藏，转而呈现PVST的VLAN设置）

域配置：

* \*域名：【text文本框】用于标识MST域，最长32字符，支持输入数字 字母 : . - \_ 默认使用MAC地址，但只使用前一半，后一半均为0
* \*修订级别：【text文本框】用于标识MST域。取值为0-65535的整数，默认0

MST实例：

MST实例从0开始编号。各型号个数限制如下表所示：

|  |  |  |
| --- | --- | --- |
| **型号** | **芯片** | **实例上限** |
| GWN7801(P)/02(P)/03(P) | RTL838X | 16 |
| GWN7811(P)/12P/13(P)/21P/23P/30/31 | RTL930X | 32 |
| GWN7806(P)/GWN7816(P)/GWN7832 | RTL931X | 64 |

* 实例ID：选择需要配置的一个实例ID。
* VLAN：【多选】用来将指定VLAN映射到指定生成树实例上。默认情况下，所有VLAN均映射到实例0即CIST上。

注：同一个VLAN有且只能映射到一个实例ID上。

* 优先级：【text文本框】设置交换设备在指定生成树中实例的优先级，决定该交换机是否会被选为根桥的重要依据。取值范围为0-61440的整数，以4096为步长，默认32768。

MST实例列表：

* 列表显示实例ID、映射的VLAN、优先级、网桥标识符、指定的根网桥、根端口、根路径开销、剩余的跳数
* 支持编辑

MST端口设置：

* MSTI：【单选】选择需要配置端口的实例ID。
* 接口：选择需要配置的交换机接口，包括电口、光口和聚合接口。支持多选进行批量配置。
* 路径开销：【text文本框】配置当前端口在指定生成树上的端口路径开销，决定该端口是否会被选为根端口。全局 长路径开销的取值范围为0-200000000的整数，全局 短路径开销的取值范围为0-65535的整数，默认为0，表示自动进行路径开销计算。
* 优先级：【Text文本框】设置当前端口在生成树计算时的优先级，改变当前端口的端口优先级，从而影响端口的PDI，最终影响该端口是否会被选举成为指定端口。取值范围为0-240的整数，以16为步长，默认128。

MST端口列表：

* 列表显示端口、路径开销、优先级、角色、状态、模式(STP/RSTP/MSTP)、类型(内部/边缘)、指定网桥、指定端口ID、指定路径开销、剩余跳数
* 角色有Root Port(根端口)、Designated Port(指定端口)、Alternate Port、Backup Port、Master Port和Disabled Port。
* 状态有Disabled、Listening、Learning、Forwarding、Blocking
* 支持编辑

当模式选择“PVST”时，需变更为如下设置：

（1）全局设置：仅保留生成树开关（关闭时有BPDU处理）、模式和路径开销设置。

（2）端口设置：在PVST模式下，仅“边缘端口”“BPDU保护”“BPDU过滤”的配置可生效。

（3）隐藏MST相关的实例和端口设置，新增VLAN设置和PVST端口设置，具体如下：

VLAN设置：

* VLAN：列表显示已添加的所有VLAN，从中选择
* PVST使能：【开关】设置是否在VLAN上开启PVST功能，默认关闭。

注：PVST使能的VLAN个数上限为各平台实例上限个数-1。故，建议交互在PVST使能下显示剩余使能个数。其中，未使能PVST的VLAN均保留在实例0中

* 桥优先级：【text文本框】设置VLAN的桥优先级。值越小，优先级越高。取值范围为0-61440的整数，以4096为步长，默认为32768。
* Hello Time (s)/联络时间：【text文本框】设置交换设备在当前VLAN生成树内发送BPDU的时间间隔，用于检测链路是否存在故障。取值范围为1-10的整数，默认2秒。
* Max Age (s) /最大老化时间：【text文本框】设置交换设备在当前VLAN生成树端口上的BPDU在设备上保存的最大时长，其根据此时间判断从上游交换设备收到的BPDU是否超时。取值范围为6-40的整数，默认20秒。
* Forward Delay (s)/转发延迟时间：【text文本框】在网络拓扑改变后，设置交换设备在当前VLAN生成树的端口状态迁移的延迟时间。取值范围为4-30的整数，默认15秒。

注：3个时间配置时，必须满足如下关系：（Hello Time+1）\*2≤Max Age≤（Forward Time-1）\*2

VLAN列表：

* 列表显示VLAN、PVST使能状态、桥优先级、Hello Time、Max Age、Forward Delay，及此VLAN生成树的运行信息，包括桥ID、根桥ID、根端口、根路径开销、拓扑变更次数、最后一次变更时间
* 支持编辑

PVST端口设置：

* 实例：【单选】选择需要配置端口的VLAN实例，选项为VLAN设置处的VLAN。
* 接口：选择需要配置的交换机接口，包括电口、光口和聚合接口。支持多选进行批量配置。
* 路径开销：【text文本框】配置当前端口在指定生成树上的端口路径开销，决定该端口是否会被选为根端口。全局 长路径开销的取值范围为0-200000000的整数，全局 短路径开销的取值范围为0-65535的整数，默认为0，表示自动进行路径开销计算。
* 优先级：【Text文本框】设置当前端口在生成树计算时的优先级，改变当前端口的端口优先级，从而影响端口的PDI，最终影响该端口是否会被选举成为指定端口。取值范围为0-240的整数，以16为步长，默认128。

PVST端口列表：

* 列表显示端口、路径开销、优先级、角色、状态、指定桥ID、指定端口ID、指定路径开销
* 角色、状态、指定桥ID、指定端口ID、指定路径开销以后台返回为准
* 支持编辑

## ERPS (FP3) 【待评审】

【功能概述】

ERPS（Ethernet Ring Protection Switching，以太环网保护切换技术），是ITU定义的一种二层破环协议标准，又称为G.8032，定义了RAPS（Ring Auto Protection Switching）协议报文和保护倒换机制。它是一个专门应用于以太环网的链路层协议，在以太环网完整时能够防止数据环路引起的广播风暴，而当以太环网上一条链路断开时能迅速恢复环网上各个节点之间的通信。

ERPS协议提供了一种快速以太环网保护机制，能够在环网发生故障时，快速地恢复网络传输，从而保障交换机在环网拓扑情况下的高可用性、高可靠性。ERPS目前支持v1和v2版本，v2完全兼容v1，并扩展了4个功能：（1）相交环等多环组网方式；（2）子环传输RAPS报文采用虚通道或非虚通道；（3）人工进行阻塞点的切换，包括强制切换和手工切换；（4）ERPS环的回切模式可配置。【GWN78XX暂仅支持v1版本，即只支持单环】

对于STP，ERPS优化了环网检测机制，有选择性的阻塞网络冗余链路，防止广播风暴的形成和MAC地址表不稳定等现象，支持小于50ms的收敛时间，保证通信质量，还提供了强大的兼容性，作为ITU-T发布的破环标准协议，与支持该协议的各厂家都兼容，实现互通。

**ERPS基本概念**

1.ERPS环：一个环形连接的以太网网络拓扑称为一个ERPS环，相连设备配置了相同的控制VLAN。ERPS环分为主环和子环。缺省情况下，ERPS环都是主环，主环是封闭的环，子环是非封闭的环，需要配置，且只有ERPSv2版本支持。一个ERPS环可以由单个主环构成，也可以由多个环网构成，在多个环网中可以有多个主环和多个子环。【GWN78XX暂仅支持单环】

2.节点：加入ERPS环的二层交换设备称为节点。每个节点不能多于2个端口加入同一个ERPS环。

* Owner节点：主节点，负责阻塞和放开本节点上位于RPL上的端口，防止形成环路，从而进行链路切换。
* Neighbor节点：邻居节点，RPL上和Owner节点相连的节点，协同Owner节点阻塞和放开本节点上位于RPL上的端口，进行链路切换。
* Interconnection节点：互联节点，多环模型中连接多个环的节点，互联节点处于子环，主环无互联节点。在子环互联节点之间的链路的协议报文上送模式中，子环的协议报文在互联节点终结，数据报文不被终结。
* Normal节点：普通节点，除了上述三种节点外的所有节点。普通节点负责接收和转发链路中的协议报文和数据报文。

3.端口角色：ERPS协议中规定的端口角色主要有RPL owner端口、RPL neighbor端口（只有ERPSv2版本支持）和普通端口3种类型。

* RPL owner端口：一个ERPS环只有一个RPL owner端口由用户配置决定，通过阻塞RPL owner端口转发用户流量来防止ERPS环中产生环路。当RPL owner端口所在设备收到故障报文得知ERPS环上其他节点或链路故障时，会自动放开RPL owner端口，此端口恢复流量的接收和发送，保证流量不会中断。RPL owner端口所在的链路即为环保护链路RPL。
* RPL neighbor端口：RPL neighbor端口是与RPL owner端口直接相连的端口。正常情况下，RPL owner端口和RPL neighbor端口都会被阻塞，以防止环路产生当ERPS环出现故障时，RPL owner端口和RPL neighbor端口都会被放开。引入RPL neighbor端口角色可以减少RPL neighbor端口所在设备刷新FDB表项的次数。
* 普通端口：在ERPS环中，除RPL owner端口和RPL neighbor端口以外的都是普通端口。普通端口负责监测自己直连的ERPS协议的链路状态，并把链路状态的变化消息及时通知其他端口。

4.ERPS实例：ERPS组网中一个环可以支持多个实例，每个实例都是一个逻辑环。每个实例中有自己的协议通道和数据通道，以及RPL owner端口、RPL neighbor端口；每个实例作为一个独立的协议实体，维护各自的状态和数据。不同环ID的报文通过目的MAC地址来区分（目的MAC地址的最后一个字节表示环ID）；具有相同环ID报文，通过其携带的VLAN ID来区分其所属的ERPS实例，即报文中的环ID和VLAN ID唯一确定一个实例。

5.端口状态：在ERPS环中，启动ERPS协议的端口状态分为两种：

* Forwarding：端口既转发用户流量又接收/发送ERPS协议报文
* Discarding：端口仅能发送和接收ERPS协议报文

6.控制VLAN：在ERPS环中，控制VLAN用来传递ERPS协议报文。控制VLAN对用户不可见，只能由系统自动决定ERPS环成员端口加入哪些控制VLAN。每个ERPS环都有自己的控制VLAN。当端口加入已经配置控制VLAN的ERPS环后，端口将自动加入控制VLAN。不同ERPS环不能使用相同ID的控制VLAN。

7.数据VLAN：与控制VLAN相对，数据VLAN用来传递数据报文。每个ERPS环都有自己的保护VLAN，保护VLAN通过配置生成树实例实现。

8.保护实例：对于运行ERPS协议的二层设备，传递ERPS协议报文和数据报文的VLAN必须映射到保护实例中，这样ERPS协议才会按照其阻塞原则对这些报文进行转发或阻塞；否则，VLAN报文可能会在成环的网络中产生广播风暴导致网络不可用。

9.定时器：ERPS协议中使用的定时器主要有Guard Timer定时器、WTR（Wait to Restore）Timer定时器、Holdoff Timer定时器和WTB（Wait to Block）Timer定时器（仅ERPSv2版本支持）。

* Guard Timer：联络故障或节点故障所涉及到的设备在故障恢复或执行清除操作后，向其他设备发送NR RAPS报文，并同时启动Guard Timer定时器，在该定时器超时前不处理NR RAPS报文，目的是防止收到过期的NR RAPS报文。如果定时器超时后还能收到其他端口发送的NR RAPS报文，则本端口的转发状态变为Forwarding状态。
* WTR Timer：RPL owner端口由于其他设备或链路故障而被放开后，当故障恢复时，有的端口可能还未由Down状态变为Up状态。为了防止立即阻塞RPL owner端口而引起网络震荡，当RPL owner端口收到某端口的NR RAPS报文后，会启动WTR Timer定时器。如果在定时器未超时前收到其他端口的SF RAPS报文，则关闭WTR Timer定时器。如果在WTR Timer定时器超时前始终没有收到其他端口的SF RAPS报文，则当WTR Timer定时器超时后，阻塞RPL owner端口，发送NRRB RAPS报文。其他端口在收到该报文后，再将自己端口的转发状态设置为Forwarding状态。
* Holdoff Timer：对于运行ERPS的二层网络，保护倒换的顺序可能会有不同的要求。例如：多层业务的应用中，服务器出现故障后，用户可能会希望能有一段时间恢复服务器的故障，而客户端感知不到，既不会立即进行保护倒换。可设置合适的Holdoff Timer定时器，当发生故障时，故障并不会立即上传ERPS，而只有当Holdoff Timer定时器超时后，如果故障仍未能恢复才会上报，从而给服务层提供修复链路的机会，避免不必要的故障上报。
* WTB Timer【FP3暂不支持】：当清除端口的手工切换状态（强制切换或手工切换）时，启用WTB Timer定时器，因为ERPS环内可能存在多个手工切换阻塞节点，只有当定时器超时后清除操作才起作用，这样可以防止立即阻塞RPL owner端口而引起阻塞点震荡。WTB Timer定时器不支持配置，该定时器的值为Guard Timer定时器的值加5s，缺省值为7s。

10.回切/非回切模式：当ERPS链路恢复正常后，可以通过设置ERPS的回切/非回切模式来决定是否从新阻塞RPL owner端口。缺省情况下，ERPS环处于回切模式。ERPSv1版本只支持回切模式，ERPSv2版本两种模式均支持。

* 回切模式：如果链路故障恢复，等待WTR时间后，会重新阻塞RPL owner端口。阻塞链路会重新切回到RPL上。
* 非回切模式：如果链路故障恢复，不启动WTR Timer定时器，而且阻塞链路还保持在原来的故障链路上，不会重新切回到RPL上。

12.阻塞点切换方式：由于RPL owner端口所在链路可能拥有更高的带宽，此时可以考虑将带宽低的链路进行阻塞，让用户流量回到RPL上进行传输。ERPS支持通过人为的配置来干预端口的阻塞，包括强制切换（Force Switch）、手工切换（Manual Switch，仅ERPSv1版本支持）和清除。

* 强制切换：配置了强制切换的端口会马上被阻塞，不管环上其他链路是否存在故障等情况
* 手工切换：如果环的状态为Idle或Pending时，配置手工切换的端口就会阻塞，否则不阻塞。
* 清除：清除本地配置的手工切换和强制切换功能；当ERPS环处于回切模式时，在WTB Timer定时器或WTR Timer定时器超时之前，手工触发回切动作；当ERPS环处于非回切模式时，手工触发回切动作。

12.子环RAPS报文传输方式【FP3暂不支持】：ERPSv2版本除了支持单环组网，还支持相交环等多环组网方式。在相交环组网中，子环RAPS报文传输方式分为虚通道VC（Virtual-Channel）和非虚通道NVC（Non-Virtual-Channel）两种方式。缺省情况下，子环RAPS报文传输方式为非虚通道方式。

* 虚通道方式：子环的RAPS协议报文会通过相交节点在主环内运行，即相交节点不终结子环的协议报文。子环的阻塞端口会同时阻塞子环的RAPS协议报文和数据流量。
* 非虚通道方式：子环的RAPS协议报文会在相交节点上终结，子环的阻塞端口仅阻塞数据流量，不阻塞子环的RAPS协议报文。

|  |  |  |
| --- | --- | --- |
| 子环RAPS报文传输方式 | 优点 | 缺点 |
| 虚通道 | 可应用于多个子环不连续的特殊组网中 | 子网的RAPS通道受相连的网络拓扑影像，需要在RAPS通道所在网络为虚通道预留资源、分配控制VLAN ID等 |
| 非虚通道 | 不需要相邻网络预留资源、分配控制VLAN ID等 | 不能应用于多个子环不连续的特殊组网中 |

**ERPS协议报文**

R-APS（Ring Automatic Protection Switching，环网自动保护倒换）报文是ERPS的协议报文。协议提供了R-APS报文级别的设置功能。节点不处理R-APS报文级别比自己大的报文。同一环上同一实例内的节点R-APS报文级别必须相同。

|  |  |
| --- | --- |
| 报文类型 | 说明 |
| (NR,RB)(No Request,RPL Block，链路恢复，RPL阻塞)报文 | 由Owner节点在Idle状态下发送，通知其它节点RPL端口被阻塞。其它节点收到(NR,RB)报文后放开自身的无故障端口，更新各自MAC地址表项。链路稳定在Idle状态下时，Owner节点周期性发送(NR,RB)报文 |
| NR(No Request，链路恢复)报文 | 当链路故障恢复后，由恢复端口所在节点发送，Owner节点收到NR报文后启动WTR定时器，在恢复端口所在节点收到(NR,RB)报文后停止发送NR报文 |
| SF(Signal Fail，信号失败)报文 | 当链路出现信号收发失败时，由故障端口所在节点发送，Owner和Neighbor节点收到SF报文后，放开各自的RPL端口。故障未消除前，故障端口所在节点周期性发送SF报文 |
| MS(Manual Switch，手工切换)报文 | 由配置MS模式的节点发送，配置MS模式的端口被阻塞，其它节点收到MS报文后放开自身无故障端口，更新各自MAC地址表项。链路在MS状态下，MS报文周期性发送 |
| FS(Forced Switch，强制切换)报文 | 由配置FS模式的节点发送，配置FS模式的端口被阻塞，其它节点收到FS报文后放开自身所有端口，更新各自MAC地址表项。链路在FS状态下，FS报文周期性发送 |
| Flush(泛洪)报文 | 如果子环拓扑有变化，互联节点以广播形式发送Flush报文通知主环刷新MAC地址表项 |

主环和子环的协议报文只能在自己的环内传输，子环上除Flush报文以外的其它协议报文在互联节点被终结；子环的数据报文可以透传至主环。

**ERPS协议状态**：ERPS定义了6种状态

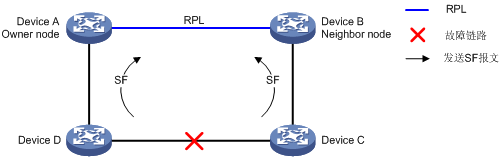
* Init状态：环端口不完整时（非互联节点的端口数量小于2或互联节点的端口数量小于1），处于Init状态
* Idle状态：环初始化过后进入到稳定状态，当Owner节点接入Idle状态后，其它节点随之进入Idle状态。其中，Owner节点和Neighbor节点的RPL端口为阻塞状态，即RPL不通；Owner节点定时发送(NR,RB)报文
* Protection状态：当环网某段链路出现故障，环路经过保护切换，最终稳定到的状态。Owner节点和Neighbor节点的RPL端口放开，即RPL放开，保证整个环网仍然是通的。当链路中某个节点进入到Protection状态后，其它节点随之进入Protection状态
* MS状态：MS状态下可以手动切换流量转发路径。当对链路中某个节点进行MS操作后，其它节点随之进入MS状态
* FS状态：FS状态下可以强制切换流量转发路径。当对链路中某个节点进行FS操作后，其它节点随之进入FS状态
* Pending状态：Pending状态是一个不稳定的状态，是各状态在进行跳转时的一个过渡状态

环路正常时，处于Idle状态；链路发生故障后，处于Protection状态。

**ERPS运行机制**

ERPS采用ITU-T G.8032/Y.1344中定义的连续性检测进行链路双向转发检测，能够定位故障点并检测故障时单向还是双向的。ERPS通过通告的消息来判断链路的状态，并作出相应的处理。ERPS的控制报文类型主要有SF和NR，如果检测到链路出现信号收发失败就发送SF消息，检测到链路恢复就发送NR消息。如果检测到链路状态变化，连续发三个报文，之后的报文每隔5s发送一次。

1.链路down告警机制：当链路中的节点发现自己任何一个属于ERPS环的端口down时，都会阻塞故障端口并立刻发送SF报文通知链路上其它节点发生了故障，其它节点在收到此报文后放开非故障阻塞端口，并刷新MAC地址表项。

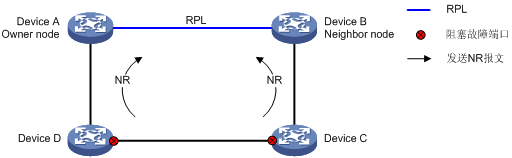


2.链路恢复机制：当故障链路恢复后，先阻塞之前处于故障状态的端口，启动Guard定时器并发送NR报文通知Owner节点故障链路已恢复。Owner节点在收到NR报文后，启动WTR定时器，如果定时器在超时前，没有收到SF报文，则当定时器超市后，Owner节点阻塞RPL端口，并向外周期性发送(NR,RB)报文；故障恢复节点在收到(NR,RB)报文后放开临时阻塞的故障恢复端口；Neighbor节点收到(NR,RB)报文后阻塞RPL端口，链路恢复。

Owner节点在链路的恢复处理中，有2种方式：

方式一：回切模式。Owner节点在故障消除收到NR报文后，会启动WTR/WTB定时器。在定时器超时之前，如果Owner节点没有收到SF报文，就切换端口状态，阻塞RPL端口，清除MAC地址表项，发送(NR,RB)报文，其它节点放开非故障的阻塞端口，清除各自MAC地址表项。定时器超时后，切换回Idle状态。

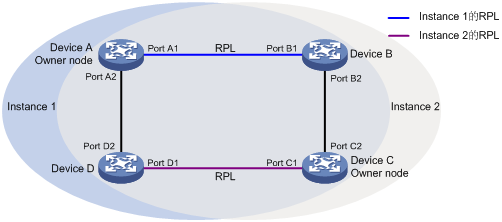
方式二：非回切模式【FP3暂不支持】。Owner收到NR报文后，不执行任何操作。



3.多实例与负载分担机制

在同一个环网中，可能同时存在多个VLAN的数据流量，ERPS可以实现流量的负载分担，即不同VLAN的流量沿不同的路径进行转发。

通过在同一个环网上配置多个ERPS实例，不同ERPS实例发送不同VLAN的流量，实现不同VLAN的数据流量在该环网中的拓扑不同，从而达到负载分担的目的。



**ERPS多实例**

在普通的配置了ERPS的组网中，一个物理环上只能配置一个ERPS环，也只能指定一个阻塞点。当ERPS环处于正常状态时，阻塞端口会阻止所有的业务数据通过。这样，所有业务数据在ERPS环上只能通过一条路径传输，阻塞端口另一侧的链路空闲，造成带宽浪费。

为了提高链路利用率，ERPS多实例支持在一个物理环路上配置两个逻辑ERPS环路。每个ERPS环上所有设备、端口角色、控制VLAN等都遵循基本的ERPS原则。相应地，一个物理环路上有两个阻塞端口，各个阻塞端口分别检测物理环路的完整性，并相应的阻塞或放开，彼此互不影响。每个ERPS环上均需要配置一个保护实例，每个保护实例代表一个VLAN范围。不同的ERPS环计算出的拓扑仅对该ERPS环有效，不影响其他ERPS环。通过给每个ERPS配置不同的保护实例，各阻塞端口只对本ERPS环所保护的VLAN有效。属于不同VLAND的数据流量就可以通过不同的路径传输，从而实现流量的负载分担和链路备份，最大化利用了链路资源。

【配置参数】

全局设置：

* ERPS：【开关】设置开启全局ERPS功能，默认关闭。
* ~~互联节点Flush透传【FP3暂不支持】：【开关】子环拓扑发生变化时，会发送Flush报文。当开启此功能后，子环的Flush报文会透传至主环中。~~

环设置：【FP3暂仅支持ERPSv1版本单环】

* ~~\*环ID：【text文本框】设置环ID，取值范围为1-8的整数，环ID具有唯一性~~
* ~~描述：【text文本框】设置环的描述说明，0-64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示~~
* ~~封装环网ID：【开关】设置ERPS协议报文的目的MAC是否封装环网ID，默认关闭。在与其他厂商设备互通时，若对方设备发送的ERPS协议报文中的目的MAC携带了环网ID，则无法实现互通，需要先开启此功能。~~
* ~~ERPS版本：【单选】设置ERPS环的版本，选项有{ERPSv1 | ERPSv2}，默认ERPSv1。~~
* ~~回切模式：【开关】当且仅当ERPS版本选择“ERPSv2”时支持配置。默认关闭。ERPSv1版本仅支持回切模式，ERPSv2支持回切和非回切模式。~~
* ~~环类型：【单选】设置此ERPS环的类型，选项有{主环|子环}，默认主环。~~
* ~~虚通道：【开关】当且仅当环类型选择“子环”时支持配置子环节点上RAPS报文的传输方式。默认关闭，即子环默认使用非虚通道方式进行RAPS报文传输。当子环的链路是不连续的多个部分时，需要采用虚通道传出方式。~~
* 控制VLAN：【text文本框】设置此ERPS环的控制VLAN，用于转发ERPS协议报文，取值范围为1-4094的整数。

注：1.控制VLAN必须是未被创建、未被其他功能模块使用且未和任何接口关联的VLAN。一旦创建，将会在[*6.7.1 VLAN/VLAN*](#_VLAN)处自动生成该VLAN。

2.同一ERPS环中的所有设备必须配置相同的控制VLAN。

~~3.不同ERPS环的控制VLAN必须不相同。~~

4.若接口已加入ERPS环，则接口将自动加入控制VLAN，[*6.7.1 VLAN/端口成员*](#_VLAN)处，Trunk接口的Trunk允许通过的VLAN将会显示此控制VLAN，Hybrid接口的Tagged VLAN将会显示此控制VLAN。

* ~~保护实例：【下拉框，单选】设置ERPS环的保护实例，选项为MST实例，默认空。~~
* ~~通知环：【多选】设置本ERPS环向其他ERPS环通告网络拓扑变化，选项为{其余的环ID|自动选择新创建的环}。当其他ERPS网络受到本ERPS环的拓扑变化消息后，会在本网络内发送Flush-FDB报文。通知本网络内的所有设备清除MAC地址，重新学习下游网络拓扑变化后的MAC地址，从而保证用户流量不中断。~~
* ~~拓扑变化保护时间间隔 (秒)：【text文本框】设置本ERPS环拓扑变化的保护时间间隔，抑制拓扑变化通告。取值范围为1-600的整数，默认2秒。~~
* ~~阈值：【text文本框】设置本ERPS环拓扑变化保护时间间隔内处理拓扑变化报文并立即刷新转发表项的阈值，取值范围为1-255的整数，默认3。~~
* 定时器：设置ERPS环的WTR定时器、Guard定时器和Holdoff定时器。
* WTR定时器 (分钟)：【text文本框】设置ERPS环的WTR定时器，取值范围为1-12的整数，默认5分钟
* Guard定时器 (厘秒)：【text文本框】设置ERPS环的Guard定时器，取值范围为1-200的整数，默认200厘秒
* Holdoff定时器 (百毫秒)：【text文本框】设置ERPS环的Holdoff定时器，取值范围为0-100的整数，默认0百毫秒。

~~环列表：~~

* ~~列表显示环ID、环描述、ERPS版本、回切模式、环类型、虚通道、控制VLAN、端口1+连接状态+角色+转发状态、端口2+连接状态+角色+转发状态、环状态~~
* ~~以环ID为索引，支持编辑~~
* ~~环类型编辑时，若从主环切换为子环，必须确保当前环中没有接口，否则需要先退出接口。~~
* 控制VLAN~~/保护实例~~编辑时，若已有接口加入ERPS环，则无法修改，必须先退出接口。
* 支持删除
* 支持基于ERPS环进行端口设置，且支持对阻塞点保护切换方式的清除操作

注：1.进行端口设置前，必须先在环上配置好控制VLAN~~和保护实例~~，否则需先将端口退出环。

2.加入ERPS环的端口必须未使能生成树功能。

3.加入ERPS环的端口类型必须为Trunk或Hybrid。

* ~~环ID：【下拉框，单选】从已有环ID中选择~~
* ~~ERPS版本：显示所选环的ERPS版本~~
* 端口1：进行端口1的端口、角色和保护切换设置
* 端口：【单选】从交换机接口中选择，包括电口、光口和聚合接口
* 角色：【下拉框】设置端口角色。环的ERPS版本为ERPSv1的选项有{RPL Owner端口|普通端口}，环的ERPS版本为ERPSv2的选项有{RPL Owner端口|RPL Neighbor端口|普通端口}，默认RPL Owner端口
* 保护切换：【下拉框】设置ERPS环中节点设备或链路故障发生或回复后，端口的保护切换机制。环的ERPS版本为ERPSv1的选项有{强制切换}，环的ERPS版本为ERPSv2的选项有{强制切换|手工切换}，默认强制切换。
* 端口2：进行端口2的端口、角色和保护切换设置
* 端口：【单选】从交换机接口中选择，包括电口、光口和聚合接口
* 角色：【下拉框】设置端口角色。环的ERPS版本为ERPSv1的选项有{RPL Owner端口|普通端口}，环的ERPS版本为ERPSv2的选项有{RPL Owner端口|RPL Neighbor端口|普通端口}，默认RPL Owner端口
* 保护切换：【下拉框】设置ERPS环中节点设备或链路故障发生或回复后，端口的保护切换机制。环的ERPS版本为ERPSv1的选项有{强制切换}，环的ERPS版本为ERPSv2的选项有{强制切换|手工切换}，默认强制切换。

注：端口1和端口2最多有且仅有1个端口可以作为RPL Owner或RPL Neighbor端口

* 支持对ERPS环执行阻塞点保护切换操作的清除功能
* ~~支持对每个ERPS环的端口和环信息进行详情查看~~

~~实例设置：~~

~~同步使用生成树MST实例，进行实例ID与VLAN的映射关系配置。~~

~~数据统计：~~

* ~~显示设备ERPS环的端口协议报文的发送和接收统计情况，包括环ID、端口、端口Tx/Rx、SF报文、NR报文、NRRB报文、FS报文、MS报文、Event事件数~~
* ~~默认显示设备所有端口数据统计，支持按照环筛选显示~~

# IP业务/IP

## VLAN接口/VLAN Interface(FP1D)

【功能概述】

不同VLAN间的主机不能直接通信，需要通过路由器或三层交换协议进行转发。设备提供VLAN接口，实现对报文的三层转发功能，从而实现设备与网络上其他设备进行通信。

VLAN接口是一种三层模式下的虚拟接口，主要用于实现VLAN间的三层互通。它不作为物理实体存在于设备上。每个VLAN对应一个IPv4和IPv6接口，通过为其配置相应的IP地址，可以作为本VLAN内各端口的网关地址，这样不同VLAN间的报文就可以通过VLAN接口在三层路由上互相转发。

GWN78XX系列交换机，所有VLAN接口的IP地址均可用于访问交换机。同时，继续支持管理VLAN功能。指定的管理VLAN，自动为交换机分配默认IP地址192.168.0.254，当设备获取到DHCP的IP时自动替换，以便访问。

接口数量规格见下表（不包含loopback接口），包括IPv4接口和IPv6接口，必须共用VLAN；一旦为IPv4创建VLAN接口，IPv6接口会自动创建成功，反之，亦然；每个VLAN接口支持MTU设置，供IPv4和IPv6双栈使用；一个VLAN接口有且仅有一个状态提示，即IPv4接口和IPv6接口共用状态显示，IPv4接口或IPv6接口任一有效（详见下方接口判断依据），状态即Up，两者均不有效则为Down。

|  |  |  |
| --- | --- | --- |
| **型号** | **芯片** | **VLAN接口数量上限** |
| GWN7801(P)/02(P)/03(P)/11(P)/12P/13(P)/21P/30/31 | RTL838X/9300 | 16 |
| GWN7806(P)/16(P)/23P/32 | RTL9310 | 32 |

【配置参数】

**（一）IPv4接口：**

* VLAN：输入VLAN ID进行IPv4接口创建，取值范围为1-4094的整数。若VLAN不存在则会自动创建VLAN以确保可以生成VLAN的IPv4接口。

注：IPv4和IPv6共用VLAN接口。若IPv4/v6接口数量尚未达到上限，支持上述创建方式；若VLAN接口数量达到上限，则仅支持直接从VLAN IPv4接口列表中选择进行配置。

* MTU：【text文本框】设置VLAN接口的MTU值，取值范围为1280-9216，默认1500。

注：此MTU为IPv4接口和IPv6接口共用。

配置IPv4地址：设置VLAN接口使用的IPv4地址。

* IPv4地址类型：设置IPv4地址的获取方式，选项有{DHCP|静态IP}，默认静态IP。
* DHCP：自动获取分配的IPv4地址及其掩码。
* 网关优先级(FP2)：【text文本框】设置DHCP获取到的网关使用优先级，取值范围为2-255的整数，默认2。取值越小，优先级越高。网关使用优先级为：静态配置的网关>设置了优先级的网关(优先级从大到小)>VLAN接口上DHCP获取到的网关（VLAN ID从小到大，先到先得）。静态配置的网关网段与任一接口网段相同，则静态配置的网关生效，否则生效网关按照网关优先级配置进行选择，若优先级相同则以VLAN ID小的网关优先生效。
* 静态IP
* \*IPv4地址：以点分十进制形式设置VLAN接口的IPv4地址，若格式错误需要报错提示“您输入的IP地址格式不正确，请重新输入”。

注：1.各VLAN接口的IPv4地址不能位于相同的子网也不能存在包含关系，即IP网段不能冲突，否则需要报错提示“IP地址网段已被使用，请重新输入”。——底层已支持，采用错误码形式上报显示

2.IP地址冲突检测，当接口IP地址与其他设备的IP地址冲突时，需要产生一条Alert等级的告警。

* 掩码：【单选】选择子网掩码的配置格式，选项有{网络掩码|前缀长度}，默认网络掩码。
* \*网络掩码：【IPv4地址格式的text输入框】支持按照IPv4地址格式点分十进制输入掩码地址。
* 前缀长度：【text文本框】设置掩码前缀长度，取值范围为8-30的整数。

注：由于交换机各个端口包括L3接口的MAC地址与设备MAC一致，导致当多个接口连在同一台上级路由器上，单靠MAC地址无法获取IP地址，此时需要使用到内置GWN模式，即获取IP的设备标识(Client ID)从MAC地址变为VLAN+MAC+Port的形式，IPv6和IPv4获取地址同理。

IPv4接口列表：

* 列表显示VLAN IPv4接口名称、状态（Up | Down）、类型(静态|动态)、IPv4地址、掩码
* 支持编辑和删除

注：1.若使用此IP地址登录，修改/删除确认时，需提示“IP地址失效，需要重新登录，确认修改？”，点击<确定>进行保存，并自动退出登录，用户需重新在浏览器输入新的IP地址进行访问。若当前仅剩下访问交换机IP地址所使用的VLAN IPv4接口这一条，则不能删除。管理VLAN这一表项始终不能删除。

2.若VLAN接口用于DHCP服务器的接口地址池/DHCP中继，则禁止编辑和删除

3.当删除VLAN接口时，其对应的所有静态和动态邻居表项也会同步删除

* 支持分页显示
* 支持按IPv4接口、状态、类型进行筛选，按VLAN和IP地址进行搜索

注：（1）系统默认有一条缺省VLAN 1（初始管理VLAN）的接口IPv4地址，可以编辑也可以删除（当且仅当存在其他IPv4接口且不作为管理VLAN时支持删除）；

（2）随着管理VLAN的设置，需要突出显示VLAN接口作为管理VLAN，在接口名称前以“\*”标识。支持为管理VLAN自动分配192.168.0.254的IP地址，当DHCP获取到IP时自动替换，以供用户访问。

（3）系统默认还存在一条loopback接口（不算在VLAN接口数量限制内）的IPv4地址信息，状态默认Up，MTU默认1500，地址信息固定，支持配置IP地址（仅支持手动配置，掩码长度支持8-30和32）。默认具体显示信息如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IPv4接口 | 状态 | MTU | 类型 | IPv4地址 | 掩码 |
| loopback | Up | 1500 | 静态 | -- | -- |
| \* VLAN1 | Up | 1500 | 静态（若接入DHCP服务器，会显示动态；具体根据实际系统上报显示） | 192.168.0.254（若接入DHCP服务器，会显示DHCP获取IP地址；具体根据实际系统上报显示） | 255.255.255.0（具体根据实际系统上报显示） |

注：loopback接口和VLAN接口状态的判断依据分别为：（IPv4和IPv6任一满足即可）

（1）loopback接口有IP地址时，状态始终为Up；若无IP地址，则始终为Down；

（2）VLAN接口状态为Up需同时满足2个条件：a.VLAN接口内的端口只要有一个Up即可；b.VLAN接口必须具有IP地址。

**（二）IPv6接口：**

* VLAN：输入VLAN ID进行IPv6接口创建，取值范围为1-4094的整数。若VLAN不存在则会自动创建VLAN以确保可以生成VLAN的IPv6接口。

注：IPv4和IPv6共用VLAN接口。若VLAN IPv4/v6接口数量尚未达到上限，支持上述创建方式；若VLAN接口数量达到上限，则仅支持直接从IPv6接口列表中选择进行设置。

* IPv6使能：【开关】设置是否使能VLAN接口的IPv6属性，默认关闭。开启后，需配置VLAN接口的MTU和IPv6地址。
* MTU：【text文本框】设置VLAN接口的MTU值，取值范围为1280-9216，默认1500。

注：此MTU为IPv4接口和IPv6接口共用。

配置IPv6地址：设置VLAN IPv6接口使用的IPv6地址，支持链路本地地址和全球单播地址。

* 链路本地地址：每个接口只能有一个链路本地地址，支持自动生成和手动配置，默认自动生成链路本地地址。
* \*IPv6地址~~/前缀~~：以冒号十六进制形式设置IPv6接口的IPv6地址，默认fe80::~~/64~~，将会根据此信息与接口标识自动生成。支持编辑，手动配置时默认为fe80::，前10bit无法编辑（由于页面以16进制输入，而前10bit是以2进制限制，故前端不做编辑限制，开放给用户配置，由底层校验进行错误提示）。~~/64，仅支持修改后64位的IPv6地址内容。~~

注：默认所有VLAN IPv6接口的链路本地地址均相同，支持修改。

* 全球单播地址：每个接口只允许有1个全球单播地址，支持手动配置静态地址、通过DHCPv6服务器（有状态DHCPv6）自动获取、无状态DHCPv6自动配置、通过无状态自动配置（SLAAC）方式生成，四者互斥。

（1）手动配置静态IPv6地址：需配置IPv6地址和前缀长度，前缀长度1-128均可配，默认64。

* \*IPv6地址/前缀长度：设置IPv6地址，按IPv6的冒号十六进制格式(IPv6地址共128bit，每16bit为一段，段之间用“:”分隔)输入IPv6地址，否则需要提示“您输入的IP地址格式错误，请重新输入”。 前缀长度的输入范围为1-128的整数，默认64。

（2）有状态DHCPv6自动获取：通过DHCPv6服务器获取IPv6地址和前缀。

（3）无状态DHCPv6自动配置：根据路由通告提供前缀、DNS等，DHCPv6仅提供其他配置信息，不分配地址，需要借助RA报文的前缀进行地址分配。

（4）无状态自动配置（SLAAC）：利用EUI-64格式形成，利用RA报文中的前缀信息结合设备MAC地址自动生成，仅支持生成前64位地址，且前缀长度固定64。

* 网关优先级(FP2)：【text文本框】当且仅当全球单播地址选择“有状态DHCPv6”“无状态DHCPv6”和“无状态自动配置”时支持配置。设置自动获取到的网关使用优先级，取值范围为2-255的整数，默认2。取值越小，优先级越高。网关使用优先级为：静态配置的网关>设置了优先级的网关(优先级从大到小)>VLAN接口上自动获取到的网关（VLAN ID从小到大，先到先得）。静态配置的网关网段与任一接口网段相同，则静态配置的网关生效，否则生效网关按照网关优先级配置进行选择，若优先级相同则以VLAN ID小的网关优先生效。
* ~~EUI-64：【开关】设置是否以EUI-64标准格式生成IPv6地址，默认关闭。无状态DHCPv6自动配置时，默认开启。~~
* ~~\*IPv6地址/前缀长度：【text文本框】以冒号十六进制形式设置IPv6接口的全球单播地址和前缀长度。EUI-64开启后，仅支持配置前64位。前缀长度默认64，不可更改。~~

注：（1）IPv6地址冲突检测：各VLAN接口的IPv6地址不能位于相同的子网也不能存在包含关系，即IPv6网段不能冲突，否则需要报错提示“IPv6地址网段已被使用，请重新输入”。——底层已支持，采用错误码形式上报显示；IP地址冲突检测，当接口IP地址与其他设备的IP地址冲突时，需要产生一条Alert等级的告警。

（2）IPv6地址不做配置如下地址：（a）环回地址~~(::1/128)~~；（b）未指定地址~~(::/128)~~；（c）组播地址；——底层已支持，采用错误码形式上报显示

（3）无状态自动配置生成的IPv6全球单播地址，每个VLAN接口均支持。~~整个设备有且仅有1个，故只允许1个接口配置此类型地址。~~

IPv6接口列表：

* 列表显示VLAN IPv6接口名称、状态（Up | Down）、全球单播地址、链路本地地址、已加入的组地址（动态生成，个数不定；交互设计上可以显示已加入的组地址个数，点击查看详细信息）
* 列表支持删除和编辑

注：1.若使用此IPv6地址登录，修改/删除确认时，需提示“IPv6地址失效，需要重新登录，确认修改？”，点击<确定>进行保存，并自动退出登录，用户需重新在浏览器输入新的IPv6地址进行访问。若当前仅剩下访问交换机IPv6地址所使用的VLAN IPv6接口这一条，则不能删除。当使用IPv4地址访问交换机时，允许删除全部VLAN IPv6接口（除loopback接口和管理VLAN IPv6接口外）。

2. 若VLAN接口用于DHCP服务器的接口地址池/DHCP中继，则禁止编辑和删除

3.当删除VLAN接口时，其对应的所有静态和动态邻居表项也会同步删除

* 列表支持分页显示
* 支持按IPv6接口、状态进行筛选，按VLAN和IPv6地址进行搜索

注：（1）系统默认存在一条loopback接口（不算在VLAN接口数量限制内）的IPv6地址信息，状态默认Up，IPv6使能默认关闭，MTU默认1500，地址信息固定，支持编辑全球单播地址和链路本地地址（均仅支持手动配置, 前缀长度支持1-128）。

（2）系统默认存在一条缺省VLAN 1（初始管理VLAN）IPv6接口，其状态Up，接口未使能故无相应IPv6地址，可以编辑也可以删除（当且仅当存在其他IPv6接口且不作为管理VLAN时支持删除）。默认具体显示信息如下：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| IPv6接口 | 状态 | 接口使能状态 | MTU | 全球单播地址 | 链路本地地址（不显示前缀长度） | 已加入的组地址 |
| loopback | Up | Disable | 1500 | -- | -- | 具体根据实际系统上报显示 |
| \* VLAN 1 | Up | Disable | 1500 | -- | -- | -- |

注：loopback接口能力默认关闭，只有当VLAN IPv6接口使能后，才会开启。

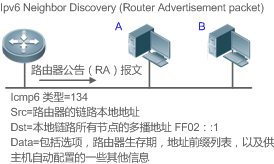
loopback接口和VLAN接口状态的判断依据分别为：（IPv4和IPv6任一满足即可）

（1）loopback接口有IP地址时，状态始终为Up；若无IP地址，则始终为Down；

（2）VLAN接口状态为Up需同时满足2个条件：a.VLAN接口内的端口只要有一个Up即可；b.VLAN接口必须具有IP地址。

**IPv6 ND RA功能：**

交换机定期发送路由器公告报文给下级设备所有节点。



路由器公告报文中通常包含如下内容：

* 一个或多个IPv6地址前缀（用于on-link确定或无状态地址自动配置）
* IPv6地址前缀的有效期
* 主机自动配置使用的方式（有状态还是无状态）
* 作为缺省设备的信息（即决定本设备是否要作为缺省设备，如果是那么还宣布自己充当缺省设备的时间）
* 提供给主机配置的一些其它信息如跳数限制、MTU、邻居请求重传间隔时间等

路由器公告报文同时也用来应答主机发出的路由器请求（RS）报文，路由器请求报文允许主机一旦启动后可以立即获得自动配置的信息而无需等待设备发出的路由器公告报文（RA）。当主机刚启动时如果没有单播地址，那么主机发出的路由器请求报文将使用未指定地址（0:0:0:0:0:0:0:0）作为请求报文的源地址，否则使用已有的单播地址作为源地址，路由器请求报文使用本地链路所有设备组播地址（FF02::2）作为目的地址。作为应答路由器请求（RS）报文的路由器公告（RA）报文将使用请求报文的源地址作为目的地址（如果源地址是未指定地址那么将使用本地链路所有节点组播地址FF02::1）。

在路由器公告报文中下列参数是可被配置的：

* Ra-interval：路由器公告报文的发送间隔
* Ra-lifetime：路由器生存期，即设备是否充当本地链路的缺省路由器以及充当该角色的时间
* Prefix：本地链路的IPv6地址前缀，用于on-link确定或无状态地址自动配置，包括前缀的其他参数配置
* Ns-interval：邻居请求报文重传的时间间隔
* Reachabletime：检测到邻居可到达事件后认为邻居时可到达的所维持的时间
* Ra-hoplimit：路由器公告（RA）报文跳数的值，用于设置主机发送单播报文的hop-limit
* Ra-mtu：路由器公告（RA）报文的MTU字段的值
* Managed-config-flag：决定了收到该路由器公告的主机是否要使用全状态自动配置来获取地址
* Other-config-flag：决定了收到该路由器公告的主机是否将使用DHCPv6来获取除IPv6地址以外的其他信息进行自动配置

【配置参数】

* VLAN接口：选择已有的VLAN接口。
* 接口使能：【开关】设置是否在接口上使能路由器公告报文的发送，默认关闭，即禁止路由器公告发送。
* 路由选项信息：【开关】设置是否在RA报文中添加路由选项信息，默认关闭。
* 时间间隔 (秒)：【text文本框】设置发送RA报文的时间间隔，取值范围为1-1800的整数，默认600秒。
* 生存时间 (秒)：【text文本框】设置RA报文的存活时间，取值范围为0-9000的整数，默认1800秒。设置为0代表下级设备不会将交换机地址更新到自己的默认路由表项中。
* 标志位：【多选】选项有{M Flag | O Flag}，默认均不选。
* M Flag：设置是否在RA报文中添加有状态自动配置地址的标志位，默认关闭，即下级主机通过无状态自动配置获取IPv6地址（通过RA报文向主机发布IPv6地址前缀信息自动生成IPv6地址）。若开启，则下级主机通过有状态自动配置获取IPv6地址。
* O Flag：设置是否在RA报文中添加有状态自动配置其他信息的标志位，默认关闭，即下级主机进行无状态自动配置（通过RA报文向主机发布除IPv6地址外的其他配置信息，包括生存时间、邻居可达时间和重传时间、链路的MTU值等）。若开启，下级主机可通过有状态自动配置获取除IPv6地址外的其他配置信息。
* IPv6地址/前缀：设置RA报文中的前缀信息，以IPv6地址/前缀长度的形式配置。IPv6地址按IPv6的冒号十六进制格式(IPv6地址共128bit，每16bit为一段，段之间用“:”分隔)输入IPv6地址，否则需要提示“您输入的IP地址格式错误，请重新输入”；前缀长度的输入范围为1-128的整数。通过IPv6地址和前缀长度固定，可以计算出RA报文携带的IPv6前缀。支持添加多个，至多8个。每个前缀需配置如下信息：
* 有效存活时间 (秒)：【text文本框】设置前缀信息的有效存活时间，用于确定前缀的on-link状态。取值范围为0-4294967295的整数，默认2592000秒。
* 首选存活时间 (秒)：【text文本框】设置前缀信息的首选存活时间，不能大于有效存活时间。取值范围为0-4294967295的整数，默认604800秒。
* 标志位：【多选】选项有{A Flag | O Flag | R Flag}，默认选中A Flag。A Flag表示配置的前缀可以用于无状态地址自动配置，A Flag标志位是RA报文前缀选项中的自治地址配置标志位；O Flag表示本链路内的主机RA报文中的前缀不是分配给本地链路的；R Flag表示主机使用路由器的全局IP地址，而不是链路本地地址。
* 默认路由优先级：【下拉框】设置RA报文中的默认路由优先级，选项有{低 | 中 | 高}，默认中。

IPv6路由通告列表：

* 列表显示VLAN接口名称、接口使能、路由选项信息、时间间隔、生存时间、标志位、前缀信息、默认路由优先级
* 支持编辑

**（三）管理VLAN**

设置VLAN接口作为交换机的管理VLAN，默认为VLAN 1。有且仅有管理VLAN具有自动为交换机分配默认IP地址192.168.0.254，当DHCP获取到IP时自动更新IP的功能，以便用户访问。

当①交换机断开与DHCP服务器的连接 或 ②无法从DHCP上获取IP 或 ③管理VLAN Down时，会自动恢复为192.168.0.254的地址，若此时与其他VLAN的IP地址有冲突，允许系统强制设置管理IPv4地址，但需进行“IP地址与其他VLAN（建议最好指明是哪个VLAN或哪些VLAN）冲突”的提示，并建议用户立即手动修改IP地址。与之同时，需辅助生成一条Warning的syslog告警提示。

* 管理VLAN：【下拉框】设置指定的VLAN作为设备管理VLAN，默认选中VLAN 1。

注：选中的管理VLAN，在IPv4接口列表和IPv6接口列表中会标记出管理VLAN（在表项的VLAN接口名称前加“\*”进行标识）。

* IPv4默认网关(FP2)：【text文本框】设置IPv4协议栈的默认网关，按照IPv4地址格式点分十进制输入
* IPv6默认网关(FP2)：【text文本框】设置IPv6协议栈的默认网关，以IPv6地址格式输入。当输入链路本地地址时，还需选择出接口（VLAN接口）

注：1.IPv4和IPv6默认网关的配置，与静态路由添加的默认路由里的下一跳地址保持一致。当设备尚未存在默认路由或仅存在DHCP的默认路由时，一旦配置了此处的默认网关，则自动生成一条下一跳地址为该网关地址的默认路由，后续若修改，则默认路由处自动同步更新；若默认路由编辑下一跳，此处的默认网关也同步更新。

2.当清空网关时，会同步删除默认路由，确定时需提示可能会托管而无法远程访问，具体为IPv4默认网关：“确定修改？IPv4网关默认为空，可能导致交换机托管而无法远程访问。”；IPv6默认网关：“确定修改？IPv6默认网关为空，可能导致交换机托管而无法通过IPv6地址进行远程访问。”

## DHCP (FP1D)

【功能概述】

**DHCP：**

动态主机配置协议DHCP是一种用于集中对用户IP地址进行动态管理和配置的技术。DHCP不仅允许计算机动态地获取IP地址，而且能够分配其他配置参数，例如客户端的启动配置文件，使客户端仅用一个消息就获取它所需要的所有配置信息。

DHCP协议采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的配置信息。DHCP可以提供两种地址分配机制，网络管理员可以根据网络需求为不同的主机选择不同的分配策略。

* 动态分配机制：通过DHCP为主机分配一个有使用期限（即租期）的IP地址
* 静态分配机制：网络管理员通过DHCP为指定的主机分配固定的IP地址

DHCP组网中，主要包括以下三个概念：

* DHCP服务器：负责从地址池中选择IP地址分配至DHCP客户端，还可以为DHCP客户端提供其他网络参数，如默认网关地址、DNS服务器地址和WINS服务器地址。DHCP服务器可以接收处理来自本网段或跨网段由DHCP中继转发的DHCP请求报文。
* DHCP客户端：发送DHCP请求报文、通过BOOTP或DHCP协议请求获取IP地址等网络参数的设备。
* DHCP中继：负责转发DHCP服务器和DHCP客户端之间的DHCP报文，协助DHCP服务器向DHCP客户端动态分配网络参数的设备。

DHCP客户端广播发送请求报文（即目的IP地址为255.255.255.255），位于同一网段内的DHCP服务器能够接收请求报文。如果DHCP客户端和DHCP服务器不在同一网段，DHCP服务器无法接收来自客户端的请求报文，此时，需要通过DHCP中继来转发DHCP报文。不同于传统的IP报文转发，DHCP中继接收到DHCP请求或应答报文后，会重新修改报文格式并生成一个新的DHCP报文再进行转发。

**DHCP租期：**DHCP服务器给每个分配给客户端的IP地址定义一个使用期限，该使用期限被称为租期。在租期到期前，DHCP客户端如果仍需要使用该IP地址，可以请求延长租期；如果不需要，可以主动释放该IP地址。在没有其他空闲地址可用的情况下，DHCP服务器会把客户端主动释放的IP地址重新分配给其他客户端。

DHCP服务器动态分配的所有IP地址都受租期时长的限制，不同的DHCP服务器配置的租期时长可以不同。静态分配的IP地址不受租期时长的限制，使用期限为无限长。

DHCP客户端不会等到租期到期后再申请IP地址，这样会导致IP地址被服务器回收，然后分配给其他客户端。为保证能够使用原来的IP地址，客户端会在租期到期前的某个时间点就开始申请延长租期。

**DHCP地址池：**DHCP服务器可以为客户端分配的所有IP地址的集合。除IP地址外，地址池内还可以配置租期、子网掩码、默认网关等网络参数。在DHCP服务器为客户端分配IP地址时，这些网络参数也一并分配给客户端。根据创建方式的不同，地址池可以分为基于接口方式的地址池和基于全局方式的地址池。

* 基于接口方式的地址池：在DHCP服务器与客户端相连的接口上配置IP地址，地址池是跟此接口地址所属同一网段的IP地址，且地址池中地址只能分配给此接口下的客户端。
* 基于全局方式的地址池：在全局创建指定网段的地址池，且地址池中地址可以分配给设备所有接口下的客户端。当DHCP服务器与客户端不在同一网段时，需要部署DHCP中继。

DHCP服务器依据是否部署DHCP中继来选择地址池。无DHCP中继场景下，DHCP服务器选择与接收DHCP请求报文的接口IP地址处于同一网段的地址池。有DHCP中继场景下，DHCP服务器选择与DHCP请求报文中giaddr字段（标识客户端所在网段）位于同一网段的地址池。

根据客户端的数量和接入断开的时间、频率来确定地址池内需要部署的IP地址数量。根据IP地址的使用情况，地址池内的IP地址可以分为多种状态，包括：

* Used：此IP地址已使用
* Idle：此IP地址处于空闲状态
* Static-bind：此IP地址已绑定MAC地址且未使用
* Static-bind used：此IP地址与MAC地址绑定且已使用
* Disable：此IP地址无法使用
* Expired：此IP地址租期已过，处于空闲状态。地址池中IP地址到期后是Expired状态。地址池内保留Expired状态IP地址的分配记录，目的是当用户重新关联请求IP地址时，分配原来使用过的IP地址给用户，保持用户IP地址的稳定性。当地址池中Idle状态的IP地址耗尽时，地址池内会自动回收Expired状态的IP地址，然后分配给新用户，无需手动清理。
* Conflict：此IP地址与网络上其他地址冲突。当地址池中Idle状态和Expired状态的IP地址耗尽时，地址池会自动回收Conflict状态的IP地址，然后分配给其他用户，无需手动清理。

**DHCPv6：**

DHCPv6是针对IPv6编址方案设计，与其他IPv6地址分配方式（手工配置、通过路由器通告消息中的网络前缀无状态自动配置）相比，具有如下特点：（1）更好地控制IPv6地址的分配，DHCPv6方式不仅可以记录为IPv6主机分配的地址，还可以为特定的IPv6主机分配特定的地址，以便于网络管理；（2）支持为网络设备分配IPv6前缀，便于全网络的自动配置和网络层次性管理；（3）除了为IPv6主机分配IPv6地址/前缀外，还可以分配DNS服务器IPv6地址等网络配置参数。

DHCPv6是一种运行在客户端和服务器之间的协议，与DHCP一样，所有的协议报文都是基于UDP的。但是由于在IPv6中没有广播报文，因此DHCPv6使用组播报文，客户端也无需配置服务器的IPv6地址。

**IPv6地址分配类型：**

* 手动配置：手动配置IPv6地址/前缀及其他网络配置参数（DNS、NIS、SNTP服务器地址等参数）。
* 无状态自动地址分配：由接口ID生成链路本地地址，再根据路由通告报文RA包含的前缀信息自动配置本机地址。
* 有状态自动地址分配：即DHCPv6方式。DHCPv6又分为两种：
* DHCPv6有状态自动分配。DHCPv6服务器自动分配IPv6地址/PD前缀及其他网络配置参数（DNS、NIS、SNTP服务器地址等参数）
* DHCPv6无状态自动分配。主机IPv6地址仍然通过路由通告方式自动生成，DHCPv6服务器只分配除IPv6地址以外的配置参数，包括DNS、NIS、SNTP服务器等参数

DHCPv6基本协议架构中，主要包括以下三种角色：

* DHCPv6客户端，通过与DHCPv6服务器进行交互，获取IPv6地址/前缀和网络配置信息，完成自身的地址配置功能。
* DHCPv6中继代理，负责转发来自客户端方向或服务器方向的DHCPv6报文，协助DHCPv6客户端和DHCPv6服务器完成地址配置功能。一般情况下，DHCPv6客户端通过本地链路范围的组播地址与DHCPv6服务器通信，以获取IPv6地址/前缀和其他网络配置参数。如果服务器和客户端不在同一个链路范围内，则需要通过DHCPv6中继代理来转发报文，这样可以避免在每个链路范围内都部署DHCPv6服务器，既节省了成本，又便于进行集中管理。
* DHCPv6服务器，负责处理来自客户端或中继代理的地址分配、地址续租、地址释放等请求，为客户端分配IPv6地址/前缀和其他网络配置信息。

**DHCPv6基本概念：**

* 组播地址
* 在DHCPv6协议中，客户端不用配置DHCPv6 server的IPv6地址，而是发送目的地址为组播地址的Solicit报文来定位DHCPv6服务器。
* 在DHCP协议中，客户端发送广播报文来定位服务器。为避免广播风暴，在IPv6中，已经没有了广播类型的报文，而是采用组播报文。在DHCPv6用到的组播地址有两个：（1）FF02::1:2(All DHPC Reay Agents and Servers)，所有DHCPv6服务器和中继代理的组播地址，这个地址是链路范围的，用于客户端和相邻的服务器及中继代理之间通信；（2）FF05::1:3(All DHCP Servers)，所有DHCPv6服务器组播地址，这个地址是站点范围的，用于中继代理和服务器之间的通信，站点内的所有DHCPv6服务器都是此组的成员。
* UDP端口号：DHCPv6报文承载在UDPv6上，客户端侦听的目的端口号是546，服务器和中继代理侦听的端口号是547。
* DHCP唯一标识符（DUID）：每个服务器或客户端有且只有一个唯一标识符，服务器使用DUID来识别不同的客户端，客户端则使用DUID来识别服务器。客户端和服务器DUID的内容分别通过DHCPv6报文中的Client Identifier和Server Identifier选项来携带。两种选项的格式一样，通过option-code字段的取值来区分是Client Identifier还是Server Identifier选项。
* 身份联盟（IA）：使服务器和客户端能够识别、分组和管理一系列相关IPv6地址的结构。每个IA包括一个IAID和相关联的配置信息。客户端必须为它的每一个要通过服务器获取IPv6地址的接口关联至少一个IA。客户端用给接口关联的IA来从服务器获取配置信息，每个IA必须明确关联到一个接口。IA的身份由IAID唯一确定，同一个客户端的IAID不能重复出现，IAID不应因设备重启等因素而发生丢失或改变。IA中的配置信息由一个或多个IPv6地址以及T1和T2生存期组成，IA中的每个地址都有首选生存期和有效生存期。一个接口至少关联一个IA，一个IA可以包含一个或多个地址信息。

**DHCPv6 PD工作原理：**DHCPv6 PD是一种前缀分配机制，下游网络设备不需要再手工指定用户侧链路的IPv6地址前缀，只需要向上游网络设备提出前缀分配申请，上游网络设备便可以分配合适的地址前缀给下游设备，下游设备把获得的前缀（一般前缀长度小于64）进一步自动细分成64前缀长度的子网网段，把细分的地址前缀再通过路由通告（RA）至与IPv6主机直连的用户链路上，实现IPv6主机的地址自动配置，完成整个系统层次的地址布局。

**DHCPv6中继工作原理：**

* DHCPv6客户端向所有DHCPv6服务器和DHCPv6中继发送目的地址为FF02::1:2（组播地址）的请求报文。
* 根据DHCPv6中继转发报文有如下两种情况：
* 如果DHCPv6中继和DHCPv6客户端位于同一个链路上，即DHCPv6中继为DHCPv6客户端的第一跳中继，中继转发直接来自客户端的报文，此时DHCPv6中继实质上也是客户端的IPv6网关设备。DHCPv6中继收到客户端的报文后，将其封装在Relay-Forward报文的中继消息选项（Relay Message Option）中，并将Relay-Forward报文发送给DHCPv6服务器或下一跳中继。
* 如果DHCPv6中继和DHCPv6客户端不在同一个链路上，中继收到的报文是来自其他中继的Relay-Forward报文。中继构造一个新的Relay-Forward报文，并将Relay-Forward报文发送给DHCPv6服务器或下一跳中继。
* DHCPv6服务器从Relay-Forward报文中解析出DHCPv6客户端的请求，为DHCOv6客户端选取IPv6地址和其他配置参数，构造应答消息，将应答消息封装在Relay-Reply报文的中继消息选项中，并将Relay-Reply报文发送给DHCPv6中继。
* DHCPv6中继从Relay-Reply报文中解析出DHCPv6服务器的应答，转发给DHCPv6客户端。如果DHCPv6客户端接收到多个DHCPv6服务器的应答，则根据报文中的服务器优先级选择一个DHCPv6服务器，后续从该DHCPv6服务器获取IPv6地址和其他网络配置参数。

**IPv6地址/前缀的分配与更新原则**

IPv6地址分配的优先次序：

* 选择IPv6地址池：DHCPv6服务器的接口可以绑定IPv6地址池，DHCPv6服务器将选择该IPv6地址池为接口下的DHCPv6客户端分配地址/前缀。对于存在中继的场景，DHCPv6服务器的接口可以不绑定IPv6地址池，而是根据报文中第一个不为0的“link-address”字段（标识DHCPv6客户端所在链路范围），选择与地址池中已配置的网络前缀或IPv6地址前缀属于统一链路范围的地址池。
* 选择IPv6地址/前缀：确定地址池后，DHCPv6服务器将按照下面部照为DHCPv6客户端分配IPv6地址/前缀。
* 如果地址池中为客户端指定了地址/前缀，优先从地址池中选择与客户端DUID匹配的地址/前缀分配给客户端。
* 如果客户端报文中的IA选项携带了有效的地址/前缀，优先从地址池中选择该地址/前缀分配给客户端。如果该地址/前缀在地址池中不可用，则另外分配一个空闲地址/前缀给客户端。如果IPv6前缀长度比指定分配长度达，则按指定分配长度来分配。
* 从地址池中选择空闲地址/前缀分配给客户端，保留地址、冲突地址和已被分配的地址不能再分配给客户端。其中，保留地址包括未指定地址、组播地址、环回地址、链路本地地址、NSAP和任播地址等。
* 如果没有合适的IPv6地址/前缀可以分配，则分配失败。

DHCPv6地址租约更新：DHCPv6服务器为DHCPv6客户端分配的地址是有租约的，租约由生命期（包括地址的首选生命期和有效生命期构成）和续租时间点（IA的T1、T2）构成。地址有效生命期结束后，DHCPv6客户端不能再使用该地址。在有效生命期到达之前，如果DHCPv6客户端希望继续使用该地址，则需要更新地址租约。DHCPv6客户端为了延长其与IA关联的地址的有效生命期和首选生命期。在T1时刻，发送包含IA先选挂的Renew报文给服务器，其中IA选项中携带需要续租的IA地址选项。如果DHCPv6客户端一直没有收到T1时刻续租报文的回应报文，那么在T2时刻，DHCPv6客户端通过Rebind报文向DHCPv6服务器继续续租地址。

IP地址预留：DHCPv6服务器支持预留IPv6地址，即保留部分IPv6地址不参与动态分配，比如预留的IPv6地址可作为DNS服务器的IPv6地址。

### DHCP服务器/DHCP Server

GWN78XX交换机要求支持：

DHCP服务器功能支持如下功能：

* 为网络中的多个VLAN指定特定的地址池，实现不同VLAN的设备获得不同网段的IP地址。
* 当客户端向交换机申请IP地址时，交换机判断接收请求报文的端口所属的默认VLAN，从该VLAN接口IP所属的地址池中选取合适的地址分配给客户端。
* 如果服务器和客户端之间搭建了DHCP中继设备，DHCP请求报文经过DHCP中继设备时报文中的giaddr字段将被填入中继设备上客户端连接的接口IP地址，服务器将在此IP网段地址池中选择合适的IP地址分配给客户端。如果DHCP服务器上没有创建中继设备IP地址段的地址池，客户端将无法获得IP地址。
* IP地址重复分配检测功能，避免因同一地址重复分配而造成的网络中IP冲突。采用免费ARP进行检测。

分配IP地址的优先次序：

* DHCP服务器中与客户端MAC地址手动绑定的IP地址
* DHCP服务器曾经分配给客户端的IP地址
* 客户端发送的DHCP-DISCOVER报文中指定的IP地址
* 选择合适的地址池，从中顺序查找可供分配的第一个IP地址

DHCP服务器在交换机上的配置要点：

* ~~为每个网段保留特定的IP地址不做分配，如网关地址、网段广播地址、服务器地址等~~
* 支持全局地址池和接口地址池，接口地址池用于交换机直接分配给其下级客户端IP地址，全局地址池支持用于提供给中继服务器进行IP地址分配使用。~~当接口地址池分配完后，可以使用全局地址池给接口下的客户端分配IP地址。~~
* 为特殊用户群手动绑定静态IP，当收到特殊用户群的IP申请时，交换机将为客户端分配租期为无限长的固定IP地址
* 创建动态分配地址池，网络中的设备申请IP地址时，可以获得相应接口地址池中的空闲地址

DHCPv6服务器在交换机上的配置要点：

* ~~为每个网段保留特定的IPv6地址不做分配，如网关地址、组播地址、服务器地址等~~
* 为特殊用户群手动绑定静态IPv6，当收到特殊用户群的IPv6申请时，交换机将为客户端分配租期为无限长的固定IPv6地址
* 创建动态分配地址池，网络中的设备申请IPv6地址时，可以获得相应接口地址池中的空闲地址

FP1阶段暂不支持DHCPv6 Server功能。

【配置参数】

**（一）DHCP：**

**全局设置：**

* DHCP服务：【开关】设置是否开启全局DHCP服务，默认关闭。

**地址池设置：**

添加：至多添加128个

* 地址池类型：【单选】设置DHCP地址池类型，选项有{全局地址池 | 接口地址池}。
* \*地址池名称：【text文本框】设置DHCP服务器地址池名称，名称唯一，最多输入64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示

当地址池类型为“全局地址池”时：

* IP地址池子网地址：【text文本框】设置全局地址池可分配的网段地址。
* 子网掩码：【text文本框】设置分配给DHCP客户端的IP地址的子网掩码。
* 网关地址：【text文本框】设置全局地址池的出口网关地址。可添加多个，至多8个。

当地址池类型为“接口地址池”时：

* 接口：【下拉框】从已有的VLAN IPv4接口（仅支持静态IP配置的VLAN接口）中选择，以VLAN IPv4接口名称为基准显示，并以接口IPv4地址和子网掩码作为DHCP客户端的网关地址和子网掩码。

注：一旦使用静态IP的VLAN接口创建接口地址池或中继服务器后，VLAN接口处禁止编辑和删除

* \*地址池：【IP地址范围】设置动态分配的IP地址范围，包括开始地址和结束地址。其中，可配置的地址网段以VLAN IPv4接口内的网段为准，必须在VLAN IPv4接口的网段内，否则需报错提示“输入的IP网段不合法，请重新输入”。
* \*租期 (分钟)：【text文本框】设置地址池中分配的IP地址使用有效期，取值为60-2880的整数，默认120分钟。
* DNS服务器：【text文本框】设置此地址池的DNS服务器地址，使DHCP客户端能够通过域名访问Internet上的主机。默认使用VLAN接口IP地址作为DNS服务器。可添加多个，至多8个
* WINS服务器：【text文本框】设置配给客户端的WINS服务器地址，实现DHCP客户端主机名到IP地址的解析。可添加多个，至多8个。
* Netbios节点类型：【下拉框】设置DHCP客户端在网络上使用NetBIOS协议通信时，需要在主机名和IP地址之间建立映射关系。根据获取映射关系方式的不同，NetBIOS节点分为4种，选项为{b类节点（广播模式节点） | p类节点（混合h模式节点） | m类节点（混合m模式节点） | h类节点（端到端模式节点）}，默认为空。
* DHCP选项：主要包含三类，分别如下：DHCP选项支持添加多个，至多8个，Option43可以根据业务不同添加多个，除Option43外的option均只能添加一个
* DHCP选项：【text文本框】设置DHCP选项，取值为2-254的整数，不包括50-54,56,58,59,61和82。
* 类型：【下拉框】设置选项内容的类型，有{十六进制数串 | ASCII字符串 | IP地址}，默认十六进制数串。
* 业务：【下拉框】当且仅当DHCP选项为43 且 类型为ASCII时，需支持GS的业务，包括VoIP线和数通平台线，业务支持具体详见下方表格，默认自定义

|  |  |
| --- | --- |
| **子选项** | **业务** |
| / | 自定义 |
| 1 | ACS URL |
| 2 | ProvisioningCode |
| 66 | 固件服务器升级路径 |
| 132 | VLAN ID |
| 133 | VLAN 优先级 |
| 223 | Manager服务器地址(Switch/Router) |
| 224 | Manager服务器地址(AP) |
| 245 | AP的管理VLAN |
| 256 | 路由器的AP模式 |

* 选项内容：【text文本框】 根据类型，选项内容设置有不同的要求。
  + - 当类型为“十六进制数串”时，选项内容为0-256个字符，且位数必须为偶数
    - 当类型为“ASCII字符串”时，选项内容为0-255个字符串
    - 当类型为“IP地址”时，选项内容为IP地址，需满足IPv4地址格式要求，否则报错提示。至多输入8个

列表：

* 列表显示地址池名称、地址池类型、VLAN IPv4接口（仅接口地址池显示，否则为--）、子网地址/掩码(全局地址池)或地址池(接口地址池)
* 支持编辑，以地址池类型和名称为索引
* 支持删除
* 支持分页

**绑定表：**显示已分配的IP地址

添加静态绑定IP：至多添加2048个

* 地址池名称：【下拉框】从已有的地址池中选择某一个作为客户端IP绑定的来源。
* IPv4地址：【text文本框】设置在地址池内的某个IPv4地址作为某一客户端指定的IPv4地址。输入需满足IPv4地址格式，否则报错提示；若不在地址池范围内，也需报错提示。
* 客户端名称：【text文本框】设置客户端的名称，最长64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示
* 客户端MAC地址：【text文本框】设置客户端的MAC地址，输入格式为HH:HH:HH:HH:HH:HH(其中，H为1-2位的十六进制数)，形如00:10:DC:28:A4:E9
* 硬件地址类型：【下拉框】设置客户端的硬件地址类型，选项有{Ethernet II | IEEE 802.3}，默认Ethernet II。
* 客户端ID：【text文本框】设置绑定的客户端ID，以十六进制格式输入，4-200字符且必须为偶数个

列表：

* 列表显示客户端名称/MAC地址、IP地址、类型（动态|静态）、剩余租约有效期（仅动态有）
* 支持编辑静态IP绑定表项，只允许修改地址池名称、IPv4地址和客户端名称
* 支持删除静态IP绑定表项
* 支持一键绑定动态IP表项为静态表项
* 支持分页
* 支持刷新
* 支持按IP地址、客户端名称、客户端MAC地址进行搜索匹配

**（二）DHCPv6**【FP1暂不支持】

**全局配置：**

DHCPv6：

* DHCPv6服务：【开关】设置是否开启全局DHCPv6服务，默认关闭。
* DUID：【下拉框】设置DHCPv6服务器的DUID，选项有{ ll | llt }，默认设备以ll方式自动生成DUID，并要求显示实际的DUID值。

**IPv6 PD地址池：**至多添加256个

* PD地址池名称：【text文本框】设置IPv6 PD地址池名称，名称唯一，最多输入64字符，允许输入的字符有数字0-9、字母a-z/A-Z和特殊字符.\_@ 和空格（仅允许空格在字符中间）
* 地址前缀/前缀长度：【text文本框】设置IPv6 PD地址池前缀和前缀长度，前缀长度最大63，根据前缀与前缀长度相匹配原则进行修改。
* 有效生存期/Valid Lifetime (秒)：【text文本框】设置前缀的有效生存期，取值为60-4294967295的整数。
* 首选生存期/Preferred Lifetime (秒)：【text文本框】设置前缀的首选生存期，取值为60-4294967295的整数

PD地址池列表：

* 列表显示PD地址池名称、地址前缀/前缀长度、有效生存期、首选生存期
* 支持编辑，以PD地址池名称为索引
* 支持删除
* 支持分页

**DHCPv6地址池设置：**

添加DHCPv6地址池：至多添加256个

* \*地址池名称：【text文本框】设置DHCP服务器地址池名称，名称唯一，最多输入64字符，允许输入的字符有数字0-9、字母a-z/A-Z和特殊字符.\_@ 和空格（仅允许空格在字符中间）
* IPv6地址分配方式：【下拉框】设置客户端IPv6地址分配方式，选项有{无状态DHCPv6 | 有状态DHCPv6}，默认有状态DHCPv6。有状态DHCPv6除了分配IPv6地址外，还分配前缀和其他网络配置参数，而无状态DHCPv6仅分配IPv6地址，其余的需通过路由通告来自动生成。
* 前缀/前缀长度：【下拉框】从已有的IPv6 PD地址池中选择，以PD地址池名称为基准显示，选择后在下方显示指定PD地址池相应的前缀/前缀长度（不可编辑）。
* DNS服务器：【text文本框】设置此地址池的DNS服务器地址，使DHCPv6客户端能够通过域名访问Internet上的主机。默认使用VLAN接口IPv6地址作为DNS服务器。可添加多个，至多8个
* SIP服务器：【text文本框】设置DHCPv6服务器为客户端分配的SIP服务器地址。可添加多个，至多8个
* NIS服务器：【text文本框】设置DHCPv6服务器为客户端分配的NIS服务器地址。可添加多个，至多8个
* NISP服务器：【text文本框】设置DHCPv6服务器为客户端分配的NISP服务器地址。可添加多个，至多8个
* SNTP服务器：【text文本框】设置DHCPv6为客户端分配的SNTP服务器地址。可添加多个，至多8个

DHCPv6地址池列表：

* 列表显示地址池名称、地址前缀/前缀长度
* 支持编辑
* 支持删除
* 支持分页

**绑定表：**显示已分配的IPv6地址

添加静态绑定IPv6：至多添加2048个

* 地址池名称：【下拉框】从已有的地址池中选择某一个作为客户端IPv6绑定的来源。
* IPv6地址前缀/前缀长度：【text文本框】显示地址池内IPv6地址前缀/前缀长度。支持编辑，前缀长度最大64，根据前缀与前缀长度相匹配原则进行修改，且需判断修改是否有效，否则均需报错。

注：从地址池内继承的前缀固定不能修改。

* 客户端名称：【text文本框】设置客户端的名称，最长64字符，允许输入的字符有数字0-9、字母a-z/A-Z和特殊字符.\_@- 和空格（仅允许空格在字符中间）
* 客户端MAC地址：【text文本框】设置客户端的MAC地址，输入格式为HH:HH:HH:HH:HH:HH(其中，H为1-2位的十六进制数)，形如00:10:DC:28:A4:E9
* 硬件地址类型：【下拉框】设置客户端的硬件地址类型，选项有{Ethernet | IEEE802}，默认Ethernet。
* 客户端DUID：【text文本框】设置绑定的客户端DUID，以十六进制格式输入，4-200字符且必须为偶数个

列表：

* 列表显示客户端名称、IPv6地址/前缀长度、类型（动态|静态）、剩余租约有效期（仅动态有）
* 支持编辑静态IPv6绑定表项
* 支持删除静态IPv6绑定表项
* 支持一键绑定动态IPv6表项为静态表项
* 支持分页
* 支持刷新
* 支持按IPv6地址、客户端名称进行搜索匹配

### DHCP中继/DHCP Relay

设备作为DHCP中继时，需要配置DHCP中继代理的DHCP服务器的IP地址，以实现中继转发DHCP客户端和服务器之间的DHCP报文。配置DHCP服务器的IP地址方法有两种：（1）在接口下配置；（2）在DHCP服务器组下配置。

配置DHCPv6中继功能时，一般支持两种配置方式：

（1）直接在接口上配置DHCPv6服务器或下一跳中继的IPv6地址：适用于DHCPv6中继对端连接一个DHCPv6服务器或下一跳中继的场景。

（2）在接口上绑定DHCPv6服务器组：先在全局创建DHCPv6服务器组，可以配置向DHCPv6服务器组添加多个DHCPv6服务器或下一跳中继的IPv6地址，然后在接口上配置DHCPv6中继所对应的DHCPv6服务器组，适用于DHCPv6中继对端连接多个DHCPv6服务器组或下一跳中继的场景，从而实现DHCPv6中继对DHCPv6服务器或下一跳中继的灵活选择和统一管理。

DHCPv6客户端和DHCPv6服务器之间可以连接多个DHCPv6中继，当设备作为DHCPv6中继时，如果对端连接的是DHCPv6服务器，使能DHCPv6中继是需要指定DHCPv6服务器的IPv6地址；如果对端连接的是下一跳中继，则需要指定下一跳中继的IPv6地址，并在下一跳中继上指定对端DHCPv6服务器或下一跳中继的IPv6地址。

GWN78xx系列支持在接口下配置。

注：若在同一VLAN接口上同时开启了DHCP服务和DHCP中继，优先处理本地DHCP 服务器（接口地址池）的流程，即优先使用本地DHCP服务器（接口地址池）分配IP地址。当本地服务器无法分配IP地址时，再通过DHCP中继使用远程服务器分配IP地址。

【配置参数】

**（一）DHCP中继**

**全局配置：**

前提：开启DHCP中继功能之前，需开启DHCP功能。

* DHCP中继：【开关】设置是否开启全局DHCP中继功能，默认关闭。
* 轮询：【开关】设置是否开启DHCP中继的轮询功能，默认关闭。
* TTL：【text文本框】设置DHCP请求报文在经过DHCP中继三层转发之后的TTL值，取值为1-16的整数，默认4。

**DHCP服务器：**

添加：至多添加256个

* 接口：【下拉框】从已有的VLAN接口（仅支持静态IP配置的VLAN接口）中选择，以VLAN接口名称为基准显示。

注：一旦使用静态IP的VLAN接口创建接口地址池或中继服务器后，VLAN接口处禁止编辑和删除

* DHCP服务器地址：【text文本框】设置DHCP服务器的地址，需满足IPv4地址格式，否则报错提示。支持添加多个，最多10个

注：DHCP服务器地址不能是DHCP中继网关的接口IP地址，否则会导致DHCP客户端无法获取IP地址。

DHCP服务器列表：

* 列表显示接口、DHCP服务器地址
* 支持编辑，以接口为索引
* 支持删除
* 支持分页

**（二）DHCPv6中继**【FP1暂不支持】

* DHCPv6中继：【开关】设置是否开启全局DHCPv6中继功能，默认关闭。
* DHCPv6服务器：
* DHCPv6中继：【开关】设置是否开启接口的DHCPv6中继功能，默认关闭。
* IPv6地址：【text文本框】设置DHCPv6服务器或下一跳中继的IPv6地址。设备通过查找路由将中级报文发送此IPv6地址。需满足IPv6地址格式，否则报错提示。支持添加多个，至多8个。

## ARP表/ARP Table (FP1D)

【功能概述】

地址解析协议ARP是用来将IP地址解析为MAC地址的协议。在局域网中，当主机或其它三层网络设备有数据要发送给另一台主机或三层网络设备时，需要知道对方的网络层地址（即IP地址）。因为IP地址必须封装成帧才能通过物理网络发送，因此发送方还需要知道接收方的实际物理地址（即MAC地址），这就需要一个从IP到MAC地址的映射。ARP即实现将IP地址解析为MAC地址。主机或三层网络设备上会维护一张ARP表，存储IP地址与MAC地址的关系。

ARP表项包括动态ARP表项和静态ARP表项。

**动态ARP表项：**由ARP协议通过ARP报文自动生成和维护，可以被老化，可以被新的ARP报文更新，可以被静态ARP表项覆盖。当到达老化时间、接口down时，设备会立即删除响应的动态ARP表项。

**静态ARP表项：**由网络管理员手工建立的IP地址和MAC地址之间固定的映射关系，不会被老化，不会被动态ARP表项覆盖，可以保证网络通信的安全性。静态ARP表项可以限制本端设备和指定IP地址的对端设备通信时只使用指定的MAC地址，此时攻击报文无法修改本端设备的ARP表中IP地址和MAC地址的映射关系，从而保护了本端设备和对端设备间的正常通信。可以分为短静态ARP表项和长静态ARP表项。

短静态ARP表项：手工建立IP地址和MAC地址之间固定的映射关系，未同时指定VLAN和出接口。如果出接口是处于二层模式的以太网接口，短静态ARP表项不能直接用于报文转发。当需要发送报文时，设备会先发送ARP请求报文，如果收到的ARP应答报文中的源IP地址和源MAC地址与所配置的IP地址和MAC地址相同，则将收到ARP应答报文的VLAN和接口加入该静态ARP表项中，后续设备可以直接用该静态ARP表项转发报文。

长静态ARP表项【GWN78XX不支持】：手工建立IP地址和MAC地址之间固定的映射关系，并同时制定该ARP表项所在VLAN和出接口。长静态ARP表项可以直接用于报文转发。

**免费ARP：**设备主动使用自己的IP地址作为目的IP地址发送ARP请求。其有如下作用：

* IP地址冲突检测：当设备接口的协议状态变为Up时，设备主动对外发送免费ARP报文。正常情况下不会受到ARP应答，如果收到，则表明本网络中存在与自身IP地址重复的地址。如果检测到IP地址冲突，设备会周期性地广播发送免费ARP应答报文，直到冲突解除。
* 用于通告一个新的MAC地址：发送方更换了网卡，MAC地址变化了，为了能够在动态ARP表项老化前通告网络中其他设备，发送方可以发送一个免费ARP。

设备收到免费ARP报文后，

* 如果未使能ARP表项严格学习功能，设备会进行ARP学习；
* 如果使能了ARP表项严格学习功能，则进行如下判断：
* 如果免费ARP报文中源IP地址和自己的IP地址相同，则周期性地广播发送免费ARP应答报文，告知此IP地址在网络中存在冲突，直到冲突解除
* 如果免费ARP报文中源IP地址和自己的IP地址不同，免费ARP报文是在VLAn接口收到的，并且设备上已经有免费ARP报文中源IP地址对应的动态ARP表项，则进行ARP学习，即根据收到的免费ARP报文更新该ARP表项，其余情况收到免费ARP报文后均不进行ARP学习。

**ARP动态学习组播MAC：**默认情况下，设备收到源MAC地址为组播MAC地址的ARP报文时，不会进行ARP学习。

各型号设备ARP数量上限具体如下：(ARP与NDP，邻居表共用)

|  |  |  |
| --- | --- | --- |
| **型号** | **芯片** | **ARP数量上限** |
| GWN7801(P)/02(P)/03(P) | RTL83XX | 256 |
| GWN7806(P)/11(P)/12P/13(P)/21P/30/31/16(P)/23P/32 | RTL9300/9310 | 1024 |

【配置参数】

**全局配置：**

* 老化时间 (秒)：【text文本框】设置动态ARP表项的老化时间。到达老化时间后，动态ARP表项自动删除。取值范围为60-21600的整数，默认1200秒。

注：与邻居发现的老化时间为同一配置。

添加静态ARP表项：

* VLAN：【下拉框，单选】从已有的VLAN接口中选择。
* \*IP地址：【text文本框】设置静态ARP表项的IPv4地址，需要与VLAN接口的IPv4地址同网段，也需要满足IPv4地址格式，否则报错提示。
* \*MAC地址：【text文本框】设置静态ARP表项的MAC地址，只能输入单播MAC地址，否则报错提示。

注：若VLAN和IPv4地址相同，MAC地址不同，则直接覆盖处理，即修改ARP的映射关系。

ARP表：当删除VLAN接口时，其对应的所有静态和动态邻居表项也会同步删除

* 列表显示VLAN、IP地址、MAC地址、接口（交换机逻辑接口，包括电口、光口和聚合接口，泛洪显示“--”）、类型（静态|动态）、老化时间（只有动态有）
* 支持编辑静态ARP表项，仅MAC地址可修改
* 支持一键将动态ARP表项保存为静态ARP表项
* 支持删除静态ARP表项
* ~~支持一键清空静态ARP表项~~
* 支持搜索过滤，以VLAN/IP/MAC/类型/状态进行过滤
* 支持刷新

## 邻居发现/ND (FP1D)

【功能概述】

邻居发现协议NDP是IPv6协议体系中一个重要的基础协议，替代了IPv4的ARP和ICMP路由器发现，定义了使用ICMPv6报文实现地址解析，邻居不可达性检测、重复地址检测、路由器发现、重定向以及ND代理等功能。

ND本身基于ICMPv6实现，以太网协议类型为0x86DD，即IPv6报文，IPv6下一个报头字段值为58，表示ICMPv6报文，由于ND协议使用的所有报文均封装在ICMPv6报文中。一般来说，ND被看作是第3层的协议。在三层完成地址解析，主要带来以下几个好处：（1）地址解析在三层完成，不同的二层介质可以采用相同的地址解析协议；（2）可以使用三层的安全机制避免地址解析攻击；（3）使用组播方式发送请求报文，减少了二层网络的性能压力。

地址解析过程中使用了两种ICMPv6报文：邻居请求报文NS和邻居通告报文NA。

* NS报文：Type字段值为135，Code字段值为0，在地址解析中的作用类似于IPv4中的ARP请求报文。
* NA报文：Type字段值为136，Code字段值为0，在地址解析中的作用类似于IPv中的ARP应答报文。

**邻居不可达性检测**：通过邻居或到达邻居的通信，会因各种原因而中断，包括硬件故障等。如果目的地失效，则恢复是不可能的，通信失败；如果路径失效，则恢复是可能的。因此节点需要维护一张邻居表，每个邻居都有相应的状态，状态之间可以迁移。

邻居状态有5种，分别为：未完成（Incomplete）、可达（Reachable）、陈旧（Stable）、延迟（Delay）、探查（Probe）。

**重复地址检测DAD**是在接口使用某个IPv6单播地址之前进行的，主要是为了探测是否有其它的节点使用了该地址。尤其是在地址自动配置的时候，进行DAD检测是很必要的。一个IPv6单播地址在分配给一个接口之后且通过重复地址检测之前称为试验地址。此时该接口不能使用这个试验地址进行单播通信，但是仍然会加入两个组播组：ALL-NODES组播组和试验地址所对应的Solicited-Node组播组。IPv6重复地址检测技术和IPv4中的免费ARP类似：节点向试验地址所对应的Solicited-Node组播组发送NS报文。NS报文中目标地址即为该试验地址。如果收到某个其他站点回应的NA报文，就证明该地址已被网络上使用，节点将不能使用该试验地址通讯。

**路由器发现功能**用来发现与本地链路相连的设备，并获取与地址自动配置相关的前缀和其他配置参数。在IPv6中，IPv6地址可以支持无状态自动配置，即主机通过某种机制获取网络前缀信息，然后主机自己生成地址的接口标识部分。路由器发现功能是IPv6地址自动配置功能的基础，主要通过以下两种报文实现：

* 路由器通告RA报文：每台设备为了让二层网络上的主机和设备知道自己的存在，定时都会组播发送RA报文，RA报文中会带有网络前缀信息，及其他一些标志位信息。RA报文的Type字段值为134。
* 路由器请求RS报文：很多情况下主机接入网络后希望尽快获取网络前缀进行通信，此时主机可以立刻发送RS报文，网络上的设备将回应RA报文。RS报文的Type字段值为133。

地址自动配置：IPv6地址增长为128位，且终端节点多，对于自动配置的要求更为迫切，除保留了DHCP作为有状态自动配置外，还增加了无状态自动配置。无状态自动配置即自动生成链路本地地址，主机根据RA报文的前缀信息，自动配置全球单播地址等，并获取其他相关信息。

默认路由器优先级和路由信息发现：当主机所在的链路中存在多个设备时，主机需要根据报文的目的地址选择转发设备。在这种情况下，设备通过发布默认路由优先级和特定路由信息给主机，提高主机根据不同的目的地选择合适的转发设备的能力。在RA报文中，定义了默认路由优先级和路由信息两个字段，帮助主机在发送报文时选择合适的转发设备。主机收到包含路由信息的RA报文后，会更新自己的路由表。当主机向其他设备发送报文时，通过查询该列表的路由信息，选择合适的路由发送报文。主机收到包含默认设备优先级信息的RA报文后，会更新自己的默认路由列。当主机向其他设备发送报文时，如果没有路由可选，则首先查询该列表，然后选择本链路内优先级最高的设备发送报文；如果该设备故障，主机根据优先级从高到低的顺序，依次选择其他设备。

**重定向**：当网关设备发现报文从其它网关设备转发更好，它就会发送重定向报文告知报文的发送者，让报文发送者选择另一个网关设备。重定向报文也承载在ICMPv6报文中，其Type字段值为137，报文中会携带更好的路径下一跳地址和需要重定向转发的报文的目的地址等信息。

**ND Proxy**：为了满足用户更安全、更灵活的组网需求，IPv6网络通常被划分为多个VLAN，VLAN内的主机间可以直接通信，而VLAN间不能直接互通。同一VLAN内还可以配置端口隔离，同一端口隔离组的端口之间互相二层隔离，但是最终用户终端之间总是有互通需求的，即不同VLAN间或同一端口隔离组的部分用户会有互通的需求。类似于IPv4网络的ARP代理，ND代理用于解决上述IPv6网络互通问题。

|  |  |
| --- | --- |
| **ND代理方式** | **适用场景** |
| VLAN内ND Proxy | 需要互通的主机处于相同网段，并且属于相同VLAN，但是VLAN内配置了端口隔离的场景 |
| VLAN间ND Proxy | 需要互通的主机处于相同网段，但属于不同VLAN的场景 |

* VLAN内ND Proxy：当VLAN内配置了端口隔离时，属于相同VLAN的用户间无法实现互通。此时，在关联了VLAN的接口上使能VLAN内ND Proxy功能，可以实现用户间三层互通。
* VLAN间ND Proxy：如果两台主机处于相同网段但属于不同的VLAN，用户间要进行三层互通，可以在关联了这些VLAN的接口上使能VLAN间ND Proxy功能。VLAN间ND Proxy功能一般应用于IPv6网络的VLAN聚合场景。当属于不同的Sub-VLAN的主机间要实现三层互通时，可以在Super-VLAn对应的VLANIF接口上使能VLAN间ND Proxy功能，使得该Super-VLAN下所有Sub-VLAN之间均可互相访问。

GWN78xx系列交换机暂仅支持动静态ND表项。

各型号设备ND数量上限具体如下：(ARP与NDP，邻居表共用)

|  |  |  |
| --- | --- | --- |
| **型号** | **芯片** | **ND数量上限** |
| GWN7801(P)/02(P)/03(P) | RTL83XX | 256 |
| GWN7806(P)/11(P)/12P/13(P)/21P/30/31/16(P)/23P/32 | RTL9300/9310 | 1024 |

【配置参数】

**全局配置：**

* 老化时间 (秒)：【text文本框】设置动态邻居表项的老化时间。到达老化时间后，动态邻居表项自动删除。取值范围为60-21600的整数，默认1200秒。

注：与ARP的老化时间为同一配置。

添加静态邻居表项：

* VLAN：【下拉框，单选】从已有VLAN接口中选择。
* \*IPv6地址：【text文本框】设置静态邻居表项的IPv6地址，要与VLAN接口的IPv6地址同网段，也需满足IPv6地址格式，否则报错提示。
* \*MAC地址：【text文本框】设置静态邻居表项的MAC地址，只能输入单播MAC地址，否则报错提示。

注：添加时，当且仅当三者完全相同时，直接覆盖处理，不做去重判断；若VLAN和IPv6地址相同，MAC地址不同，则直接覆盖处理，即修改ND的映射关系。

邻居表：当删除VLAN接口时，其对应的所有静态和动态邻居表项也会同步删除

* 列表显示VLAN、IPv6地址、MAC地址、接口（交换机逻辑接口，包括电口、光口和聚合接口，泛洪显示“--”）、类型（静态|动态）、老化时间（只有动态有）、Router(Yes|No)、状态（主要有2类：~~"Incomplete"、~~ "Reachable"、"Stale"~~、 "Delay"、 "Probe"、"Failed"和"Permanent"~~）
* 支持编辑静态邻居表项，仅MAC地址可修改
* 支持一键将动态邻居表项保存为静态邻居表项
* 支持删除静态邻居表项
* ~~支持一键清空静态邻居表项~~
* 支持搜索过滤，以VLAN/IP/MAC/类型/Router/状态进行过滤
* 支持刷新

## 域名系统/DNS (FP1D)

【功能概述】

域名系统DNS提供域名与IP地址之间的转换服务。IPv4 DNS提供域名和IPv4地址之间的转换，IPv6 DNS提供域名和IPv6地址之间的转换。设备作为DNS客户端，当用户在设备上进行某些应用（如Telnet到一台设备或主机）时，可以直接使用便于记忆的、有意义的域名，通过域名系统将域名解析为正确的地址。

DNS域名解析分为静态域名解析和动态域名解析，二者可以配合使用。在解析域名时，首先采用静态域名解析（查找静态域名解析表），如果静态域名解析不成功，再采用动态域名解析。由于动态域名解析可能会花费一定的时间，且需要域名服务器的配合，因而可以将一些常用的域名放入静态域名解析表中，这样可以大大提高域名解析效果。

**静态DNS：**静态域名解析通过静态域名解析表进行，用户手动建立域名和IP地址之间的对应关系表，将一些常用的域名放入表中。当客户端需要域名所对应的IP地址时，首先到静态域名解析表中查找指定的域名，从而获得所对应的IP地址，提高域名解析的效率。

**动态DNS：**使用动态域名解析时，需要手工指定域名服务器的地址。动态域名解析通过向域名服务器查询域名和地址之间的对应关系来实现将域名解析为地址。

动态域名解析支持域名后缀列表功能。用户可以预先设置一些域名后缀，在域名解析的时候，用户只需要输入域名的部分字段，系统会自动将输入的域名加上不同的后缀进行解析。如，用户想查询域名grandstream.com，那么可以先在后缀列表中配置com，然后输入grandstream进行查询，系统会自动将输入的域名与后缀连接成grandstream.com进行查询。使用域名后缀的时候，根据用户输入域名方式的不同，查询方式分成以下几种情况：

* 如果用户输入的域名中没有“.”，比如grandstream，系统认为是一个主机名，会首先加上域名后缀进行查询，如果所有后缀的域名查询都失败，将使用最初输入的域名（如grandstream）进行查询。
* 如果用户输入的域名中间有“.”，比如，系统直接用它进行查询，如果查询失败，再依次加上各个域名后缀进行查询。
* 如果用户输入的域名最后有“.”，比如grandstream.com，表示不需要进行域名后缀添加，系统直接用输入的域名进行查询，不论成功与否都直接返回。如果用户输入的字符中最后一个字符为“.”，就只根据用户输入的字符进行查找，而不会去匹配用户预先设置的域名后缀，因此最后这个“.”，也被称为查询终止符。带有查询终止符的域名，称为绝对域名或完全合格域名FQDN。

FP1D暂不支持IPv6相关业务。

【配置参数】

**全局配置：**

* DNS：【开关】设置是否将交换机指定为一个DNS客户端，来通过一个或对多个配置的DNS服务器将DNS名称解析为IP地址，默认开启。
* 域名后缀：【text文本框】设置域名后缀，交换机会对非完全限定的域名进行追加，并将其转换为FQDN，最长64字符，允许输入的字符有字母、数字和特殊字符.\_- 。支持添加多个，至多8个

**DNS域名服务器：**

* DNS域名服务器地址：【text文本框】设置DNS域名服务器地址，可以是IPv4地址，也可以是IPv6地址【FP1D暂不支持】，需满足IP地址格式，否则报错提示。

注：1.支持添加多个，至多8个

2.DNS域名服务器默认按照添加顺序从远到近排序，优先级也是如此，即最早添加的优先级最高。

3.DNS域名服务器地址还可以从DHCP或DHCPv6中获取，但优先级低于用户手动配置的。

**静态域名：**

添加：至多添加32个

* 主机名：【text文本框】设置主机名，最长191字符，允许输入的字符有数字、字母和特殊字符.\_- 主机名具有唯一性
* IP地址：【text文本框】设置与域名绑定的IP地址，支持输入IPv4地址，也支持输入IPv6地址【FP1D暂不支持】。需满足IP地址格式，否则报错提示

注：主机名只能对应一个IPv4地址或IPv6地址，但允许多个主机名对应同一个IP地址

**域名映射表：**

* 列表显示主机名、类型（动态|静态）、老化时间（仅动态有）、IP地址
* 支持清除所有静态映射关系
* 支持编辑静态映射关系
* 支持刷新

# 路由业务/Routing

路由是路由器根据收到的数据包的目的地址选择最优路径，并转发到通往目标网络的下一个网络节点的过程，而此路径下的最后一个路由节点则将数据转发给目标主机。（路由器既指传统意义上的路由器，也指运行了路由协议的以太网交换机）

在一次路由过程中选择最优路径是路由器需要完成的最重要的工作。路由器通过维护一张路由表来记录网络中的路径信息，并根据一定的路由选择协议在路由表中选择一条最优路径进行数据转发。最佳路由的选取与发现此路由的路由协议的优先级、路由的度量有关。当多条路由的协议优先级与路由度量都相同时，可以实现负载分担，缓解网络压力；当多条路由的协议优先级与路由度量不同时，可以构成路由备份，提高网络的可靠性。

路由协议是路由器之间维护路由表的规则，用于发现路由，生成路由表，并指导报文转发。常用的路由协议有RIP、OSPF等，不同的协议有不同的算法，对于发往同一目标网络的路径选择结果也可能不一样。路由表中的每一个路由条目基本都包含如下基本属性：

* 目标IP地址：用于标识该路由条目所指向的目标网络
* 子网掩码：用于标识目标网络的子网掩码
* 下一跳：用于指定通往目标网络的下一跳路由节点，路由器将数据转发给下一跳路由节点后，由下一跳路由节点将数据发往再下一跳路由节点或目标网络。下一跳路由必须是本地可达的，配置路由条目时可以通过Ping工具测试是否可达
* 出接口：用于标识数据从本地发出的出接口

路由条目依据来源不同，可以分为三类：

* 通过链路层协议发现的，通常与路由器直接连接的网络的路由称为直连路由
* 通过网络管理员手动配置的路由称为静态路由，不随着网络拓扑的改变而自动变化
* 通过动态路由协议发现的路由称为动态路由，可随着网络拓扑的改变而自动变化

## 路由表/Routing Table (FP1D)

【功能概述】

在一次路由过程中选择最优路径是路由器或运行了路由协议的以太网交换机需要完成的最重要工作。通过维护一张路由表来记录网络中的路径信息，并根据一定的路由选择协议在路由表中选择一条最优路径进行数据转发。

分别显示交换机有效的IPv4路由表和IPv6路由表，路由条目包括：默认路由、直连路由、静态路由和动态路由。

【配置参数】

**（一）IPv4路由表**

~~全局配置：~~

* ~~路由转发：【开关】设置是否进行IPv4路由转发，默认开启。~~

路由表：

* 列表显示协议；类型（默认路由，类型为DHCP或静态|直连路由|静态路由|RIP|OSPF）、目的IP地址、掩码、优先级、下一跳、出接口、Flags~~、老化时间（仅动态路由有）~~

Flags有S(select)、R(reject)、F(FIB)、A(active)、B(blackhole)。S代表选中的路由；R代表被拒绝的路由；F代表该路由下发到转发表；A代表有效的下一跳；B代表黑洞路由

* 列表存有一条默认路由
* ~~支持编辑，仅支持编辑下一跳。目的IP地址为0.0.0.0，路由类型为Default，掩码为0.0.0.0，优先级为1，下一跳地址为VLAN 1 的IPv4地址所在网段（后8 bit为1），出接口为VLAN 1~~
* ~~支持删除，需进行二次确认，并提供风险说明“一旦删除，可能导致交换机托管而无法远程访问”~~
* 若在部分情况下，不存在默认路由，则支持添加，需前往[*IPv4静态路由*](#_静态路由/Static_Routing_(FP1D))配置页面。
* 直连路由：跟随IPv4接口自动生成和删除，不可编辑。列表默认存有一条VLAN 1 IPv4接口的直连路由（不可编辑和删除，删除会跟随VLAN 1的IPv4接口删除进行自动去除），目的IP地址为VLAN 1的IPv4地址所在网段（后8bit为0），掩码长度根据设备自动上报显示，出接口为VLAN 1，无下一跳地址和优先级
* 静态路由与动态路由同步各自路由表里的显示
* 支持搜索过滤，按路由协议筛选，按目的IP地址/下一跳/出接口进行搜索过滤
* 支持刷新
* 支持分页

**（二）IPv6路由表**

~~全局配置：~~

* ~~路由转发：【开关】设置是否进行IPv6路由转发，默认开启。~~

IPv6路由表：

* 列表显示协议类型（RA|直连路由|静态路由|RIPng|OSPFv3）、目的IPv6地址、前缀长度、优先级、下一跳、出接口、Flags~~、老化时间（仅动态路由有）~~
* 默认路由：默认无。当使能IPv6功能后，才会显示。~~增删改逻辑同IPv4默认路由。编辑时仅能编辑下一跳（若下一跳地址为链路本地地址，则同时支持编辑下一跳和出接口）；删除时，若VLAN IPv6接口使能，需二次确认，并提供风险说明”一旦删除，可能导致交换机托管而无法通过IPv6地址进行远程访问”。~~
* 直连路由：跟随IPv6接口自动生成和删除，不可编辑。列表默认无直连路由
* 静态路由与动态路由同步各自路由表里的显示
* 支持搜索过滤，按路由协议筛选，按目的IP地址/下一跳/出接口进行搜索过滤
* 支持刷新
* 支持分页

## 静态路由/Static Routing (FP1D)

【功能概述】

一种需要管理员手动配置的特殊路由。

静态路由在不同网络环境中有不同的目的：

* 当网络结构比较简单时，只需配置静态路由就可以使网络正常工作
* 在复杂网络环境中，配置静态路由可以改进网络的性能，并可为重要的应用保证带宽

但当网络发生故障或拓扑发生变化时，静态路由不会自动更新，必须重新手动配置。

静态路由有五个主要的参数：目的地址和掩码、出接口和下一跳地址、优先级。

**目的地址和掩码：**IPv4的目的地址为点分十进制格式，掩码可以用点分十进制表示，也可用掩码长度表示。IPv6的目的地址为128bit，通常为8组，每组4个十六进制数的形式，每组十六进制数间用冒号分隔，掩码一般用掩码长度表示。当目的地址和掩码都为零时，表示静态缺省路由。

**出接口和下一跳地址：**在配置静态路由时，根据不同的出接口类型，指定出接口和下一跳地址。

* 对于点到点类型的接口，只需指定出接口。因为指定发送接口即隐含指定了下一跳地址，这时认为与该接口相连的对端接口地址就是路由的下一跳地址。
* 对于NBMA类型的接口，配置下一跳IP地址。因为这类接口支持点到多点网络，除了配置静态路由外，还需在链路层建立IP地址到链路层地址的映射，这种情况下，不需要指定出接口。
* 对于广播类型的接口，必须指定通过该接口发送时对应的下一跳地址。因为以太网接口是广播类型的接口，会导致出现多个下一跳，无法唯一确定下一跳。

**优先级：**对于不同的静态路由，可以为它们配置不同的优先级，优先级数字越小优先级越高。配置到达相同目的地的多条静态路由，如果指定相同优先级，则可实现负载分担；如果指定不同优先级，则可实现路由备份。

GWN78XX系列交换机，静态路由不支持指定出接口，根据下一跳地址所在网段，自动匹配到相应出接口。

IPv4/IPv6静态路由限制：

|  |  |  |  |
| --- | --- | --- | --- |
| **型号** | **芯片** | **动态路由支持与否** | **静态路由数量上限** |
| GWN7801(P)/02(P)/03(P) | RTL83XX | 不支持 | 32 |
| GWN7806(P) | RTL9310 | 不支持 | 512 |
| GWN7811(P)/12P/13(P)/21P/30/31 | RTL9300 | 支持 | 32 |
| GWN7816(P)/23P/32 | RTL9310 | 支持 | 32 |

【配置参数】

**IPv4静态路由：**

添加IPv4静态路由：支持添加默认路由

* 目的IP地址：【text文本框】设置路由条目到达的目标网络地址。输入格式为点分十进制，若格式错误则报错提示“您输入的格式不正确，请重新输入”。
* 掩码：【text文本框】设置目的IP地址的掩码，可以以点分十进制格式输入，也可以输入掩码长度，取值为0-32。
* 网关：【单选】选择配置网关接口，选项有{下一跳 | 出接口}。
* 下一跳：【text文本框】设置通往目标IP地址的路由路径上下一个路由节点的IP地址。输入格式为点分十进制，若格式错误则报错提示“您输入的格式不正确，请重新输入”。
* 出接口：【下拉框】设置通往目标IP地址的路由路径的下一跳出口，选项有{VLAN接口 | loopback | null}，默认为空。

注：1.目的IP地址必须与下一跳地址属于不同网段，否则报错提示；

2. 下一跳和出接口必须2选1进行配置。

* 优先级：【text文本框】设置静态路由的优先级，数值越小优先级越高。取值范围为1-255，默认1。

**IPv4静态路由列表：**显示交换机上配置的IPv4静态路由条目，未必生效

* 列表显示目的IP地址、掩码、优先级、下一跳、出接口
* ~~下一跳配置IP地址的情形下，若配置的静态路由生效，则会显示出相应的出接口（IPv4接口），否则显示inactive状态；下一跳配置接口的情形下，出接口根据选择的接口显示，出接口有IP则在下一跳处显示，表明此路由生效，若无则显示“--”~~
* 添加静态路由时，需判断目的IP地址网段、下一跳和优先级：若网段一样，下一跳不一样，优先级一样，作为等价路由，均支持添加；若网段一样，下一跳一样，优先级不一样，作为相同路由直接覆盖处理。
* 添加目的IP地址为0.0.0.0的默认路由时，网关仅支持配置下一跳
* 支持编辑手动添加的静态路由表项，仅能编辑目的IP地址和优先级
* 默认路由，仅能编辑下一跳
* 支持删除单条/批量/全部IPv4静态路由表项
* 删除默认路由时，需进行二次确认，并提供风险说明“一旦删除，可能导致交换机托管而无法远程访问”
* 支持搜索过滤，按目的IP地址/下一跳/出接口进行搜索过滤
* 支持分页

**IPv6静态路由：**

添加IPv6静态路由：

* 目的IPv6地址：【text文本框】设置路由条目到达的目标网络地址。需为有效单播地址，输入格式为冒号十六进制格式，共128bits，每16bit为一段，段之间用“:”分隔，每段用十六进制表示。若格式错误则报错提示“您输入的格式不正确，请重新输入”。
* 前缀长度：【text文本框】设置目的IP地址的前缀长度，取值为0-128，默认64。
* 网关：【单选】选择配置网关接口，选项有{下一跳 | 出接口}。
* 下一跳：【text文本框】设置通往目标IPv6地址的路由路径上下一个路由节点的IPv6地址。需为有效单播地址，输入格式为冒号十六进制，若格式错误则报错提示“您输入的格式不正确，请重新输入”。
* 出接口：【下拉框】设置通往目标IP地址的路由路径的下一跳出口，选项有{VLAN接口 | loopback | null}，默认为空。

注：1. 目的IPv6地址必须与下一跳地址属于不同网段，否则报错提示；

2. 若下一跳地址为全球单播地址，下一跳和出接口必须2选1配置；

3. 若下一跳地址为链路本地地址，则必须同时支持编辑下一跳和出接口，出接口只能是VLAN接口。

* 优先级：【text文本框】设置静态路由的优先级，数值越小优先级越高。取值范围为1-255，默认1。

**IPv6静态路由表：**显示交换机上配置的IPv6静态路由条目，未必生效

* 列表显示目的IPv6地址、前缀长度、优先级、下一跳、出接口
* ~~下一跳配置IP地址的情形下，若配置的静态路由生效，则会显示出相应的出接口（IPv6接口），否则显示inactive状态；下一跳配置接口的情形下，出接口根据选择的接口显示，出接口有IP则在下一跳处显示，表明此路由生效，若无则显示“--”~~
* 添加静态路由时，需判断目的IP地址网段、下一跳和优先级：若网段一样，下一跳不一样，优先级一样，作为等价路由，均支持添加；若网段一样，下一跳一样，优先级不一样，作为相同路由直接覆盖处理。
* 添加目的IPv6地址为全零的默认路由时，网关仅支持配置下一跳
* 支持编辑静态路由，仅能编辑目的IPv6地址和优先级
* 默认路由，仅能编辑下一跳
* 若下一跳地址为链路本地地址，则同时支持编辑下一跳和出接口，出接口只能是VLAN接口
* 支持删除单条/批量/全部IPv6静态路由表项
* 删除默认路由时，需二次确认，并提供风险提示“一旦删除，可能导致交换机托管而无法通过IPv6地址进行远程访问”
* 支持搜索过滤，按目的IP地址/下一跳/出接口进行搜索过滤
* 支持分页

## 动态路由/Dynamic Routing(FP1D)

【仅GWN781X/2X/3X系列L3交换机支持】

对动态路由协议的分类可以采用以下不同标准：

根据作用范围不同，路由协议可分为：

* 内部网关协议IGP：在一个自治系统内部运行。常见的IGP协议包括RIP、OSPF和IS-IS。
* 外部网关协议EGP：运行于不同自治系统之间。BGP是目前最常用的EGP协议。

根据使用算法不同，路由协议可分为：

* 距离矢量协议：包括RIP和BGP。其中，BGP也被称为路径矢量协议。
* 链路状态协议：包括OSPF和IS-IS。

以上两种算法的主要区别在于发现路由和计算路由的方法不同。

GWN781X/2X/3X系列交换机暂仅支持RIP/RIPng和OSPF/OSPFv3动态路由协议。

### RIP

【功能概述】

RIP（Routing Information Protocol，路由信息协议），是一种基于距离矢量算法的协议，使用跳数作为度量来衡量到达目的网络的距离。RIP通过UDP报文进行路由信息的交换，使用的端口号为520。

跳数最少的路径为最优路径，路由器到与它直接相连网络的跳数为0，每经过一个路由器，跳数就加1，跳数被称为度量值。为限制收敛时间，RIP规定度量值的取值范围为0-15的整数，数值16表示无穷大，即目的网络不可达。故，其主要应用于规模较小的网络中，如校园网、结构较简单的地区性网络。

**RIP特性**：（1）设计单一。如果到相同目的站点有2条不同带宽的路径，但跳数相同，RIP仍认为两条路径是等距离的；（2）适用于规模较小的网络；（3）基于用户数据报协议（UDP）的协议；（4）为提高性能，防止产生路由循环，RIP支持水平分割和毒性反转功能。

**RIP的基本原理：**

RIP要求交换机维护一个RIP路由表，该表记录了所有可达目的地的路由项。RIP定期以广播形式（RIPv2支持广播和组播两种方式）向所有邻居发送包含整个路由表的更新信息，并依赖邻居向它的邻居传递更新信息。其邻居交换机接收到这些信息后进行路由计算，更新路由表。每条路由项都包含如下信息：

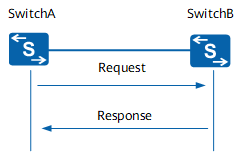
* 目的网络：目的网络的IP地址和子网掩码。该IP地址和子网掩码共同决定了一个网络，到达该网络的报文可通过此路由条目进行转发。
* 下一跳地址：为到达目的网络，需要经过的相邻交换机的接口IP地址。
* 度量值：到达目的网络所需要的跳数。
* 接口名称：交换机转发报文通过的出接口。
* 老化时间：从路由条目最后一次被更新到现在所经过的时间。若该路由条目在超时计时器规定的时间内没有被更新，其跳数将被设为16，表示网络不可达。

RIP定义了两种报文类型：请求报文和响应报文（或称为更新报文）。

* 请求Request报文：向邻居交换机请求发送整个或部分路由表。
* 响应Response报文（更新报文）：可以是对邻居交换机的请求作出应答，也可以是主动向邻居交换机发送更新。

**RIP路由表的形成：**

RIP启动时，初始路由表仅包含本设备的一些直连接口路由。通过相邻设备互相学习路由表项，才能实现各网段路由互通。



* RIP初始化时，交换机会从每个启动RIP协议的接口广播请求报文。该请求报文包含当前交换机学习到的全部路由信息，即整个路由表，并向相邻设备请求完整的路由表。
* 之后，交换机不断地侦听来自其他交换机的RIP响应报文。接收到请求报文且启用RIP协议的邻居交换机会回送包含它们的路由表的响应报文。不关心路由更新信息的主机和其他设备则丢弃该请求报文。
* 当发出请求报文的路由器收到响应报文时，它将开始处理附加在响应报文中的路由信息。对本地RIP路由表中尚未记录的路由表项，路由器直接将该路由信息添加到本地RIP路由表中；对本地已记录的路由表项，则按如下规则处理：
* 如果已有表项和新表项的来源接口相同，则无条件地根据最新路由信息更新本地路由表；
* 如果已有表项和新表项的来源接口不同，则比较它们的度量值，将度量值较小的作为自己的路由表项，如果度量值相同，则保留旧的表项。

这样，经过一段时间的路由信息收集与更新，交换机就可以通过相邻设备收集整个网络的全部信息，完成网络收敛。

**RIP的更新与维护：**

为应对网络拓扑变化，RIP采用定期更新和老化机制来保证RIP路由表的实时性、有效性和稳定性。RIP协议在更新和维护路由信息时主要使用三个定时器：

* 更新定时器：当此定时器超时时，立即发送更新报文。默认每30秒发送一次。
* 老化定时器：交换机会为每一条新建的路由条目设置一个老化时间，如果交换机在老化时间内接收到该条目的更新报文，则保持该路由条目并将超时计时器初始化，重新计时；否则，该条目的跳数将被设置为16，即目的网络不可达，并启动垃圾收集定时器。默认180秒老化。
* 垃圾收集定时器：如果垃圾收集定时器超时，不可达路由没有收到来自同一邻居的更新报文，则该路由将从RIP路由表中彻底删除。默认120秒。

**防止环路机制：**

RIP是通过邻居之间相互通告自己的路由表来建立和维护RIP路由表的，交换机并不知道网络的全局情况，不仅收敛速度慢，还存在发生路由环路的可能。为提高性能，防止产生路由环路，RIP增加了如下特性来最大限度避免环路的产生。

* 计数到无穷：将度量值等于16定义为无穷大，即网络不可达。当发生网络环路时，在环路中循环的路由条目的度量值增加到16之后即被认为不可达，这样可以有效防止路由条目在环路中无休止地传输。默认使能该功能。
* 水平分割：交换机不会把从某个接口学到的路由信息再从该接口发回给邻居设备，这样交换机就不会接收到由自身传达出去的路由信息，既减少了带宽消耗，又可以防止路由环路。
* 毒性反转：交换机从某个接口学到路由条目后，会将该路由条目的度量值设为16（即指明该路由不可达），再从原来的接口发回邻居设备，可以清楚邻居路由表中的无用路由，收敛速度比水平分割更快。当同时启用水平分割和毒性反转时，只有毒性反转功能生效。
* 触发更新：一旦某条路由的度量值发生了变化，交换机就会立刻向邻居设备发布更新报文，而不是等到更新定时器超时再发送。触发更新机制可以避免在多个交换机之间形成路由环路，同时也可以加速网络的收敛速度。

**RIP版本：**

RIP包括RIPv1和RIPv2。RIPv2在RIPv1协议的基础上增加了一些扩展特性，应用更加灵活。

RIPv1：有类别路由协议，只支持以广播方式发布协议报文。RIPv1的协议报文无法携带掩码信息，只能识别A、B、C类自然网段的路由，故无法支持路由聚合，也不支持不连续子网。

RIPv2：无分类路由协议，支持可变长子网掩码、报文认证、无类域间路由、外部路由标记和组播。与RIPv1相比，具有优势：（1）支持外部路由标记，可以在路由策略中根据Tag对路由进行灵活的控制；（2）报文中携带掩码信息，支持路由聚合和无类域间路由；（3）支持指定下一跳，在广播网上可以选择到目的网段最优的下一跳地址；（4）支持以组播方式发送更新报文，使用的组播地址是保留的D类地址224.0.0.9，只有支持RIPv2的设备才能接收协议报文，减少资源消耗；（5）支持对协议报文进行验证，增强安全性。

RIPv2的路由聚合【FP1D阶段暂不支持】：同一个自然网段内的不同子网的路由在向外（其它网段）发送时聚合成一个网段的路由发送，可提高大型网络的可扩展性和效率，缩减路由表。

GWN7810/20/30系列交换机支持基于RIP进程的有类聚合：聚合后的路由使用自然掩码的路由形式发布，RIPv2聚合是按类聚合的，聚合得到最优的度量值。例如，对于10.1.1.0/24（度量值为2）和10.1.2.0/24（度量值为3）两条路由，会聚合成10.0.0.0/8（度量值为2）。但在启用了水平分割或毒性反转的情况下，有类聚合将失效，因为水平分割或毒性反转将抑制一些路由的发布，配置了有类聚合时一条聚合路由可能是聚合了从不同的接口上学到的路由，这样在向外发布时就会产生冲突。

引入外部路由：RIP不仅可以通过与邻居交换路由表学习路由信息，还可以引入其他进程或其它协议例如静态路由学到的路由信息，从而丰富路由表项。

路由重新分配：当交换机使用路由选择协议通告从其他方式（如另一个路由选择协议、静态路由或直连目标网络）学习到的路由时，交换机将执行重新分配。如果设置RIP进程通告来自静态路由进程的路由，这就是重新分配静态路由。IP路由选择协议的能力相差非常大，对路由重新分配影响最大的协议特性是度量值和管理距离的差异性。

* RIP默认度量值：执行路由重新分配的交换机将为被重新分配的路由指派度量值。例如，运行RIP协议的交换机引入外部静态路由，路由器会为静态路由重新分配度量值，然后向其他运行RIP的交换机通告这些路由。RIP协议在引入外部路由时，为其重新分配的度量值默认为12。
* RIP管理距离：当交换机正在运行多个路由选择协议，并从每个协议都学习到一条到达相同目标网络的路由。由于每一个路由选择协议均使用自己的度量定义最优路径，例如RIP使用跳数。为了判断最优路径，各路由协议都被赋予了一个管理距离。管理距离被看作是一个可信度测度，管理距离的数值越小，协议的可信度越高。其中，255表示任何来自不可信源端的路由。RIP管理距离默认120。

【配置参数】

**全局配置：**

* RIP：【开关】设置是否开启交换机的RIP功能，默认关闭。
* RIP版本：【单选】选择使用的RIP协议版本，选项有{ RIPv1 | RIPv2}，默认RIPv2。选择“RIPv1”时，仅发送和接收RIPv1报文，发送报文时采用广播方式；当选择“RIPv2”时，仅发送RIPv2报文，接收RIPv1和RIPv2报文，发送报文时采用组播方式。
* RIP距离：【text文本框】设置RIP协议的管理距离，取值范围为1-255，默认120。
* 自动路由聚合【FP1D阶段暂不支持】：【开关】当且仅当RIP版本选择“RIPv2”时支持配置。设置是否开启路由条目的自动聚合功能。开启后，多条路由条目在网络边界可以汇聚成一条路由条目，起到减小发送的路由条目的作用。默认关闭。
* 引入外部路由：【多选】选择引入的外部路由类型，选项有{直连路由|静态路由|OSPF}。
* 引入外部路由的度量值：【text文本框】设置在引入外部路由时重新分配的度量值，取值范围为1-16，默认1。

注：每个外部路由类型单独设置度量值。

* 定时器：
* 更新定时器 (秒)：【text文本框】设置RIP发送更新报文的时间间隔，取值范围为5-2147483647的整数，默认30秒。
* 老化定时器 (秒)：【text文本框】设置路由条目的有效期。如果在此时间段内该条目未被更新，则该条目的跳数将被设置为16，即目的网络不可达。取值范围为5-2147483647的整数，默认180秒。
* 垃圾收集定时器 (秒)：【text文本框】如果垃圾收集定时器超时，不可达路由没有收到来自同一邻居的更新报文，则该路由将从RIP路由表中彻底删除。取值范围为5-2147483647的整数，默认120秒。

全局RIP运行状态：支持刷新

* 显示RIP运行信息，以大文本框显示，内容直接由底层提供，诸如：

Routing Protocol is "rip"

Sending updates every 30 seconds with +/-50%, next due in 15 seconds

Timeout after 180 seconds, garbage collect after 120 seconds

Outgoing update filter list for all interface is not set

Incoming update filter list for all interface is not set

Default redistribution metric is 1

Redistributing:

Default version control: send version 2, receive version 2

Interface Send Recv Key-chain

vlan200 2 2

Routing for Networks:

vlan200

Routing Information Sources:

Gateway BadPackets BadRoutes Distance Last Update

78.11.78.11 0 0 120 00:00:06

Distance: (default is 120)

**接口配置：**

前提：全局RIP功能开启才可用

* VLAN：选择进行配置的VLAN IPv4接口，可单选也可多选，多选时至多选择10个VLAN接口。
* RIP：【开关】设置是否开启VLAN接口的RIP功能，默认关闭。
* RIP发送版本：【单选】选择VLAN接口使用的发送报文的RIP版本号，选项有{默认 | RIPv1 | RIPv2 | RIPv1&RIPv2}，默认“默认”，即使用全局配置。
* RIP接收版本：【单选】选择VLAN接口使用的接收报文的RIP版本号，选项有{默认 | RIPv1 | RIPv2 | RIPv1&RIPv2}，默认“默认”，即使用全局配置。
* RIPv2广播：【开关】设置是否开启RIPv2的广播特性。开启后，借口将使用RIPv2的报文格式，发送广播报文，接收广播和组播报文。
* 接口抑制：【开关】设置是否禁用VLAN接口上的路由更新功能，默认关闭，即允许接口上的路由更新。
* 路由环路保护：【单选】选择防路由环路的功能，选项有{水平分割 | 毒性反转}，默认水平分割。

当RIP发送/接收版本包含RIPv2时，需要支持RIPv2报文认证功能，具体如下：

* 认证方式：【单选】设置接口所接收和发送的报文使用的认证方式，选项有{关闭 | 简单认证 | MD5认证}，默认关闭，即不认证。
* 当选择“禁用”时，不进行报文认证功能。
* 当选择“简单认证”时，使用简单密码认证，需要配置密钥。其将被添加在RIP报文头部，只有使用相同认证类型和密钥的设备才能互相通信。
* 当选择“MD5认证”时，使用MD5认证，需要配置密钥，密钥ID默认为1且不可配置。
* 密钥：【text文本框】设置接口认证时使用的密钥，输入长度限制在1-16字符。

接口列表：

* 显示接口、接口地址（IP/掩码长度的显示方式）、接口状态、RIP发送版本、RIP接收版本、RIPv2广播、接口抑制、路由环路保护、认证类型

注：当接口无接口地址时，禁止编辑

* 支持编辑

**路由通告：**

* 目的地址/掩码：设置目的地址和掩码长度，掩码长度取值范围为0-32的整数。当发送RIPv1报文时，掩码长度固定为0。允许添加多个，至多512个
* 批量添加/删除时，每一批次支持至多10个

**邻居信息：**

* 列表显示接口、RIP版本、默认距离、更新时间、邻居地址
* 支持刷新

**~~路由表：~~**~~包含生效和无效的表项~~

* ~~列表显示目的网络（目的IP地址/掩码）、下一跳地址、度量值、出接口、老化时间、Flags~~
* ~~支持刷新~~

### RIPng

【功能概述】

RIPng是RIP在IPv6网络中的应用，主要在IPv6网络中提供路由功能。

RIPng和RIP的差异，具体如下：

* RIPng使用UDP的521端口发送和接收路由信息。
* RIPng的目的地址使用128bits的前缀长度。
* RIpng使用128bits的IPv6地址作为下一跳地址。
* RIPng使用链路本地地址fe80::/10作为源地址发送RIPng路由信息更新报文。
* RIPng使用组播方式周期性地发送路由信息，并使用FF02::9作为链路本地范围内的路由器组播地址。
* RIPng报文由头部和多个路由表项组成。在同一个RIPng报文中，路由表项的最大数目根据接口的MTU值来确定。

【配置参数】

**全局配置：**

* RIPng：【开关】设置是否开启交换机的RIPng功能，默认关闭。
* 引入外部路由：【多选】选择引入的外部路由类型，选项有{直连路由|静态路由|OSPFv3}。
* 引入外部路由的度量值：【text文本框】设置在引入外部路由时重新分配的度量值，取值范围为1-16，默认1。

注：每个外部路由类型单独设置度量值。

* 定时器：
* 更新定时器 (秒)：【text文本框】设置RIP发送更新报文的时间间隔，取值范围为5-2147483647的整数，默认30秒。
* 老化定时器 (秒)：【text文本框】设置路由条目的有效期。如果在此时间段内该条目未被更新，则该条目的跳数将被设置为16，即目的网络不可达。取值范围为5-2147483647的整数，默认180秒。
* 垃圾收集定时器 (秒)：【text文本框】如果垃圾收集定时器超时，不可达路由没有收到来自同一邻居的更新报文，则该路由将从RIP路由表中彻底删除。取值范围为5-2147483647的整数，默认120秒。

全局RIPng运行状态：支持刷新

* 显示RIPng运行信息，以大文本框显示，内容直接由底层提供，诸如：

Routing Protocol is "RIPng"

Sending updates every 30 seconds with +/-50%, next due in 1 seconds

Timeout after 180 seconds, garbage collect after 120 seconds

Outgoing update filter list for all interface is not set

Incoming update filter list for all interface is not set

Default redistribution metric is 1

Redistributing:

Default version control: send version 1, receive version 1

Interface Send Recv

vlan200 1 1

Routing for Networks:

vlan200

Routing Information Sources:

Gateway BadPackets BadRoutes Distance Last Update

fe80::200:ff:fe00:9999

0 0 120 00:00:02

**接口配置：**

前提：全局RIPng功能开启才可用

* VLAN：选择进行配置的VLAN IPv6接口，可单选也可多选，多选时至多选择10个VLAN接口。单选时，在VLAN接口下显示接口的链路本地地址和全球单播地址。
* RIPng：【开关】设置是否开启VLAN接口的RIPng功能，默认关闭。
* 接口抑制：【开关】设置是否禁用VLAN接口上的路由更新功能，默认关闭，即允许接口上的路由更新。
* 路由环路保护：【单选】选择防路由环路的功能，选项有{水平分割 | 毒性反转}，默认水平分割。

接口列表：

* 显示接口、接口地址（链路本地地址和全球单播地址均显示，以IPv6地址/前缀长度的显示方式）、接口状态、接口抑制、路由环路保护

注：当接口无全球单播接口地址时，禁止编辑

* 支持编辑

**路由通告：**

* 目的IPv6地址/掩码：设置目的地址和掩码长度，掩码长度取值范围为1-128的整数。允许添加多个，至多512个
* 批量添加/删除时，每一批次支持至多10个

**邻居信息：**

* 列表显示接口、RIPng版本、默认距离、更新时间、邻居地址
* 支持刷新

**~~路由表：~~**~~包含生效和无效的表项~~

* ~~列表显示目的网络（目的IPv6地址/掩码）、下一跳地址、度量值、出接口、老化时间、Flags~~
* ~~支持刷新~~

### OSPF

【功能概述】

开放式最短路径优先OSPF是一个基于链路状态的内部网关协议。其具备如下特点：

* 适用范围广：适用于更大规模的网络（最大可支持几百台设备）；
* 快速收敛：一旦网络拓扑发生变化，交换机之间能够快速通告信息，更新路由；
* 无自环：交换机之间仅同步链路状态信息，每台交换机独立计算路由，不会生成自环；
* 区域划分：将一个大的路由域划分为多个较小的区域，可以节省系统资源和网络带宽，使路由稳定可靠；
* 路由分类：将路由分为多种类型区别对待，支持灵活的控制策略；
* 等价路由：支持等价路由；
* 支持认证：支持报文认证，保障协议交互过程的安全；
* 组播发送：支持以组播地址发送协议报文，可以避免干扰无关者、节省系统资源。

OSPF与RIP的对比：

|  |  |
| --- | --- |
| **RIP** | **OSPF** |
| 基于距离矢量算法，以跳数作为度量方式，忽略带宽的影响 | 基于链路状态，以链路开销作为度量方式，并把带宽作为参考值，度量方式更科学 |
| RIP的跳数限制为15个，限制了RIP的网络规模 | 没有跳数限制，适用的网络规模更大 |
| 按照路由通告进行路由更新和选择，交换机不了解整个网络拓扑，容易产生路由环路 | 每台交换机都能够通过链路状态数据库LSDB掌握全网拓扑，通过最短路径优先算法SPF计算路由，不会产生路由环路 |
| 收敛速度慢，路由更新会经历一段抑制和垃圾收集期，容易导致路由器之间的路由不一致。 | 收敛速度快，因为路由更新是及时的，并且能够快速传递到整个网络。 |
| 不能处理可变长子网掩码（VLSM） | 能够处理VLSM，灵活进行IP地址分配 |

**基本概念：**

* 路由域：一个AS中的所有设备必须相互连接，运行相同的路由协议。因为，AS也被称为路由域。运行OSPF的AS也被称为OSPF路由域，简称OSPF域。
* OSPF进程：OSPF支持多实例，每个实例对应一个OSPF进程。一台设备上可以启用一个OSPF进程，也可以启用多个OSPF进程。每个OSPF进程独立执行OSPF协议，相互隔离。Process ID只有本地意义，不影响相邻接口上的OSPF报文交互。注：GWN781X/2X/3X暂仅支持1个OSPF进程。
* Router ID：OSPF支持多区域。将一个OSPF域划分为多个区域，有助于缓解大规模网络的计算压力。区域是从逻辑上将设备划分为不同的组，每个组用区域号来标识。区域的边界是设备，一台设备可以只属于一个区域，也可以属于多个区域。一个网段（链路）只能属于一个区域，或者说每个运行OSPF的接口必须指明属于哪一个区域。
* OSPF路由器：有（1）区域内路由器，该类路由器的所有接口都属于同一个OSPF区域；（2）区域边界路由器（ABR），用来连接骨干区域和常规区域，ABR同事属于两个以上的区域，其中一个必须是骨干区域；（3）骨干路由器，至少有一个接口属于骨干区域，所有的ABR和骨干区域内的路由器都是骨干路由器；（4）自治系统边界路由器（ASBR），用来与其他AS交换路由信息。
* 虚链路【FP1D阶段暂不支持】：逻辑链路，属于骨干区域，用于解决在物理网络上骨干区域不连续或骨干区域与常规区域不能直接相连的问题。虚链路只能穿越一个常规区域，该区域称为传输区域。虚链路两端的设备均为ABR。

**OSPF报文类型**共有5种，分别如下：

（1）Hello报文

* 邻居发现：使能OSPF功能的接口会周期性地发送Hello报文，与网络中其他收到Hello报文的交换机协商报文中的指定参数，决定是否建立邻居关系；
* 建立双向通信：如果交换机发现收到的Hello报文的邻居列表中有自己Router ID，则认为已经和对端建立了双向通信，邻居关系建立；
* 指定DR和BDR：Hello报文包含DR优先级和Router ID等信息，每台交换机将自己选出的DR和BDR写入Hello报文的DR和BDR字段中，然后进行DR和BDR的选择；
* 保活：在建立邻居关系后，使能OSPF功能的接口仍周期性地发送Hello报文维护邻居关系，如果在一定的时间间隔内没有收到邻居发来的Hello报文，则中断邻居关系。

（2）DD报文：描述本地LSDB的摘要信息，用于在OSPF邻居之间进行数据库同步

（3）LSR报文：用于向对方请求所需的LSA。只有在OSFP邻居双方成功交换DD报文后，才会向对方发出LSR报文。

（4）LSU报文：用来向对端发送其所需要的LSA或泛洪本端更新的LSA，其报文内容是多条完整的LSA集合。为了实现泛洪的可靠性传输，需要LSAck报文对其进行确认，对没有收到确认报文的LSA进行重传，重传的LSA是直接发送到邻居的。

（5）LSAck报文：用来对接收到的LSU报文进行确认，内容是需要确认的LSA的Header。一个LSAck报文可对多个LSA进行确认。

**OSPF**共支持4种网络类型，分别如下：

（1）广播类型Broadcast：当链路层协议是Ethernet或FDDI时，缺省情况下，OSPF认为网络类型是Broadcast。在该类型的网络中：a.通常以组播形式发送Hello报文、LSU报文和LSAck报文。其中，224.0.0.5的组播地址为OSPF设备的预留IP组播地址；224.0.0.6的组播地址为OSPF DR/BDR的预留IP组播地址；b.以单播形式发送DD报文和LSR报文。

（2）NBMA类型Non-Broadcast Multi-Access：当链路层协议是帧中继或X.25时，缺省情况下，OSPF认为网络类型是NBMA。在该类型的网络中，以淡泊形式发送协议报文（Hello报文、DD报文、LSR报文、LSU报文和LSAck报文）。

（3）点到多点P2MP类型：没有一种链路层协议会被缺省的认为是P2MP类型。点到多点必须是由其他的网络类型强制更改的。常用做法是将非全连通的NBMA改为点到多点的网络。在该类型的网络中：a.以组播形式（224.0.0.5）发送Hello报文；b.以单播形式发送其他协议报文（DD报文、LSR报文、LSU报文和LSAck报文）。

（4）点到点P2P类型：当链路层协议是PPP、HDLC或LAPB时，缺省情况下，OSPF认为网络类型是P2P。在该类型的网络中，以组播形式（224.0.0.5）发送协议报文（Hello报文、DD报文、LSR报文、LSU报文和LSAck报文）。

**OSPF运行机制：**

（1）通过交互Hello报文形成邻居关系

交换机运行OSPF协议后，会从所有启动OSPF协议的接口上发送Hello报文。如果两台设备共享一条公共数据链路，并且能够成功协商各自Hello报文中所指定的某些参数，就能形成邻居关系。当互为邻居的设备在彼此的Hello报文中找到自己的Router ID时，双向通信就建立了。

（2）通过泛洪LSA通告链路状态信息

形成邻居关系的交换机之间进一步交互LSA形成邻接关系。每台交换机根据自己周围的网络拓扑结构生成LSA，LSA描述了交换机所有的链路、接口、邻居及链路状态等信息。交换机通过交互这些链路信息来了解整个网络的拓扑信息。

（3）通过组建LSDB形成带权有向图

通过LSA的泛洪，交换机会把收到的LSA汇总记录在LSDB中。最终，所有交换机都会形成同样的LSDB。LSA是对交换机周围网络拓扑结构的描述，而LSDB则是对整个自治系统的网络拓扑结构的描述，LSDB是LSA的汇总。

（4）通过SPF算法计算并形成路由

当LSDB同步完成之后，每一台交换机都将以其自身为根，使用SPF算法来计算一个无环路的拓扑图来描述它所知道的到达每一个目的地的最短路径（最小的路径代价）。这个拓扑图即最短路径树，交换机可借此了解到达自治系统中各个节点的最优路径。

（5）维护和更新路由表

根据SPF算法得出最短路径树后，每台交换机将计算得出的最短路径加载到OSPF路由表形成指导数据转发的路由表项。同时，邻居之间交互Hello报文进行保活，维持邻居关系或邻接关系，并且周期性地重传LSA。

**OSPF路由管理**：通过人为配置，可以合理规划或优化OSPF路由，实现管理的目的。

**路由重新分配**：将设备上存在的“其他路由协议的路由、其他OSPF进程的路由、静态路由、直连路由”引入OSPF进程，以LSA Type5、7的方式发送给邻居。路由重新分配不能引入缺省路由。其常用于AS间互联。通过在ASBR上配置路由重新分配，可以将AS外部的路由信息传播到AS内部，也可以将AS内部的路由信息传播到AS外部。

**引入缺省路由**：通过在ASBR上配置命令，可以将一条缺省路由引入OSPF进程，以LSA Type5、7的方式发送给邻居。其常用于AS间互联，以一条缺省路由代替所有AS外部的路由信息。

**路由聚合**【FP1D阶段暂不支持】：ABR将具有相同前缀的路由信息聚合为一条路由，并将聚合后的路由发布给邻居。路由聚合有助于减轻协议交互负担、减小路由表的规模。OSPF有2种路由聚合方式。

* 区域间路由聚合：区域间路由聚合在ABR上完成，主要用于聚合AS内区域之间的路由。ABR向其他区域发送路由信息时，以网段为单位发布LSA Type3。如果该区域中存在一些连续的网段，ABR可以将这些连续的网段聚合成一个网段，这样ABR只发送一条聚合后的LSA，所有属于命令指定的聚合网段范围的LSA将不会再被单独发送出去。
* 外部路由聚合：在ASBR上完成，主要用于聚合OSPF引入的外部路由。ASBR将对引入的聚合地址范围内的LSA Type5进行聚合。当配置了NSSA区域时，还要对引入的聚合地址范围内的LSA Type7进行聚合。如果本地设备既是ASBR又是ABR，则对由LSA Type7转化成的LSA Type5进行聚合处理。

**路由过滤**【FP1D阶段暂不支持】：OSPF支持使用路由策略对路由信息进行过滤。缺省情况下，OSPF不进行路由过滤。其可应用于以下几方面：

* 路由引入：OSPF可以引入其他路由协议学习到的路由。在引入时可以通过配置路由策略来过滤路由，只引入满足条件的路由。
* 引入路由发布：OSPF引入了路由后会向其它邻居发布引入的路由信息。可以通过配置过滤规则来过滤向邻居发布的路由信息。该过滤规则只在ASBR上配置才有效。
* 路由学习：通过配置过滤规则，可以设置OSPF对接收到的区域内、区域间和自治系统外部的路由进行过滤。其只作用于路由表项的添加与否，即只有通过过滤的路由才被添加到本地路由表中，但所有的路由仍可以在SOPF路由表中被发布出去。
* 区域间LSA学习：通过命令可以在ABR上配置对进入本区域的Summary LSA进行过滤。该配置只在ABR上有效（只有ABR才能发布Summary LSA）。区域间LSA学习和路由学习之间的差异在于：区域间LSA学习直接怼进入区域的LSA进行过滤；路由学习不是对LSA进行过滤而是对LSA计算出来的路由是否添加本地路由表进行过滤，学习到的LSA是完整的。
* 区域间LSA发布：通过命令可以在ABR上配置对本区域出方向的Summary LSA进行过滤。该配置只在ABR上有效。

**路由代价（包括跳数和距离）**：如果网络中存在冗余链路或设备，则从本地到目的网络之间可能存在多条路径。OSPF选择其中总代价最小的路径形成OSPF路由。一条路径的总代价等于沿途链路上的代价之和。通过修改沿途链路上的代价，使一条路径的总代价最小，即可使OSPF选择此路径形成路由。

**OSPF管理距离（AD）**：用于评价路由的可信度，取值范围为0-255的整数。AD值越小，则表示此路由更值得信任。到达同一目的地存在多条路由时，设备优先选择AD值较小的路由。AD值较大者，称为浮动路由（作为最优路由的备份）。缺省情况下，每种来源的路由对应一个AD值。AD值为本地概念，修改AD值只会影响当前设备上的路由选择。直连路由缺省AD值为0，静态路由为1，OSPF路由为110，RIP路由为120，不可达路由为255。

**增强安全性、可靠性：**

认证是为了阻止非法接入网络的路由器和伪造OSPF报文的主机参与OSPF协议过程。在OSPF接口（或虚链路两端）对收到的OSPF报文进行认证。如果认证失败，则丢弃报文，邻接关系将不能被建立。启动认证功能后，可以避免学到非认证、无效路由，避免通告有效路由到非认证设备。在广播类型网络中，认证还可以避免非认证设备成为指定设备的可能性，保证了路由系统的稳定性和抗入侵性。

MTU校验：OSPF在收到DD时会校验邻居接口的MTU和自己接口的MTU是否相同。如果收到的DD报文中指示接口的MTU大于接收接口的MTU，则邻接关系将不能被建立。关闭MTU的校验，可以避免此问题。

源地址校验：通常情况下，OSPF收到报文的源地址和接口会在同一个网段。不过在点到点链路是哪个，链路两端的地址是独立设置的，可以不要求在同一个网段，在此场景下，由于点到点链路协商过程中会告知对端的地址信息，因此OSPF会检查报文的源地址是否就是协商时对端通告的地址，若不是则认为报文非法并丢弃该报文。特别地，对于unnumbered接口，OSPF始终不进行地址校验。但在某些应用场景中，可能会出现源地址不如上面所述，导致OSPF校验失败，比如点到点链路上，协商的对端地址无法获取。在这种场景中，需要关闭源地址校验功能，以保证OSPF邻居正常建立。

双向维持：OSPF设备之间通过周期性发送Hello报文来维持邻接关系。在较大的网络中，可能会出现大量的报文收发，占用较高的CPU和内存资源，造成部分报文的延迟或丢弃。如果Hello报文的处理超出了死亡间隔，将导致邻接关系断开。如果启用双向维持功能，则除了Hello报文外，DD、LSU、LSR、LSAck报文也能用来维持邻居之间的双向通信，从而使邻接关系更加稳定。

并发邻居交互限制：当设备同时与多个邻居交换数据时，其性能会收到影响。限制OSPF进程可并发交互（发起或接受）的邻居最大数目，使设备可以分批与邻居进行交互，有助于保障数据转发或其它关键业务。

邻居震荡抑制：一种震荡抑制方式，通过延迟邻居建立或调整链路开销为最大值的方法达到抑制震荡的目的。在邻居频繁震荡时，启动震荡抑制，实现邻居延迟建立或实现业务流量延迟经过频繁震荡的链路，达到抑制震荡的目的。

Overflow【FP1D阶段暂不支持】：OSPF要求同一个区域中的路由器保存相同的LSDB。随着网络上路由数量不断增加，一些设备由于系统资源有限，不能承载如此多的路由信息，有可能导致设备系统资源耗尽而失效的故障，这种状态称为数据库超限。Overflow是通过限制LSDB中外部路由的数量，达到控制LSDB规模的目的。当设备上的外部路由数量达到上限时，进入Overflow状态：删除LSDB中自己产生的外部路由、不产生新的外部路由、丢弃新收到的外部路由。Overflow状态超时后，如果外部路由数量低于上限，则恢复正常状态。

GR【FP1D阶段暂不支持】：设备普遍采用了控制和转发分离的技术。在网络拓扑保持稳定的情况下，启用GR（平滑重启）功能的设备在控制层面的重启过程中转发层面能够继续指导数据的转发，同时控制层面邻居关系的重建以及路由计算等动作不会影响转发层面的功能，从而避免了路由震荡引发的业务中断，提高了整网的可靠性。目前，GR功能只在主备切换和系统升级过程中使用。

Fast Hello：当发生链路故障后，OSPF需要一段时间（约40秒）才能感知邻居私网。而后再将此信息传播出去，并重新计算SPF。这期间会发生流量中断。启动Fast Hello功能（即将邻居死亡时间设置为1秒）后，一旦发生链路故障，OSPF可以在1秒内感知到邻居私网，从而大大加快路由收敛，避免流量中断。

**网管功能：**MIB、Syslog等使OSPF更易于管理。

MIB：设备端维护的设备状态信息集。管理程序可以对MIB节点进行查阅和设置。设备上可以同时启动多个OSPF进程，但OSPF MIB只能与一个OSPF进程绑定。

Trap：系统检测到故障而产生的通知，告警中携带对应的故障信息。启动Trap功能，则设备可以主动将告警信息发送到网管设备。

Syslog：日志记录了用户对设备的操作以及特定事件等信息。允许日志记录邻接状态变化。

GWN781X/2X/3X只支持1个进程。

【配置参数】

**全局配置：**

* OSPF：【开关】设置是否开启OSPF功能，默认关闭。
* \*路由器ID：【text文本框】设置交换机的Router ID，是一个32bits的无符号整数，以IP地址格式配置。仅支持手动配置Router ID，且需确保Router ID具有唯一性。注：若OSPF已经建立了邻接关系，路由器ID要生效，需要重启OSPF进程。该动作将会导致OSPF路由失效进而重新计算，请谨慎使用。
* 兼容RFC1583/Compatible RFC1583：【开关】当多条路径到达同一个AS外部目的地时，必须确定最优路径。设置是否确定采用RFC1583中使用的优先规则，默认关闭。
* Opaque LSA：【开关】设置是否启用Opaqua LSA处理能力，默认关闭。
* SPF定时器：
* 等待时间 (毫秒)：【text文本框】定义SPF定时器的等待时间，以毫秒为单位，取值范围为0-600000的整数，默认0。OSPF路由进程接收到拓扑变化，触发的SPF定时器至少要在该等待时间后执行。
* 最小间隔时间 (毫秒)：【text文本框】定义两次SPF定时器之间的最小时间间隔，以毫秒为单位，取值范围为0-600000的整数，默认50毫秒。
* 最长间隔时间 (毫秒)：【text文本框】定义两次SPF定时器之间的最大时间间隔，以毫秒为单位，取值范围为0-600000的整数，默认5000毫秒。
* LSA控制参数：
* LSA传输延迟 (毫秒)：【text文本框】设置收到新LSA的最小延迟时间，以毫秒为单位，取值范围为0-5000的整数，默认5000毫秒。
* LSA到达时间 (毫秒)：【text文本框】设置LSA最小接收间隔，以毫秒为单位，取值范围为0-600000的整数，默认1000毫秒。
* ~~更新间隔时间 (秒)：【text文本框】设置LSA更新间隔时间，以秒为单位，取值范围为10-1800的整数，默认10秒。~~
* 通告最大度量：【开关】设置运行OSPF协议的路由设备通告最大度量，以使其他路由设备在SPF计算中不优先将该设备作为传输节点。默认关闭。
* 路由度量值：【开关】默认关闭。开启后，设置不同类型OSPF路由对应的度量值。注：若OSPF已经同步了LSDB，路由度量值要生效，需要重启OSPF进程。该动作将会导致路由失效进而重新计算，请谨慎使用。
* 区域内路由度量值：【text文本框】设置区域内的路由度量值，取值范围为1-255的整数，默认为110。
* 区域间路由度量值：【text文本框】设置区域间的路由度量值，取值范围为1-255的整数，默认为110。
* 外部路由度量值：【text文本框】设置外部的路由度量值，取值范围为1-255的整数，默认为110。
* 始终通告默认路由：【开关】设置OSPF是否无条件产生缺省路由，不管本地是否存在缺省路由。默认关闭。开启后，设置默认路由度量值及其类型。
* 默认路由度量值：【text文本框】设置缺省路由初始的度量值，取值范围为1-16777214的整数，默认1。
* 默认路由度量类型：【单选】选择缺省路由的类型。OSPF外部路由有2种类型，{类型1 | 类型2}，默认类型2。“类型1”，不同路由设备上看到的度量值不一样；“类型2”，所有路由设备看到的度量值都一样。
* 外部路由引入：【多选】选择引入的外部路由类型，选项有{直连 |静态 |RIP}。
* 引入外部路由的度量值：【text文本框】设置在引入外部路由时重新分配的度量值，取值范围为0-16777214，默认1。
* 引入外部路由的度量类型：【单选】设置引入的外部路由类型，选项有{类型1 | 类型2}，默认类型2。

注：每个外部路由单独设置度量值和类型。

* <重启进程>按钮：点击后，二次确认是否重启OSPF进程。一旦进程重启，设备间已建立的邻接关系将会重新协商。

全局OSPF运行状态：支持刷新

* 显示OSPF运行信息，以大文本框显示，内容直接由底层提供，诸如：

OSPF Routing Process, Router ID: 91.91.91.91

Supports only single TOS (TOS0) routes

This implementation conforms to RFC2328

RFC1583Compatibility flag is enabled

OpaqueCapability flag is disabled

Initial SPF scheduling delay 0 millisec(s)

Minimum hold time between consecutive SPFs 500 millisec(s)

Maximum hold time between consecutive SPFs 5000 millisec(s)

Hold time multiplier is currently 1

SPF algorithm last executed 25m26s ago

Last SPF duration 0 usecs

SPF timer is inactive

LSA minimum interval 2500 msecs

LSA minimum arrival 500 msecs

Write Multiplier set to 20

Refresh timer 10 secs

This router is an ASBR (injecting external routing information)

Number of external LSA 2. Checksum Sum 0x00010867

Number of opaque AS LSA 0. Checksum Sum 0x00000000

Number of areas attached to this router: 1

Area ID: 0.0.0.0 (Backbone)

Number of interfaces in this area: Total: 1, Active: 1

Number of fully adjacent neighbors in this area: 1

Area has no authentication

SPF algorithm executed 29 times

Number of LSA 4

Number of router LSA 2. Checksum Sum 0x0000ba54

Number of network LSA 1. Checksum Sum 0x0000bf9b

Number of summary LSA 1. Checksum Sum 0x00000c5f

Number of ASBR summary LSA 0. Checksum Sum 0x00000000

Number of NSSA LSA 0. Checksum Sum 0x00000000

Number of opaque link LSA 0. Checksum Sum 0x00000000

Number of opaque area LSA 0. Checksum Sum 0x00000000

**区域设置：**

区域列表：

* 显示区域ID（以IPv4地址格式显示，由底层处理转换）、区域类型、Stub区域及No Summary的状态 或 NSSA区域及No Summary状态和转换类型
* 开启接口OSPF功能后，即存在一条区域0.0.0.0的配置
* 区域ID唯一。若多个接口绑定同一个区域，则列表只显示1个
* 区域根据接口设置处配置的区域ID自动生成和删除，也随CLI创建而显示
* 支持编辑，以区域ID为索引
* ~~支持单个/批量删除~~

编辑时，仅支持编辑除区域ID外的其他属性，具体如下：

~~添加：至多添加256个区域~~

* 区域ID：【仅显示】显示选择的OSPF区域号，以IPv4地址格式显示。
* ~~网络地址：【text文本框】设置OSPF区域的子网地址。~~
* ~~掩码长度：【text文本框】设置区域子网地址掩码长度，取值为8-30的整数，默认24。~~

~~注：需确保配置的区域地址与接口地址处于同一网段，才能在接口上正常使能OSPF功能。~~

* 区域类型：【单选】设置将此区域设为Stub还是NSSA区域，选项有{None| Stub区域 | NSSA区域}，默认None。当区域ID设置为0.0.0.0时，不支持区域类型设置。

当选择“Stub区域”时，

* No Summary：【开关】设置是否禁止ABR向Stub区域内发送LSA type 3（Summary LSA），即将此区域配置为Totally Stub区域。

当设置为“NSSA区域”时，

* No Summary：【开关】设置是否禁止ABR向区域内发送LSA Type3（Summary LSA），即将此区域配置为Totally NSSA区域。
* 转换类型：【单选】当NSSA区域中有多个ABR时，系统会根据规则自动选择一个ABR作为转换器（通常情况下NSSA区域选择Router ID最大的设备），将LSA Type7转换为LSA Type5。设置转换类型，选项有{Never | ~~Candidate |~~ Always}，默认Never。

**接口设置：**

* 接口：从已有的VLAN IPv4接口中选择，不包括loopback接口。选择VLAN接口后，在下方呈现接口的IPv4地址/掩码长度信息（只读）。
* OSPF：【开关】设置是否在接口上使能OSPF功能，默认关闭。
* 区域ID：【text文本框】设置区域ID，可以以IPv4地址格式配置，也可以输入0-4294967295间的整数，默认0.0.0.0。~~【仅显示，不支持配置】显示使能后加入的区域。~~
* 网络类型：【单选】设置接口的网络类型，选项有{点对点 | 广播 | NBMA | 点对多点}，默认广播。当网络类型选择“NBMA”时，需提示“邻居地址请前往***NBMA邻居***进行设置”。
* 接口抑制：【开关】设置是否禁用VLAN接口上的路由更新功能，即抑制收发OSPF报文，默认关闭，即允许接口上的路由更新。
* 忽略MTU校验：【开关】设置是否对DD报文中的MTU字段不进行检查，默认关闭，即对DD报文中的MTU进行检查。
* LSA重传时间间隔 (秒)：【text文本框】当路由设备发送完一个LSA报文，该报文还保留在发送缓冲队列中，如果在指定的时间间隔时间内，没有得到邻居的确认，则将重新发送该报文。取值范围为3-65535的整数，默认5秒。
* LSA传输延迟时间 (秒)：【text文本框】设置接口传输LSA报文的延迟时间，取值范围为1-500的整数，默认1秒。
* Hello报文发送时间间隔 (秒)：【text文本框】当且仅当开启“Fast Hello”功能时隐藏，不可配置。设置接口发送Hello报文的时间间隔，取值范围为1-65535的整数，默认10秒。
* Fast Hello：【开关】开启后，一旦发生链路故障，OSPF可以在1秒内感知到邻居私网，从而加快路由收敛。开启后，“Hello报文发送时间间隔 (秒)”隐藏，不支持配置；“邻居失效时间”默认设置为1，不可编辑；新增“Hello报文数/秒”配置。
* Hello报文数/秒：【text文本框】设置每秒发送的Hello报文数，取值范围为1-10，默认1。
* 邻居失效时间 (秒)：【text文本框】设置相邻邻居的失效时间，取值范围为1-65535的整数，默认40秒。当且仅当开启“Fast Hello”功能时，默认设置为1，不可编辑。
* 开销值/Cost值：【text文本框】设置接口的开销值，取值范围为1-65535的整数，默认10。
* 优先级：【text文本框】设置接口选择DR时的优先级，取值范围为0-255的整数，默认1。
* 认证方式：【单选】设置接口所接收和发送的报文使用的认证方式，选项有{关闭 | 简单认证 | MD5认证}，默认关闭，即不认证。
* 当选择“禁用”时，不进行报文认证功能。
* 当选择“简单认证”时，使用简单密码认证，需要配置密钥。
* 密钥：【text文本框】设置接口认证时使用的密钥，输入长度限制在1-8字符。支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示
* 当选择“MD5认证”时，使用MD5认证，需要配置密钥ID。
* 密钥ID：【text文本框】设置接口MD5认证时使用的密钥ID，取值范围为1-255的整数。
* 密钥：【text文本框】设置接口MD5认证时使用的密钥，输入长度限制在1-16字符。支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示

接口列表：

* 显示接口、接口地址（以IPv4地址/掩码长度显示）、状态、区域ID、网络类型、接口抑制、忽略MTU校验、LSA重传时间间隔、LSA传输延迟时间、Hello报文发送时间间隔、邻居失效时间、开销值、优先级、认证方式
* 支持查看接口详情信息
* 支持编辑

~~网段设置：~~

* ~~接口：【下拉框】选择VLAN接口，选择后显示接口地址/掩码长度~~
* ~~区域ID：【text文本框】设置区域ID，可以以IPv4地址格式配置，也可以输入0-4294967295间的整数，默认0.0.0.0~~

**NBMA邻居：**

添加邻居：支持添加多个邻居，至多256个，每个VLAN接口（不包含loopback）最多5个邻居生效

* 邻居：【text文本框】当*[接口设置/接口]*的网络类型选择“NBMA”时，需要手动指定邻居，根据与VLAN接口同网段的来自动匹配。以邻居IP地址的方式进行设置
* Hello报文间隔 (秒)：【text文本框】设置邻居发送Hello报文的时间间隔，取值范围为1-65535的整数，默认60
* 优先级：【text文本框】设置参与选举DR时的优先级，取值范围为0-255的整数，默认为0，即表示不参与选举

邻居列表：

* 显示邻居、Hello报文间隔、优先级、接口地址（VLAN ID+IP地址的格式显示，只读）
* 支持编辑，以邻居为索引
* 支持批量删除，每一批次支持至多10个

**~~接口统计信息：~~**

* ~~显示接口、接收的Hello报文数、发送的Hello报文数、接收的DD报文数、发送的DD报文数、接收的LSR报文数、发送的LSR报文数、接收的LSU报文数、发送的LSU报文数、接收的LSAck报文数、发送的LSAck报文数、接收的丢弃报文数、发送的丢弃报文数、状态改变次数、Full的邻居数~~

**邻居信息：**显示当前进程下的所有邻居信息

* 显示邻居总数
* 每位邻居显示邻居ID/Neighbor ID、优先级/Priority、状态/State、消亡时间/Dead Time、邻居地址/Neighbor IP Address、邻居接口/Neighbor Interface、~~重传计数/Retransmit Counter、请求计数Request Counter、数据库摘要计数/DB Summary Counter、~~运行时间/Up Time
* 支持查看邻居详情信息

**database信息：**

* Database支持选择10类中的一类信息进行展示 (具体信息以底层返回为准进行显示，建议使用大文本框显示)
* 类型选项有{database | asbr-summary | nssa-external | external | network | summary | router | opaque-link | opaque-area | opaque-as | max-age}，默认均不选
* Self-originate：支持在10类信息中是否展示交换机自己生成的信息
* 具体的Database信息以底层返回为准，用大文本框显示

**~~路由表：~~**~~共有3张表~~

~~表1：network表~~

* ~~显示接口、目的IP地址/掩码、目的地址类型（路由器|网络|丢弃）、路径开销、区域ID、路由类型（区域内|区域间|Type1的外部路由|Type2的外部路由）~~
* ~~支持分页~~

~~表2：router表~~

* ~~显示接口、目的IP地址/掩码、目的地址类型（路由器|网络|丢弃）、路径开销、flag（ASBR）、下一跳、区域ID、路由类型（区域内|区域间|Type1的外部路由|Type2的外部路由）~~
* ~~支持分页~~

~~表3：external表~~

* ~~显示接口、目的IP地址/掩码、目的地址类型（路由器|网络|丢弃）、路径开销、tag、下一跳、区域ID、路由类型（区域内|区域间|Type1的外部路由|Type2的外部路由）~~
* ~~支持分页~~

### OSPFv3

【功能概览】

OSPFv3是运行于IPv6的OSPF路由协议，其在OSPFv2的基础上做了修改，是一个独立的路由协议。

OSPFv3和OSPF的差异，具体如下：

* OSPFv3不在位于数据包和链路状态公告LSA起始位置的报文头部插入基于IP的数据；
* OSPFv3利用独立于网络协议的信息，来执行过去需要IP报文头部数据的关键任务，如识别发布路由数据的LSA。

**OSPFv3报文**公有5种，分别如下：

* Hello：周期性发送，用来发现OSPF邻居，维持邻接关系
* DD：描述本地LSDB的摘要信息，用于在OSPF邻居之间进行数据库同步
* LSR：用于向对方请求所需的LSA。只有在OSPF邻居双方成功交换DD报文后，才会向对方发出LSR报文。
* LSU：用于向对方发送其所需要的LSA。
* LSAck：用来对收到的LSA进行确认。

**LSA类型**共有9种，分别如下：

|  |  |
| --- | --- |
| **LSA类型** | **说明** |
| Router-LSA（Type 1） | 由每个设备始发，描述了设备的链路状态和代价，在始发设备所属区域内传播 |
| Network-LSA（Type 2） | 由DR始发，描述本链路的链路状态，在DR所属区域内传播 |
| Inter-Area-Prefix-LSA（Type 3） | 由ABR始发，描述到其它区域的路由，通告给非Totally STUB、NSSA区域 |
| Inter-Area-Router-LSA（Type 4） | 由ABR始发，描述到ASBR的路由，通告给除ASBR所在区域的其他区域 |
| AS-external-LSA（Type 5） | 由ASBR始发，描述到AS外部的路由，通告到所有区域（除了STUB、NSSA区域） |
| NSSA LSA（Type 7） | 由ASBR始发，描述到AS外部的路由，仅在NSSA区域内传播 |
| Link-LSA（Type 8） | 由每个设备始发，描述每个链路的link-local地址、IPv6前缀地址，并提供将会在Network-LSA中设置的链路选项，仅在此链路内传播 |
| Intra-Area-Prefix-LSA（Type 9） | 每个设备及DR都会产生一个或多个此类LSA，在所属的区域内传播。   * 设备产生的此类LSA，描述与Route-LSA相关联的IPv6前缀地址 * DR产生的此类LSA，描述与Network-LSA相关联的IPv6前缀地址 |

**OSPFv3区域类型**公有3类，分别如下：

|  |  |
| --- | --- |
| **区域类型** | **作用** |
| Totally Stub Area | 允许ABR发布Type3缺省路由，不允许自治系统外部路由和区域间的路由 |
| Stub Area | 和Totally Stub区域的不同在于，该区域允许区域间路由 |
| NSSA Area | 和Stub区域的不同在于该区域允许自治系统外部路由的引入，由ASBR发布LSA Type7通告给本区域，这个LSA Type7在ABR上转换成LSA Type5，并且泛洪到整个OSPFv3域中 |

OSPFv3与OSPFv2协议比较，具体如下表：

|  |  |
| --- | --- |
| **相同点** | **不同点** |
| * 网络类型和接口类型 * 接口状态机和邻居状态机 * 链路状态数据库LSDB * 泛洪机制 * 相同类型的报文：Hello、DD、LSR、LSU、LSAck * 路由计算基本相同 | * OSPFv3基于链路，而不是网段。只要在同一链路，就可以不配置IPv6全局地址而直接建立联系。 * OSPFv3上移除了IP地址的意义。其可以不依赖IPv6全局地址的配置来计算出OSPFv3的拓扑结构。IPv6地址仅用于Vlink接口及报文的转发。 * OSPFv3的报文即LSA格式发生改变。 * OSPFv3报文不包含IP地址； * OSPFv3的Router LSA和Network LSA里不包含IP地址。IP地址部分由新增的两类LSA宣告 * OSPFv3的Router ID、Area ID和LSA State ID不再表示IP地址，但仍保留IPv4地址格式。 * 广播、NBMA及P2MP网络中，邻居不再由IP地址标识，只由Router ID标识。 * OSPFv3的LSA报文里添加LSA的泛洪范围。 * OSPFv3可存储或泛洪不识别的报文，而OSPF只能简单丢弃不识别的报文。 * OSPFv3允许泛洪范围为区域或链路本地，并且设置U位的不识别报文存储或通过Stub区域。 * OSPFv3支持一个链路上多个进程。 * OSPFv3利用IPv6链路本地地址在同一链路上发现邻居及自动配置等。运行IPv6的设备不转发目的地址为链路本地地址的IPv6报文，此类报文只在同一链路有效。链路本地单播地址从fe80::/10开始。 * 新增两种LSA * Link LSA：用于设备宣告各个链路是哪个对应的链路本地地址及其所配置的IPv6全局地址，仅在链路内洪泛 * Intra Area Prefix LSA：用于向其他设备宣告本设备或本网络（广播网及NBMA）的IPv6全局地址信息，在区域内洪泛 * OSPFv3只通过Router ID来标识邻居。OSPF在广播、NBMA、P2P和P2MP网络中是通过IPv4接口地址来标识的，而在vlink网络中是通过Router ID来标识。 |

GWN781X/2X/3X仅支持1个进程。

【配置参数】

**全局配置：**

* OSPFv3：【开关】设置是否开启OSPFv3功能，默认关闭。
* 路由器ID：【text文本框】设置交换机的Router ID，是一个32bits的无符号整数，以IPv4地址格式配置。仅支持手动配置Router ID，且需确保Router ID具有唯一性。注：若与邻居建立完全连接，此时修改Router ID则须重启OSPF进程才能生效。
* SPF计算：
* 等待时间 (毫秒)：【text文本框】定义SPF计算的等待时间，以毫秒为单位，取值范围为0-600000的整数，默认0。OSPFv3路由进程接收到拓扑变化，触发的SPF计算至少要在该等待时间后执行。
* 最小间隔时间 (毫秒)：【text文本框】定义两次SPF运算之间的最小时间间隔，以毫秒为单位，取值范围为0-600000的整数，默认50毫秒。
* 最长间隔时间 (毫秒)：【text文本框】定义两次SPF运算之间的最大时间间隔，以毫秒为单位，取值范围为0-600000的整数，默认5000毫秒。
* LSA到达时间 (毫秒)：【text文本框】设置LSA接收间隔，以毫秒为单位，取值范围为0-600000的整数，默认1000毫秒。
* 路由度量值：设置不同类型OSPF路由对应的度量值。
* 区域内路由度量值：【text文本框】设置区域内的路由度量值，取值范围为1-255的整数，默认为110。
* 区域间路由度量值：【text文本框】设置区域间的路由度量值，取值范围为1-255的整数，默认为110。
* 外部路由度量值：【text文本框】设置外部的路由度量值，取值范围为1-255的整数，默认为110。
* 引入外部路由：【多选】选择引入的外部路由类型，选项有{直连路由 |静态路由 |RIPng}。
* 引入外部路由的度量值【FP1D暂不支持】：【text文本框】设置在引入外部路由时重新分配的度量值，取值范围为0-16777215，默认1。
* 引入外部路由的度量类型【FP1D暂不支持】：【单选】设置引入的外部路由类型，选项有{类型1 | 类型2}。

注：每个外部路由单独设置度量值和类型。

* <重启进程>按钮：点击后，二次确认是否重启OSPFv3进程。一旦进程重启，设备间已建立的邻接关系将会重新协商。

全局OSPFv3运行状态：支持刷新

* 显示OSPFv3运行信息，以大文本框显示，内容直接由底层提供，诸如：

OSPFv3 Routing Process (0) with Router-ID 0.0.0.0

Running 02:50:02

LSA minimum arrival 1000 msecs

Initial SPF scheduling delay 0 millisec(s)

Minimum hold time between consecutive SPFs 50 millsecond(s)

Maximum hold time between consecutive SPFs 5000 millsecond(s)

Hold time multiplier is currently 1

SPF algorithm has not been run$

SPF timer is inactive

Number of AS scoped LSAs is 0

Number of areas in this router is 1

Area 0.0.0.0

Number of Area scoped LSAs is 2

Interface attached to this area: vlan200

SPF has not been run

**区域设置：**

区域列表：

* 列表显示区域ID（以IPv4地址格式显示，由底层转换）、区域类型、Stub区域的No Summary开关状态
* 开启接口OSPFv3功能后，即存在一条区域0.0.0.0的配置
* 区域ID唯一。若多个接口绑定同一个区域，则列表只显示1个
* 区域根据接口设置处设置的区域ID自动生成和删除，也随CLI创建而显示
* 支持编辑，以区域ID为索引

编辑时，仅支持编辑除区域ID外的其他属性，具体如下：

* 区域ID：【仅显示】显示选择的区域ID。
* 区域类型：【单选】选项有{None | Stub}，默认None。当区域ID设置为0.0.0.0时，不支持区域类型设置。
* No Summary：【开关】当且仅当区域类型选择“Stub“时支持配置。设置是否允许ABR只向Stub区域内发送一条缺省路由的LSA type 3（Summary LSA），不生成任何其它Summary LSA，即将此区域配置为Totally Stub区域。

**接口配置：**

* 接口：从已有的VLAN IPv6接口中选择。选择接口后，在接口下方显示接口的链路本地地址和全球单播地址（只读）。
* OSPFv3：【开关】设置是否在接口上开启OSPFv3功能。
* 区域ID：【text文本框】设置接口加入的区域ID，可以以IPv4地址格式配置，也可以输入0-4294967295间的整数，默认0.0.0.0。~~一旦配置好，即接口上开启OSPFv3功能。~~
* 网络类型：【单选】设置接口的网络类型，选项有{点对点 | 广播}，默认广播。
* 接口抑制：【开关】设置是否禁用VLAN接口上的路由更新功能，默认关闭，即允许接口上的路由更新。
* MTU：【text文本框】设置接口上的MTU（协议报文的MTU），取值范围为1-65535，默认1500。
* 忽略MTU校验：【开关】设置是否对DD报文中的MTU字段不进行检查，默认关闭，即对DD报文中的MTU进行检查。
* LSA重传时间间隔 (秒)：【text文本框】当路由设备发送完一个LSA报文，该报文还保留在发送缓冲队列中，如果在指定的时间间隔时间内，没有得到邻居的确认，则将重新发送该报文。取值范围为3-65535的整数，默认5秒。
* Hello报文发送时间间隔 (秒)：【text文本框】设置接口发送Hello报文的时间间隔，取值范围为1-65535的整数，默认10秒。
* LSA传输延迟时间 (秒)：【text文本框】设置接口传输LSA报文的延迟时间，取值范围为1-800的整数，默认1秒。
* 邻居失效时间 (秒)：【text文本框】设置相邻邻居的失效时间，取值范围为1-65535的整数，默认40秒。
* 开销值/Cost值：【text文本框】设置接口的开销值，取值范围为1-65535的整数，默认10。
* 优先级：【text文本框】设置接口选择DR时的优先级，取值范围为0-255的整数，默认1。

接口列表：

* 显示接口、接口地址（链路本地地址和全球单播地址均显示，以IPv6地址/前缀长度的显示方式）、状态、区域ID（以IPv4地址格式显示，由底层处理）、网络类型、接口抑制、MTU、忽略MTU校验、LSA重传时间间隔、Hello报文发送时间间隔、LSA传输延迟时间、邻居失效时间或乘数、开销值、优先级
* 支持查看接口详情信息
* 支持编辑

**邻居信息：**显示当前进程下的所有邻居信息，每个VLAN接口（不包含loopback）最多5个邻居实际生效

* 显示邻居总数
* 每位邻居显示邻居ID、优先级、状态、消亡时间、邻居地址、接口地址(VLAN ID及其链路本地地址)、运行时间
* 支持查看邻居详情，具体详细信息以后台返回为准
* 支持刷新

**database信息：**

* Database支持选择10类中的一类信息进行展示 (具体信息以底层返回为准进行显示，建议使用大文本框显示)
* 类型选项有{database | router | network | inter-prefix | inter-router | group-membership | type-7 | link | intra-prefix}，默认为第一个选项
* Self-originate：支持在10类信息中是否展示交换机自己生成的信息

具体的Database信息以底层返回为准，用大文本框显示

**~~路由表：~~**~~共有3张表~~

~~表1：network表~~

* ~~显示接口、目的IP地址/掩码、目的地址类型（路由器|网络|丢弃）、路径开销、区域ID、路由类型（区域内|区域间|Type1的外部路由|Type2的外部路由）~~
* ~~支持分页~~

~~表2：router表~~

* ~~显示接口、目的IP地址/掩码、目的地址类型（路由器|网络|丢弃）、路径开销、flag（ASBR）、下一跳、区域ID、路由类型（区域内|区域间|Type1的外部路由|Type2的外部路由）~~
* ~~支持分页~~

~~表3：external表~~

* ~~显示接口、目的IP地址/掩码、目的地址类型（路由器|网络|丢弃）、路径开销、tag、下一跳、区域ID、路由类型（区域内|区域间|Type1的外部路由|Type2的外部路由）~~
* ~~支持分页~~

## 策略路由/Policy Routing (FP3)

## VRRP (FP3) 【待评审】

【功能概述】

虚拟路由冗余协议（Virtual Router Redundancy Protocol，VRRP）通过把几台路由设备联合组成一台虚拟的路由设备，将虚拟路由设备的IP地址作为用户的默认网关实现与外部网络通信。当网关设备发生故障时，VRRP机制能够选举新的网关设备承担数据流量，从而保障网络的可靠通信。

**优点**

（1）冗余备份：VRRP可以将多台路由设备配置为缺省网关路由器，当出现单点故障的时候通过备份链路进行业务传输，从而降低网络故障的可能性，保证用户的各种业务不中断传输。

（2）负载分担：VRRP可以实现多台设备同时承担业务流量，从而减轻主用设备上数据流量的承载压力，在路由设备之间更均衡地分担流量。

（3）联动功能：VRRP联动可以监视上行链路的故障。当上行接口或链路故障时，VRRP备份组的Master设备降低优先级，充为，确保Master路由器为最佳的VRRP路由设备，保证流量的正常转发。

**VRRP基本概念**

1.VRRP路由器：运行VRRP协议的设备。

2.虚拟路由器：又称VRRP备份组，由一个Master设备和多个Backup设备组成，被当作一个共享局域网内主机的缺省网关。

3.Master路由器：承担转发报文任务的VRRP设备，包括ARP响应和转发IP数据包。

4.Backup路由器：一组不承担转发任务的VRRP设备，只负责监听Master路由器的状态。当Master设备出现故障时，将通过竞选成为新的Master设备。

5.VRID：虚拟路由器的标识。

6.虚拟IP地址：虚拟路由器的IP地址，一个虚拟路由器可以有一个或多个IP地址，由用户配置。

7.IP地址拥有者：如果一个VRRP设备将虚拟路由器IP地址作为真实的接口地址，则该设备称为IP地址拥有者，此时此VRRP组的优先级为255。如果IP地址拥有者是可用的，通常它将称为Master，其接口的IP地址与虚拟路由器的IP地址相同。IP地址拥有者接收处理目的IP地址为虚拟路由器的IP地址的报文。

8.虚拟MAC地址：虚拟路由器根据VRID生成的MAC地址。一个虚拟路由器拥有一个虚拟MAC地址，格式为00-00-5E-00-01-(VRID)（VRRP for IPv4）或00-00-5E-00-02-(VRID)（VRRP for IPv6）。当虚拟路由器回应ARP请求时，使用虚拟MAC地址，而不是接口真实的MAC地址。

**协议报文**

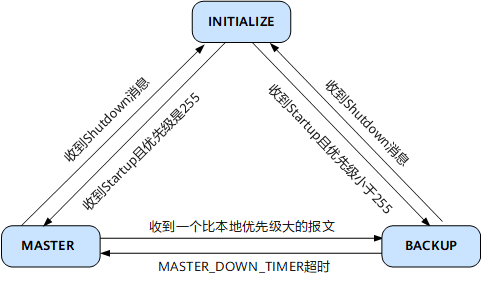
VRRP协议报文用来将Master设备的优先级和状态通告给同一备份组的所有Backup设备。其封装在IP报文中，拥有专门的VRRP组播地址。在IP报文头中国，源地址为发送报文接口的主IP地址（不是虚拟IP地址，接口真实IP地址中选出来得一个主用IP地址，通常选择配置的第一个IP地址），目的地址是224.0.0.18，TTL是255，协议号是112。

VRRP协议包括2个版本：VRRPv2、VRRPv3。VRRPv2仅适用于IPv4，VRRPv3适用于IPv4和IPv6。

|  |  |  |
| --- | --- | --- |
| 报文字段 | VRRPv2 | VRRPv3 |
| Version | VRRP协议版本号，取值为2 | VRRP协议版本号，取值为3 |
| Type | VRRP通告报文的类型，取值为1，表示Advertisement | |
| VRID | 虚拟路由器ID，取值范围为1-255 | |
| Priority | Master设备在备份组中的优先级，取值范围为0-255。0表示设备停止参与VRRP备份组，用来使Backup设备尽快成为Master设备，而不必等到计时器超时；255则保留给IP地址拥有者。缺省值为100 | |
| Count IP Addrs/Count IPvX Addr | 备份组中虚拟IPv4地址的个数 | 备份组中虚拟IPv4或虚拟IPv6地址的个数 |
| Auth Type | VRRP报文的认证类型，包括：   * 无认证 * 简单认证 * MD5认证 | -- |
| Adver Int/Max Adver Int | VRRP通告报文的发送时间间隔，单位秒，缺省值为1秒 | VRRP通告报文的发送时间间隔，单位厘秒，缺省值为100厘秒（1秒） |
| IP Address/IPvX Address(es) | VRRP备份组的虚拟IPv4地址，所包含的地址数定义在Count IP Addrs字段 | VRRP备份组的虚拟IPv4地址或虚拟IPv6地址，所包含的地址数定义在Count IPvX Addrs字段 |
| Authentication Data | VRRP报文的认证字。目前仅明文简单认证和MD5认证才用到 | -- |
| rsvd | -- | VRRP报文的保留字段，必须设置为0 |

**VRRP工作原理**

1.VRRP状态机



* Initialize：为VRRP不可用状态，在此状态时设备不会对VRRP报文做任何处理。通常刚配置VRRP时或设备检测到故障时会进入Initialize状态。收到接口Up的消息后，如果设备优先级为255，则直接成为Master设备；如果优先级小于255，则会先切换至Backup状态
* Master：当VRRP设备处于Master状态时，将进行：（1）定时(Advertisement Interval)发送VRRP通告报文；（2）以虚拟MAC地址响应对虚拟IP地址的ARP请求；（3）转发目的MAC地址为虚拟MAC地址的IP报文；（4）如果是虚拟IP地址的拥有者，则接收目的IP地址为这个虚拟IP地址的IP报文；（5）如果收到比自己优先级大的报文，立即成为Backup；（6）如果收到与自己优先级相等的VRRP报文且本地接口IP地址小于对端接口IP，立即成为Backup；（7）当接收到接口的Shutdown事件时，转为Initialize状态
* Backup：当VRRP设备处于Backup状态时，将进行：（1）接收Master发送的VRRP通告报文，判断Master的状态是否正常；（2）对虚拟IP地址的ARP请求，不做响应；（3）收到目的IP地址为虚拟IP地址的IP报文时按照正常二层转发流程进行处理；（4）如果收到比自己优先级小的报文时，默认立即升主，如果配置了不抢占，则重置定时器；如果配置了抢占延迟，则重置定时器，待抢占延迟到期再升主。收到比自己优先级大的报文时，重置定时器。如果收到优先级和自己一样的报文，则重置定时器，不进一步比较IP地址。Master\_Down\_Interval(=3\*Advertisement\_Interval+Skew\_time)定时器，Backup设备在该定时器超时后仍未收到通告报文，则会转换为Master状态；（5）如果收到比自己优先级小的报文且不是0，丢弃报文，立即成为Master；如果收到报文优先级为0，定时器时间设置为Skew\_time（偏移时间，=(256-Priority)/256）：（6）当接收到Master\_Down\_Interval定时器超时的消息时，Backup状态才会转为Master状态；（7）当接收到接口的Suhtdown消息时，转为Initialize状态

2.工作过程

* VRRP备份过程组中的设备根据优先级选举出Master。Master设备通过发送免费ARP报文，将虚拟MAC地址通知给与它连接的设备或主机，从而承担报文转发任务
* Master设备周期性向备份组内所有Backup设备发送VRRP通告报文，以公布其配置信息（优先级等）和工作状态
* 如果Master设备出现故障，VRRP备份组中的Backup设备将根据优先级重新选举新的Master
* VRRP备份组状态切换时，Master设备由一台设备切换为另一台设备，新的Master设备会立即发送携带虚拟路由器的虚拟MAC地址和虚拟IP地址信息的免费ARP报文，刷新与它连接的主机或设备中的MAC表项，从而把用户流量引到新的Master设备上，整个过程对用户完全透明
* 原Master设备故障恢复时，若该设备为IP地址拥有者（优先级为255），将直接切换至Master状态；否则，将首先切换至Backup状态，且其优先级恢复为故障前配置的优先级

3.VRRP优先级

VRRP根据优先级来确定虚拟路由器中每台设备的角色（Master设备或Backup设备）。优先级越高，越有可能成为Master设备。

初始创建的VRRP设备工作在Initialize状态，收到接口Up的消息后，如果设备的优先级为255，则直接成为Master设备；如果小于255，则会先切换至Backup状态，待Master\_Down\_Interval定时器超时后再切换至Master状态。首先切换至Master状态的VRRP设备通过VRRP通告报文的交互获知虚拟设备中其他成员的优先级，进行Master的选举：

* 如果VRRP报文中Master设备的优先级高于或等于自己的优先级，则Backup设备保持Backup状态
* 如果VRRP报文中Master设备的优先级低于自己的优先级，采用抢占的方式Backup设备将切换至Master状态，采用非抢占的方式Backup设备仍保持Backup状态
* 如果多个VRRP设备同时切换到Master状态，通过VRRP通告报文的交互进行协商后，优先级较低的VRRP设备将切换Backup状态，优先级最高的VRRP设备成为最终的Master设备；优先级相同时，VRRP设备上VRRP备份组所在接口主IP地址较大的成为Master设备
* 如果创建的VRRP设备为IP地址拥有者，收到接口Up消息后，将会直接切换至Master状态

4.VRRP抢占功能

VRRP设备的工作方式有2种：

* 抢占模式：如果Backup设备的优先级高于当前Master设备，则主动将自己切换成Master设备。为防止频繁切换，支持配置抢占延时
* 非抢占模式：只要Master设备没有出现故障，Backup设备即使随后被配置了更高优先级也不会成为Master设备

5.VRRP路由器状态的通告

* 当Master设备主动放弃Master地址（如退出备份组）时，会发送优先级为0的通告报文，用来使Backup设备快速切换成Master设备，而不用等到Master\_Down\_Interval定时器超时。这个切换时间称为Skew\_time，计算方式为（256-Backup设备优先级）/256，单位秒
* 当Master设备发生故障而不能发送通告报文时，Backup设备无法立即知晓其工作状态。等到Master\_Down\_Interval定时器超时后，才会认为Master设备无法正常工作，从而将状态切换为Master。Master\_Down\_Interval定时器计算方式为3\*Advertisement\_Interval+Skew\_time，单位秒

6.安全认证

VRRPv2在通告报文中支持的认证方式包括不认证、简单认证和MD5认证。同一VRRP备份组的认证方式和认证字必须相同，否则Master设备和Backup设备无法协商成功。

**冗余备份：局域网中路由设备配置单备份组实现简单的路由冗余**

**负载分担：局域网中路由设备配置多备份组实现流量的负载均衡**

负载分担与冗余备份的不同点在于：（1）负载分担方式需要加入多个VRRP备份组，各备份组的Master设备可以不同；（2）同一台VRRP设备可以加入多个备份组，在不同的备份组中具有不同的优先级。

**管理VRRP**

当设备运行多个VRRP备份组时，每个VRRP备份组都需要维护自己的状态机，设备之间会产生大量的VRRP协议报文。为减少协议报文对带宽的占用和CPU资源消耗，可以将其中一个VRRP备份组配置为管理VRRP备份组（mVRRP），其余业务VRRP备份组与管理VRRP备份组进行绑定。

* 管理VRR备份组：与普通VRRP备份组一样，通过VRRP协议报文协商VRRP设备的主备状态。部署位置有2种情况：
* 管理VRRP与业务VRRP在同一侧。此时管理VRRP备份组作为网管使用，既负责协商设备的主备状态，也承担业务流量。此时在配置管理VRRP之前必须先创建普通VRRP备份组并配置虚拟IP地址，该虚拟IP地址即为用户设置的网关地址。
* 管理VRRP部署在Master和Backup之间的直连链路上。此时管理VRRP备份组不作为网管使用，仅负责协商设备的主备状态，不承担业务流量。因此，管理VRRP不需要具有虚拟IP地址，用户可以直接在接口上创建管理VRRP备份组。
* 业务VRRP备份组：普通VRRP备份组与管理VRRP备份组绑定后成为业务VRRP备份组（也称为成员VRRP备份组）。业务VRRP备份组不发送VRRP协议报文，状态由所在接口状态及与其绑定的管理VRRP备份组的状态共同决定。

**VRRP与接口状态联动**

当Master设备上行接口故障时，由于VRRP无法感知非备份组内接口的状态变化，可能会导致业务中断。通过联动接口状态，配置VRRP监视上行接口，当被监视的接口故障时，调整Master设备优先级，触发VRRP主备切换，减小接口故障对业务转发的影响。

IPv4 VRRP配置：

* 配置单备份组时，通过设置备份组号和虚拟IP地址，可以在指定的局域网段上添加一个备份组，从而启动对应接口的VRRP单备份功能
* 配置多备份组时，在同一个接口上配置多个VRRP备份组，可以实现负载均衡同时通过互相备份来提供更稳定可靠的网络服务
* 通过设置监视接口，动态的调整备份组的优先级，实现动态故障检测，实现备份组的状态切换

IPv6 VRRP配置：

* 配置IPv6 VRRP单备份组时，通过设置备份组号和虚拟IPv6地址，可以在指定的局域网段上添加一个备份组，从而启动对应接口的VRRP单备份功能
* 配置IPv6 VRRP多备份组时，在同一个接口上配置多个IPv6 VRRP备份组，可以实现负载均衡同时通过互相备份来提供更稳定可靠的网络服务
* 通过设置监视接口，动态调整备份组的优先级，实现动态故障监测，实现备份组的状态切换

注意点：

* 同一个VRRP备份组内路由设备上VRRP需要配置相同的虚拟IPv4地址
* 实现VRRP多备份组相互备份，需要通过在接口上配置多个相同的VRRP备份组，且通过配置不同优先级等形式形成互为主备关系，从而实现VRRP多备份组功能
* 启动VRRP需要在VLAN接口上配置

【配置参数】

先行在VLAN接口处设置好VLAN接口的IP地址，包括IPv4地址和IPv6地址。

全局设置：

* VRRP：【开关】设置是否在交换机上开启VRRP功能，默认关闭
* Master设备发送免费ARP报文时间间隔 (秒)：【text文本框】设置Master设备定时发送免费ARP报文的时间间隔，用来刷新下游交换机上的MAC地址表项。取值范围为30-1200的整数，默认120秒
* 状态恢复延迟时间 (秒)：【text文本框】设置VRRP备份组在接收到接口Up事件时不立刻响应，等到该延迟时间后再进行相应处理，防止因接口的频繁震荡而导致VRRP状态频繁切换。取值范围为0-60的整数，默认0秒

VRRP备份组设置：

添加VRRP备份组：

* VRID：【text文本框】设置虚拟路由器标识，取值范围为1-255的整数，具有唯一性
* 类型：【单选】设置该虚拟路由器的类型，选项有{IPv4 VRRP| IPv6 VRRP}
* 接口：【下拉框】选择该虚拟路由器绑定的VLAN接口，必须为已存在IP地址的VLAN接口。选择后，在下方显示该VLAN接口的IP地址（根据类型的选择设置相应的IP地址）
* 虚拟IP地址：【text文本框】设置此虚拟路由器VRRP备份组的虚拟IP地址，以IP地址格式输入（根据类型的选择设置相应的IP地址）

管理VRRP备份组：

* 绑定管理VRRP备份组；【开关】设置是否绑定管理VRRP备份组，默认关闭。
* 管理VRRP备份组：【下拉框】选择指定的VRRP备份组作为该业务VRRP备份组的管理VRRP备份组。绑定之后，业务VRRP状态机就丧失了独立性，即会删除协议定时器，不再收发协议报文，通过直接拷贝管理备份组的状态来实现自己的状态机。成员VRRP备份组与管理VRRP备份组绑定之后不再周期发送VRRP通告报文，需要依赖免费ARP或网关回应的ARP应答刷新MAC。

注：1.双栈业务VRRP同时存在时，业务VRRPv4仅能与管理VRRPv4绑定，业务VRRPv6仅能与管理VRRPv6绑定；

2.一个接口上最多能够配置一个业务VRRPv4和一个业务VRRPv6；

3.一个接口下有多个业务VRRP，则只有一个业务VRRP可以绑定管理VRRP。

* 优先级：【text文本框】当且仅当绑定管理VRRP备份组开启后，不支持配置。设置交换机在VRRP备份组中的优先级，取值范围为1-254的整数，默认100。数值越大，优先级越高。

注：当虚拟IP地址设置得与VLAN接口IP地址一样时，优先级固定为255，此处配置可配但不生效

* VRRP版本：【单选】当且仅当类型选择“IPv4 VRRP”时支持配置。选择VRRP备份组的VRRP协议版本号，选项有{VRRPv2 | VRRPv3}，默认VRRPv2。IPv6 VRRP默认使用VRRPv3协议版本。
* VRRPv3通告报文发送模式：【下拉框】当VRRP版本选择“VRRPv3”时支持配置，选项有{仅v2 | 仅v3| v2&v3}，默认仅v3。
* 抢占方式：【单选】设置交换机在VRRP备份组中的抢占模式，选项有{立即抢占 |延迟抢占}，默认立即抢占。
* 抢占延时 (秒)：【text文本框】当抢占方式选择“延迟抢占”时支持配置，取值范围为1-3600的整数
* VRRP通告报文发送时间间隔 (秒)：【text文本框】设置Master设备定时向组内Backup设备发送VRRP通告报文的时间间隔。当VRRP类型为“VRRPv2”时，取值范围为1-255的整数；当VRRP类型为“VRRPv3”时，取值范围为1-40的整数，默认值均为1秒。
* 认证方式：【下拉框】当且仅当VRRP版本选择”VRRPv2“时支持配置，选项有{无|简单认证|MD认证}，默认无。
* \*密钥：【text文本框】当选择“简单认证”或“MD5认证”时，支持配置密钥，长度为1-8字符

平滑倒换：

* VRRP协议报文时间间隔学习功能：【开关】使能VRRP协议报文时间间隔学习功能，默认开启。开启后，设备上非Master状态的VRRP会进行通告报文时间间隔学习，调整自身定时器与对应Master发送通告报文的时间间隔保持同步。
* 平滑倒换：【开关】当且仅当VRRP协议报文时间间隔学习功能开启后，才支持配置，默认开启。开启平滑倒换功能后，Backup备份组将学习平滑倒换时间，使VRRP在平滑倒换期间的超时时间延长，保证在此时间内VRRP状态不变。
* VRRP协议报文发送时间间隔 (秒)：【text文本框】设置平滑倒换期间，VRRP协议报文发送时间间隔。Master设备在使能了平滑倒换功能后，主备倒换期间，以此时间间隔发送VRRP报文。取值范围为1-255秒，默认100秒

与接口状态联动：

注：当设备为IP地址拥有者时，不允许配置监视接口

* 监视接口：【多选，至多8个】选择被监视的上行接口，选项为VLAN接口，必须为非备份组内的VLAN接口。当被监视的接口down时，调整交换机的优先级，触发主备进行切换，实现业务正常转发；当被监视的接口状态恢复时，设备在备份组中的优先级将恢复至原来的值。
* 优先级增加值：【text文本框】当被监视的接口状态变为Down时，优先级增加的数值，增加后最高只能为254。取值范围为1-255的整数
* 优先级降低值：【text文本框】当被监视的接口状态变为Down时，优先级降低的数值，降低后最低只能为1。取值范围为1-255的整数，默认10

VRRP备份组列表：

* 列表显示VRID、类型、VLAN接口/IP地址、虚拟IP地址、优先级（若为业务VRRP备份组则显示“--”）、优先级、VRRP版本、抢占方式、VRRP通告报文发送时间间隔、认证方式、平滑倒换、状态
* 支持添加，至多255个
* 支持编辑，以VRID为索引
* 支持单个/批量/全部删除

数据统计：显示VRRP备份组的报文收发统计信息

* 列表显示VRID、VLAN接口、切换至Master状态的次数、切换至Backup状态的次数、切换至Initialize状态的次数、收到的Advertisement报文数、发送的Advertisement报文数、Advertisement时间间隔错误的次数、认证错误次数、TTL错误次数、收到优先级为0的Advertisement报文数、发送优先级为0的Advertisement报文数、收到的无效类型VRRP报文数、收到虚拟IP地址列表错误次数、不能识别认证类别的报文数、不匹配认证的报文数、报文长度错误次数、业务VRRP因绑定管理VRRP后所丢弃的接收报文数、收到的攻击报文数、自发自收的报文数
* 支持筛选指定VRID或VLAN接口进行查看

# 组播业务/Multicast

## IP组播 (FP3)

【功能概述】

IP组播（IP Multicasting）是对硬件组播的抽象，是对标准IP网络层协议的扩展内组播路由协议。

IP组播通信是IP报文从一个源发出，被转发到一组特定的接收者。相对于单播和广播，IP组播可以有效地节约网络带宽、降低网络负载，避免广播堵塞带来的诸如摄像头花屏、视频马赛克等问题，被广泛应用于IPTV、实时数据传送和多媒体会议等网络业务。

**组播基本概念**

1.组播组：用IP组播地址进行标识的一个集合。任何用户主机（或其他接收设备），加入一个组播组，就成为了该组成员，可以识别并接收发往该组播组的组播数据。

2.组播源：信息的发送者，一个组播源可以同时向多个组播组发送数据，多个组播源也可以同时向一个组播组发送报文。

3.组播组成员：所有加入某组播组的主机称为该组播组的成员。组播组中的成员是动态的，主机可以在任何时刻加入或离开组播组。

4.组播路由器：支持三层组播功能的路由器或交换机。组播路由器不仅能够提供组播路由功能，也能够在与用户连接的末梢网段上提供组播组成员的管理功能。

配置组播流二层流向控制：通过配置组播允许转发出口，确保组播流的报文仅允许从这些端口转发。只控制组播流在端口上的转发行为，不直接影响组播协议对协议报文的处理。但是由于组播协议（如PIM-DM后PIM-SM）的某些特性是依赖组播数据流驱动的，所以组播路由协议的行为仍然可能被影响。

配置组播不间断转发参数：正常运行情况下，SSP将硬件组播转发表实时同步到从管理板。当管理板切换后，原从管理板组播控制面配置命令加载，组播协议（IGMP Snooping等）重新收敛。组播不间断转发（Non-Stop Forwarding）功能保证在组播协议重新收敛的时间段内，组播数据流的转发不间断。当设置的协议收敛时间超时后，在协议收敛时间内未被更新过的所有组播转发表项将被删除。

配置组播硬件表项溢出覆盖机制：创建组播转发表项时，如果硬件转发表项资源已满，将删除最早创建的硬件表项资源，添加新增的表项。

IP组播地址：IPv4中IP组播使用D类地址格式，D类地址的前四位是1110，因为D类地址范围为224.0.0.0-239.255.255.255，每个D类IP地址标志一个组播组。

## IGMP (FP3)

## MLD (FP3)

## IGMP Snooping (FP1C)

【功能概述】

基本原理：

IGMP Snooping作为一种IPv4二层组播协议，通过侦听三层组播设备和用户主机之间发送的组播协议报文来维护组播报文的出接口信息，从而管理和控制组播数据报文在数据链路层的转发。当主机和上游三层设备之间传递的IGMP协议报文通过二层组播设备时，IGMP Snooping分析报文携带的信息（报文类型、组播组地址、接收报文的接口灯），根据这些信息建立和维护二层组播转发表，从而指导组播数据在数据链路层按需转发。

基本概念：

|  |  |  |
| --- | --- | --- |
| 端口角色 | 作用 | 如何生成 |
| 路由器端口（Router Port）  注：路由器端口都是指二层组播设备上朝向组播路由器的接口 | 二层组播设备上朝向三层组播设备（DR或IGMP查询器）一侧的接口，二层组播设备从此接口接收组播数据报文 | * 由协议生成的路由器端口叫做动态路由器端口。收到源地址不为0.0.0.0的IGMP普遍组查询报文或PIM Hello报文（三层组播设备的PIM接口向外发送的用于发送并维持邻居关系的报文）的接口都将被视为动态路由器端口 * 手动配置的路由器端口叫做静态路由器端口 |
| 成员端口（Member Port） | 又称组播组成员端口，表示二层组播设备上朝向组播组成员一侧的端口，二层组播设备往此接口发送组播数据报文 | * 由协议生成的成员端口叫做动态成员端口。收到IGMP Report报文的接口，二层组播设备会将其标识为动态成员端口 * 手工配置的成员端口叫做静态成员端口 |

路由器端口和成员端口，是二层组播转发表项中的一个重要信息：出接口。其中，路由器端口相当于上游接口，成员端口相当于下游接口。通过协议报文学习到的端口，对应的为动态表项；而手工配置的端口，对应的为静态表项。动态表项会定时老化，当动态路由器端口在其老化时间超时前没有受到IGMP Query或PIM Hello报文，设备将把该接口从路由器端口列表中删除，如果长期稳定转发IGMP Report或Leave报文到上游IGMP查询器，则配置其为静态路由器端口；动态成员端口亦如此，若需要固定接收发往某组播组或组播源组的数据，可以配置其为静态成员端口。

除了出接口外，每条表项还包括组播组地址和VLAN ID。

* 组播组地址，可以为组播IP地址，也可以为组播IP地址映射后的组播MAC地址，按照IP地址转发的模式可以避免MAC地址转发模式中的地址重复问题。
* VLAN ID，指定了二层广播域范围。如果使用了组播VLAN功能，入VLAN ID为组播VLAN ID，出VLAN ID为主机所在的用户VLAN ID，否则入VLAN ID和出VLAN ID均为主机所在VLAN ID。

工作机制：

二层组播设备运行了IGMP Snooping后，收到不同的IGMP协议报文会进行不同的处理，并在此过程中建立起二层组播转发表项。

|  |  |  |
| --- | --- | --- |
| IGMP工作阶段 | 二层组播设备收到的报文类型 | 处理方式 |
| 普遍组查询  IGMP查询器定期向本地网段内的所有主机与路由器发送IGMP查询组查询报文，以查询该网段有哪些组播组的成员 | IGMP组播组查询报文 | 向VLAN内除接收接口外的其他所有接口转发，并对接收接口做如下处理：   * 如果路由器端口列表中尚未包含该接口，则将其添加进去，并启动老化定时器 * 如果路由器端口列表中已包含该动态路由器端口，则重置老化定时器 |
| 成员报告  有两种情况：   * 成员收到IGMP普遍组查询报文后，回应IGMP报告报文 * 成员主动向IGMP查询器发送IGMP报告报文以声明加入该组播组 | IGMP报告报文 | 向VLAN内所有路由器端口转发。从报文中解析出主机要加入的组播组地址，并对接收接口做如下处理：   * 如果不存在该组对应的转发表项，则创建转发表现，将该接口作为动态成员端口添加到出接口列表中，并启动老化定时器 * 如果已存在该组对应的转发表项，但出接口列表中未包含该接口，则将该接口作为动态成员端口添加到出接口列表，并启动老化定时器 * 如果已存在该组对应的转发表项，且出接口列表中已包含该动态成员端口，则重置其老化定时器 |
| 成员离开组播组  有两个阶段：   * 运行IGMPv2或IGMPv3的成员发送IGMP离开保温，以通知IGMP查询器自己离开了某个组播组 * IGMP查询器收到IGMP离开报文后，从中解析出组播组地址，并通过接收接口向该组播组发送IGMP特定组查询报文/IGMP特定源组查询报文 | IGMP离开报文 | 判断离开的组是否存在对应的转发表项，以及转发表项出接口列表是否包含报文的接收接口：   * 如果不存在该组对应的转发表项，或者该组对应转发表项的出接口列表中不包含接收接口，二层组播设备不转发该报文，将其直接丢弃 * 如果存在该组对应的转发表项，且转发表项的出接口列表中包含该接口，二层组播设备会将报文向VLAN内所有路由器端口转发   对于IGMP离开报文的接收接口（假定为动态成员端口），二层组播设备在其老化时间内：   * 如果从该接口收到了主机响应IGMP特定组/源组查询的报告报文，表示接口下还有该组的成员，于是重置其老化定时器 * 如果没有从该接口收到主机响应IGMP特定组/源组查询的报告报文，则表示接口下已没有该组成员，则在老化时间超时后，将接口从该组的转发表项出接口列表中删除 |
| IGMP特定组查询报文/IGMP特定源组查询报文 | 向有特定组成员的接口转发 |

此外，当二层组播设备收到PIM Hello报文时，向VLAN内除接收接口外的其他所有接口转发，并对接收接口做如下处理：

* 如果路由器端口列表中已包含该动态路由器端口，则重置老化定时器
* 如果路由器端口列表中尚未包含该接口，则将其添加进去，并启动老化定时器

如果配置了静态路由器端口，二层组播设备收到IGMP报告和离开报文也会向静态路由器端口转发。如果配置了静态成员端口，则转发表项中会添加该接口为出接口。

当二层组播设备上建立了二层组播转发表项以后，二层组播设备接收到组播数据报文时，依据报文所属VLAN和报文的目的地址（即组播组地址）查找转发表项是否存在对应的“出接口信息”。如果存在，则将报文发送到相应的组播组成员端口和路由器端口；如果不存在，则丢弃该报文或将报文在VLAN内广播。

【配置参数】

**IGMP Snooping与MLD Snooping的公共配置：**

* 未知组播报文：【下拉框】设置交换机对未知组播报文的处理方法，选项有{泛洪|丢弃|转发至路由器端口}，默认泛洪。选项“转发至路由器端口”仅限IGMP Snooping或MLD Snooping开启时才可配置。

**全局配置：**

* IGMP Snooping：【开关】设置是否开启IGMP Snooping功能，默认关闭。
* 组播转发模式：【单选】设置VLAN内组播数据报文的转发模式，选项有{基于MAC| 基于IP}，默认基于MAC。
* IGMP版本：【单选】设置IGMP版本号，选项有{IGMPv2|IGMPv3}，默认IGMPv2。
* 报文抑制：【开关】当且仅当IGMP版本选择IGMPv2时，支持配置。设置是否开启Report~~和Leave~~报文抑制功能，默认关闭。开启后，针对每一个组播组，交换机会在第一次有成员加入需要建立组播表项，以及响应IGMP查询报文时，向上游转发一份Report报文~~；在最后一个组成员离开需要删除组播表项时，向上游转发一份Leave报文~~。

**基于VLAN的IGMP Snooping设置：**

* VLAN：选择需要配置IGMP Snooping的VLAN，可多选。
* IGMP Snooping：【开关】设置是否对VLAN开启IGMP Snooping功能，默认关闭。
* 路由器端口自动学习：【开关】设置VLAN内的路由器端口自动学习功能，默认开启。
* 端口快速离开：【开关】设置是否开启VLAN内端口快速离开功能，默认关闭。
* 查询健壮性：【text文本框】用于计算端口老化时间，用来指示当前VLAN内的IGMP健壮系数。取值为1-7的整数，默认2。
* 查询间隔 (秒)：【text文本框】设置发送IGMP普遍组查询报文的时间间隔。取值为30-18000的整数，默认125秒。
* 查询最大响应时间 (秒)：【text文本框】设置VLAN里通用查询最大响应时间。取值为5-20的整数，默认10秒。
* 最后一个成员查询次数：【text文本框】设置发送特定查询报文的次数。取值为1-7的整数，默认2。
* 最后一个成员查询间隔：【text文本框】设置最后一个成员查询报文的时间间隔。取值为1-25的整数，默认1秒。

VLAN列表：

* 列表显示VLAN、IGMP Snooping状态、路由器端口自动学习、端口快速离开、查询健壮性、查询间隔、查询最大响应间隔、最后一个成员查询次数、最后一个成员查询间隔
* 支持编辑

**IGMP Snooping查询器：**

* VLAN：选择需要配置IGMP Snooping查询器的VLAN，可多选。
* IGMP Snooping查询器：【开关】设置是否开启VLAN上的IGMP Snooping查询器，默认关闭。
* IGMP Snooping查询器运行版本：【下拉框】设置IGMP Snooping查询器的运行版本，选项有{IGMPv2|IGMPv3}，默认IGMPv2。
* IP地址：【text文本框，非必填】为空时即使用VLAN IPv4地址。

注：IP地址无法设置全1、全0、组播和127.0.0.1地址，否则以底层错误码形式报错。可以学习这些地址，但不支持手动设置。

IGMP Snooping查询器列表：

* 列表显示VLAN、查询器开关、运行版本、查询器状态和IP地址
* 支持编辑

**路由器端口：**

* VLAN：选择静态路由器端口的关联VLAN，从已有VLAN中选择，可多选
* 静态端口/Static Port：选择需要设置静态路由器端口的交换机端口，包括电口、光口和聚合接口。可多选
* 禁用端口/Forbidden Port：选择不能用于组播路由转发的交换机端口，包括电口、光口和聚合接口。可多选

注：禁用端口和静态端口互斥。

路由器端口列表：

* 列表包含手动静态配置的路由器端口，也包含动态路由器端口，还有禁用端口
* 列表显示VLAN、路由器端口（上述三类）、老化时间（只有动态路由器端口有）
* 支持编辑
* 支持删除
* 支持刷新

**组播地址表：**

支持添加静态组播地址表项：

* VLAN：【单选】设置组播MAC地址表项所属的VLAN。
* 组播地址：【text文本框】设置待添加的组播IPv4地址。输入格式要求满足IPv4地址格式。
* 成员端口：选择静态组播地址表项的成员端口，包括电口、光口和聚合接口，可多选。

组播地址列表：

* 列表显示VLAN、组播地址、源IP地址（仅IGMPv3支持，IGMPv2显示“--”）、成员端口、地址类型（静态|动态）、老化时间（单位秒，只有动态组播地址有）
* 支持编辑静态组播地址，仅支持编辑成员端口
* 支持删除静态组播地址
* 支持刷新

**组播策略：**

添加组播策略：最多添加128条

* 策略ID：【text文本框】设置组播策略的ID，取值为1-128的整数
* 动作：【下拉框】设置组播策略对指定报文的动作，选项有{允许|拒绝}，默认允许。
* 组播地址：【text文本框】设置组播IPv4地址，采用点分十进制输入，需要校验格式，若输入不符合规范则报错提示。支持输入IPv4地址，也支持输入IPv4地址范围。

组播策略列表：

* 列表显示策略ID、动作、组播地址
* 支持编辑组播策略
* 支持删除单条/批量/全部组播策略。若组播策略已被端口引用，则无法删除，必须先解除端口与组播策略的绑定

**组播端口表：**

* 接口：选择需要配置的端口，包括电口、光口和聚合接口，可多选。
* 最大组播组数：【text文本框】设置允许端口加入的组播组最大数量，取值为0-256的整数，默认256。选择0时，表示不允许端口加入组播组。
* 动作：【下拉框】设置当端口组播超过限制之后的动作，选项有{拒绝|替换}，默认拒绝。拒绝表示不再学习IGMP Report报文创建新的转发表项，替换表示更新之前学习到的表项。
* 组播策略：【开关】默认关闭。
* 策略ID：【下拉框】选择端口使用的组播策略。若无

组播端口列表：

* 列表显示端口、最大组播组数、动作、组播策略
* 支持编辑

## MLD Snooping(FP1C)

【功能概述】

基本原理：

MLD Snooping作为一种IPv6二层组播协议，通过侦听三层组播设备和用户主机之间发送的组播协议报文来维护组播报文的出端口信息，从而管理和控制组播数据报文在数据链路层的转发。当主机和上游三层设备之间传递的MLD协议报文通过二层设备时，MLD Snooping分析报文携带的信息，根据这些信息建立和维护二层组播转发表，从而指导组播数据在数据链路层按需转发。

基本概念：

|  |  |  |
| --- | --- | --- |
| 端口角色 | 作用 | 如何生成 |
| 路由器端口（Router Port）  注：路由器端口都是指二层设备上朝向组播路由器的接口，而不是指路由器上的接口。 | 二层设备上朝向三层组播设备（DR或MLD查询器）一侧的接口，二层设备从此接口接收组播数据报文。 | * 由协议生成的路由器端口叫做动态路由器端口。收到源地址不为0::0的MLD普遍组查询报文或IPv6 PIM Hello报文（三层组播设备PIM接口向外发送的用于发现并维持邻居关系的报文）的接口都将被视为动态路由器端口。 * 手工配置的路由器端口叫做静态路由端口。 |
| 成员端口（Member Port） | 又称组播组成员端口，表示二层设备上朝向组播组成员一侧的端口，二层设备往此接口发送组播组数据报文 | * 由协议生成的成员端口叫做动态成员端口。收到MLD报告报文的接口，二层设备会将其标识为动态成员端口 * 由手工配置的成员端口叫做静态成员端口 |

路由器端口和成员端口，是二层组播转发表项中的一个重要信息：出接口。其中路由器端口相当于上游接口，成员端口相当于下游接口。通过协议报文学习到的端口，对应的为动态表项；而手工配置的端口，对应的为静态表项。除了出接口外，每条表项包包括组播组地址和VLAN。

* 组播组地址，可以为组播IP地址，也可以为组播IP地址映射后的组播MAC地址。按照IP地址转发的模式可以避免MAC地址转发模式中的地址重复问题。
* VLAN，指定了二层广播域范围。如果使用了组播VLAN功能，入VLAN ID为组播VLAN ID，出VLAN ID为主机所在的用户VLAN ID。否则入VLAN ID和出VLAN ID均为主机所在VLAN ID。

工作机制：

二层设备运行了MLD Snooping后，收到不同的MLD协议报文会进行不同的处理，并在此过程中建立起二层组播转发表项。

|  |  |  |
| --- | --- | --- |
| 二层设备收到的报文类型 | MLD工作阶段 | 处理方式 |
| MLD普遍组查询报文 | 普遍组查询  MLD查询器定期向本地网段内的所有主机与路由器发送MLD普遍组查询报文，以查询该网段有哪些组播组的成员 | 向VLAN内除接收接口外的其他所有接口转发，并对接收接口做如下处理：   * 如果路由器端口列表中已包含该动态路由器端口，则重置老化定时器。 * 如果路由器端口列表中尚未包含该接口，则将其添加进去，并启动老化定时器。 |
| MLD报告报文 | 成员报告关系   * 有两种情况： 成员收到MLD普遍组查询报文后，回应MLD报告报文 * 成员主动向MLD查询器发送MLD报告报文以声明加入该组播组 | 向VLAN内所有路由器端口转发。从报文中解析出主机要加入的组播组地址，并对接收接口做如下处理：   * 如果不存在该组对应的转发表项，则创建转发表项，将该接口作为动态成员端口添加到出接口列表中，并启动老化定时器 * 如果已存在该组对应的转发表项，但出接口列表中未包含该接口，则将该接口作为动态成员端口添加到出接口列表，并启动老化定时器 * 如果已存在该组所对应的转发表项，且出接口列表中已包含该动态成员端口，则重置其老化定时器 |
| MLD离开报文 | 成员离开组播组  有两个阶段：   * 成员发送MLD离开报文，以通知组播路由器自己离开了某个组播组 * MLD查询器收到MLD离开报文后，从中解析出组播组地址，并通过接收接口向该组播组发送MLD最后侦听者查询报文/MLD特定源组查询报文 | 判断离开的组是否存在对应的转发表项，以及转发表项出接口列表是否包含报文的接收接口：   * 如果不存在该组对应的转发表项，或者该组对应转发表项的出接口列表中不包含接收接口，二层设备不转发该报文，将其直接丢弃 * 如果存在该组对应的转发表项，且转发表项的出接口列表中包含该接口，二层设备会将报文向VLAN内所有路由器端口转发   对于MLD离开报文的接收接口（假定为动态成员端口），二层设备在其老化时间内：   * 如果从该接口收到了主机响应该特定组查询的MLD报告报文，表示接口下还有该组的成员，于是重置其老化定时器。 * 如果没有从该接口收到主机响应特定组查询的MLD报告报文，则表示接口下已没有该组成员，则在老化时间超时后，将接口从该组的转发表项出接口列表中删除 |
| MLD最后侦听者查询报文/MLD特定源组查询报文 | 向有特定组成员的接口转发 |

此外，当二层设备收到IPv6 PIM Hello报文时，向VLAN内除接收接口外的其他所有接口转发，并对接收接口做如下处理：

* 如果路由器端口列表中已包含该动态路由器端口，则重置老化定时器
* 如果路由器端口列表中尚未包含该接口，则将其添加进去，并启动老化定时器

如果是静态配置路由器端口，二层设备收到MLD报告和离开报文也会向静态路由器端口转发。如果配置了静态成员端口，则转发表项中会添加该接口为出接口。当二层设备上建立了二层组播转发表项以后，二层设备接收到组播数据报文时，依据报文所属VLAN和报文的目的地址（即IPv6组播组地址）查找转发表项是否存在对应的“出接口信息”。如果存在，则将报文发送到所有组播组成员端口；如果不存在，则丢弃该报文或将报文在VLAN内广播。

【配置参数】

**IGMP Snooping与MLD Snooping的公共配置：**

* 未知组播报文：【下拉框】设置交换机对未知组播报文的处理方法，选项有{泛洪|丢弃|转发至路由器端口}，默认泛洪。选项“转发至路由器端口”仅限IGMP Snooping或MLD Snooping开启时才可配置。

**全局配置：**

* MLD Snooping：【开关】设置是否开启MLD Snooping功能，默认关闭。
* 组播转发方式：【单选】设置组播数据报文的转发方式，选项有{DMAC-VID | DIP-VID}，默认DMAC-VID。
* MLD版本：【单选】设置IGMP版本号，选项有{MLDv1|MLDv2}，默认MLDv1。
* 报文抑制：【开关】当且仅当MLD版本选择“MLDv1”时，支持配置。设置是否开启Report~~和Leave~~报文抑制功能，默认关闭。开启后，针对每一个组播组，交换机会在第一次有成员加入需要建立组播表项，以及响应MLD查询报文时，向上游转发一份Report报文~~；在最后一个组成员离开需要删除组播表项时，向上游转发一份Leave报文~~。

**VLAN设置：**

* VLAN：选择需要配置MLD Snooping的VLAN，可多选。
* MLD Snooping：【开关】设置是否对VLAN开启MLD Snooping功能，默认关闭。
* 路由器端口自动学习：【开关】设置VLAN内的路由器端口自动学习功能，默认开启。
* 端口快速离开：【开关】设置是否开启VLAN内端口快速离开功能，默认关闭。
* 查询健壮性：【text文本框】用于计算端口老化时间，用来指示当前VLAN内的MLD健壮系数。取值为1-7的整数，默认2。
* 查询间隔 (秒)：【text文本框】设置MLD普遍组查询报文的时间间隔。取值为30-18000的整数，默认125秒。
* 查询最大响应时间 (秒)：【text文本框】设置VLAN里通用查询最大响应时间。取值为5-20的整数，默认10秒。
* 最后一个成员查询次数：【text文本框】设置发送特定查询报文的次数。取值为1-7的整数，默认2。
* 最后一个成员查询间隔：【text文本框】设置最后一个成员查询报文的时间间隔。取值为1-25的整数，默认1秒。

VLAN列表：

* 列表显示VLAN、MLD Snooping状态、路由器端口自动学习、端口快速离开、查询健壮性、查询间隔、查询最大响应间隔、最后一个成员查询次数、最后一个成员查询间隔
* 支持编辑

MLD Snooping查询器设置：

* VLAN：选择需要配置MLD Snooping的VLAN，可多选。
* MLD Snooping查询器：【开关】设置是否开启VLAN上的MLD Snooping查询器，默认关闭。
* MLD Snooping查询器运行版本：【下拉框】设置MLD Snooping查询器的运行版本，选项有{MLDv1|MLDv2}，默认MLDv1。
* IPv6地址：【text文本框，非必填】为空时即使用VLAN IPv6地址。

注：IPv6地址无法设置全1、全0、组播和loopback接口地址，否则以底层错误码形式报错。可以学习这些地址，但不支持手动设置。

MLD Snooping查询器列表：

* 列表显示VLAN、查询器开关、运行版本、查询器状态和IPv6地址(默认VLAN IP，支持修改)
* 支持编辑

路由器端口：

* VLAN：选择静态路由器端口的关联VLAN，从已有VLAN中选择，可多选
* 静态端口/Static Port：选择需要设置静态路由器端口的交换机端口，包括电口、光口和聚合接口。可多选
* 禁用端口/Forbidden Port：选择不能用于组播路由转发的交换机端口，包括电口、光口和聚合接口。可多选

注：禁用端口和静态端口互斥。

路由器端口列表：

* 列表包含手动静态配置的路由器端口，也包含动态路由器端口，还有禁用端口
* 列表显示VLAN、路由器端口（上述三类）、老化时间（只有动态路由器端口有）
* 支持编辑
* 支持删除
* 支持刷新

**组播地址表：**

支持添加静态组播地址表项：

* VLAN：【单选】设置组播MAC地址表项所属的VLAN。
* 组播地址：【text文本框】设置待添加的组播IPv6地址。输入格式要求满足IPv6地址格式。
* 成员端口：选择静态组播地址表项的成员端口，包括电口、光口和聚合接口，可多选。

组播地址列表：

* 列表显示VLAN、组播地址、源IP地址（仅MLDv2支持，MLDv1显示“--”）成员端口、地址类型（静态|动态）、老化时间（单位秒，只有动态组播地址有）
* 支持编辑静态组播地址
* 支持删除静态组播地址
* 支持刷新

**组播策略：**

添加组播策略：最多添加128条

* 策略ID：【text文本框】设置组播策略的ID，取值为1-128的整数
* 动作：【下拉框】设置组播策略对指定报文的动作，选项有{允许|拒绝}，默认允许。
* 组播地址：【text文本框】设置组播IPv6地址，需要校验格式，若输入不符合规范则报错提示。支持输入IPv6地址，也支持输入IPv6地址段。

组播策略列表：

* 列表显示策略ID、动作、组播地址
* 支持编辑组播策略
* 支持删除单条/批量/全部组播策略。若组播策略已被端口引用，则无法删除，必须先解除端口与组播策略的绑定

**组播端口表：**

* 接口：选择需要配置的端口，包括电口、光口和聚合接口，可多选。
* 最大组播组数：【text文本框】设置允许端口加入的组播组最大数量，取值为0-256的整数，默认256。选择0时，表示不允许端口加入组播组。
* 动作：【下拉框】设置当端口组播超过限制之后的动作，选项有{拒绝|替换}，默认拒绝。拒绝表示不再学习MLD Report报文创建新的转发表项，替换表示更新之前学习到的表项。
* 组播策略：【下拉框】选择端口使用的组播策略。

组播端口列表：

* 列表显示端口、最大组播组数、动作、组播策略
* 支持编辑

## MVR (FP3) 【待评审】

【功能概述】

Multicast VLAN Registration（组播VLAN注册），通过配置组播VLAN的方式，将交换机的原属于不同用户的VLAN的成员端口加入到组播VLAN内，并在使能了IGMP Snooping功能以后，使不同VLAN内的用户共用一个组播VLAN。这样，组播流只在一个组播VLAN内传输，从而节省了带宽。

三层的IGMP协议广泛用于IPv4网络组播。在二层网络中，IGMP协议使用资源效率低下，例如：即使少数几个接收者（receivers）连接到交换机的几个端口，交换机仍然需要将组播流量泛洪到所有端口。

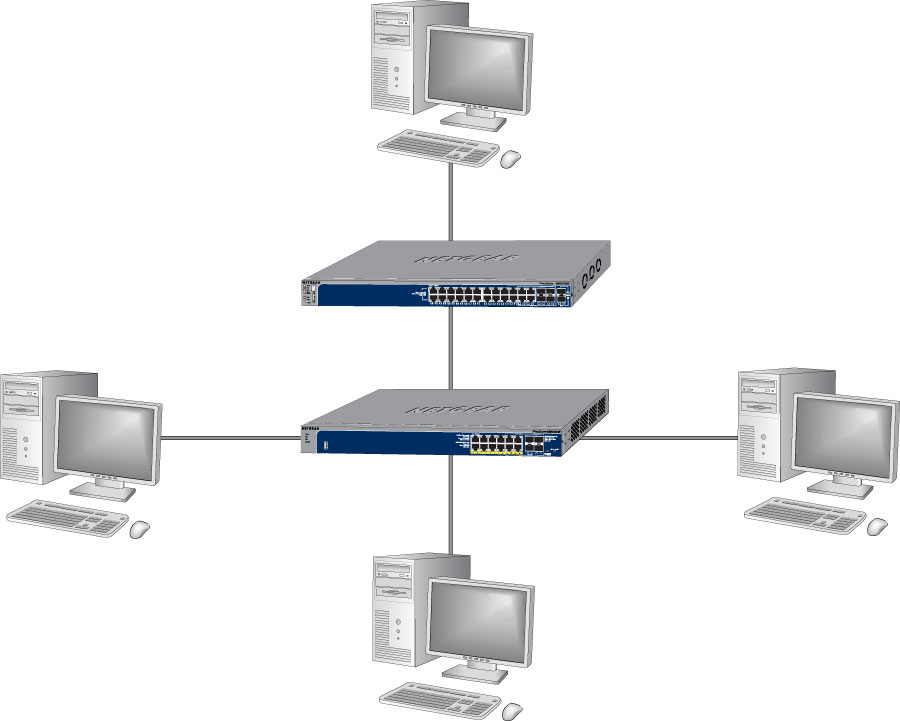
为了解决这个问题，人们提出了IGMP Snooping协议，但当接收者（receivers）位于不同VLAN时，IGMP Snooping却无能为力（IGMP Snooping通常只在单个VLAN中配置与生效）。组播VLAN注册（MVR）旨在解决接收者处于不同VLAN时的问题，它使用一个专用的、手工配置的VLAN（组播VLAN）在二层网络中转发组播流量，同时能与IGMP Snooping协同使用。

MVR像IGMP Snooping协议一样，允许二层交换机监听IGMP控制协议。两个协议彼此独立运作，可同时配置在交换机上。如果同时开启两个特性，MVR将只监听静态配置到其MVR功能上的组的John和Report消息，而其他组的仍然由IGMP Snooping进行管理。

配置MVR功能时，有两种类型的MVR端口：源端口和接收端口

* 源端口：组播VLAN中的组播流经过的端口
* 接收端口：监听组播主机连接到交换机的端口。它可以使用（或不使用）除组播VLAN外的任何VLAN。这意味着，开启MVR功能的交换机将组播VLAN源端口的VLAN tag替换为接收端口使用的VLAN tag。

组播VLAN是在特定网络中手动配置的、专用于MVR的VLAN。对于所有的源端口，它需要被明确配置，常用于在网络中传输组播流，同时避免组播流在不同VLAN中的重复。



RP(VLAN 1003)

RP(VLAN 1002)

RP(VLAN 1001)

组播客户端

组播客户端

组播客户端

MVR

SP(VLAN 999)

IGMP

组播源

MVR特性被设计作为基于以太网的服务提供网络中大范围展开组播应用，例如：服务提供网络中使用组播协议的电视频道广播、终端为大屏幕电视或电脑。

MVR支持2种模式：

* 兼容模式：MVR交换机不学习组播组。由于MVR不从主机（RP端口）转发IGMP报告到IGMP路由器（SP端口），组播组需要手动配置。使用该模式后，需手动配置IGMP路由器传输所有的组播流到MVR交换机主机。默认情况下，交换机使用兼容模式。
* 动态模式：MVR交换机监听从源端口发出的IGMP查询并将IGMP报告从主机转发到组播VLAN上的IGMP路由器来学习现有组播组（组播VLAN带有恰当的VLAN ID转换）。

源端口：tagged组播VLAN

接收端口：untagged组播VLAN

【配置参数】

全局配置：

* MVR：【开关】设置是否开启交换机MVR功能，默认关闭。
* 组播VLAN：【下拉框，单选】从已有VLAN中选择一个作为组播VLAN，默认VLAN 1
* MVR模式：【单选】设置MVR的模式，选项有{兼容模式 | 动态模式}，默认兼容模式
* MVR查询器响应时间 (秒)：【text文本框】设置查询器的响应时间，取值范围为1-10的整数，默认1秒
* 组开始地址：【text文本框】设置MVR组播地址的开始地址，IPv4组播地址格式
* 组数：【text文本框】设置MVR组地址数量，取值范围为1-128的整数，默认1。此处设置的个数为组地址添加的最大个数上限
* MVR最大组播组数：显示值，默认128
* MVR当前组播组数：显示值，默认0

端口设置：

* 接口：选择交换机的接口，包括电口、光口和聚合接口，可多选
* 类型：【单选】设置所选端口的类型，选项有{无| 源端口| 接收端口}，默认无
* 立即离开：【开关】设置是否开启所选端口的立即离开功能，默认关闭。

端口列表：

* 列表显示端口、类型、立即离开和状态
* 支持编辑

组地址设置：

添加组地址：

* VLAN：显示组播VLAN
* 组地址：【text文本框】设置组播IPv4地址，输入格式满足IPv4地址格式。输入范围为全局设置的组地址起始地址-组数上限的组地址结束地址
* 成员端口：当且仅当全局设置/MVR模式选择“兼容模式”时配置有效。选择静态组播地址表项的成员端口，包括电口、光口和聚合接口，可多选

组地址列表：

* 列表显示VLAN、组地址、状态、成员端口、成员类型（静态|动态）、老化时间（单位秒，只有动态成员端口有）
* 支持编辑静态组播地址，仅支持编辑成员端口
* 支持删除静态组播地址
* 支持刷新

# QoS(FP1B)

【功能概述】

网络的普及和业务的多样化使得互联网流量激增，从而产生网络拥塞，增加转发时延，严重时还会产生丢包，导致业务质量下降甚至不可用。所以，要在网络上开展这些实时性业务，就必须解决网络拥塞问题，最好的办法是增加网络的带宽，但从运营、维护的成本考虑，这不现实，最有效的解决方案是应用一个“有保证”的策略对网络流量进行管理。QoS技术就是在这种背景下发展起来的。QoS即服务质量，其目的是针对各种业务的不同需求，为其提供端到端的服务质量保证。QoS是有效利用网络资源的工具，它允许不同的流量不平等的竞争网络资源，语音、视频和重要的数据应用在网络设备中可以优先得到服务。

QoS的服务模型DiffServ，其基本原理是将网络中的流量分成多个类，每个类享受不同的处理，尤其是网络出现拥塞时不同的类会享受不同级别的处理，从而得到不同的丢包率、时延以及时延抖动。同一类的业务在网络中会被聚合起来统一发送，保证相同的时延、抖动、丢包率等QoS指标。在此模型中，业务流的分类和汇聚工作在网络边缘由边界节点完成。边界节点可以通过多种条件（比如报文的源地址和目的地址、ToS域中的优先级、协议类型等）灵活地对报文进行分类，对不同的报文设置不同的表及字段，而其他节点只需要简单地识别报文中的这些标记，即可进行资源分配和流量控制。

在DiffServ模型中，应用程序发出报文前，不需要预先向网络提供资源申请，而是通过设置报文中的QoS参数信息，来告知网络节点它的QoS需求。网络不需要为每个流维护状态，而是根据每个报文流指定的QoS参数信息来提供差分服务，即对报文的服务等级划分，有差别地进行流量控制和转发，提供端到端的QoS保证。DiffServ模型充分考虑了IP网络本身灵活性、可扩展性强的特点，将复杂的服务质量保证通过报文自身携带的信息转换为单跳行为，从而大大减少了信令的工作，是当前网络中的主流服务模型。

基于DiffServ模型的QoS组成，主要分为以下几大类：

* 报文分类和标记

要实现差分服务，需要首选将数据包分为不同的类别或者设置为不同的优先级。报文分类即把数据包分为不同的类别，可以通过MQC配置中的流分类实现；报文标记即为数据包设置不同的优先级，可以通过优先级映射和重标记优先级实现。

* 流量监管、流量整形和接口限速

流量监管和流量整形可以将业务流量限制在特定的带宽内，当业务流量超过额定带宽时，超过的流量将被丢弃或缓存。其中，将超过的流量丢弃的技术称为流量监管，将超过的流量缓存的技术称为流量整形。接口限速分为基于接口的流量监管和基于接口的流量整形。

* 拥塞管理和拥塞避免

拥塞管理在网络发生拥塞时，将报文放入队列中缓存，并采取某种调度算法安排报文的转发次序。而拥塞避免可以监管网络资源的使用情况，当发现拥塞有加剧的趋势时采取主动丢弃报文的策略，通过调整流量来解决网络的过载。

其中，报文分类和标记是实现差分服务的前提和基础；流量监管、流量整形、接口限速、拥塞管理和拥塞避免从不同方面对网络流量及其分配的资源实施控制，是提供差分服务的具体体现。

## 端口优先级/Port Priority

【配置参数】

GWN7800系列L2+交换机和GWN7810/20/30系列L3交换机，均采用基于接口配置，具体如下：

* 接口：选择需要配置优先级的交换机接口，包括电口、光口和聚合接口。可多选。

入方向：

* 信任模式：【下拉框】设置接口的信任模式，选项有{None | 802.1p | DSCP | 802.1p-DSCP| IP优先级}，默认None。
* 当选择“None”时，即不信任任何报文优先级，使用接口默认优先级。
* 当选择“802.1p”时，指定对报文按照VLAN的802.1p优先级进行映射，两层tag时用外层tag的优先级映射。
* 当选择“DSCP”时，指定对报文按照DSCP优先级进行映射。
* 当选择“802.1p-DSCP”时，指定对报文优先按照DSCP优先级进行映射，当DSCP匹配不到时使用VLAN的802.1p优先级进行映射。
* 当选择“IP优先级”时，指定对报文按照IP优先级进行映射。
* CoS：设置接口的CoS优先级，取值范围为0-7的整数，默认0。

出方向：

* 重标记：设置对出方向报文进行优先级重标记。
* 重标记CoS：【开关】设置是否开启出方向报文的PHB到802.1p的映射功能，默认关闭。
* 重标记DSCP：【开关】设置是否开启出方向报文的PHB到DSCP的映射功能，默认关闭。
* 重标记IP优先级：【开关】设置是否开启出方向报文的IP优先级映射功能，默认关闭。

注：重标记DSCP和IP优先级重标记二者只能选其一开启。

接口优先级列表：

* 列表显示接口名称、入方向（信任模式、CoS）、出方向（重标记的CoS/DSCP/IP优先级的状态）
* 支持编辑接口的优先级配置

## 优先级映射/Priority Mapping

【功能概述】

优先级映射用来实现报文携带的QoS优先级与设备内部优先级（又称为本地优先级，是设备内部区分报文服务等级的优先级）之间的转换，从而设备根据内部优先级提供有差别的QoS服务质量。用户可以根据网络规划在不同网络中使用不同的QoS优先级字段，例如VLAN网络中使用802.1p，IP网络中使用DSCP。当报文经过不同字段时，为了保持报文的优先级，需要在连接不同网络的设备上配置这些优先级字段的映射关系。当设备连接不同网络时，所有进入设备的报文，其外部优先级字段（包括DSCP和IP）都被映射为802.1p优先级，再根据802.1p优先级映射为内部优先级；设备根据内部优先级进行队列调度的QoS处理。

优先级映射实现从DSCP到802.1p、丢弃优先级、DSCP优先级的映射，其过程如下：

1.在报文进入设备时，在端口信任报文携带的DSCP优先级的情况下，DSCP根据MAT Table被映射为802.1p优先级；

2.设备根据802.1p与内部优先级（也就是服务等级）之间默认的映射关系确定报文进入的队列，从而针对队列进行流量整形、拥塞避免、队列调度等处理；

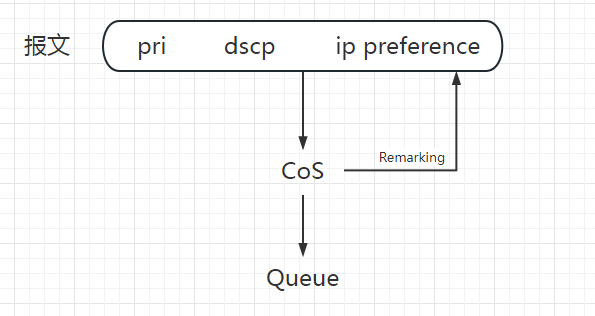
3.在报文离开设备时，设备修改报文发送出去时所携带的优先级，以便其他设备根据报文的优先级提供相应的QoS服务。

服务等级是指报文在设备内部的服务质量，它决定了报文在设备内部所属的队列类型。服务等级有8种取值，即8种PHB，优先级从高到低依次为CS7、CS6、EF、AF4、AF3、AF2、AF1、BE。

**QoS优先级字段：**

为了在Internet上针对不同的业务提供有差别的QoS服务质量，人们根据报文头中的某些字段记录QoS信息，从而让网络中的各设备根据此信息提供有差别的服务质量。这些QoS相关的报文字段包括：Precedence字段、DSCP字段、VLAN帧头中的802.1p优先级（或称CoS字段）。

配置优先级后，设备将根据报文携带的优先级或接口优先级进行优先级映射，确定报文进入的队列和报文出设备时携带的优先级，从而提供差异化的服务。



注：交换机的CoS与队列优先级相同。

【配置参数】

**802.1p-CoS的映射关系表：**

* 列表显示802.1p值与CoS的优先级映射关系
* 802.1p：默认按照0-7的顺序显示，不可更改
* CoS：CoS取值0-7，默认按照0-7的顺序与802.1p值一一对应，支持修改
* 支持一键重置802.1p-CoS的优先级映射关系。

**CoS-802.1p的重标记映射关系表：**

* 列表显示CoS与802.1p的重标记优先级映射关系
* CoS：默认按照0-7的顺序显示，不可更改
* 802.1p：802.1p取值0-7，默认按照0-7的顺序与CoS一一对应，支持修改
* 支持一键重置CoS-802.1p的重标记优先级映射关系。

**DSCP-CoS的映射关系表：**

* 列表显示DSCP值与CoS的优先级映射关系
* DSCP：默认按照0-63的顺序显示，不可更改（DSCP值需显示对应的AFxx、CSx、EF等信息）
* CoS：队列取值0-7，默认按照DSCP 0-7对应CoS 0、DSCP 8-15对应CoS 1的顺序依次一一对应，支持修改
* 支持一键重置DSCP- CoS的优先级映射关系

**CoS -DSCP的重标记映射关系表：**

* 列表显示CoS与DSCP值的优先级映射关系
* CoS：默认按照0-7的顺序显示，不可更改
* DSCP：DSCP取值为0-63，默认按照DSCP 0对应CoS 0、DSCP8对应CoS 1，DSCP 16对应CoS 2依次一一对应显示，支持修改（DSCP值需显示对应的AFxx、CSx、EF等信息）
* 支持一键重置 CoS-DSCP的重标记优先级映射关系

**IP优先级- CoS的映射关系表：**

* 列表显示IP优先级与CoS的映射关系
* IP优先级：默认按照0-7的顺序显示，不可更改
* CoS：CoS取值0-7，默认按照0对应CoS 0、1对应CoS 1的顺序依次一一对应，支持修改
* 支持一键重置IP优先级- CoS的优先级映射关系

**CoS-IP优先级的重标记映射关系表：**

* 列表显示CoS与IP优先级的重标记映射关系
* CoS：默认按照0-7的顺序显示，不可更改
* IP优先级：IP优先级取值0-7，默认按照0-7的顺序与CoS一一对应，支持修改
* 支持一键重置CoS -IP优先级的重标记优先级映射关系

## 队列调度/Queue Scheduling

【功能概述】

配置队列调度后，当网络中发生拥塞时，设备将按照指定的调度策略决定报文转发时的处理次序，以达到高优先级报文优先被调度的目的。

**队列调度算法：**按照交换机接口进行队列调度

* 严格优先（SP，Strict Priority）调度：对优先级最高的流提供最先服务，直到该优先级没有流为止才对次高优先级的流提供服务。交换机每个接口支持8个队列（队列0-7），队列7为最高优先级队列，队列0为最低优先级队列。弊端：拥塞发生时，如果高优先级队列中长时间有报文存在，那么低优先级队列中的报文得不到调度机会，数据无法被传输。
* 加权轮询（WRR，Weighted Round Robin）调度：每个优先级队列被分配一定的带宽，按优先级从高到低依次为各个优先级队列提供服务，当高优先级队列已经用完分配的所有带宽后，自动转向次优先级的队列为其提供服务。
* 基本WRR队列：基本WRR队列包含多个队列，用户可以定制各队列的权重，WRR按设定的参数进行加权轮询调度。
* 分组WRR队列：所有队列全部采用WRR调度，用户可根据需要将输出队列划分为WRR优先级队列组1和WRR优先级队列组2。进行队列调度时，设备首先在优先级队列组1中进行轮询调度，优先级队列组1中没有报文发送时，设备才在优先级队列组2中进行轮询调度。也可配置队列加入SP分组，采用严格优先级调度算法，调度时先调度SP组，然后调度其他WRR优先组。
* 加权公平队列（WFQ，Weighted Fair Queue）调度：在尽可能保证公平（带宽、延迟）的基础上增加优先权方面的考虑，使高优先权的报文获得优先调度的机会多于低优先权的报文。WFQ能够按流的“会话”信息（协议类型、源和目的IP地址、源和目的TCP或UDP端口、ToS域中的优先级位等）自动进行流分类，并且尽可能多地提供队列，以将每个流均匀地放入不同队列中，从而在总体上均衡各个流的延迟。在出队的时候，WFQ按流的优先级（Precedence）来分配每个流应占有出口的带宽。优先级的数值越小，所得的带宽越少；反之，所得的带宽越多。
* 基本WFQ队列：基本WFQ队列包含多个队列，用户可以定制各队列的权重，队内的流按照流的优先级计算每个流的贷款比例，WFQ按设定的参数进行加权公平调度。
* 分组WFQ队列：所有队列全部采用WFQ调度，用户可根据需要将输出队列划分为WFQ优先级队列组1和WFQ优先级队列组2。进行队列调度时，设备首先在优先级队列组1中进行加权公平调度，优先级队列组1中没有报文发送时，设备才在优先级队列组2中进行加权公平调度。也可以配置队列加入SP分组，采用严格优先级调度算法。调度时先调度SP组，然后调度其他WFQ优先组。

【配置参数】

(FP1D)优化：

GWN780X二层交换机和GWN781X/2X/3X三层交换机，均采用基于接口配置，具体如下：

* 接口：选择需要进行调度算法的交换机接口，包括电口、光口和聚合接口。可多选。
* 调度算法：【下拉框】选项有{严格优先级(SP) | 加权轮询(WRR) | 加权公平队列(WFQ) | SP-WRR | SP-WFQ}，默认严格优先级(SP)。
* 严格优先级(SP)：严格按照优先级对队列进行调度。
* 加权轮询(WRR)：设置按照加权轮询对队列进行调度。
* 队列：队列取值为0-7，默认按照0-7的顺序显示，不可更改
* 权重：【text文本框】设置每个队列的权重，按包进行设置，取值范围为1-127的整数
* 加权公平队列(WFQ)：设置按照加权公平队列进行调度。
* 队列：队列取值为0-7，默认按照0-7的顺序显示，不可更改
* 权重：【text文本框】设置每个队列的权重，按字节进行设置，取值范围为1-127的整数
* SP-WRR：先加入SP组，采用严格优先级调度，然后再按照WRR的权重进行调度
* 队列：队列取值为0-7，默认按照0-7的顺序显示，不可更改
* 权重：【text文本框】设置每个队列的权重，按包进行设置，取值范围为0-127的整数，0代表SP
* SP-WFQ：先加入SP组，采用严格优先级调度，然后再按照WFQ的权重进行调度
* 队列：队列取值为0-7，默认按照0-7的顺序显示，不可更改
* 权重：【text文本框】设置每个队列的权重，按字节进行设置，取值范围为0-127的整数，0代表SP

接口队列调度列表：

* 列表显示接口名称、调度算法、8个队列。支持查看8个队列的详情，包括每个队列及其权重。
* 支持编辑接口的队列调度配置

## 队列整形/Queue Shaping

【功能概述】

当报文的发送速率大于接收速率，或者下游设备的接口速率小于上游设备的接口速率时，可能会引起网络的拥塞。如果不限制用户发送的业务流量大小，大量用户不断突发的业务数据会使网络更加拥挤。为了使有限的网络资源更有效地为用户服务，需要对用户的业务流量加以限制。

流量监管、流量整形和接口限速就是一种通过对流量规格进行监督，以限制流量及其资源使用的流控策略。

流量整形是一种主动调整流量输出速率的措施，其作用是限制流量与突发，使这类报文以比较均匀的速率向外发送。流量整形通常使用缓冲区和令牌桶来完成，当报文的发送速率过快时，首先在缓冲区进行缓存，在令牌桶的控制下，再均匀地发送这些被缓冲的报文。

【配置参数】

* 接口：选择需要队列整形的交换机接口，包括电口、光口。

配置接口出方向的队列整形：

* 队列：队列取值为0-7，默认按照0-7的顺序显示，不可更改
* 队列整形：【开关】设置是否开启指定队列的流量整形功能，默认关闭。开启后，需配置队列的最大整形速率和瞬间能够通过的承诺突发流量。
* 最大速率/CIR (Kbps)：【text文本框】设置整形的最大速率，默认的取值范围为16-1000000Kbp（千兆电口/光口）或16-2500000Kbps（2.5G电口）或16-10000000Kbps（万兆光口），必须为16的整数倍，默认为端口速率。

注：端口最大速率的最大值和默认值规则：最大值和默认值为端口基本配置处设置的速率值，若设置“自协商”，则为端口速率最大值。

* 承诺突发流量/CBS (Byte)：【text文本框】设置瞬间能够通过的承诺突发流量，取值范围为678-53247Bytes（9300芯片平台）/1368-532478Bytes（9310芯片平台），默认为53247Bytes。

注：CBS L2 838X芯片平台交换机不支持，L2 93XX芯片平台和L3交换机支持。

接口队列整形列表：

* 列表显示接口名称、8个队列整形。支持查看8个队列整形，包括整形开关状态、最大整形速率和承诺突发流量
* 支持编辑接口的流量整形配置

## 端口限速/Rate Limit

【功能概述】

接口限速可以对一个接口上发送或者接收全部报文的总速率进行限制。接口限速也是采用令牌桶进行流量控制。如果在设备的某个接口配置了接口限速，所有经由该接口发送的报文首先要经过接口限速的令牌桶进行处理。如果令牌桶中有足够的临牌，则报文可以发送；反之，报文将被丢弃或者被缓存。

【配置参数】

* 接口：选择需要限速的交换机接口，包括电口、光口。

入方向限速：

* 入方向限速：【开关】设置是否开启接口入方向的速率限制，默认关闭。开启后，需配置承诺信息速率。
* CIR (Kbps)：【text文本框】设置承诺信息速率，即流量能够通过的平均速率，默认的取值范围为1-1000000Kbps(千兆电口和光口)或1-2500000Kbps（2.5G电口）或1-10000000Kbps（万兆光口），必须为16的整数倍，默认为端口速率。

注：端口最大速率的最大值和默认值规则：最大值和默认值为端口基本配置处设置的速率值，若设置“自协商”，则为端口速率最大值。

* CBS (Byte)：【text文本框】设置瞬间能够通过的承诺突发流量，取值范围为32768- 2147483647 Bytes（9300芯片平台） / 32768-65535 Bytes（9310芯片平台）。

注：CBS L2 838X芯片平台交换机不支持，L2 93XX芯片平台和L3交换机支持。

出方向限速：

* 出方向限速：【开关】设置是否开启接口入方向的速率限制，默认关闭。开启后，需配置承诺信息速率。

CIR (Kbps)：【text文本框】设置承诺信息速率，即流量能够通过的平均速率，取值范围为1-1000000Kbps(千兆电口和光口)或1-2500000Kbps（2.5G电口）或1-10000000Kbps（万兆光口），必须为16的整数倍，默认为端口速率。

注：端口最大速率的最大值和默认值规则：最大值和默认值为端口基本配置处设置的速率值，若设置“自协商”，则为端口速率最大值。

* CBS (Byte)：【text文本框】设置瞬间能够通过的承诺突发流量，取值范围为678-53247 Bytes（9300芯片平台） / 1368-53247 Bytes（9310芯片平台）。

注：CBS L2 838X芯片平台交换机不支持，L2 93XX芯片平台和L3交换机支持。

端口限速列表：

* 列表显示接口名称、入方向限速开关状态及其CIR和CBS、出方向限速开关状态及其CIR和CBS。
* 支持编辑接口的限速配置

# 安全业务/Security

## 风暴控制/Storm Control(FP1B)

【功能概述】

流量抑制可以通过配置阈值来限制广播、未知组播、未知单播、已知组播和已知单播报文的速率，防止广播、未知组播报文和未知单播报文产生广播风暴，防止已知组播报文和已知单播报文的大流量冲击。

风暴控制可以通过阻塞报文或关闭端口来阻断广播、未知组播和未知单播报文的流量。设备支持对接口下的上述三类报文分别按包速率、字节速率、百分比进行风暴控制。在一个检测时间间隔内，设备监控接口下接收的三类报文的平均速率并和配置的最大阈值相比较，当报文速率大于配置的最大阈值时，设备会对该接口进行风暴控制，执行配置好的风暴控制动作。风暴控制动作包括阻塞报文和关闭/shutdown接口。

* 如果对报文进行阻塞，当接口上接收报文的平均速率小于指定的最小阈值时，风暴控制会放开在接口上对该报文的阻塞。
* 如果动作为关闭/shutdown接口，则需要手动执行命令来开启接口，或者使能接口状态自动恢复为UP功能。

【配置参数】

全局配置：

IFG即帧间隙，设备在流量控制时，缺省情况下是包括帧间隙的，即统计的流量速率包括帧间隙。

* IFG：【开关】当且仅当单位设置为“Kbps”时支持配置。设置报文数据统计是否包含帧间隙，默认包含。

接口配置：

* 接口：选择需要配置的交换机接口，包括电口和光口。支持多选进行批量配置。
* 风暴控制：【开关】设置是否开启接口的风暴控制功能，默认关闭。开启后，支持对广播、未知组播、未知单播报文进行风暴控制。

广播报文|未知组播报文|未知单播报文设置（3类单独设置）：

* 开启：【开关】设置是否开启广播报文/未知组播报文/未知单播报文的风暴阈值设置，默认关闭。
* 控制阈值：【text文本框】设置风暴控制的最大阈值。根据不同单位设置不同的取值范围。Kbps：16-1000000（千兆电口/光口）或16-2500000Kbps（2.5G电口）或16-10000000Kbps（万兆光口）的整数，必须为16的整数倍，；pps：1-262143（RTL83XX系列）或1-16777215（RTL93XX系列）的整数；%：1-100的整数（FP1阶段%暂不支持）。
* 单位：【下拉框】设置风暴控制的单位，选项有{Kbps|pps|%}。

注：单位为全局设置。当单位为Kbps时，控制阈值的最大值规则：最大值为端口基本配置处设置的速率值，若设置“自协商”，则为端口速率最大值。

* 动作：【下拉框】设置当接口对应报文超过风暴控制后的处理动作，选项有{丢弃|关闭}。“丢弃”即将超过控制阈值的报文丢弃；“关闭/shutdown”即将超过抑制阈值的接口关闭。

风暴控制接口列表：

* 列表显示接口名称、风暴控制开关状态、广播阈值、未知组播阈值、未知单播阈值、动作
* 支持编辑单个/批量/全部接口风暴控制配置

## 端口安全/Port Security(FP1B)

【功能概述】

端口安全通过将接口学习到的MAC地址转换为安全MAC地址（包括安全动态MAC地址、安全静态MAC地址和Sticky MAC），阻止非法用户通过本接口和交换机通信，从而增强设备的安全性。

安全MAC地址分为：安全动态MAC、安全静态MAC和Sticky MAC。

|  |  |  |
| --- | --- | --- |
| 类型 | 定义 | 特点 |
| 安全动态MAC地址 | 使能端口安全而未使能Sticky MAC功能时转换的MAC地址 | 设备重启后表项会丢失，需要重新学习。  默认不会被老化，只有在配置安全MAC的老化时间后才可以被老化。  安全动态MAC地址的老化类型分为：绝对时间老化和相对时间老化   * 如设置绝对老化时间为5分钟：系统每隔1分钟计算一次每隔MAC地址的存在时间，若大于5分钟，则激励将该安全动态MAC地址老化。否则，等待下1分钟再检测计算 * 如设置相对老化时间为5分钟：系统每隔1分钟检测一次是否有该MAC的流量。若没有流量，则经过5分钟后该安全动态MAC地址老化 |
| 安全静态MAC地址 | 使能端口安全时手动配置的静态MAC地址 | 不会被老化，手动保存配置后重启设备不会丢失 |
| Sticky MAC地址 | 使能端口安全后又同时使能Sticky MAC功能后转换的MAC地址 | 不会被老化，手动保存配置后重启设备不会丢失 |

当端口安全功能或Sticky MAC功能开启/关闭时，接口上的MAC地址会变化或被删除。

|  |  |  |
| --- | --- | --- |
| 功能 | 开启 | 关闭 |
| 端口安全功能 | 接口上之前学习到的动态MAC地址表项将被删除，之后学习到的MAC地址将变为安全动态MAC地址 | 接口上的安全动态MAC地址将被删除，重新学习动态MAC地址 |
| Sticky MAC功能 | 接口上的安全动态MAC地址表项将转化为Sticky MAC地址，之后学习到的MAC地址也变为Sticky MAC地址 | 接口上的Sticky MAC地址，会转换为安全动态MAC地址 |

接口上安全MAC地址数达到限制后，如果收到源MAC地址不存在（即不在端口安全MAC地址表中）的报文，无论目的MAC地址是否存在，交换机即认为有非法用户攻击，就会根据配置的动作对接口做保护处理。默认，Restrict动作是丢弃该报文并上报告警。

安全MAC地址也属于静态MAC地址，接口上配置静态MAC地址漂移检测功能后，如果收到报文的源MAC地址已经存在其他接口的静态MAC中，交换机即认为存在静态MAC地址漂移，就会根据配置的动作对端口做保护处理。

|  |  |
| --- | --- |
| 动作 | 说明 |
| Restrict | 丢弃源MAC地址不存在的报文并上报告警 |
| Protect | 只丢弃源MAC地址不存在的报文，不上报告警 |
| 关闭 | 接口状态被置为error-down，并上报告警。  默认情况下，接口关闭后不会自动恢复，只能由网络管理员在接口下使能接口。  如果希望被关闭的接口可以自动恢复，可以在[***端口自动恢复***](#_端口自动恢复)使能接口状态自动恢复为Up的功能，并设置接口自动恢复为Up的延时时间，使被关闭的接口经过延时时间后能够自动恢复。 |

【配置参数】

全局设置：

* 端口安全：【开关】设置全局开启端口安全功能，默认关闭。
* 速率 (包/秒)：【text文本框】设置MAC地址学习达到上限后上报给CPU的限速，取值为1-600的整数，默认100。

端口设置：

* 接口：选择需要配置的交换机接口，包括电口和光口。可多选。
* 端口安全：【开关】默认关闭。开启后，进行MAC地址学习，包括动态MAC地址和静态MAC地址。
* 最大MAC数：【text文本框】设置接口进行MAC地址学习的最大数量，取值范围为1-256的整数，默认为1。达到最大数量后，如果收到源MAC地址不存在的报文，无论目的MAC地址是否存在，交换机均认为有非法用户攻击，就会根据端口保护配置对接口进行保护处理。
* Sticky MAC：【开关】当端口安全开启后，支持开启Sticky MAC功能。默认关闭。开启后，接口会将学习到的安全动态MAC地址转化为Sticky MAC。如果已经达到最大MAC数，将丢弃该接口学习到的非Sticky MAC表项中的MAC地址，并根据接口保护模式的配置，决定是否上报Trap告警。
* 端口保护：【下拉框】设置当接口学习到的MAC地址达到最大数量或出现静态MAC地址漂移时的保护动作，有{Restrict | Protect| Shutdown}，默认Protect。选择Restrict表示丢弃源MAC地址不存在的报文并上报告警；选择Protect表示丢弃源MAC地址不存在的报文，但不上报告警；选择“Shutdown”表示强制接口shutdown。

端口安全列表：

* 列表显示接口名称、端口安全开关状态、最大MAC数、实际MAC学习数、添加的静态安全MAC地址数、Sticky MAC功能开启状态、保护动作/保护的次数。
* 支持编辑单个/批量/全部端口安全配置。

**安全MAC地址**

添加静态安全MAC地址：

* MAC地址：用于配置静态安全MAC地址，格式为HH:HH:HH:HH:HH:HH(其中，H为1-2位的十六进制数)，必须为单播MAC地址，不可设置为FFFF-FFFF-FFFF、组播地址和全零MAC地址。
* VLAN：【text文本框】配置静态安全MAC地址所属于的VLAN域，取值范围为1-4094。
* 接口：【单选】选择交换机接口进行安全MAC配置，包括电口和光口。

注：（1）同一接口，不能配置相同的VLAN与MAC地址；

（2）同一接口，可以在不同VLAN里配置相同的MAC地址，但在同一VLAN里不能配置相同的MAC地址。

总结：接口、VLAN和MAC不能配置相同，需做去重判断。

安全MAC地址列表：

* 列表显示地址类型（静态|动态|Sticky）、接口名称、VLAN、MAC地址
* 静态为手动配置的静态安全MAC地址
* 动态为开启端口安全功能，自动学习到的MAC地址
* Sticky为开启Sticky安全后，将动态安全MAC地址转换为Sticky的MAC地址
* 支持以MAC为索引，编辑静态安全MAC地址的所属VLAN和接口
* 支持删除单个/批量/全部静态安全MAC地址

## 端口隔离/Port Isolation(FP1C)

【功能概述】

采用端口隔离功能，可以实现同一VLAN内端口之间的隔离。用户只要将端口加入到隔离组中，就可以实现隔离组内端口之间二层数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。

受软件限制，目前仅支持一个隔离组，默认关闭端口隔离功能，即无端口加入到隔离组中。加入后，各端口之间进行双向隔离。

【配置参数】

* 接口：选择需要配置端口隔离的交换机接口，包括电口、光口和聚合接口，可多选。
* 端口隔离：【开关】设置是否开启端口的隔离功能，默认关闭。

端口列表：

* 列表显示接口、隔离状态
* 支持编辑

## ACL(FP1B)

【功能概述】

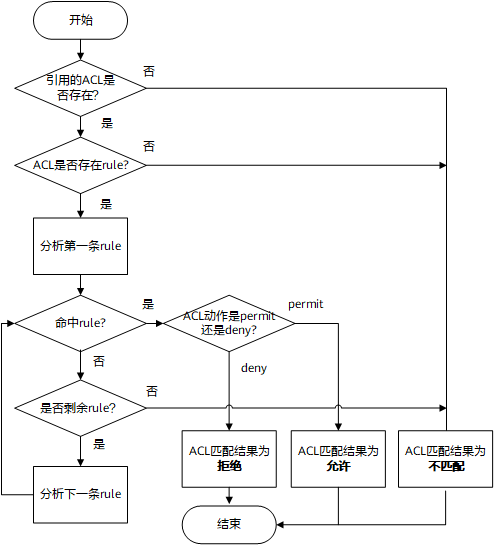
访问控制列表ACL是由一条或多条规则组成的集合。规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源地址、目的地址、端口号等。ACL本质上是一种报文过滤器，规则是过滤器的滤芯。设备基于这些规则进行报文匹配，可以过滤出特定的报文，并根据应用ACL的业务模块的处理策略来允许或组织该报文通过。

交换机支持的ACL规则包括过滤IPv4报文的ACL、过滤IPv6报文的ACL、既支持过滤IPv4报文又过滤IPv6报文的二层ACL和专家级ACL。各类ACL优先级为：基本IPv6 ACL=高级IPv6 ACL>链路层ACL>基本IPv4 ACL>高级IPv4 ACL>专家级ACL

|  |  |  |  |
| --- | --- | --- | --- |
| ACL类型 | ~~编号范围~~ | 适用的IP版本 | 规则定义描述 |
| 基本ACL | ~~2000-2999~~ | IPv4 | 仅使用报文的源IP地址、分片信息和生效时间段来定义规则 |
| ~~4000-4999~~ | IPv6 | 可使用IPv6报文的源IPv6地址、分片信息和生效时时间段来定义规则 |
| 高级ACL | ~~3000-3999~~ | IPv4 | 既可使用IPv4报文的源IP地址，也可使用目的IP地址、IP协议类型、ICMP类型、TCP源/目的端口、UDP源/目的端口号、生效时间段等来定义规则 |
| ~~5000-5999~~ | IPv6 | 可以使用IPv6报文的源IPv6地址、目的IPv6地址、IPv6协议类型、ICMPv6类型、TCP源/目的端口、UDP源/目的端口号、生效时间段等来定义规则 |
| 二层ACL | ~~6000-6999~~ | IPv4&IPv6 | 使用报文的以太网帧头信息来定义规则，如根据源MAC地址、目的MAC地址、二层协议类型等 |
| 专家级ACL(FP3) | ~~7000-7999~~ | IPv4&IPv6&MAC | IP ACL与MAC ACL的组合，实现在同一条规则中同时根据报文的二层头部信息和报文三层或四层信息对进出设备的报文进行控制，以决定报文处理 |
| ACL80（Expert高级ACL，自定义ACL）(FP3) |  | 报文前80字节 | 针对报文的前80个字节进行匹配过滤。报文的SMAC/DMAC/SIP/DIP不计算在任意指定的字段中，ACL80在匹配报文的以上这些字段后，还能再匹配额外指定的16个字节内容 |

**ACL的匹配机制**：

设备将报文与ACL规则进行匹配时，遵循“一旦命中即停止匹配”的规则。



一条ACL由多条规则组成，这些规则可能存在重复甚至矛盾的地方，因此在将一个报文与ACL的各条规则进行匹配时，需要有明确的规则匹配顺序来确定规则执行的优先级。设备支持的AC匹配顺序是“配置顺序”模式，即按照ACL规则编号从小到大的顺序进行报文匹配，编号越小，优先级越高，优先被匹配。

**ACL的生效时间段**：

ACL的生效时间段可以规定ACL规则在何时段内生效，以达到网络优化的目的。

**基于ACL的简化流策略**(FP2)

基于ACL的简化流策略是指通过将报文信息与ACL规则进行匹配，为符合相同ACL规则的报文提供相同的QoS服务，实现对不同类型业务的差分服务。

当用户希望对进入网络的流量进行控制时，可以配置ACL规则根据报文的源IP地址、分片标记、目的IP地址、源端口号、源MAC地址等信息对报文进行匹配，进而配置基于ACL的简化流策略实现对匹配ACL规则的报文过滤、流量监管、流镜像、重定向、重标记或流量统计。

【配置参数】

根据ACL类型，分开进行设置，主要分为3类，IPv4 ACL、IPv6 ACL和链路层ACL。

1. 链路层ACL

添加：

* ACL名称：【text文本框】设置链路层ACL的名称，便于记忆。最多输入64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示

规则设置：

注：1.一个ACL支持设置多条规则，至多128。当有规则设置(除规则编号外)完全相同时，需提示“此规则已存在”。

2.若所有规则遍历完成后，没有匹配的，则直接Deny报文。

3.一旦ACL添加规则后，系统默认生成一条默认规则，行为丢弃，优先级最低。

* 规则编号：【text文本框】设置规则的编号，此决定了规则的匹配顺序，编号越小越优先被匹配。取值范围为1-2147483647。
* 数据行为：【下拉框】设置对匹配该规则的报文执行的动作，选项有{丢弃|放行|shutdown}，默认放行。“丢弃”即拒绝匹配的报文通过，“放行”即允许匹配的报文通过，“shutdown”即表示自动将端口shutdown。
* 源MAC地址：【下拉框】设置源MAC地址，选项与{Any|自定义}，默认Any，即匹配任意源MAC地址。设置为“自定义”后，需要配置匹配的源MAC地址及其掩码。
* 源MAC地址：【text文本框】输入格式为HH:HH:HH:HH:HH:HH(其中，H为1-2位的十六进制数)。
* 源MAC地址掩码：【text文本框】输入格式为HH:HH:HH:HH:HH:HH(其中，H为1-2位的十六进制数)
* 目的MAC地址：【下拉框】设置目的MAC地址，选项与{Any|自定义}，默认Any，即匹配任意目的MAC地址。设置为“自定义”后，需配置匹配的目的MAC地址及其掩码。
* 目的MAC地址：【text文本框】输入格式为HH:HH:HH:HH:HH:HH(其中，H为1-2位的十六进制数) 。默认为空，表示匹配任意目的MAC。
* 目的MAC地址掩码：【text文本框】输入格式为HH:HH:HH:HH:HH:HH(其中，H为1-2位的十六进制数)
* 协议类型：【下拉框】设置匹配报文的类型，选项有{Any|自定义}，默认Any，表示任意类型。选择“自定义”，则需输入匹配的协议类型，范围为0x0000-0xFFFF。其中，0x0806对应ARP，0x0800对应IP，0x86dd对应IPv6，0x8847对应MPLS，0x8035对应RARP。
* VLAN：【text文本框】设置规则匹配报文的VLAN，默认Any，匹配任意VLAN报文。支持用户自定义匹配报文的VLAN，范围为0-4095。
* 802.1p优先级：【下拉框】设置规则匹配报文的VLAN的优先级，选项有{Any|0|1|2|3|4|5|6|7}，默认Any。其中，0对应Best Effort，1对应Background，2对应Excellent Effort，3对应Critical Application，4对应Video，5对应Voice，6对应Internetwork Control，7对应Network Control。
* 时间策略(FP1D)：【下拉框】设置链路层ACL规则生效的时间段，选项为已存在的时间策略，支持弹窗新建时间策略，具体配置详见[*系统→时间策略*](#_时间策略/Time_Policy)。

链路层ACL列表：

* 列表显示ACL名称、规则个数
* 支持查看规则，规则显示规则编号、数据行为、源MAC地址及其掩码、目的MAC地址及其掩码、协议类型、VLAN、802.1p优先级及其掩码和时间策略。(当源MAC地址、目的MAC地址、协议类型、VLAN和802.1p优先级为空时，其对应的掩码无效)、统计计数值（若未开启则显示“禁用”，开启则显示实际的计数值+单位）~~、镜像（若未开启则显示“禁用”，开启则以“镜像组/类型”方式显示）、优先级映射（若未开启则显示“禁用”，开启则显示优先级值）（此3项均需设置高级设置后才显示）~~
* ACL一旦与端口绑定后，支持Mirror、Statistic和Priority Remapping这3个高级设置(FP2)
* 统计计数：【开关】设置规则命中后是否开启报文命中统计，默认关闭。开启后，需要设置如下内容：
* \*统计ID：【text文本框】设置规则命中后的统计ID，取值范围为1-32的整数
* 统计单位：【单选】设置规则命中后的统计方式，选项有{按包 | 按字节}，默认按包统计

注：由于芯片差异，838X芯片平台必须包含统计计数开关、统计ID和统计单位设置，9300芯片平台统计计数默认开启，只需设置统计单位即可，9310芯片平台统计计数默认开启，无需设备统计单位，其默认按包/字节一起统计

* 镜像：【单选(FP2)】设置规则命中后是否加入镜像组进行观察，选项有{禁用|SPAN|RSPAN}，默认禁用。开启后，需要设置如下内容：
* 镜像组：【下拉框】选择规则命中后加入的镜像组，选项为{镜像组1 | 镜像组2 | 镜像组3 | 镜像组4}，镜像组只能选择空的镜像组，否则需提示“镜像组已绑定端口”。

注：页面需提示“镜像功能需要前往维护→诊断→镜像配置~~观察口~~生效”。一旦配置完成，维护→诊断→镜像处需显示ACL相关内容，详情见[*[维护→诊断→镜像]*](#_13.2.5.1_端口镜像/Port_Mirroring(FP1B))处的说明

* ~~类型：【单选】设置镜像抓的数据报文类型，选项有{原始报文 | 修改后的报文}，默认原始数据包，即抓原始进来的数据报文，而修改数据包则是抓经ACL修改过的数据报文~~

~~注：由于芯片差异，838X芯片平台支持原始报文和修改后报文的镜像抓取，93XX芯片平台仅支持原始报文的镜像抓取，故配置项“类型”仅838X芯片平台支持，93XX芯片平台默认使用原始报文进行镜像抓取~~

* 优先级映射：【开关】设置规则命中后是否对报文在交换机内部优先级进行映射，默认关闭。开启后，需要设置如下内容：
* 优先级：【text文本框】设置报文重映射后的优先级，取值范围为0-7的整数
* 限速：【下拉框】设置对匹配ACL规则的报文进行限速，选项有{禁用| 各个限速组ID}，默认禁用。~~开启后，需设置如下内容：~~
* ~~CIR (Kbps)：【text文本框】设置指定承诺信息速率，取值范围为1-10000000Kbps（万兆光口），必须为16的整数倍。~~
* ~~CBS (Byte)：【text文本框】设置指定承诺突发尺寸，即瞬间能够通过的承诺突发流量，取值范围为678-53247 Bytes（9300芯片平台） / 1368-53247 Bytes（9310芯片平台）。~~

~~注：CBS L2 838X芯片平台交换机不支持，L2 93XX芯片平台和L3交换机支持。~~

* 重定向(FP3) 【待评审】：【下拉框】设置对匹配ACL规则的报文进行重定向，支持重定向到CPU、指定接口或指定下一跳地址，选项有{禁用 | 重定向至CPU| 重定向至接口| 重定向至下一跳}，默认禁用。
* 重定向至接口：【下拉框】当且仅当重定向选择“重定向至接口”时支持配置，选项为不包括ACL绑定接口的其他所有物理接口和聚合接口
* 下一跳地址：【text文本框】当且仅当重定向选择“重定向至下一跳”时支持配置，将报文重定向给非直连路由的下一跳，选项为路由表中非直连路由的下一跳地址，包括IPv4和IPv6地址
* 支持编辑链路层ACL
* 支持删除链路层ACL

2. IPv4 ACL

添加：

* ACL名称：【text文本框】设置IPv4 ACL的名称，便于记忆。最多输入64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示

规则设置：

注：1.一个ACL支持设置多条规则，至多128。当有规则设置(除规则编号外)完全相同时，需提示“此规则已存在”。

2.若所有规则遍历完成后，没有匹配的，则直接Deny报文。

3.一旦ACL添加规则后，系统默认生成一条默认规则，行为丢弃，优先级最低。

* \*规则编号：【text文本框】设置规则的编号，此决定了规则的匹配顺序，编号越小越优先被匹配。取值范围为1-2147483647。
* 数据行为：【下拉框】设置对匹配该规则的报文执行的动作，选项有{丢弃|放行|shutdown}，默认放行。“丢弃”即拒绝匹配的报文通过，“放行”即允许匹配的报文通过，“shutdown”即表示自动将端口shutdown。
* 协议类型：【下拉框+输入框结合】显示IPv4支持的不同协议类型，支持任意协议类型，也支持用户自定义，自定义时允许输入的范围为0-255。

默认可供选择的选项有{Any | ICMP(1) | IP in IP(4) | TCP(6) | EGP (8) | IGP (9) | UDP(17) | HMP(20) | RDP(27) | IPV6(41) | IPV6:ROUT(43) | IPV6:FRAG(44) | RSVP(46) | IPv6:ICMP(58) | OSPF(89) | PIM(103) | L2TP(115) | 自定义}。

匹配条件：

* \*源IP地址：【下拉框】设置源IP地址，选项有{Any|自定义}，默认Any，即匹配任意源IP地址。设置为“自定义”后，需配置源IP地址及其掩码。
* 源IP地址：【text文本框】设置IP报文的源IP地址。按IPv4地址格式（点分十进制）进行输入，否则需提示“您输入的IPv4地址格式不正确，请重新输入”。
* 掩码：【text文本框】设置IP报文的源IP地址掩码，以点分十进制格式表示，换算成二进制后，0表示不关心，1表示匹配，与子网掩码相同。掩码中的0或1可以是不连续的，比如可以是0.255.0.255。按IPv4地址格式（点分十进制）进行输入，否则需提示“您输入的掩码格式不正确，请重新输入”。
* 目的IP地址：【下拉框】设置目的IP地址，选项有{Any|自定义}，默认Any，即匹配任意目的IP地址。设置为“自定义”后，需配置目的IP地址及其掩码。
* 目的IP地址：【text文本框】设置IP报文的目的IP地址。按IPv4地址格式（点分十进制）进行输入，否则需提示“您输入的IPv4地址格式不正确，请重新输入”。
* 掩码：【text文本框】设置IP报文的目的IP地址掩码，以点分十进制格式表示，换算成二进制后，0表示不关心，1表示匹配，与子网掩码相同。掩码中的0或1可以是不连续的，比如可以是0.255.0.255。按IPv4地址格式（点分十进制）进行输入，否则需提示“您输入的掩码格式不正确，请重新输入”。
* 源端口：【下拉框+输入框结合】当协议类型选择“TCP”或“UDP”时，需要设置TCP/UDP的目的端口。设置匹配TCP/UDP报文的源端口，可以是任意端口，也可以为单个端口，也可以为端口范围，取值范围为0-65535。
* 目的端口：【下拉框+输入框结合】当协议类型选择“TCP”或“UDP”时，需要设置TCP/UDP的目的端口。设置匹配TCP/UDP报文的目的端口，可以是任意端口，也可以为单个端口，也可以为端口范围，取值范围为0-65535。
* TCP标志位：当协议类型选择“TCP”时，需要设置TCP标志位。

TCP标志位有Urg、Ack、Psh、Rst、Syn、Fin共6种，每种有3种设置方式，分别为Set、Unset、Don’t care，默认Don’t Care。

* ICMP消息类型和消息码：当协议类型选择“ICMP”时，需要设置匹配ICMP报文的消息类型和消息码。
* 消息类型：【下拉框+输入框结合】设置ICMP的消息类型，显示IPv4不同的消息类型，默认支持任意类型，也支持用户自定义，自定义时允许输入的范围为0-255。

默认可供选择的选项有{Any | Echo Reply(0) | Destination Unreachable(3) | Source Quench(4) | Redirect(5) | Alternate Host Address(6) | Echo Request (8) | Router Advertisement(9) | Time Exceeded(11) | Timestamp Request(13) | Timestamp Reply(14) | Information Request(15) | Information Reply(16) | Address Mask Request(17) | Address Mask Reply(18) | Traceroute(30) | Datagram Conversion Error(31) | Mobile Host Redirect(32) | IPv6 Where Are You(33) | IPv6 I Am Here(34) | Mobile Registration Request(35) | Mobile Registration Reply(36) | Domain Name Request(37) | Domain Name Reply(38) | Skip(39) | 自定义}。

* 消息码：【下拉框+输入框结合】设置ICMP的消息码，支持任意消息码，也支持用户自定义消息码，自定义时允许输入的范围为0-255。
* ToS类型：【下拉框】设置匹配ToS的类型，选项有{Any | 匹配DSCP | 匹配IP优先级}。当选择“匹配DSCP”或“匹配IP优先级”，需要分别配置DSCP优先级和IP优先级。
* DSCP优先级：【text文本框】设置DSCP优先级，取值范围为0-63。
* IP优先级：【text文本框】设置IP优先级，取值范围为0-7。
* 时间策略(FP1D)：【下拉框】设置IPv4 ACL规则生效的时间段，选项为已存在的时间策略，支持弹窗新建时间策略，具体配置详见[*系统→时间策略*](#_时间策略/Time_Policy)。

IPv4 ACL列表：

* 列表显示ACL名称、规则个数
* 支持查看规则，规则显示规则编号、数据行为、协议类型、源IP地址及其掩码/前缀、目的IP地址及其掩码/前缀、TCP/UDP源端口和目的端口（协议类型选择TCP或UDP时显示）、TCP标识位（协议类型选择TCP时显示）、ICMP消息类型和消息码（协议类型选择ICMP时显示）、DSCP优先级或IP优先级和时间策略、统计计数值（若未开启则显示“禁用”，开启则显示实际的计数值）~~、镜像（若未开启则显示“禁用”，开启则以“镜像组/类型”方式显示）、优先级映射（若未开启则显示“禁用”，开启则显示优先级值）（此3项均需设置高级设置后才显示）~~
* ACL一旦与端口绑定后，支持Mirror、Statistic和Priority Remapping这3个高级设置(FP2)
* 统计计数：【开关】设置规则命中后是否开启报文命中统计，默认关闭。开启后，需要设置如下内容：
* \*统计ID：【text文本框】设置规则命中后的统计ID，取值范围为1-32的整数
* 统计单位：【单选】设置规则命中后的统计方式，选项有{按包 | 按字节}，默认按包统计

注：由于芯片差异，838X芯片平台必须包含统计计数开关、统计ID和统计单位设置，9300芯片平台统计计数默认开启，只需设置统计单位即可，9310芯片平台统计计数默认开启，无需设备统计单位，其默认按包/字节一起统计

* 镜像：【单选(FP2)】设置规则命中后是否加入镜像组进行观察，选项有{禁用|SPAN|RSPAN}，默认禁用。开启后，需要设置如下内容：
* 镜像组：【下拉框】选择规则命中后加入的镜像组，选项为{镜像组1 | 镜像组2 | 镜像组3 | 镜像组4}，镜像组只能选择空的镜像组，否则需提示“镜像组已绑定端口”。

注：页面需提示“镜像功能需要前往维护→诊断→镜像配置~~观察口~~生效”。一旦配置完成，维护→诊断→镜像处需显示ACL相关内容，详情见[*[维护→诊断→镜像]*](#_13.2.5.1_端口镜像/Port_Mirroring(FP1B))处的说明

* ~~类型：【单选】设置镜像抓的数据报文类型，选项有{原始报文 | 修改后的报文}，默认原始数据包，即抓原始进来的数据报文，而修改数据包则是抓经ACL修改过的数据报文~~

~~注：由于芯片差异，838X芯片平台支持原始报文和修改后报文的镜像抓取，93XX芯片平台仅支持原始报文的镜像抓取，故配置项“类型”仅838X芯片平台支持，93XX芯片平台默认使用原始报文进行镜像抓取~~

* 优先级映射：【开关】设置规则命中后是否对报文在交换机内部优先级进行映射，默认关闭。开启后，需要设置如下内容：
* 优先级：【text文本框】设置报文重映射后的优先级，取值范围为0-7的整数
* 限速：【下拉框】设置对匹配ACL规则的报文进行限速，选项有{禁用| 各个限速组ID}，默认禁用。~~开启后，需设置如下内容：~~
* ~~CIR (Kbps)：【text文本框】设置指定承诺信息速率，取值范围为1-10000000Kbps（万兆光口），必须为16的整数倍。~~
* ~~CBS (Byte)：【text文本框】设置指定承诺突发尺寸，即瞬间能够通过的承诺突发流量，取值范围为678-53247 Bytes（9300芯片平台） / 1368-53247 Bytes（9310芯片平台）。~~

~~注：CBS L2 838X芯片平台交换机不支持，L2 93XX芯片平台和L3交换机支持。~~

* 重定向(FP3) 【待评审】：【下拉框】设置对匹配ACL规则的报文进行重定向，支持重定向到CPU、指定接口或指定下一跳地址，选项有{禁用 | 重定向至CPU| 重定向至接口| 重定向至下一跳}，默认禁用。
* 重定向至接口：【下拉框】当且仅当重定向选择“重定向至接口”时支持配置，选项为不包括ACL绑定接口的其他所有物理接口和聚合接口
* 下一跳地址：【text文本框】当且仅当重定向选择“重定向至下一跳”时支持配置，将报文重定向给非直连路由的下一跳，选项为IPv4路由表中非直连路由的下一跳地址
* 支持编辑IPv4 ACL
* 支持删除IPv4 ACL

3. IPv6 ACL

添加：

* ACL名称：【text文本框】设置IPv4 ACL的名称，便于记忆。最多输入64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示

规则设置：

注：1.一个ACL支持设置多条规则，至多128。当有规则设置(除规则编号外)完全相同时，需提示“此规则已存在”。

2.若所有规则遍历完成后，没有匹配的，则直接Deny报文。

3.一旦ACL添加规则后，系统默认生成一条默认规则，行为丢弃，优先级最低。

* \*规则编号：【text文本框】设置规则的编号，此决定了规则的匹配顺序，编号越小越优先被匹配。取值范围为1-2147483647。
* 数据行为：【下拉框】设置对匹配该规则的报文执行的动作，选项有{丢弃|放行|shutdown}，默认放行。“丢弃”即拒绝匹配的报文拒绝通过，“放行”即允许匹配的报文通过，“shutdown”即表示自动将端口shutdown。
* 协议类型：【下拉框+输入框结合】显示IPv6支持的不同协议类型，支持任意协议类型，也支持用户自定义，自定义时允许输入的范围为0-255。

默认可供选择的选项有{ Any | TCP(6) | UDP(17) | ICMP(58) | 自定义}。

匹配条件：

* \*源IP地址：【下拉框】设置源IP地址，选项有{Any|自定义}，默认Any，即匹配任意源IP地址。设置为“自定义”后，需配置源IP地址及其掩码。
* 源IP地址：【text文本框】设置IP报文的源IP地址。按IPv6地址格式（类似X:XX::X:X（IPv6地址共128bits，每16bits为一段，段之间用:分隔）进行输入，否则需提示“您输入的IPv6地址格式不正确，请重新输入”。
* 前缀长度：【text文本框】设置IP报文的源IP地址前缀长度，取值范围为1-128。
* 目的IP地址：【下拉框】设置目的IP地址，选项有{Any|自定义}，默认Any，即匹配任意目的IP地址。设置为“自定义”后，需配置目的IP地址及其掩码。
* 目的IP地址：【text文本框】设置IP报文的目的IP地址。按IPv6地址格式（类似X:XX::X:X。IPv6地址共128bits，每16bits为一段，段之间用:分隔）进行输入，否则需提示“您输入的IPv6地址格式不正确，请重新输入”。
* 前缀长度：【text文本框】设置IP报文的目的IP地址前缀长度，取值范围为1-128。
* 源端口：【下拉框+输入框结合】当协议类型选择“TCP”或“UDP”时，需要设置TCP/UDP的目的端口。设置匹配TCP/UDP报文的源端口，可以是任意端口，也可以为单个端口，也可以为端口范围，取值范围为0-65535。
* 目的端口：【下拉框+输入框结合】当协议类型选择“TCP”或“UDP”时，需要设置TCP/UDP的目的端口。设置匹配TCP/UDP报文的目的端口，可以是任意端口，也可以为单个端口，也可以为端口范围，取值范围为0-65535。
* TCP标志位：当协议类型选择“TCP”时，需要设置TCP标志位。

TCP标志位有Urg、Ack、Psh、Rst、Syn、Fin共6种，每种有2种设置方式，分别为Set、Unset、Don’t care，默认Don’t Care。

* ICMP消息类型和消息码：当协议类型选择“ICMP”时，需要设置匹配ICMP报文的消息类型和消息码。
* 消息类型：【下拉框+输入框结合】设置ICMP的消息类型，显示IPv4不同的消息类型，默认支持任意类型，也支持用户自定义，自定义时允许输入的范围为0-255。

默认可供选择的选项有{Any | Destination Unreachable(1) | Packet Too Big2(2) | Time Exceeded(3) | Parameter Problem(4) | Echo Request(128) | Echo Reply(129) | MLD Query(130) | MLD Report(131) | MLD Done(132) | Router Solication(133) | Router Advertisement(134) | ND NS(135) | ND NA(136) | MLDv2 Report(143) | 自定义}。

* 消息码：【下拉框+输入框结合】设置ICMP的消息码，支持任意消息码，也支持用户自定义消息码，自定义时允许输入的范围为0-255。
* ToS类型：【下拉框】设置匹配ToS的类型，选项有{Any | 匹配DSCP | 匹配IP优先级}。当选择“匹配DSCP”或“匹配IP优先级”，需要分别配置DSCP优先级和IP优先级。
* DSCP优先级：【text文本框】设置DSCP优先级，取值范围为0-63。
* IP优先级：【text文本框】设置IP优先级，取值范围为0-7。
* 时间策略(FP1D)：【下拉框】设置IPv6 ACL规则生效的时间段，选项为已存在的时间策略，支持弹窗新建时间策略，具体配置详见[*系统→时间策略*](#_时间策略/Time_Policy_1)。

IPv6 ACL列表：

* 列表显示ACL名称、规则个数
* 支持查看规则，规则显示规则编号、数据行为、协议类型、源IP地址及其掩码/前缀、目的IP地址及其掩码/前缀、TCP/UDP源端口和目的端口（协议类型选择TCP或UDP时显示）、TCP标志位（协议类型选择TCP时显示）、ICMP消息类型和消息码（协议类型选择ICMP时显示）、DSCP优先级或IP优先级和时间策略、统计计数值（若未开启则显示“禁用”，开启则显示实际的计数值）~~、镜像（若未开启则显示“禁用”，开启则以“镜像组/类型”方式显示）、优先级映射（若未开启则显示“禁用”，开启则显示优先级值）（此3项均需设置高级设置后才显示）~~
* ACL一旦与端口绑定后，支持Mirror、Statistic和Priority Remapping这3个高级设置(FP2)
* 统计计数：【开关】设置规则命中后是否开启报文命中统计，默认关闭。开启后，需要设置如下内容：
* \*统计ID：【text文本框】设置规则命中后的统计ID，取值范围为1-32的整数
* 统计单位：【单选】设置规则命中后的统计方式，选项有{按包 | 按字节}，默认按包统计

注：由于芯片差异，838X芯片平台必须包含统计计数开关、统计ID和统计单位设置，9300芯片平台统计计数默认开启，只需设置统计单位即可，9310芯片平台统计计数默认开启，无需设备统计单位，其默认按包/字节一起统计

* 镜像：【单选(FP2)】设置规则命中后是否加入镜像组进行观察，选项有{禁用|SPAN|RSPAN}，默认禁用。开启后，需要设置如下内容：
* 镜像组：【下拉框】选择规则命中后加入的镜像组，选项为{镜像组1 | 镜像组2 | 镜像组3 | 镜像组4}，镜像组只能选择空的镜像组，否则需提示“镜像组已绑定端口”。

注：页面需提示“镜像功能需要前往维护→诊断→镜像配置~~观察口~~生效”。一旦配置完成，维护→诊断→镜像处需显示ACL相关内容，详情见[*[维护→诊断→镜像]*](#_13.2.5.1_端口镜像/Port_Mirroring(FP1B))处的说明

* ~~类型：【单选】设置镜像抓的数据报文类型，选项有{原始报文 | 修改后的报文}，默认原始数据包，即抓原始进来的数据报文，而修改数据包则是抓经ACL修改过的数据报文~~

~~注：由于芯片差异，838X芯片平台支持原始报文和修改后报文的镜像抓取，93XX芯片平台仅支持原始报文的镜像抓取，故配置项“类型”仅838X芯片平台支持，93XX芯片平台默认使用原始报文进行镜像抓取~~

* 优先级映射：【开关】设置规则命中后是否对报文在交换机内部优先级进行映射，默认关闭。开启后，需要设置如下内容：
* 优先级：【text文本框】设置报文重映射后的优先级，取值范围为0-7的整数
* 限速：【下拉框】设置对匹配ACL规则的报文进行限速，选项有{禁用| 各个限速组ID}，默认禁用。~~开启后，需设置如下内容：~~
* ~~CIR (Kbps)：【text文本框】设置指定承诺信息速率，取值范围为1-10000000Kbps（万兆光口），必须为16的整数倍。~~
* ~~CBS (Byte)：【text文本框】设置指定承诺突发尺寸，即瞬间能够通过的承诺突发流量，取值范围为678-53247 Bytes（9300芯片平台） / 1368-53247 Bytes（9310芯片平台）。~~

~~注：CBS L2 838X芯片平台交换机不支持，L2 93XX芯片平台和L3交换机支持。~~

* 重定向(FP3) 【待评审】：【下拉框】设置对匹配ACL规则的报文进行重定向，支持重定向到CPU、指定接口或指定下一跳地址，选项有{禁用 | 重定向至CPU| 重定向至接口| 重定向至下一跳}，默认禁用。
* 重定向至接口：【下拉框】当且仅当重定向选择“重定向至接口”时支持配置，选项为不包括ACL绑定接口的其他所有物理接口和聚合接口
* 下一跳地址：【text文本框】当且仅当重定向选择“重定向至下一跳”时支持配置，将报文重定向给非直连路由的下一跳，选项为IPv6路由表中非直连路由的下一跳地址
* 支持编辑IPv6 ACL
* 支持删除IPv6 ACL

4. Expert ACL (FP3) 【待评审】

Expert ACL的规则不仅可以包含IP ACL和MAC ACL，同时可以指定基于VLAN ID来匹配报文

添加：

* ACL名称：【text文本框】设置Expert ACL的名称，便于记忆。最多输入64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示

规则设置：

注：1.一个ACL支持设置多条规则，至多128。当有规则设置(除规则编号外)完全相同时，需提示“此规则已存在”。

2.若所有规则遍历完成后，没有匹配的，则直接Deny报文。

3.一旦ACL添加规则后，系统默认生成一条默认规则，行为丢弃，优先级最低。

* \*规则编号：【text文本框】设置规则的编号，此决定了规则的匹配顺序，编号越小越优先被匹配。取值范围为1-2147483647。
* 数据行为：【下拉框】设置对匹配该规则的报文执行的动作，选项有{丢弃|放行|shutdown}，默认放行。“丢弃”即拒绝匹配的报文通过，“放行”即允许匹配的报文通过，“shutdown”即表示自动将端口shutdown。

协议类型+以太网类型 2选1设置：

* 协议类型：【下拉框+text输入框结合】显示支持的不同协议类型，支持任意协议类型，也支持用户自定义，自定义时允许输入的范围为0-255。默认可供选择的选项有{Any | EIGRP | GRE | ICMP | IGMP | IP | IP in IP | NOS | ODPF | TCP | UDP |自定义}。
* 以太网类型：【text文本框】设置匹配报文的以太网类型，选项有{Any|自定义}，默认Any，表示任意类型。选择“自定义”，则需输入匹配的协议类型，范围为0x0000-0xFFFF。其中，0x0806对应ARP，0x0800对应IP，0x86dd对应IPv6，0x8847对应MPLS，0x8035对应RARP。
* 外层CoS：【text文本框】设置匹配指定二层报文外层Tag中的优先级，取值范围为0-7
* 内层CoS：【text文本框】设置要匹配指定二层报文内层Tag中的优先级，取值范围为0-7
* 外层VLAN：【text文本框】设置匹配二层报文外层Tag中的VLAN ID，匹配任意VLAN报文。支持用户自定义匹配报文的VLAN，范围为0-4095
* 内层VLAN：【text文本框】设置匹配二层报文内层Tag中的VLAN ID，匹配任意VLAN报文。支持用户自定义匹配报文的VLAN，范围为0-4095
* 源主机：【下拉框】设置匹配源主机发出的IP报文或二层报文，选项有{Any|自定义}，默认Any，即匹配任意源主机地址。

设置为“自定义”后，需要配置匹配的源主机地址及其掩码。

* 源主机地址：【text文本框】输入格式为32位点分十进制（IPv4地址格式）
* 源主机地址掩码：【text文本框】输入格式为32位点分十进制（IPv4地址格式）
* 目的主机：【下拉框】设置匹配目的主机发出的IP报文或二层报文，选项有{Any|自定义}，默认Any，即匹配任意目的主机地址。

设置为“自定义”后，需配置匹配的目的主机地址及其掩码。

* 目的主机地址：【text文本框】输入格式为32位点分十进制（IPv4地址格式）
* 目的主机地址掩码：【text文本框】输入格式为32位点分十进制（IPv4地址格式）
* ToS类型：【下拉框】设置匹配ToS的类型，选项有{Any | 匹配DSCP | 匹配IP优先级}。当选择“匹配DSCP”或“匹配IP优先级”，需要分别配置DSCP优先级和IP优先级。
* DSCP优先级：【text文本框】设置DSCP优先级，取值范围为0-63。
* IP优先级：【text文本框】设置IP优先级，取值范围为0-7。
* 分片：【开关】设置匹配非首片的IP分片报文，默认关闭。
* 时间策略：【下拉框】设置Expert ACL规则生效的时间段，选项为已存在的时间策略，支持弹窗新建时间策略，具体配置详见[*系统→时间策略*](#_时间策略/Time_Policy_1)。

Expert ACL列表：

* 列表显示ACL名称、规则个数
* 支持查看规则，规则显示规则编号、数据行为、协议类型或以太网类型、源主机地址及其掩码、目的主机地址及其掩码、DSCP优先级或IP优先级、分片和时间策略、统计计数值（若未开启则显示“禁用”，开启则显示实际的计数值）
* ACL一旦与端口绑定后，支持Mirror、Statistic和Priority Remapping这3个高级设置
* 统计计数：【开关】设置规则命中后是否开启报文命中统计，默认关闭。开启后，需要设置如下内容：
* \*统计ID：【text文本框】设置规则命中后的统计ID，取值范围为1-32的整数
* 统计单位：【单选】设置规则命中后的统计方式，选项有{按包 | 按字节}，默认按包统计

注：由于芯片差异，838X芯片平台必须包含统计计数开关、统计ID和统计单位设置，9300芯片平台统计计数默认开启，只需设置统计单位即可，9310芯片平台统计计数默认开启，无需设备统计单位，其默认按包/字节一起统计

* 镜像：【单选】设置规则命中后是否加入镜像组进行观察，选项有{禁用|SPAN|RSPAN}，默认禁用。开启后，需要设置如下内容：
* 镜像组：【下拉框】选择规则命中后加入的镜像组，选项为{镜像组1 | 镜像组2 | 镜像组3 | 镜像组4}，镜像组只能选择空的镜像组，否则需提示“镜像组已绑定端口”。

注：页面需提示“镜像功能需要前往维护→诊断→镜像配置~~观察口~~生效”。一旦配置完成，维护→诊断→镜像处需显示ACL相关内容，详情见[*[维护→诊断→镜像]*](#_13.2.5.1_端口镜像/Port_Mirroring(FP1B))处的说明

* 优先级映射：【开关】设置规则命中后是否对报文在交换机内部优先级进行映射，默认关闭。开启后，需要设置如下内容：
* 优先级：【text文本框】设置报文重映射后的优先级，取值范围为0-7的整数
* 限速：【下拉框】设置对匹配ACL规则的报文进行限速，选项有{禁用| 各个限速组ID}，默认禁用。~~开启后，需设置如下内容：~~
* ~~CIR (Kbps)：【text文本框】设置指定承诺信息速率，取值范围为1-10000000Kbps（万兆光口），必须为16的整数倍。~~
* ~~CBS (Byte)：【text文本框】设置指定承诺突发尺寸，即瞬间能够通过的承诺突发流量，取值范围为678-53247 Bytes（9300芯片平台） / 1368-53247 Bytes（9310芯片平台）。~~

~~注：CBS L2 838X芯片平台交换机不支持，L2 93XX芯片平台和L3交换机支持。~~

* 重定向：【下拉框】设置对匹配ACL规则的报文进行重定向，支持重定向到CPU、指定接口或指定下一跳地址，选项有{禁用 | 重定向至CPU| 重定向至接口| 重定向至下一跳}，默认禁用。
* 重定向至接口：【下拉框】当且仅当重定向选择“重定向至接口”时支持配置，选项为不包括ACL绑定接口的其他所有物理接口和聚合接口
* 下一跳地址：【text文本框】当且仅当重定向选择“重定向至下一跳”时支持配置，将报文重定向给非直连路由的下一跳，选项为IPv6路由表中非直连路由的下一跳地址
* 支持编辑Expert ACL
* 支持删除Expert ACL

5. 自定义ACL（ACL80）(FP3) 【待评审】

自定义ACL也称为ACL80，针对报文的前80个字节进行匹配过滤。报文的SMAC/DMAC/SIP/DIP/ETYPE不计算在任意指定的字段中，ACL80在匹配报文的以上这些字段之后，还能再匹配额外指定的16个字节内容。

对于任意一个16字节字段，可以按照bit形式与所设置的值进行比较或不比较，即允许对16个字节的任意一个比特设置该值为0或1。在对任何一个字节进行过滤时，有三个要素：匹配域内容、匹配域掩码以及匹配的起始位置。匹配域内容和匹配域掩码二者的比特位是一一对应的。过滤规则指明需要过滤字段值，过滤域模板指明过滤规则中对应字段是否需要过滤（1表示匹配对应过滤规则的比特位，0表示不匹配），所以当需要匹配某个比特时，必须将过滤域模板中对应的比特位设置为1。如果过滤域模板比特位设置为0，无论过滤规则中对应的比特位是什么，都不会匹配。

添加：

* ACL名称：【text文本框】设置Expert ACL的名称，便于记忆。最多输入64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示

规则设置：

注：1.一个ACL支持设置多条规则，至多128。当有规则设置(除规则编号外)完全相同时，需提示“此规则已存在”。

2.若所有规则遍历完成后，没有匹配的，则直接Deny报文。

3.一旦ACL添加规则后，系统默认生成一条默认规则，行为丢弃，优先级最低。

* \*规则编号：【text文本框】设置规则的编号，此决定了规则的匹配顺序，编号越小越优先被匹配。取值范围为1-2147483647。
* 数据行为：【下拉框】设置对匹配该规则的报文执行的动作，选项有{丢弃|放行|shutdown}，默认放行。“丢弃”即拒绝匹配的报文通过，“放行”即允许匹配的报文通过，“shutdown”即表示自动将端口shutdown。
* 报文类型：【下拉框】设置匹配的指定报文头，选项有{L2-head| IPv4-head| IPv6-head| L4-head}

当选择“L4-head“时，支持配置UDP、TCP的源端口和目的端口

* 源端口：【下拉框+输入框结合】设置匹配TCP/UDP报文的源端口，可以是任意端口，也可以为单个端口，也可以为端口范围，取值范围为0-65535
* 目的端口：【下拉框+输入框结合】设置匹配TCP/UDP报文的目的端口，可以是任意端口，也可以为单个端口，也可以为端口范围，取值范围为0-65535
* 匹配字符串：【text文本框】设置匹配报文的字符串，16进制形式，0x开头，长度范围为3-10，最长4个字节
* 匹配字符串掩码：【text文本框】设置匹配字符串的掩码，16进制形式，0x开头，长度范围为3-10，最长4个字节。当用户定义的规则字符串对应的掩码为“1”时，ACL对该位进行匹配；当为“0”时则不进行匹配。
* 偏移：【text文本框】设置匹配报文的偏移量。若报文类型为“L2-head”，则必须满足4N+2的要求（N为≥0的整数）；反之，则必须满足4N的要求（N为≥0的整数）
* 时间策略：【下拉框】设置自定义ACL规则生效的时间段，选项为已存在的时间策略，支持弹窗新建时间策略，具体配置详见[*系统→时间策略*](#_时间策略/Time_Policy_1)。

自定义ACL列表：

* 列表显示ACL名称、规则个数
* 支持查看规则，规则显示规则编号、数据行为、xxxx和时间策略、统计计数值（若未开启则显示“禁用”，开启则显示实际的计数值）
* ACL一旦与端口绑定后，支持Mirror、Statistic和Priority Remapping这3个高级设置
* 统计计数：【开关】设置规则命中后是否开启报文命中统计，默认关闭。开启后，需要设置如下内容：
* \*统计ID：【text文本框】设置规则命中后的统计ID，取值范围为1-32的整数
* 统计单位：【单选】设置规则命中后的统计方式，选项有{按包 | 按字节}，默认按包统计

注：由于芯片差异，838X芯片平台必须包含统计计数开关、统计ID和统计单位设置，9300芯片平台统计计数默认开启，只需设置统计单位即可，9310芯片平台统计计数默认开启，无需设备统计单位，其默认按包/字节一起统计

* 镜像：【单选】设置规则命中后是否加入镜像组进行观察，选项有{禁用|SPAN|RSPAN}，默认禁用。开启后，需要设置如下内容：
* 镜像组：【下拉框】选择规则命中后加入的镜像组，选项为{镜像组1 | 镜像组2 | 镜像组3 | 镜像组4}，镜像组只能选择空的镜像组，否则需提示“镜像组已绑定端口”。

注：页面需提示“镜像功能需要前往维护→诊断→镜像配置~~观察口~~生效”。一旦配置完成，维护→诊断→镜像处需显示ACL相关内容，详情见[*[维护→诊断→镜像]*](#_13.2.5.1_端口镜像/Port_Mirroring(FP1B))处的说明

* 优先级映射：【开关】设置规则命中后是否对报文在交换机内部优先级进行映射，默认关闭。开启后，需要设置如下内容：
* 优先级：【text文本框】设置报文重映射后的优先级，取值范围为0-7的整数
* 限速：【下拉框】设置对匹配ACL规则的报文进行限速，选项有{禁用| 各个限速组ID}，默认禁用。~~开启后，需设置如下内容：~~
* ~~CIR (Kbps)：【text文本框】设置指定承诺信息速率，取值范围为1-10000000Kbps（万兆光口），必须为16的整数倍。~~
* ~~CBS (Byte)：【text文本框】设置指定承诺突发尺寸，即瞬间能够通过的承诺突发流量，取值范围为678-53247 Bytes（9300芯片平台） / 1368-53247 Bytes（9310芯片平台）。~~

~~注：CBS L2 838X芯片平台交换机不支持，L2 93XX芯片平台和L3交换机支持。~~

* 重定向：【下拉框】设置对匹配ACL规则的报文进行重定向，支持重定向到CPU、指定接口或指定下一跳地址，选项有{禁用 | 重定向至CPU| 重定向至接口| 重定向至下一跳}，默认禁用。
* 重定向至接口：【下拉框】当且仅当重定向选择“重定向至接口”时支持配置，选项为不包括ACL绑定接口的其他所有物理接口和聚合接口
* 下一跳地址：【text文本框】当且仅当重定向选择“重定向至下一跳”时支持配置，将报文重定向给非直连路由的下一跳，选项为IPv6路由表中非直连路由的下一跳地址
* 支持编辑自定义ACL
* 支持删除自定义ACL

6. 应用ACL

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。最基本的ACL应用方式，是在简化流策略或流策略中应用ACL，使设备能够基于接口或VLAN下发ACL，实现对转发报文的过滤。

ACL端口绑定：

* 接口：选择需要绑定ACL的交换机接口，包括电口、光口和聚合接口。可多选
* 链路层ACL：【下拉框】支持从已添加的链路层ACL中选择一个链路层ACL与接口绑定。
* IP ACL：【下拉框】支持从已添加的IPv4 ACL和IPv6 ACL中选择一个IP ACL与接口绑定。

注：端口绑定的ACL与VLAN绑定的ACL不能相同，必须互斥，即同一个ACL不能既绑定在端口上，又不能绑定在VLAN上。

ACL端口绑定列表：

* 列表显示接口名称、绑定的ACL

注：1.一旦绑定，ACL及其规则无法删除和编辑，需先解绑

2.绑定后的ACL，里面所有ACE即规则即可进行高级设置，包括Mirror、Statistic和Priority Remapping、限速

* 支持解除接口与ACL的绑定

ACL VLAN绑定：

* VLAN：选择需要绑定ACL的VLAN，必须为设备上已有的VLAN。可多选
* 链路层ACL：【下拉框】支持从已添加的链路层ACL中选择一个链路层ACL与VLAN绑定。
* IP ACL：【下拉框】支持从已添加的IPv4 ACL和IPv6 ACL中选择一个IP ACL与VLAN绑定。

注：端口绑定的ACL与VLAN绑定的ACL不能相同，必须互斥，即同一个ACL不能既绑定在端口上，又不能绑定在VLAN上。

ACL VLAN绑定列表：

* 列表显示VLAN、绑定的ACL

注：1.一旦绑定，ACL及其规则无法删除和编辑，需先解绑

2.绑定后的ACL，里面所有ACE即规则即可进行高级设置，包括Mirror、Statistic和Priority Remapping、限速

* 支持解除VLAN与ACL的绑定

7. 限速设置(FP2)

（1）838X芯片平台

限速参数包括Burst设置和限速组设置。

Burst设置：

* 阈值组1
* Burst Byte (bps)：【text文本框】设置Burst按包时的速率阈值，取值范围为128-8388480的整数，且必须为128的倍数，默认8388480bps
* Burst Packet (pps)：【text文本框】设置Burst按字节时的速率阈值，取值范围为1-65535的整数，默认10pps
* 阈值组2
* Burst Byte (bps)：【text文本框】设置Burst按包时的速率阈值，取值范围为128-8388480的整数，且必须为128的倍数，默认8388480bps
* Burst Packet (pps)：【text文本框】设置Burst按字节时的速率阈值，取值范围为1-65535的整数，默认10pps

限速组设置：

* 限速组ID：【单选】从限速组列表中选择限速组
* 限速类型：【单选】显示类型选项有{按包 | 按字节}，默认按包。
* Burst阈值组：【单选】选择Burst阈值组，从上述2个组中选择，将会使用阈值组中与限速类型相同的进行限速设置，默认Burst阈值组1
* 速率阈值 (Kbps)：【text文本框】当且仅当“限速类型”选择“按包”时支持配置，取值范围为16-1000000的整数，且必须为16的倍数
* 速率阈值 (pps)：【text文本框】当其仅当“限速类型”为“按字节”时支持配置，取值范围为1-262143的整数

限速组列表：

* 列表显示32个限速组、限速类型、Burst阈值组、速率阈值（带单位）
* 支持单个编辑

（2）93XX芯片平台

限速组设置：

* 限速组ID：【单选】从限速组列表中选择限速组
* 限速类型：【单选】显示类型选项有{按包 | 按字节}，默认按包。

当限速类型选择“按包”时，

* Burst Byte (bps)：【text文本框】设置Burst按包时的速率阈值，取值范围为128-8388480的整数，且必须为128的倍数，默认8388480bps
* 速率阈值 (Kbps)：【text文本框】取值范围为16-1000000的整数，且必须为16的倍数

当限速类型选择“按字节”时，

* Burst Packet (pps)：【text文本框】设置Burst按字节时的速率阈值，取值范围为1-65535的整数，默认10pps
* 速率阈值 (pps)：【text文本框】取值范围为1-262143的整数

限速组列表：

* 列表显示32个限速组、限速类型、Burst阈值（带单位）、速率阈值（带单位）
* 支持单个编辑

## IP源防护/IP Source Guard(FP1B)

【功能概述】

IP源防护攻击是一种基于二层接口的源IP地址过滤技术，它能够防止恶意主机伪造合法主机的IP地址来仿冒合法主机，还能确保非授权主机不能通过自己制定IP地址的方式来访问网络或攻击网络。

IPSG利用绑定表（源IP地址、源MAC地址、所属VLAN、入接口的绑定）去匹配检查二层接口上收到的IP报文，只有匹配绑定表的报文才允许通过，其他报文将被丢弃。绑定表分为静态和动态2种。

|  |  |  |
| --- | --- | --- |
| 绑定表类型 | 生成过程 | 适用场景 |
| 静态绑定表 | 由用户手工配置添加 | 针对IPv4和IPv6主机，适用于主机数较少且主机使用静态IP地址的场景 |
| DHCP Snooping动态绑定表（1） | 配置DHCP Snooping功能后，DHCP主机动态获取IP地址时，设备根据DHCP服务器发送的DHCP回复报文动态生成 | 针对IPv4和IPv6主机，适用于主机数较多且主机从DHCP服务器获取IP地址的场景 |
| DHCP Snooping动态绑定表（2） | 802.1X用户认证过程中，设备根据认证用户的信息生成 | 针对IPv4和IPv6主机，适用于主机数较多、主机使用静态IP地址、并且网络中部署了802.1X认证的场景。  该生成方式的表项不可开，建议配置静态绑定表 |
| ND Snooping动态绑定表 | 配置ND Snooping功能后，设备通过侦听用户用于重复地质检测的NS（Neighbor Solicitation）报文来建立 | 仅针对IPv6主机，适用于主机数较多的场景 |

绑定表生成后，IPSG基于绑定表向指定接口下发ACL，由该ACL来匹配检查所有IP报文。主机发送的报文，只有匹配绑定表才会允许通过，不匹配的报文都将被丢弃。当绑定表信息变化时，设备会重新下发ACL。缺省情况下，如果在没有绑定表的情况下使能了IPSG，设备会允许IP协议报文通过，但是会拒绝所有的数据报文。

**IPSG的过滤方式：**

静态绑定表项包括：MAC地址、IP地址、VLAN、接口。静态绑定表项中指定的信息均用于IPSG过滤接口收到的报文。

动态绑定表项包括：MAC地址、IP地址、VLAN、接口及表项类型（DHCP Snooping、DHCP Relay等）。IPSG依据该表项中的哪些信息过滤接口收到的报文，由用户设置的检查项决定，缺省是四项都进行匹配检查。常见的几种检查项如下表：

|  |  |
| --- | --- |
| 设置的检查项 | 含义 |
| 基于源IP地址过滤 | 根据源IP地址对报文进行过滤，只有源IP地址和绑定表匹配，才允许报文通过 |
| 基于源IP地址+源MAC地址过滤 | 根据源IP和源MAC对报文进行过滤，只有源IP和源MAC地址都和绑定表匹配，才允许报文通过 |
| 基于源IP地址+VLAN过滤 | 根据源IP和VLAN对报文进行过滤，只有源IP和VLAN都和绑定表匹配，才允许报文通过 |
| 基于源IP地址+源MAC地址+VLAN过滤 | 根据源IP、源MAC和VLAN对报文进行过滤，只有源IP、源MAC和VLAN都和绑定表匹配，才允许报文通过 |

**IPSG特点：**

* IP+MAC+VLAN多元组合绑定来过滤IP流量
* 可以结合DHCP Snooping的动态表项来配合使用，也可以单独发挥作用
* IPSG的配置优先级高于DHCP Snooping
* IPSG和DHCP Snooping共用配置上限

【配置参数】

* 接口：选择需要启用IPSG的交换机接口，包括电口、光口和聚合接口。可多选。
* IPSG：【开关】设置是否开启接口的IPSG功能，默认关闭。
* 校验类型：【下拉框】设置端口校验的类型，选项有{IP | IP-MAC}，默认IP。
* ~~最大条目数：【text文本框】设置接口可以生成绑定表的最大条目数，包括动态绑定条目和静态绑定条目，取值范围为0-256的整数，0表示无限制，默认为0。~~

~~注：最大条目数上限为IPv4和IPv6共用。【20230807交互评审去除】~~

IPSG列表：

* 列表显示接口名称、IPSG开关状态、最大条目数、四元绑定表项个数。
  + 支持查看每个接口的四元绑定表，显示接口、IP、MAC、VLAN、类型（静态和动态来源）。
  + 支持添加/编辑/删除四元绑定表项
* 支持编辑单个/批量/全部接口的IPSG配置

**四元绑定表：**

添加静态四元绑定条目：至多添加256个，与IPv6四元绑定表共用

* 端口：【单选】选择添加四元绑定条目的交换机接口，包括电口、光口和聚合接口。
* IP地址：【text文本框】设置IP地址，必须为有效单播地址。若输入IPv4地址，则按IPv4地址格式（点分十进制）进行输入，否则需提示“您输入的IPv4地址格式不正确，请重新输入”。
* MAC地址：【text文本框】设置指定的MAC地址，输入格式为HH:HH:HH:HH:HH:HH(其中，H为1-2位的十六进制数)，形如00:10:DC:28:A4:E9，不可设置为FFFF-FFFF-FFFF、组播地址和全零MAC地址。
* VLAN：【text文本框】设置指定的所属VLAN，取值范围为1-4094的整数。

注：一个接口可以添加多个IPSG四元绑定条目。

四元绑定表：

* 列表显示接口、IP地址、MAC地址、VLAN、类型（静态 | 动态来源）、租期（只有动态绑定表项有）
* 支持添加
* 支持删除静态绑定表
* 支持分页
* 支持导入四元绑定表(FP2)

利用csv文件，在csv文件中填写好接口、IP地址、MAC地址、VLAN id形成四元绑定表。

点击<导入>按钮，出现弹窗提示：

[点击上传csv文件。

点击下载 参考模板

<取消> <添加>]

并提供下载模板文件和上传导入文件的按钮。

导入的文件，全部做静态表项处理。若存在配置错误问题，则丢弃相应错误的表项，仅导入正确的表项；若达到绑定表项数量上限，则后续的表项不再进行导入；VLAN相同情况下，MAC地址一致IP不一致，则覆盖处理；MAC不一致IP一致，则新增；MAC和IP一致则覆盖处理。

* 支持导出四元绑定表(FP2)。一键导出，将动静态绑定表全部导出，仅包含接口、IP、MAC和VLAN信息，文件命名为IPMV\_年月日时分秒.csv

## IPv6源防护/IP Source Guard(FP2)

【功能概述】

IPv6源防护攻击是一种基于二层接口的源IPv6地址过滤技术，它能够防止恶意主机伪造合法主机的IPv6地址来仿冒合法主机，还能确保非授权主机不能通过自己制定IPv6地址的方式来访问网络或攻击网络。

IPv6SG利用绑定表（源IPv6地址、源MAC地址、所属VLAN、入接口的绑定）去匹配检查二层接口上收到的IPv6报文，只有匹配绑定表的报文才允许通过，其他报文将被丢弃。绑定表分为静态和动态2种。

|  |  |  |
| --- | --- | --- |
| 绑定表类型 | 生成过程 | 适用场景 |
| 静态绑定表 | 由用户手工配置添加 | 针对IPv6主机，适用于主机数较少且主机使用静态IP地址的场景 |
| DHCPv6 Snooping动态绑定表（1） | 配置DHCPv6 Snooping功能后，DHCv6P主机动态获取IPv6地址时，设备根据DHCPv6服务器发送的DHCv6P回复报文动态生成 | 针对IPv6主机，适用于主机数较多且主机从DHCP服务器获取IP地址的场景 |
| DHCPv6 Snooping动态绑定表（2） | 802.1X用户认证过程中，设备根据认证用户的信息生成 | 针对IPv6主机，适用于主机数较多、主机使用静态IPv6地址、并且网络中部署了802.1X认证的场景。  该生成方式的表项不可开，建议配置静态绑定表 |
| ND Snooping动态绑定表 | 配置ND Snooping功能后，设备通过侦听用户用于重复地质检测的NS（Neighbor Solicitation）报文来建立 | 仅针对IPv6主机，适用于主机数较多的场景 |

绑定表生成后，IPv6SG基于绑定表向指定接口下发ACL，由该ACL来匹配检查所有IPv6报文。主机发送的报文，只有匹配绑定表才会允许通过，不匹配的报文都将被丢弃。当绑定表信息变化时，设备会重新下发ACL。缺省情况下，如果在没有绑定表的情况下使能了IPv6SG，设备会允许IPv6协议报文通过，但是会拒绝所有的数据报文。

**IPv6SG的过滤方式：**

静态绑定表项包括：MAC地址、IPv6地址、VLAN、接口。静态绑定表项中指定的信息均用于IPv6SG过滤接口收到的报文。

动态绑定表项包括：MAC地址、IPv6地址、VLAN、接口及表项类型（DHCPv6 Snooping、DHCPv6 Relay等）。IPv6SG依据该表项中的哪些信息过滤接口收到的报文，由用户设置的检查项决定。常见的几种检查项如下表：

|  |  |
| --- | --- |
| 设置的检查项 | 含义 |
| 基于源IPv6地址过滤 | 根据源IPv6地址对报文进行过滤，只有源IPv6地址和绑定表匹配，才允许报文通过 |
| 基于源IPv6地址+源MAC地址过滤 | 根据源IPv6和源MAC对报文进行过滤，只有源IPv6和源MAC地址都和绑定表匹配，才允许报文通过 |
| 基于源IPv6地址+VLAN过滤 | 根据源IPv6和VLAN对报文进行过滤，只有源IPv6和VLAN都和绑定表匹配，才允许报文通过 |
| 基于源IPv6地址+源MAC地址+VLAN过滤 | 根据源IPv6、源MAC和VLAN对报文进行过滤，只有源IPv6、源MAC和VLAN都和绑定表匹配，才允许报文通过 |

**IPv6SG特点：**

* IPv6+MAC+VLAN多元组合绑定来过滤IP流量
* 可以结合DHCPv6 Snooping/DHCPv6 Relay的动态表项来配合使用，也可以单独发挥作用
* IPv6SG的配置优先级高于DHCPv6 Snooping/DHCPv6 Relay
* IPv6SG和DHCPv6 Snooping共用配置上限

【配置参数】

* 接口：选择需要启用IPv6SG的交换机接口，包括电口、光口和聚合接口。可多选。
* IPv6SG：【开关】设置是否开启接口的IPv6SG功能，默认关闭。
* 校验类型：【下拉框】设置端口校验的类型，选项有{IPv6 | IPv6-MAC}，默认IPv6。
* ~~最大条目数：【text文本框】设置接口可以生成绑定表的最大条目数，包括动态绑定条目和静态绑定条目，取值范围为0-256的整数，0表示无限制，默认为0。~~

~~注：最大条目数上限为IPv4和IPv6共用。【20230807交互评审去除】~~

IPv6SG列表：

* 列表显示接口名称、IPv6SG开关状态、校验类型、最大条目数、四元绑定表项个数。
  + 支持查看每个接口的四元绑定表，显示接口、IPv6、MAC、VLAN、类型（静态和动态来源）。
  + 支持添加/编辑/删除四元绑定表项
* 支持编辑单个/批量/全部接口的IPSG配置

**四元绑定表：**

添加静态四元绑定条目：至多添加256个，与IPv4四元绑定表共用

* 端口：【单选】选择添加四元绑定条目的交换机接口，包括电口、光口和聚合接口。
* IPv6地址/前缀长度：【text文本框】设置IPv6地址，按IPv6地址格式（类似X:XX::X:X。IPv6地址共128bits，每16bits为一段，段之间用:分隔）进行输入，否则需提示“您输入的IPv6地址格式不正确，请重新输入”。前缀长度取值范围为1-128的整数，默认64。
* MAC地址：【text文本框】设置指定的MAC地址，输入格式为HH:HH:HH:HH:HH:HH(其中，H为1-2位的十六进制数)，形如00:10:DC:28:A4:E9，不可设置为FFFF-FFFF-FFFF、组播地址和全零MAC地址。
* VLAN：【text文本框】设置指定的所属VLAN，取值范围为1-4094的整数。

注：一个接口可以添加多个IPv6SG四元绑定条目。

四元绑定表：

* 列表显示接口、IPv6地址、MAC地址、VLAN、类型（静态 | 动态来源）、租期（只有动态绑定表项有）
* 支持添加
* 支持删除静态绑定表
* 支持分页
* 支持导入和导出，同IPv4四元绑定表的导入导出功能，文件名为IPv6MV\_年月日时分秒.csv

## 动态ARP检测/Dynamic ARP Inspection(DAI)(FP1C)

【功能概述】

为了防御中间人攻击，避免合法用户的数据被中间人窃取，可以执行本命令使能动态ARP检测功能。设备会将ARP报文对应的源IP、源MAC、接口、BD和VLAN信息与绑定表中的信息进行比较，如果信息匹配，说明发送该ARP报文的用户是合法用户，允许此用户的ARP报文通过，否则就认为是攻击，丢弃该ARP报文。

可在接口视图、BD视图或VLAN视图下使能动态ARP检测功能。在接口视图下使能时，则对该接口收到的所有ARP报文进行绑定表匹配检查；在VLAN或BD视图下使能时。则对加入该VLAN或BD的接口收到的属于该VLAN或BD的ARP报文进行绑定表匹配检查。

当设备丢弃的不匹配绑定表的ARP报文数量较多时，如果希望设备能够以告警的方式提醒网络管理员，则可以使能动态ARP检测丢弃报文告警功能。当丢弃的ARP报文数超过告警阈值时，设备将产生告警。

【配置参数】

* DAI：【开关】设置是否开启交换机的动态ARP检测功能，默认关闭。
* VLAN：选择需要ARP检测的VLAN范围，从已有的VLAN中选择，可多选。

端口设置：

* 端口：选择需要进行ARP检测的交换机接口，包括电口、光口和聚合接口。可多选
* 信任端口：【开关】设置是否将端口设置为信任端口，默认关闭。开启后，则对接收的ARP报文不做校验。
* 源MAC地址校验：【开关】设置是否对接收的ARP应答报文校验源MAC地址进行一致性检查，即对以太网数据帧头部的源MAC地址和ARP报文数据区中的源MAC地址进行一致性检查，如果不等则将报文丢弃。默认关闭。
* 目的MAC地址校验：【开关】设置是否对接收的ARP应答报文校验目的MAC地址进行一致性检查，即对以太网数据帧头部的目的MAC地址和ARP报文数据区中的目的MAC地址进行一致性检查，如果不等则将报文丢弃。默认关闭。
* IP地址校验：【开关】设置是否对ARP报文中的源IP地址和目的IP地址进行校验，如果不合法则将报文丢弃，默认关闭。开启后，还支持允许源IP地址为全零的probe报文通过。
* 允许全零地址：【开关】设置是否允许ARP报文中IP地址为全零（0.0.0.0）的probe报文通过，默认关闭。
* 速率 (pps)：【text文本框】设置端口每秒允许接收的ARP报文个数，单位时间内超过阈值的ARP报文将被丢弃，端口同时error-down。取值范围为0-50的整数，默认0，即不限速。

端口列表：

* 列表显示端口、信任端口、源MAC地址校验、目的MAC地址校验、源IP地址校验、速率
* 支持编辑

端口数据统计表：

* 列表显示端口、ARP转发报文数、ARP源MAC地址校验错误数、ARP目的MAC地址校验错误数、ARP源IP地址校验错误数、ARP目的IP地址校验错误数、ARP报文中IP地址与MAC地址均校验错误数
* 支持刷新
* 支持清除指定端口数据

## 攻击防范/Anti Attack(FP1B)

【功能概述】

在网络中，存在着大量针对CPU的恶意攻击报文以及需要正常上送CPU的各类报文。针对CPU的恶意攻击报文会导致CPU长时间繁忙的处理攻击报文，从而引发其他业务的断续甚至系统的中断；大量正常的报文也会导致CPU占用率过高，性能下降，从而影响正常的业务。

为了保护CPU，保证CPU对正常业务的处理和响应，交换机提供了本地防攻击功能，其针对的是上送CPU的报文，主要用于保护设备自身安全，保证已有业务在发生攻击时的正常运转，避免设备遭受攻击时各业务的相互影响。

攻击防范是一种重要的网络安全特性。它通过分析上送CPU处理的报文的内容和行为，判断报文是否具有攻击特性，并配置对具有攻击特性的报文执行一定的防范措施。防范攻击主要分为畸形报文攻击防范、分片报文攻击防范和泛洪攻击防范。

**1.畸形报文攻击防范**

畸形报文攻击是通过向交换机发送有缺陷的IP报文，使得交换机在处理这样的IP包时会出现崩溃，给交换机带来损失。

畸形报文攻击主要有如下集中：

* 没有IP载荷的泛洪攻击
* IGMP空报文攻击
* LAN攻击
* Smurf攻击
* TCP标志位非法攻击

为了避免交换机被畸形报文攻击导致瘫痪，保证正常的网络服务，可以配置畸形报文攻击防范。交换机对畸形报文攻击防范的主要措施是判断是否是几种畸形报文攻击报文类型之一，若是，则直接丢弃畸形报文。

**2.分片报文攻击防范**

攻击者通过向交换机发送分片出错的报文，使得交换机在处理分片错误的报文时消耗大量的CPU资源，给交换机带来损失。分片报文攻击主要有如下几种：

* 分片数量巨大攻击
* 巨大offset攻击
* 重复分片攻击
* Tear Drop攻击
* Syndrop攻击
* NewTear攻击
* Bonk攻击
* Nesta攻击
* Rose攻击
* Fawx攻击
* Ping of Death攻击
* Jolt攻击

为了避免交换机被分片报文攻击导致瘫痪，保证正常的网络服务，可以配置分片报文攻击防范。对分片报文攻击防范的主要措施是进行速率限制，防止大量的分片报文造成CPU繁忙，保证CPU在造成攻击的情况下正常运行。

**3.TCP SYN泛洪攻击防范**

TCP YSN泛洪攻击是一种古老而有效的攻击方式。它属于拒绝服务攻击，这类攻击完全依赖于TCP连接的建立方式。攻击者向交换机发送SYN报文，然后对于交换机返回的SYN+ACK报文不作回应。交换机如果没有收到攻击者的ACK回应，就会一直等待，形成半连接。攻击者利用这种方式，让交换机生成大量的半连接，迫使其大量资源浪费在这些半连接上。

为了避免TCP SYN泛洪攻击，可以在交换机上配置TCP SYN泛洪攻击防范功能，通过限制TCP SYN报文的发送速率来防范TCP SYN泛洪攻击，保证受到攻击时系统资源不被耗尽。

**4.UDP泛洪攻击防范**

Fraggle攻击：Fraggle攻击的原理是利用UDP 7号端口，7端口的服务和ICMP echo基本一样，都是把收到的报文载荷原封不动地回复回去，以测试源和目的之间的网络状况。和Smurf攻击的原理一样，把源地址伪造成受害者地址，目的地址写成某个广播地址，目的端口为7，源端口可以不是7，也可以是7。如果该广播网络有很多主机都起了UDP echo服务，那么受害者将收到很多回复报文，达到攻击的效果。

UDP诊断端口攻击：对诊断端口（7-echo，13-daytime，19-Chargen等）随机发包，如果同时发送的数据包数量很大，造成泛洪，可能影响网络设备正常工作。很多设备厂家都会默认打开一些端口，以进行网络诊断、设备管理等作用，但同时也是暴露给攻击者一个很好的攻击机会。

为了避免UDP泛洪攻击，可以在交换机上配置UDP泛洪攻击防范。交换机上配置UDP泛洪攻击防范功能，对于端口号为7、13和19的报文，直接丢弃。

**5.ICMP泛洪攻击防范**

如果攻击者在短时间内向交换机发送大量的ICMP相应请求报文，使交换机忙于回复这些请求，会造成交换机负担过重而不能处理正常的业务。

为了避免ICMP泛洪攻击，可以在交换机上配置ICMP泛洪攻击防范功能。交换机上配置ICMP泛洪攻击防范功能，通过限制ICMP报文的速率来防范ICMP泛洪攻击。

【配置参数】

**畸形报文攻击防范：**

* Land：【开关】当报文中的源地址和目的地址一致时，认为是畸形报文攻击。设置是否丢弃该报文。默认关闭。
* Smurf Attack：【开关】设备通过检测ICMP请求报文的目标IPv4地址是广播地址或子网广播地址时，设置是否丢弃该报文来避免Smurf攻击。默认关闭，开启后需配置目标地址的掩码长度。
* \*掩码长度：【text文本框】设置设备检测ICMP请求报文的目标地址的掩码长度，取值范围为0-32，默认0。
* TCP SYN-RST Attack：【开关】TCP标志位非法攻击，设备检测到TCP报文中SYN-RST设为1时，设置是否开启TCP SYN-RST攻击防范，默认关闭。
* TCP SYN-FIN Attack：【开关】TCP标志位非法攻击，设备检测到TCP报文中SYN-FIN设为1时，设置是否开启TCP SYN-FIN攻击防范，默认关闭。
* TCP X-Mass Scan Attack：【开关】TCP标志位非法攻击，设备检测到TCP报文中序列号为0，FIN/URG/PSH均设为1时，设置是否开启TCP X-Mass扫描攻击防范，默认关闭。
* TCP SYN Nonack Sport Attack：【开关】设备检测达到TCP报文中SYN=land ack=0，并且sport(源端口)小于1024的报文时，设置是否直接丢弃该报文，默认关闭。
* TCP Null Scan Attack：【开关】设备检测到TCP报文中序列号为0，control-flags为0，设置是否直接丢弃该报文，默认关闭。

注：上述5个TCP相关的配置在交互设计上可以合并，内部分成TCP标志位非法攻击和其他两大类。

* SMAC=DMAC：【开关】设备检测到二层的源MAC和目的MAC相等时，设置是否直接丢弃该报文，默认关闭。
* ICMP Ping：【开关】设备检测到ICMP Ping IPv4报文长度大于用户设置的长度时，设置是否直接丢弃该报文，默认关闭。开启后，需配置Ping IPv4报文的有效载荷最大值。
* ICMPv6 Ping：【开关】设备检测到ICMP Ping IPv6报文长度大于用户设置的长度时，设置是否直接丢弃该报文，默认关闭。开启后，需配置Ping IPv6报文的有效载荷最大值。

注：交互设计上可以将这两者合并，做成选择IPv4和IPv6的形式。

* 最大长度 (Byte)：【text文本框】取值范围为0-65535，默认512。

注：ICMP Ping、ICMPv6 Ping两者任一开启，即可配置。

* IPv4 Ping of Death：【开关】设备检测到报文长度大于64k的报文时，设置是否直接丢弃该报文，默认关闭。
* TCP Blat：【开关】设备检测到TCP的源端口等于目的端口时，设置是否直接丢弃该报文，默认关闭。
* UDP Blat：【开关】设备检测到UDP的源端口等于目的端口时，设置是否直接丢弃该报文，默认关闭。

注：TCP和UDP Blat在交互设计上可以合并，做成选择TCP和UDP的形式。

**分片报文攻击防范：**

* ICMP Fragment：【开关】设备检测到ICMP报文分片，设置是否直接丢弃该报文，默认关闭。
* IPv6 Min Fragment：【开关】设备检测到IPv6报文分片小于用户设置的值，设置是否直接丢弃该报文，默认关闭。开启后，需要设置IPv6报文分片的最小长度。
* 最小分片长度/Minimum Fragment (Byte)：【text文本框】取值范围为0-65535，默认1240。
* TCP Fragment：【开关】设备检测到TCP报文分片，设置是否直接丢弃该报文，其中IP有效负载长度减去IP标头的值小于允许的最小TCP标头大小。默认关闭。注：TCP标头偏移量默认为1。
* TCP Min Hdr：【开关】设备检测到TCP的报文头+净荷长度小于用户设置的值时，设置是否直接丢弃该报文，此举是为了防止TCP头部被切片，默认关闭。开启后，需设置TCP报文头最小的长度。
* 最小报文头长度/Minimum Hdr (Byte)：【text文本框】取值范围为0-31，默认20。

## RADIUS(FP1C)

【功能概述】

RADIUS是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。该协议定义了基于UDP的RADIUS报文格式及其传输机制，并规定目的UDP端口1812、1813分别作为默认的认证、计费端口号。

RADIUS通过认证授权来提供接入服务，通过计费来收集、记录用户对网络资源的使用。RADIUS协议的主要特征有：（1）客户端/服务器模式；（2）安全的消息交互机制；（3）良好的扩展性。

**客户端/服务器模式**

* RADIUS客户端：一般位于网络接入服务器NAS上，可以遍布整个网络，负责传输用户信息到指定的RADIUS服务器，然后根据从服务器返回的信息进行相应处理（如接受/拒绝用户接入）。
* RADIUS服务器：一般运行在中心计算机或工作站上，维护相关的用户认证和网络服务访问信息，负责接收用户连接请求并认证用户，然后给客户端返回所有需要的信息（如接受/拒绝认证请求）。RADIUS服务器通常要维护三个数据库：（1）Users，用于存储用户信息（如用户名、密码以及使用的协议、IP地址等配置信息）；（2）Clients，用于存储RADIUS客户端的信息（如共享密钥、IP地址等）；（3）Dictionary，用于存储RADIUS协议中的属性和属性值含义的信息。

**安全的消息交互机制**

RADIUS客户端和服务器之间认证消息的交互是通过共享密钥的参与来完成的。共享密钥是一个带外传输的、客户端和服务器都知道的字符串，不需要单独进行网络传输。RADIUS报文中有一个16字节的验证字字段，包含了对整个报文的数字签名数据，该签名数据是在共享密钥的参与下利用MD5算法计算得出。收到RADIUS报文的一方要验证该签名的正确性，如果报文的签名不正确，则丢弃它。通过这种机制，保证了RADIUS客户端和RADIUS服务器之间信息交互的安全性。另外，为防止用户密码在不安全的网络上传递时被窃取，在RADIUS报文传输过程中还利用共享密钥对用户密码进行了加密。

**RADIUS报文类型**

RADIUS认证报文：

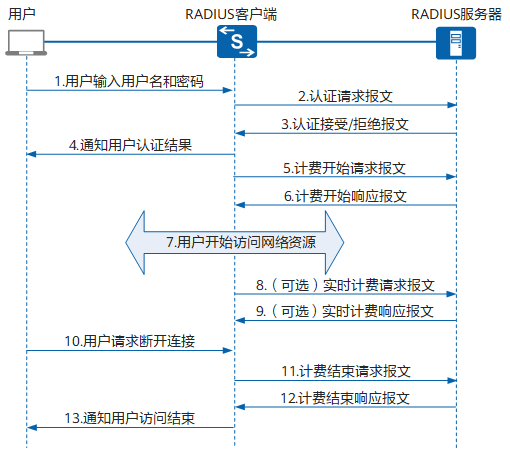
|  |  |
| --- | --- |
| 报文名称 | 说明 |
| Access-Request | 认证请求报文，是RADIUS报文交互过程中的第一个报文，用来携带用户的认证信息（如用户名、密码等）。认证请求报文由RADIUS客户端发送给RADIUS服务器，RADIUS服务器根据该报文中携带的用户信息判断是否允许接入。 |
| Access-Accept | 认证接受报文，是RADIUS服务器对RADIUS客户端发送的Access-Request报文的接受响应报文。如果Access-Request报文中的所有属性都可以接受（即认证通过），则发送该类型报文。RADIUS客户端收到此报文后，用户才能认证通过并被赋予相应的权限。 |
| Access-Reject | 认证拒绝报文，是RADIUS服务器对RADIUS客户端的Access-Request报文的拒绝响应报文。如果Access-Request报文中的任何一个属性不可接受（即认证失败），则RADIUS服务器返回Access-Reject报文，用户认证失败。 |
| Access-Challenge | 认证挑战报文。EAP中继认证时，RADIUS服务器接收到Access-Request报文中携带的用户名信息后，会随机生成一个MD5挑战字，同时将此挑战字通过Access-Challenge报文发送给用户。用户使用该挑战字对用户密码进行加密处理后，将新的用户密码信息通过Access-Request报文发送给RADIUS服务器。RADIUS服务器将收到的已加密的密码信息和本地经过加密运算后的密码信息进行对比，如果相同，则该用户为合法用户。 |

RADIUS计费报文：

|  |  |
| --- | --- |
| 报文名称 | 说明 |
| Accounting-Request(Start) | 计费开始请求报文。如果RADIUS客户端使用RADIUS模式进行计费，RADIUS客户端会在用户开始访问网络资源时，向RADIUS服务器发送计费开始请求报文。 |
| Accounting-Response(Start) | 计费开始响应报文。RADIUS服务器接收并成功记录计费开始请求报文后，需要回应一个计费开始响应报文。 |
| Accounting-Request(Interim-update) | 实时计费请求报文。为避免RADIUS服务器无法收到计费结束请求报文而继续对该用户计费，可以在RADIUS客户端上配置实时计费功能。RADIUS客户端定时向RADIUS服务器发送实时计费请求报文，减少计费误差。 |
| Accounting-Response(Interim-update) | 实时计费响应报文。RADIUS服务器接收并成功记录实时计费请求报文后，需要回应一个实时计费响应报文。 |
| Accounting-Request(Stop) | 计费结束请求报文。当用户断开连接时（连接也可以由NAS断开），RADIUS客户端向RADIUS服务器发送计费结束请求报文，其中包括用户上网所使用的的网络资源的统计信息（上网时长、进/出的字节数等），请求RADIUS服务器停止计费。 |
| Accounting-Response(Stop) | 计费结束响应报文。RADIUS服务器接收计费停止请求报文后，需要回应一个计费停止响应报文。 |

**RADIUS认证、授权、计费流程**

设备作为RADIUS客户端，负责收集用户信息（例如：用户名、密码等），并将这些信息发送到RADIUS服务器。RADIUS服务器则根据这些信息完成用户身份认证以及认证通过后的用户授权和计费。



1.当用户接入网络时，用户发起连接请求，向RADIUS客户端（即设备）发送用户名和密码。

2.RADIUS客户端向RADIUS服务器发送包含用户名和密码信息的认证请求报文。

3.RADIUS服务器对用户身份的合法性进行检验：

* 如果用户身份合法，RADIUS服务器向RADIUS客户端返回认证接受报文，允许用户进行下一步动作。由于RADIUS协议合并了认证和授权的过程，因此认证接受报文中也包含了用户的授权信息。
* 如果用户身份不合法，RADIUS服务器向RADIUS客户端返回认证拒绝报文，拒绝用户访问接入网络。

4.RADIUS客户端通知用户认证是否成功。

5.RADIUS客户端根据接收到的认证结果接入/拒绝用户。如果允许用户接入，则RADIUS客户端向RADIUS服务器发送计费开始请求报文。

6.RADIUS服务器返回计费开始响应报文，并开始计费。

7.用户开始访问网络资源。

8.（可选）在使能实时计费功能的情况下，RADIUS客户端会定时向RADIUS服务器发送实时计费请求报文，以避免因付费用户异常下线导致的不合理计费。

9.（可选）RADIUS服务器返回实时计费响应报文，并实时计费。

10.用户发起下线请求，请求停止访问网络资源。

11.RADIUS客户端向RADIUS服务器提交计费结束请求报文。

12.RADIUS服务器返回计费结束响应报文，并停止计费。

13.RADIUS客户端通知用户访问结束，用户结束访问网络资源。

**RADIUS报文重传机制**

用户认证过程中，设备会发送认证请求报文到RADIUS服务器。为避免由于网络故障、时延等原因导致设备无法收到服务器的回应报文，设备在发送认证请求报文到服务器时具有超时重传超时机制，重传次数和重传间隔通过定时器进行控制。

满足以下任意一个条件，设备停止重传：

* 收到RADIUS服务器的回应报文。收到RADIUS服务器的回应报文后，设备会停止重传，此时设备标记RADIUS服务器的状态为Up。
* 探测到RADIUS服务器的状态为Down。设备将RADIUS服务器的状态置为Down后：
* 如果达到最大重传次数，则停止重传，RADIUS服务器的状态为Down。
* 如果还没有达到最大重传次数，设备会再重传一次认证请求报文到RADIUS服务器。相当于给状态为Down的服务器一次机会。如果收到RADIUS服务器的回应报文，停止重传，并将RADIUS服务器的状态恢复为Up；如果未收到RADIUS服务器的回应报文，也停止重传，RADIUS服务器的状态为Down。
* 达到最大重传次数。达到最大重传次数后，设备会停止重传，此时：
* 如果收到RADIUS服务器的回应报文，此时设备标记RADIUS服务器的状态为Up。
* 如果已经探测到RADIUS服务器的状态为Down，设备将服务器的状态置为Down。
* 如果没收到RADIUS服务器的回应报文也没有探测到服务器的状态为Down，此时，设备不会切换服务器的状态，服务器实际上没有响应。

RADIUS报文重传是针对一个服务器而言的，如果RADIUS服务器模板中配置了多个服务器，整体重传时间取决于重传间隔、重传次数、RADIUS服务器的状态、服务器的个数以及选择服务器的算法。

**RADIUS服务器状态探测**

RADIUS服务器状态：

|  |  |  |
| --- | --- | --- |
| 状态 | RADIUS服务器是否可用 | 出现该状态的场景 |
| Up | 可用 | * RADIUS服务器的初始状态 * 设备收到RADIUS服务器的报文 |
| Down | 不可用 | 满足将RADIUS服务器的状态标记为Down的条件 |
| Force-up | 在没有可用的RADIUS服务器时，会选择Force-up状态的服务器 | Dead-time定时器超时 |

RADIUS服务器的初始状态被标记为Up。在收到RADIUS认证请求报文、并且满足将RADIUS服务器的状态标记为Down的条件时，RADIUS服务器的状态被切换为Down。触发状态切换的RADIUS认证请求报文可以是用户认证过程中发送的，也可以是管理员构造的，比如执行test-aaa命令时发送的测试报文或者自动探测时发送的探测报文。

以下几种情形下，设备会将RADIUS服务器的状态由Down切换为Up或者Force-up：

* dead-time定时器超时，将RADIUS服务器的状态由Down切换为Force-up：设备在将RADIUS服务器的状态标记为Down后就会启动dead-time定时器，该定时器定义了Down状态可持续的时长。定时器超时后，设备将服务器的状态标记为Force-up。之后，如果有新用户需要通过RADIUS方式进行认证，在没有可用的RADIUS服务器的情况下，设备会尝试和Force-up状态的服务器重新建立连接。
* 设备收到RADIUS服务器的报文，将RADIUS服务器的状态由Down切换为Up。例如，配置自动探测后，设备收到RADIUS服务器的响应报文。

将RADIUS服务器的状态标记为Down的条件：（1）RADIUS服务器最大无响应时长（max-unresponsive-interval的取值）；（2）RADIUS请求报文发送的次数；（3）RADIUS请求报文发送的时间间隔；（4）RADIUS服务器的探测周期：（5）RADIUS服务器探测周期循环次数；（6）RADIUS服务器在每个探测周期内连续无响应最大次数。

将RADIUS服务器的状态标记为Down的条件分为两种，只要满足其中一种，RADIUS服务器的状态就会被标记为Down。

* 在RADIUS服务器状态探测过程中，将RADIUS服务器标记为Down状态。系统启动后，RADIUS服务器状态探测定时器开始运行。从设备发送第一个RADIUS认证请求报文开始计算，如果设备一直没有收到RADIUS服务器的报文，并且在一个探测周期内满足条件：未收到RADIUS服务器报文的次数（n）大于或等于连续无响应的最大次数（dead-count），则记录一次通讯中断。在持续没有收到RADIUS服务器报文的情况下，探测周期循环几次，就在第几次记录通讯中断时将RADIUS服务器标记为Down。
* 将长时间无响应的RADIUS服务器标记为Down状态。在用户接入频率较低、设备收到用户认证请求报文较少、RADIUS服务器状态探测过程中将RADIUS服务器标记为Down的条件无法满足的情况下，连续两个无响应的认证请求报文的时间间隔大于max-unresponsive-interval时，RADIUS服务器被标记为Down，此机制能够确保用户获取逃生授权。

**自动探测**

RADIUS服务器的状态被标记为Down后，通过自动探测功能可以检测RADIUS服务器的可达性。自动探测功能需要手动开启。开启自动状态探测功能只需在设备的RADIUS服务器模板视图下配置自动探测用户名和密码，在RADIUS服务器上不需要配置此自动探测用户名和密码。认证无需成功，设备能收到认证失败响应报文就能证明RADIUS服务器是正常工作的。

|  |  |  |  |
| --- | --- | --- | --- |
| 服务器的状态 | 是否支持自动探测 | 何时发送自动探测报文 | 服务器状态切换的条件 |
| Down状态 | 缺省支持 | 自动探测周期过后发送 | 在探测报文的超时等待时间内，如果设备收到了RADIUS服务器的报文，会将RADIUS服务器的状态标记为Up；反之，则保持RADIUS服务器的状态为Down。 |
| Up状态 | 通过命令行radius-server detect-server up-server interval开启 | 自动探测周期过后发送 | 满足将RADIUS服务器的状态标记为Down的条件，则将RADIUS服务器的状态标记为Down；反之，则保持RADIUS服务器的状态为Up。 |
| Force-up状态 | 缺省支持 | 立即发送 | 在超时等待时间内，如果收到RADIUS服务器的报文，设备会将RADIUS服务器的状态标记为Up；反之，则将RADIUS服务器的状态标记为Down。 |

设备将RADIUS服务器的状态标记为Down之后，通过配置逃生功能，使用户能够进入逃生授权。设备探测到RADIUS服务器状态恢复为Up后，通过配置重认证功能，使用户重认证获取RADIUS服务器授权。

【配置参数】

添加RADIUS服务器：至多添加4个

* \*RADIUS服务器地址：【text文本框】设置RADIUS服务器的地址，支持输入Hostname和IP地址（包括IPv4和IPv6），需要满足各类型的地址格式要求，否则需要报错提示。
* \*端口：【text文本框】设置UDP端口号，取值为1-65535的整数，默认1812。
* \*优先级：【text文本框】设置RADIUS服务器使用的顺序，取值为0-65535的整数。每个RADIUS服务器具有唯一性。
* \*共享密钥：【text文本框】设置交换机和RADIUS服务器共享的加密密钥，默认password，支持编辑。最长64字符，允许输入的字符有字母、数字和特殊字符()<>,./’”;:[]{}\|=+-\_\*&^%$#@!~`（键盘半角全部支持）
* 最大重传次数：【text文本框】设置RADIUS服务器超时后的最大重传次数，取值为1-5的整数，默认1次。
* 超时时间 (秒)：【text文本框】设置交换机重发RADIUS报文等待RADIUS服务器应答的最长时间，取值为1-120的整数，默认10秒。

RADIUS服务器列表：

* 列表显示RADIUS服务器地址、端口、优先级、最大重传次数、超时时间
* 支持编辑
* 支持删除单条/批量/全部RADIUS服务器

## TACACS+(FP1C)

【功能概述】

TACACS+（终端访问控制器控制系统协议）是在TACACS协议的基础上进行了功能增强的安全协议。该协议与RADIUS协议的功能类似，采用客户端/服务器模式实现NAS与TACACS+服务器之间的通信。

TACACS+是一种集中式的、客户端/服务器结构的信息交互协议，使用TCP协议传输，TCP端口号为49。TACACS+提供的认证、授权和计费服务器相互独立，能够在不同的服务器上实现。其主要用于采用点对点协议PPP或虚拟私有拨号网络VPDN方式接入Internet的接入用户以及进行操作的管理用户的认证、授权和计费。

TACACS+与RADIUS协议相似：（1）结构上都采用客户端/服务器模式；（2）都使用共享密钥对传输的用户信息进行加密；（3）都有较好的灵活性和扩展性。TACACS+具有更加可靠的传输和加密特性，更适合于安全控制。

|  |  |  |
| --- | --- | --- |
| 项目 | TACACS+ | RADIUS |
| 数据传输 | 通过TCP传输，网络传输更可靠 | 通过UDP传输，网络传输效率更高 |
| 加密方式 | 除了标准的TACACS+报文头，对报文全体全部进行加密 | 只是对认证报文中的密码字段进行加密 |
| 认证和授权 | 认证与授权分离，使得认证、授权服务可以在不同的安全服务器上实现。 | 认证与授权结合，不能分离 |
| 命令行授权 | 支持对设备上的配置命令进行授权使用，即用户可使用的命令行收到命令级别和AAA授权的双重限制，某一级别的用户输入的每一条命令都需要通过TACACS+服务器授权，如果授权通过，命令才可以被执行 | 不支持对设备上的配置命令进行授权使用。用户登录设备后可以使用的命令行由用户级别决定，用户只能使用级别等于或低于用户级别的命令行 |
| 应用场景 | 适用于安全控制 | 适用于计费 |

TACACS+除报文头之外，认证、授权和计费报文的格式均不同。

**TACACS+认证报文格式**：具有三种类型

* 认证开始报文：认证开始时，客户端向服务器发送认证开始报文，该报文中包括热证类型、用户名和一些认证数据。
* 认证持续报文：客户端接收到服务器回应的认证回应报文后，如果确认认证过程没有结束，则使用认证持续报文响应。
* 认证回应报文：服务器接收到客户端发送的认证开始报文或认证持续报文后，向客户端发送的唯一一种认证报文，用于向客户端反馈当前认证的状态。

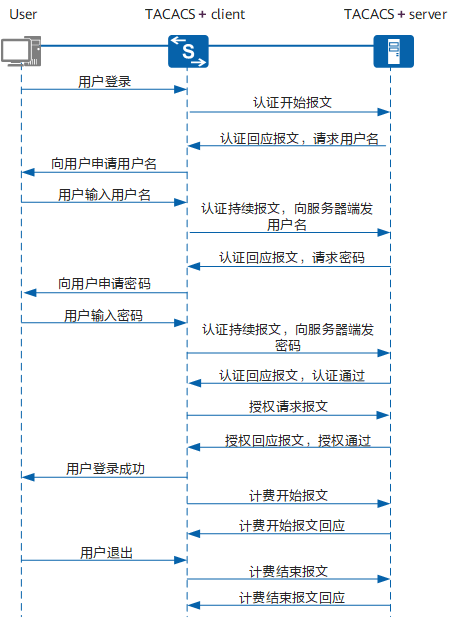
**TACACS+授权报文格式**：具有两种类型

* 授权请求报文：用户可以使用TACACS+认证而使用其他协议进行授权。如果需要通过TACACS+进行授权，则客户端向服务器发送授权请求报文，该报文中包括了授权所需的一切信息。
* 授权回应报文：服务器接收到授权请求报文后，向客户端发送授权回应报文，该报文中包括了授权的结果。

**TACACS+计费报文格式**：具有两种类型

* 计费请求报文：该报文中包括了计费所需的信息。
* 计费回应报文：服务器接收并成功记录计费请求报文后，需要回应一个计费响应报文。

**TACACS+认证、授权、计费流程**



1.Telnet用户请求登录设备。

2.TACACS+客户端收到请求之后，向TACACS+服务器发送认证开始报文。

3.TACACS+服务器发送认证回应报文，请求用户名。

4.TACACS+客户端收到回应报文后，向用户询问用户名。

5.用户输入用户名。

6.TACACS+客户端收到用户名后，向TACACS+服务器发送认证持续报文，其中包括了用户名。

7.TACACS+服务器发送认证回应报文，请求密码。

8.TACACS+客户端收到认证回应报文，向用户询问密码。

9.用户输入密码。

10.TACACS+客户端收到密码后，向TACACS+服务器发送认证持续报文，其中包括了密码信息。

11.TACACS+服务器发送认证回应报文，指示用户通过认证。

12.TACACS+客户端向TACACS+服务器发送授权请求报文。

13.TACACS+服务器发送授权回应报文，指示用户通过授权。

14.TACACS+客户端收到授权回应报文，向用户输出设备的配置界面。

15.TACACS+客户端向TACACS+服务器发送计费开始请求报文。

16.TACACS+服务器发送计费开始回应报文，指示计费开始请求报文已经收到。

17.用户请求断开连接。

18.TACACS+客户端向TACACS+服务器发送计费结束请求报文。

19.TACACS+服务器发送计费结束回应报文，指示计费结束请求报文已经收到。

【配置参数】

添加TACACS+服务器：至多添加4个

* TACACS+服务器地址：【text文本框】设置TACACS+服务器的地址，支持输入Hostname和IP地址（包括IPv4和IPv6），需要满足各类型的地址格式要求，否则需要报错提示。
* 端口：【text文本框】设置TCP端口号，取值为1-65535的整数，默认49。
* \*优先级：【text文本框】设置TACACS+服务器使用的顺序，取值为0-65535的整数。每个TACACS+服务器具有唯一性。
* 共享密钥：【text文本框】设置交换机和TACACS+服务器共享的加密密钥，最长64字符，允许输入的字符有字母、数字和特殊字符()<>,./’”;:[]{}\|=+-\_\*&^%$#@!~`（键盘半角全部支持）
* 超时时间 (秒)：【text文本框】设置交换机重发TACACS+报文等待TACACS+服务器应答的最长时间，取值为1-30的整数，默认5秒。

TACACS+服务器列表：

* 列表显示TACACS+服务器地址、端口、优先级、超时时间
* 支持编辑
* 支持删除单条/批量/全部TACACS+服务器

## AAA(FP1C)

【功能概述】

访问控制是用来控制哪些用户可以访问网络以及可以访问的网络资源。AAA是Authentication（认证）、Authorization（授权）和Accounting（计费）的简称，提供了在NAS（网络接入服务器）设备上配置访问控制的管理框架。

AAA作为网络安全的一种管理机制，以模块化的方式提供服务：（1）认证，确认访问网络的用户的身份，判断访问者是否为合法的网络用户；（2）授权，对不同用户赋予不同的权限，限制用户可以使用的服务；（3）计费，记录用户使用网路服务过程中的所有操作，包括使用的服务类型、起始时间、数据流量等，用于收集和记录用户对网络资源的使用情况，并可以实现针对事件、流量的计费需求，也对网络起到监视作用。

AAA采用客户端/服务器结构，AAA客户端运行在接入设备上，通常被称为NAS设备，负责验证用户身份与管理用户接入；AAA服务器是认证服务器、授权服务器和计费服务器的统称，负责集中管理用户信息。AAA可以通过多种协议来实现，目前设备支持基于RADIUS或TACACS+协议来实现AAA，在实际应用中，最常使用RADIUS协议。

【配置参数】

添加方法：

* \*名称：【text文本框】设置AAA的名称，最长64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示。名称具有唯一性
* 方法1：【下拉框】设置认证的首选方法，选项有{None| Local| Enable| RADIUS| TACACS+}。Empty表示认证方式为空，None表示不进行认证，Enable表示通过Enable认证后将用户权限提升至admin权限，Local表示使用本地用户认证，RADIUS表示使用RADIUS服务器认证，TACACS+表示使用TACACS+服务器认证。当且仅当选择None时，不使用备份方法。
* 方法2：作为方法1无法使用的备选方法，同方法1，选项再增加”Empty”
* 方法3：作为方法2无法使用的备选方法，同方法2
* 方法4：作为方法3无法使用的备选方法，同方法2

方法列表：

* 列表显示方法名称、使用的方法
* 存在一条默认的方法，名称为default，使用的方法1为Local
* 支持编辑
* 支持删除单条/批量/全部(除default方法)方法

登录认证：设置各种登录方式使用的身份认证方法

* Console：【下拉框】设置通过Console口登录交换机使用的认证方法，从已有的方法列表中选择，根据所选择的方法显示其对应的方法
* Telnet：【下拉框】设置通过Telnet口登录交换机使用的认证方法，从已有的方法列表中选择，根据所选择的方法显示其对应的方法
* SSH：【下拉框】设置通过SSH口登录交换机使用的认证方法，从已有的方法列表中选择，根据所选择的方法显示其对应的方法
* HTTPS：【下拉框】设置通过HTTPS口登录交换机使用的认证方法，从已有的方法列表中选择，根据所选择的方法显示其对应的方法

## 身份验证管理/802.1X(FP1C)

【功能概述】

NAC称为网络接入控制，通过对接入网络的客户端和用户的认证保证网络的安全，是一种端到端的安全技术。

NAC包括三种认证方式：802.1X认证、MAC认证和Portal认证（即Web认证）。

|  |  |  |  |
| --- | --- | --- | --- |
| 对比项 | 802.1X认证 | MAC认证 | Portal认证（Web认证） |
| 适合场景 | 新建网络、用户集中、信息安全要求严格的场景 | 打印机、传真机等哑终端接入认证的场景 | 用户分散、用户流动性大的场景 |
| 客户端需求 | 需要 | 不需要 | 不需要 |
| 优点 | 安全性高 | 无需安装客户端 | 部署灵活 |
| 缺点 | 部署不灵活 | 需登记MAC地址，管理复杂 | 安全性不高 |

NAC与AAA互相配合，共同完成接入认证功能。

* NAC：用于用户和接入设备之间的交互，NAC负责控制用户的接入方式，即用户采用802.1X，MAC或Portal中的哪一种方式接入，接入过程中的各类参数和定时器。确保合法用户和接入设备建立安全稳定的连接。
* AAA：用于接入设备与认证服务器之间的交互。AAA服务器通过对接入用户进行认证、授权和计费实现对接入用户访问权限的控制。

**802.1X认证**

802.1X协议是一种基于端口的网络接入控制协议。基于端口的网络接入控制是指在局域网接入设备的端口这一级验证用户身份并控制其访问权限。802.1X协议为二层协议，不需要达到三层，对接入设备的整体性能要求不高，可以有效降级建网成本；认证报文和数据报文通过逻辑接口分离，提高安全性。

802.1X系统为典型的客户端/服务器结构，包括三个实体：客户端、接入设备和认证服务器。

* 客户端：一般为一个用户终端设备，用户可以通过启动客户端软件发起802.1X认证。客户端必须支持局域网上的可扩展认证协议EAPoL。
* 接入设备：通常为支持802.1X协议的网络设备，它为客户端提供接入局域网的端口，该端口可以是物理端口，也可以是逻辑端口。
* 认证服务器：用于实现对用户进行认证、授权和计费，通常为RADIUS服务器。

802.1X认证协议：802.1X认证系统使用可扩展认证协议EAP来实现客户端、设备端和认证服务器之间的信息交互。EAP协议可以运行在各种底层，包括数据链路层和上层协议（如UDP、TCP等），而不需要IP地址。因此使用EAP协议的802.1X认证具有良好的灵活性。

* 在客户端与设备端之间，EAP协议报文使用EAPoL封装格式，直接承载于LAN环境中。
* 在设备端与认证服务器之间，用户可以根据客户端支持情况和网络安全要求来绝地采用的认证方式。
* EAP终结方式中，EAP报文在设备端终结并重新封装到RADIUS报文中，利用标准RADIUS协议完成认证、授权和计费。
* EAP中继方式中，EAP报文被直接封装到RADIUS报文（EAPoR）中，以便穿越复杂的网络到达认证服务器。

认证方式的选择：

* EAP中继方式的优点是设备端处理更简单，支持更多的认证方法，缺点则是认证服务器必须支持EAP，且处理能力要足够强。对于常用的EAP-TLS、EAP-TTLS、EAP-PEAP三种认证方式，EAP-TLS需要在客户端和服务器上加载证书，安全性最高，EAP-TTLS、EAP-PEAP需要在服务器上加载证书，但不需要在客户端加载证书，部署相对灵活，安全性较EAP-TLS低。
* EAP终结方式的优点是现有的RADIUS服务器基本均支持PAP和CHAP认证，无需升级服务器，但设备端的工作比较繁重，因为在这种认证方式中，设备端不仅要从来自客户端的EAP报文中提取客户端认证信息，还要通过标准的RADIUS协议对这些信息进行封装，且不能支持除MD5-Challenge之外的其它EAP认证方法。PAP与CHAP的主要区别是CHAP密码通过密文方式传输，而PAP密码通过明文的方式传输。因此PAP方式认证的安全性较低，实际应用通常采用CHAP方式认证。

802.1X授权：认证用于确认尝试接入网络的用户身份是否合法，而授权则用于指定身份合法的用户所能拥有的网络访问权限，即用户能够访问哪些资源。授权最基础也是最常使用的授权参数是VLAN、ACL和UCL组。

* VLAN：为了将受限的网络资源与未认证用户隔离，通常将受限的网络资源和未认证的用户划分到不同的VLAN。用户认证成功后，认证服务器将指定VLAN授权给用户。此时，设备会将用户所属的VLAN修改为授权的VLAN，授权的VLAN并不改变接口的配置。但是，授权的VLAN优先级高于用户配置的VLAN，即用户认证成功后生效的VLAN是授权的VLAN，用户配置的VLAN在用户下线后生效。
* ACL：用户认证成功后，认证服务器将指定ACL授权给用户，则设备会根据该ACL对用户报文进行控制。如果用户报文匹配到该ACL中动作为permit的规则，则允许其通过；若为deny，则将其丢弃。
* UCL组：用户控制列表UCL组是网络成员的集合。UCL组里面的成员，可以是PC、手机等网络终端设备，借助UCL组，管理员可以将具有相同网络访问策略的一类用户划分为同一个组，然后为其部署一组网络访问策略，满足该类别所有用户的网络访问需求。

Free-rule：用户认证成功之前，为满足用户基本的网络访问需求，需要用户认证成功前就能获取部分网络访问权限。可在free-rule模板中配置free-rule规则，满足用户的认证成功前的网络访问需求。用户的free-rule可以通过普通的free-rule定义，也可以通过ACL定义。普通的free-rule由IP地址、MAC地址、接口、VLAN等参数确定；通过ACL定义的free-rule由ACL规则确定。两种方式定义的free-rule都能够指定用户无需认证就可以访问的目的IP地址。除此之外，ACL定义的free-rule还能够指定用户认证成功前就可以访问的目的域名。

**MAC认证**

MAC认证，全称MAC地址认证，是一种基于接口和终端MAC地址对用户的访问权限进行控制的认证方法。

MAC认证系统为典型的客户端/服务器结构，包括三个实体：终端、接入设备和认证服务器。

* 终端：尝试接入网络的终端设备。
* 接入设备：是终端访问网络的网络控制点，是企业安全策略的实施者，负责按照客户网络制定的安全策略，实施相应的准入控制（允许、拒绝、隔离或限制）。
* 认证服务器：用于确认尝试接入网络的终端身份是否合法，还可以指定身份合法的终端所能拥有的网络访问权限。

用户名形式：终端进行MAC认证时使用的用户名和密码需要在接入设备上预先配置，有以下几种形式。默认情况下，终端进行MAC认证时使用的用户名和密码均为终端的MAC地址。

|  |  |  |
| --- | --- | --- |
| MAC认证时使用的用户名 | 密码 | 使用场景 |
| 终端的MAC地址 | 两种形式：   * 终端的MAC地址 * 指定的密码 | 客户端少量部署且MAC地址容易获取的场景，例如对少量接入网络的打印机进行认证 |
| 指定的用户名 | 指定的密码 | 由于同一个接口下可以存在多个终端，此时所有终端均使用指定的用户名和密码进行MAC认证，服务器仅需要配置一个账户即可满足所有终端的认证需求，适用于终端比较可信的网络环境 |
| DHCP选项，有三种形式：   * Circuit-id子选项 * Remote-id子选项 * Circuit-id子选项和remote-id子选项的组合 | 指定的密码 | 该场景下终端需通过DHCP方式获取IP地址，且需保证DHCP报文能够触发MAC认证 |

MAC认证流程：对于MAC认证用户密码的处理，有PAP和CHAP两种方式：

* PAP：设备将MAC地址、共享密钥、随机值依次排列顺序后，经过MD5算法进行HASH处理后封装在属性名“User-Password”中。
* CHAP：设备将CHAP ID、MAC地址、随机值依次排列顺序后，经过MD5算法进行HASH处理后封装在属性名“CHAP-Password”和“CHA-Challenge”中。

**Portal认证（Web认证）**

Portal认证也称为Web认证，一般将Portal认证网站称为门户网站。用户上网时，必须在门户网站进行认证。如果未认证成功，尽可以访问特定的网络资源；认证成功后，才可以访问其他网络资源。

Portal认证系统包括四个基本要素：客户端、接入设备、Portal服务器和认证服务器。

* 客户端：安装有运行HTTP/HTTPS协议的浏览器的主机。
* 接入设备：交换机、路由器等接入设备的统称，主要有三方面的作用
* 在认证之前，将认证网段内用户的所有HTTP/HTTPS请求都重定向到Portal服务器
* 在认证过程中，与Portal服务器、认证服务器交互，完成对用户身份认证、授权与计费的功能
* 在认证通过后，允许用户访问被管理员授权的网络资源
* Portal服务器：接收客户端认证请求的服务器系统，提供免费门户服务和认证界面，与接入设备交互客户端的认证信息。
* 认证服务器：与接入设备进行交互，完成对用户的认证、授权与计费。

Portal认证协议：包括Portal接入协议和Portal认证协议。

* Portal接入协议：HTTP/HTTPS协议，描述了客户端和Portal服务器之间的协议交互。客户端通过HTTP/HTTPS协议依次向Portal服务器发起连接请求和Portal认证请求。
* Portal认证协议：支持两种认证协议：
* Portal协议：描述了Portal服务器和接入设备之间的协议交互，可以用来传递用户名和密码等参数。收到客户端的Portal认证请求后，Portal服务器通过Portal协议向接入设备发起Portal认证请求（携带用户名和密码）。
* HTTP/HTTPS协议：描述了客户端和接入设备之间的协议交互，可以用来传递用户名和密码等参数。收到客户端的Portal认证请求后，Portal服务器通过HTTP/HTTPS协议通知客户端向接入设备发起Portal认证请求，然后客户端通过HTTP/HTTPS协议向接入设备发起Portal认证请求（携带用户名和密码）。

暂仅支持802.1X认证，基于MAC和基于Web (FP2)实现。

【配置参数】

**（一）802.1X认证**

**全局配置：**

* 802.1X认证：【开关】设置是否开启设备的802.1X认证功能，默认关闭。
* Guest VLAN：【开关】设置是否启用Guest VLAN功能，默认关闭。开启后，需设置Guest VLAN ID，其中的用户可以访问指定的网络资源。
* Guest VLAN ID：【下拉框】从已有的VLAN列表中选择，默认的管理VLAN 1不能设置。

端口模式设置：

* 端口：选择设置认证模式的交换机接口，包括电口和光口。可多选
* 802.1X认证：【开关】设置端口802.1X认证功能是否启用，默认关闭。
* 用户认证模式：【单选】设置端口进行认证的主机模式，选项有{基于MAC|基于端口|单用户}，默认基于MAC。选择“基于MAC”表示允许多个用户进行认证，且用户之间互不影响；选择“基于端口”表示允许多个用户认证，且只要一个用户认证通过，其余用户免认证；选择“单用户”表示只允许一个用户认证通过。
* 方法：【可多选】设置认证方法，选项有{RADIUS|Local}，默认RADIUS。
* Guest VLAN：设置是否开启端口的Guest VLAN功能，默认关闭。
* VLAN分配模式：【下拉框】设置端口上VLAN的分配模式，选项有{禁用|拒绝|静态}，默认静态。

端口模式列表：

* 列表显示端口、认证类型、用户认证模式、方法、Guest VLAN、VLAN分配模式
* 支持编辑

**端口设置：**

* 端口：选择需要设置认证的交换机接口，包括电口和光口。可多选
* 端口控制：【下拉框】设置端口控制模式，选项有{禁用| 强制认证| 强制不认证| 自动}，默认禁用。
* 重认证：【开关】设置是否对端口连接设备开启重认证功能，默认关闭。
* 最大用户数：【text文本框】设置端口允许接入的802.1X认证的最大用户数，取值为1-256的整数，默认256。
* 定时器：设置端口上认证时的各类定时器。
* 重认证时间 (秒)：【text文本框】设置重新认证的时间间隔，即当未受到客户端响应，设备重发EAP-Request/MD5-Challenge报文的时间。取值为300-2147483647的整数，默认3600秒。
* 非活跃时间间隔 (秒)：【text文本框】设置认证成功后，端口如果没有收到该终端的任何流量，就开始非活跃的计时时间间隔，取值为60-65535的整数，默认60秒。
* 静默时间 (秒)：【text文本框】设置当用户在一段时间内认证失败次数达到上限时，交换机将用户静默的时长，取值为0-65535秒，默认60秒，0表示不对用户进行静默处理。
* 超时时间 (秒)：【text文本框】设置端口802.1X认证的认证超时时间，取值为1-65535的整数，默认30秒。
* 请求超时 (秒)：【text文本框】设置端口802.1X认证请求超时的时间，取值为1-65535的整数，默认30秒。
* 服务器超时 (秒)：【text文本框】设置802.1X认证服务器超时的时间，取值为1-65535的整数，默认30秒。
* 最大请求数：【text文本框】设置端口802.1X认证时，如果在一定时间内没有收到客户端的响应，再次向客户端发起请求的最大次数，取值为1-10的整数，默认2。
* ~~最大登录次数：【text文本框】设置基于Web认证的客户端最大登录次数，取值为0或3-10 的整数，默认3次，0表示不限制登录次数。~~

端口列表：

* 列表显示端口、端口控制、重认证、最大用户数、重认证定时器、非活跃定时器、静默定时器、802.1X认证的超时时间、请求超时时间、服务器超时时间、最大请求数~~、基于Web认证的最大登录次数~~
* 支持编辑

**~~（二）基于MAC的本地用户：~~**(FP2)

~~添加：~~

* ~~MAC地址：【text文本框】输入终端设备的MAC地址，输入格式为HH:HH:HH:HH:HH:HH(其中，H为1-2位的十六进制数)，例如00:10:DC:28:A4:E9。~~
* ~~端口控制：【下拉框】设置终端用户在端口上进行认证的控制模式，选项有{强制认证|强制不认证}，默认强制认证。~~
* ~~VLAN：【text文本框】设置该终端设备在认证前允许访问的VLAN网络资源，取值为1-4094的整数，默认1。~~
* ~~重认证时间 (秒)：【text文本框】设置该终端设备重新认证的时间，取值为300-2147483647的整数，默认3600秒。~~
* ~~非活跃时间 (秒)：【text文本框】设置该终端设备的非活跃时间，取值为60-65535的整数，默认60秒。~~

~~基于MAC的本地用户列表：~~

* ~~列表显示MAC地址、控制模式、VLAN、重认证时间、非活跃时间~~
* ~~支持编辑~~
* ~~支持删除单个/批量/全部基于MAC的本地用户~~

**~~基于Web的本地用户认证：~~**(FP2)

~~添加：~~

* ~~\*用户名：【text文本框】设置基于Web认证的用户名，最长32字符，允许输入的字符有字母、数字和特殊字符.\_@~~
* ~~\*密码：【text文本框，加密】设置密码。允许输入最长32字符，允许输入的字符由数字0-9、英文字符a-z/A-Z和特殊字符()<>,./’”;:[]{}\|=+-\_\*&^%$#@!~`（键盘半角全部支持）~~
* ~~\*确认密码：【text文本框，加密】重复上述密码，若不一致则提示“密码不一致，请重新输入”~~
* ~~VLAN：【text文本框】设置用户在认证前允许访问的VLAN网络资源，取值为1-4094的整数，默认1。~~
* ~~重认证时间 (秒)：【text文本框】设置用户重新认证的时间，取值为300-2147483647的整数，默认3600秒。~~
* ~~非活跃时间 (秒)：【text文本框】设置用户的非活跃时间，取值为60-65535的整数，默认60秒。~~

~~基于Web的本地用户列表：~~

* ~~列表显示用户名、VLAN、重认证时间、非活跃时间~~
* ~~支持编辑~~
* ~~支持删除单个/批量/全部用户~~

**（四）认证会话：**

认证会话列表显示交换机上的802.1X认证会话信息。

* 列表显示会话ID、端口、MAC地址、认证状态、配置的信息包括VLAN、会话时间、非活跃时间和静默时间、授权的信息包括VLAN、重认证时间和非活跃时间
* 支持刷新
* 支持清空认证会话列表

## DHCP Snooping(FP1C)

【功能概述】

DHCP Snooping作为DHCP的一种安全特性，用于保证DHCP客户端从合法的DHCP服务器获取IP地址，并记录DHCP客户端IP地址与MAC地址等参数的对应关系，防止网络上针对DHCP攻击。

为了保证网络通信业务的安全性，引入DHCP Snooping技术，在DHCP Client和DHCP Server之间建立一道防火墙，以抵御网络中针对DHCP的各种攻击。

基本原理：

DHCP Snooping分为DHCPv4 Snooping和DHCPv6 Snooping，两者实现原理相似。使能DHCP Snooping的设备将用户（DHCP客户端）的DHCP请求报文通过信任接口发送给合法的DHCP服务器。设备根据DHCP服务器返回的DHCP ACK报文信息生成DHCP Snooping绑定表。后续，设备再从使能DHCP Snooping的接口接收用户发来的DHCP报文时，会进行匹配检查，能够有效防范非法用户的攻击。

DHCP Snooping信任功能：保证客户端从合法的服务器获取IP地址。网络中如果存在私自架设的DHCP Server仿冒者，则可能导致DHCP客户端获取错误的IP地址和网络配置参数，无法正常通信。DHCP Snooping信任功能可以控制DHCP服务器应答报文的来源，以防止网络中可能存在的DHCP Server仿冒者为DHCP客户端分配IP地址及其他配置信息。DHCP Snooping信任功能将接口分为信任接口和非信任接口：

* 信任接口正常接收DHCP服务器响应的DHCP ACK、DHCP NAK和DHCP Offer报文
* 非信任接口在接收到DHCP服务器响应的DHCP ACK、DHCP NAK和DHCP Offer报文后，丢弃该报文

DHCP绑定表记录DHCP客户端IP地址与MAC地址等参数的对应关系。

DHCP Snooping支持Option82功能，其记录了DHCP Client的位置信息。通过在DHCP请求报文中添加Option 82选项，将DHCP Client的精确物理位置信息传递给DHCP Server，从而使得DHCP Server能够为主机分配合适的IP地址和其他配置信息，实现对客户端的安全控制。

Option82包含两个常用子选项Circuit ID和Remote ID，其中Circuit ID子选项主要用来标识客户端所在的VLAN、接口等信息，Remote ID子选项主要用来标识客户端接入的设备，一般为设备的MAC地址。Option82选项携带的用户位置信息与DHCP Snooping绑定表记录的用户参数是两个相互独立的概念，没有任何关联。Option82选项携带的用户位置信息是在DHCP用户申请IP地址时（此时用户还未分配到IP地址），由设备添加到DHCP请求报文中。DHCP Snooping绑定表是在设备收到DHCP Server回应的DHCP Ack报文时（此时已为用户分配了IP地址），设备根据DHCP Ack报文信息自动生成。

设备作为DHCP Relay或设备在二层网络作为接入设备并使能DHCP Snooping功能时均可支持Option82功能。使能设备的Option82功能有Insert和Rebuild两种方式，使能方式不同设备对DHCP请求报文的处理也不同。

* Insert方式：当设备收到DHCP请求报文时，若该报文中没有Option82选项，则插入Option82选项；若该报文中含有Option82选项，则判断Option82选项中是否包含remote-id，如果包含，则保持Option82选项不变，如果不包含，则插入remote-id。
* Rebuild方式：当设备收到DHCP请求报文时，若该报文中没有Option82选项，则插入Option82选项；若该报文中含有Option82选项，则删除该Option82选项并插入管理员自己在设备上配置的Option82选项。

对于Insert和Rebuild两种方式，当设备接收到DHCP服务器的响应报文时，处理方式一致。

* DHCP响应报文中有Option82选项：
* 如果设备收到的DHCP请求报文中没有Option82选项，则设备将删除DHCP响应报文中的Option82选项，之后转发给DHCP Client。
* 如果设备收到的DHCP请求报文中有Option82选项，则设备将DHCP响应报文中的Option82选项格式还原为DHCP请求报文中的Option82选项，之后转发给DHCP Client。
* DHCP响应报文不含有Option82选项：直接转发。

暂仅支持DHCPv4 Snooping。

【配置参数】

* DHCP Snooping：【开关】设置是否开启交换机的DHCP Snooping功能，默认关闭。
* VLAN：选择需要使能DHCP Snooping的VLAN，从已有VLAN列表中选择，可多选。默认选择VLAN 1。

Option 82设置：

* Remote ID：【text文本框】设置Remote ID，默认使用交换机MAC地址，支持用户自定义，最长输入63字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示

Circuit ID：

* 端口：【单选】选择交换机接口，可以选择的接口有电口、光口和聚合接口
* VLAN：【单选】从已有的VLAN中选择
* Circuit ID：【text文本框】设置Circuit ID，最长输入63字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示

支持添加多条，相同的VLAN和Circuit ID可以添加到不同端口中，但不允许在同一端口中重复添加。

Circuit ID列表：

* 列表显示端口、VLAN、Circuit ID
* 支持编辑，只能逐条编辑
* 支持删除单条/批量/全部Circuit ID

端口设置：

* 端口：选择需要配置的交换机接口，包括电口、光口和聚合接口，可多选。
* 信任模式：【开关】设置端口的信任属性，默认关闭，即不信任。
* Chaddr校验：【开关】设置对上报的DHCP报文帧头源MAC地址与Chaddr字段是否相同进行校验，默认关闭。
* 速率 (pps)：【text文本框】当且仅当信任模式关闭时，限速功能生效。设置端口DHCP报文处理单元的速率，取值为0-300，0为不限速，默认为0。设置完成后，若实际超过最大允许速率，端口将会被error-down。
* Option 82：【开关】设置是否在DHCP报文中添加Option 82，默认关闭。
* Option 82模式：【下拉框】设置在DHCP报文中添加Option 82的策略，选项有{保留|丢弃|替换}，默认丢弃。选择“保留”即表示若报文中带有Option 82，则保持该报文中的Option 82不变并进行转发；选择“丢弃”即表示若报文中带有Option 82，则直接丢弃该报文；选择“替换”即表示若报文中带有Option 82， 则替换报文中原有的Option 82，并进行转发。

端口列表：

* 列表显示端口、信任模式、Chaddr校验、速率
* 支持编辑

数据统计表：

* 列表显示端口、转发报文数、Chaddr校验丢弃报文数、非信任端口丢弃报文数、带Option 82的非信任端口丢弃报文数、无效丢弃的报文数
* 支持清除每个端口的统计数据，也支持清除全部统计数据

## DHCPv6 Snooping(FP2)

【功能概述】

DHCPv6 Snooping是DHCPv6的一种安全特性，用来保证客户端从合法的服务器获取IPv6地址或IPv6前缀，并可以记录DHCPv6 Client IPv6地址或IPv6前缀和MAC地址的对应关系。

**DHCPv6 Snooping信任功能：**保证客户端从合法的服务器获取IPv6地址或IPv6前缀。网络中如果存在私自架设的非法DHCPv6 Server，则可能导致DHCPv6客户端获取错误的IPv6地址和网络配置参数，从而无法正常通信。为了使DHCPv6客户端能通过合法的DHCPv6服务器获取IPv6地址，DHCPv6 Snooping安全机制允许将端口设置为信任端口和非信任端口。

* 信任端口正常转发接收到的DHCPv6报文
* 非信任端口接收到DHCPv6 Server发送的应答报文后，丢弃该报文

**DHCPv6 Snooping绑定表：**通过监听DHCPv6 Server与DHCPv6 Client之间的DHCPv6报文，建立和维护一张记录DHCPv6 Client信息的DHCPv6 Snooping绑定表，该表包含用户MAC地址、IPv6地址、租期、VLAN ID、接口等信息，以此实现对用户IPv6地址使用情况的记录和监控。

**DHCPv6 Snooping前缀记录：**通过监听DHCPv6报文中的前缀和收到DHCPv6请求报文的端口信息，记录DHCPv6 Snooping前缀信息，包含客户端获取到的IPv6前缀、租约信息、与DHCPv6 Client连接的端口及该端口所属的VLAN等信息。，一次实现对用户的IPv6前缀使用情况的记录和监控。

DHCPv6 Snooping支持Option 18和37功能，与DHCP Snooping的Option 18 功能类似，记录了DHCPv6 Client的位置信息。其中，Option 18记录了DHCPv6 Client的接口信息，Option 37记录了DHCPv6 Client的MAC地址信息。通过在DHCPv6请求报文中添加Option 18或37，将DHCPv6 Client的位置信息发送给DHCPv6 Server，从而使得DHCPv6 Server能够为其分配合适的IPv6地址和其他配置信息，实现对客户端的安全控制。

* Option 18：Interface ID。其默认填充内容是接收到DHCPv6 Client请求报文的端口所属VLAN ID及端口号；扩展填充内容是自定义的字符串。在同一个网络域中，有且仅能使用其中一种。
* Option 37：Remote ID。其默认填充内容是接收到DHCPv6 Client请求报文的DHCPv6中继设备的桥MAC地址；扩展填充内容是自定义的字符串。在同一个网络域中，有且仅能使用其中一种。

使能设备的Option 18和37功能方式与Option18相同，有Insert和Rebuild两种方式，使能方式不同设备对DHCPv6请求报文的处理也不同。以Option 37为例进行说明。

* Insert方式：当设备收到DHCPv6请求报文时，若该报文中没有Option 37选项，则插入Option 37选项；若该报文中含有Option 37选项，则判断Option 37选项中是否包含remote-id，如果包含，则保持Option 37选项不变，如果不包含，则插入remote-id。
* Rebuild方式：当设备收到DHCPv6请求报文时，若该报文中没有Option 37选项，则插入Option 37选项；若该报文中含有Option 37选项，则删除该Option 37选项并插入管理员自己在设备上配置的Option 37选项。

对于Insert和Rebuild两种方式，当设备接收到DHCP服务器的响应报文时，处理方式一致。

* DHCPv6响应报文中有Option 37选项：
* 如果设备收到的DHCPv6请求报文中没有Option 37选项，则设备将删除DHCPv6响应报文中的Option 37选项，之后转发给DHCPv6 Client。
* 如果设备收到的DHCPv6请求报文中有Option 37选项，则设备将DHCPv6响应报文中的Option 37选项格式还原为DHCPv6请求报文中的Option 37选项，之后转发给DHCPv6 Client。
* DHCPv6响应报文不含有Option 37选项：直接转发。

配置限制：设备只有位于DHCPv6客户端与DHCPv6 Server之间，或DHCPv6客户端与DHCP Relay之间时，DHCPv6 Snooping功能配置后才能正常工作。

GWN78XX暂不支持DHCPv6 Snooping与IPv6动态前缀绑定表，等DHCPv6 Server支持后再支持。

【配置参数】

全局设置：

* DHCPv6 Snooping：【开关】设置是否开启交换机的DHCPv6 Snooping功能，默认关闭。
* VLAN：选择需要使能DHCPv6 Snooping的VLAN，从已有VLAN列表中选择，可多选。

Option 18设置：

* 端口：【单选】选择交换机接口，可以选择的接口有电口、光口和聚合接口
* 填充格式：【单选】设置Option 18内容的填充格式，选项有{标准格式 | 扩展格式}，默认标准格式。
* 接口ID：【下拉框，单选】当填充格式为“标准格式”时，输入VLAN ID，从全局配置的VLAN中选择；【text文本框】当填充格式为“扩展格式”时，用户自定义输入，输入长度为3-63字节

列表：

* 列表显示端口、接口ID
* 支持编辑，只能逐条编辑
* 支持删除单条/批量/全部接口 ID

Option 37设置：

* Remote ID：【text文本框】设置Remote ID，默认使用交换机MAC地址，支持用户自定义，最长输入63字符，可以输入的字符有数字、字母和特殊字符./:-{}

端口设置：

* 端口：选择需要配置的交换机接口，包括电口、光口和聚合接口，可多选。
* 信任模式：【开关】设置端口的信任属性，默认关闭，即不信任。
* 速率 (pps)：【text文本框】当且仅当信任模式关闭时，限速功能生效。设置端口DHCPv6报文处理单元的速率，取值为0-300，0为不限速，默认为0。设置完成后，若实际超过最大允许速率，端口将会被errdisble。
* Option 18：【开关】设置是否在DHCPv6报文中添加Option 18，默认关闭。
* Option 18模式：【单选】设置在DHCPv6报文中添加Option 18的策略，选项有{保留|丢弃|替换}，默认丢弃。选择“保留”即表示若报文中带有Option 18，则保持该报文中的Option 18不变并进行转发；选择“丢弃”即表示若报文中带有Option 18，则直接丢弃该报文；选择“替换”即表示若报文中带有Option 18， 则替换报文中原有的Option 18，并进行转发。
* Option 37：【开关】设置是否在DHCPv6报文中添加Option 37，默认关闭。
* Option 37模式：【单选】设置在DHCPv6报文中添加Option 37的策略，选项有{保留|丢弃|替换}，默认丢弃。选择“保留”即表示若报文中带有Option 37，则保持该报文中的Option 37不变并进行转发；选择“丢弃”即表示若报文中带有Option 37，则直接丢弃该报文；选择“替换”即表示若报文中带有Option 37， 则替换报文中原有的Option 37，并进行转发。

列表：

* 列表显示端口、信任模式、速率、Option 18及其模式、Option 27及其模式
* 支持编辑

数据统计表：

* 列表显示端口、转发报文数、非信任端口丢弃报文数、带Option 37的非信任端口丢弃报文数、带Option 18的非信任端口丢弃报文数、无效丢弃的报文数
* 支持清除每个端口的统计数据，也支持清除全部统计数据

# PoE(FP1B)

仅PoE型号支持，GWN7801P/02P/03P/06P/11P/12P/21P/23P支持PoE/PoE+，GWN7813P/16P支持PoE/PoE+/PoE++(1-8)

PoE++功能(FP1D)

【功能概述】

以太网供电PoE是指通过以太网网络进行供电，也被称为基于局域网的供电系统PoL或有源以太网。

通常，接入点的终端设备需要使用直流供电，但由于布线不足，而这些设备又需要统一的供电管理。这时，交换机接口提供供电功能，正好可以解决以上问题，并能实现端口PoE供电的精准控制。

**PoE供电过程：**

（1）检测受电设备PD：PSE在端口周期性输出电流受限的小电压，用以检测PD设备的存在。

（2）供电能力协商：PSE对PD进行分类，并协商供电功率。

（3）开始供电：在启动期内，PSE设备开始从低电压向PD设备供电，直至提供48V的直流电压。

（4）正常供电：电压达到48V后，PSE为PD设备提供稳定可靠48V的直流电，PD设备功率消耗不超过PSE最大输出功率。

（5）断电：供电过程中，PSE会不断监测PD电流输入，当PD电流消耗下降至最低值以下，或电流激增，PSE会断开电源，并重复检测过程。

**PoE的供电管理模式：**

当PSE下挂的PD越来越多时，PoE电源无法支撑给所有的PD供电，此时需要PSE对供电行为进行管理。根据供电方式的不同，将供电管理模式分为：自动模式和强制模式。

* 自动模式：PSE根据优先级，自动给PD设备上下电。用户根据接口下的PD重要性给各接口设置供电优先级，分别为Critical/最高、High/次高、Low/最低。在PSE对外供电接近满负荷的情况下，优先对优先级为Critical的接口连接的PD设备进行供电，次之为优先级为High的接口连接的PD设备供电。端口优先级相同的情况下，按照PD设备上电时间先后进行供电。
* 强制模式：跳过协商流程，直接给PD设备供电。强制模式根据设置的优先级和功率限值进行功率管理；但是功率限制无效，设置功率限值只作为功率管理参考值为该端口预留功率；在总功率需求超过供电功率时,根据优先级对端口供电。

预留功率的应用场景：

设备会根据每个接口实际消耗的功率动态地给每个接口分配功率，每个PD设备在运行过程中，其功率消耗会不断变化，系统会定期计算当前接入的所有的PD所需总功率是否超过可用PoE功率的上限，如果超过，系统会自动给优先级比较低的接口上的PD设备断电，保证其他设备的正常运行。

但是有时候会出现突发性的功率消耗激增，系统剩余可用功率无法支撑这种需求激增，而系统还未来得及计算出消耗总功率超限，从而作出断开优先级较低的接口供电的处理时，PoE电源会因为过载而导致过载保护断电，所有的PD设备下电。

通过poe power-reserved命令合理设置系统预留功率，在发生突发功率需求激增的情况下，系统预留功率可以支撑突发需求，保证系统有时间通过给优先级低的接口上的设备下电的方法保证其他设备的稳定运行

PoE&PoE+&PoE++：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **PoE** | **PoE+** | **PoE++** | |
| IEEE标准 | IEEE 802.3af | IEEE 802.3at | IEEE 802.3bt | |
| PoE类型 | 类型1 | 类型2 | 类型3 | 类型4(不支持) |
| 交换机端口电源 | | | | |
| 最大限度每个端口功率 | 15.4W | 30W | 60W | 90W |
| 端口电压范围 | 44-57V | 44-57V | 44-57V | 52-57V |
| 受电设备电源 | | | | |
| 最大限度设备电源 | 12.95W | 25.5W | 51W | 71.3W |
| 到设备的电压范围 | 36-57V | 42.5-57V | 39.9-57V | 39.9-57V |

GWN780XP和GWN7811P/12P的PoE模块每个芯片8个接口。按照顺序，芯片1对应接口1-8，芯片2对应接口9-16，以此类推...

GWN7813P/16P的PoE模块每个芯片4个端口。按照顺序，芯片1对应端口1-4，芯片2对应端口5-8，以此类推…

各型号设备PoE供电情况如下：

* GWN7801P/11P，支持802.3af/at，总供电功率120W
* GWN7802P/12P，支持802.3af/at，总供电功率240W
* GWN7803P，支持802.3af/at，总供电功率360W
* GWN7813P，支持802.3af/at/bt(1-8)，总供电功率360W
* GWN7806P，支持802.3af/at，总供电功率400W
* GWN7816P，支持802.3af/at/bt(1-8)，总供电功率[TBD]
* GWN7821P，支持802.3af/at，总供电功率[TBD]
* GWN7823P，支持802.3af/at，总供电功率[TBD]

【配置参数】

【GWN7813P】电源信息：

无论有无接入RPS电源，显示电源信息，具体如下：

* 内置电源/RPS电源的使用状态：{未使用|故障|使用中|过压|欠压|未接入(RPS电源独有)}
* 内置电源/RPS电源的LED指示灯状态

全局配置：

* <PoE重启>按钮：点击后，需二次确认是否进行PoE模块功能软重启。
* PoE预留功率 (W)：【text文本框】设置总的PoE供电的预留功率，取值为0-360W(GWN7803P/13P)，默认20W。GWN7801P/11P为0-120W，GWN7802P/12P为0-240W。

注：【GWN7813P】当内置电源故障，改用RPS电源为①系统 或 ②PSE 或 ③系统和PSE供电时，供电功率从360W降至240W，PoE预留功率取值范围调整为0-240W。

全局PoE电源信息，主要包括：

* PoE接口个数
* PoE总供电功率，单位W
* PoE预留功率，单位W
* 已配置功率，单位W
* PoE消耗功率，单位mW
* PoE供电支持类型，有802.3af/802.3at
* 芯片相关信息，包括工作状态(On/Off)、供电电压。不同型号芯片个数不一，由底层上报显示

接口PoE配置：

* 接口：选择需要配置的支持PoE供电的交换机接口。可多选。
* 供电标准：【单选】设置接口PoE供电标准，选项有{802.3af | 802.3at | 802.3bt}，默认802.3at。

注：在802.3af标准下，Class4能够正常上电，但实际供电功率限制在af标准（Class3）限制以下。802.3bt标准，仅GWN7813P/16P的端口1-8支持，当选择不局限于此类端口时，802.3bt需置灰。

* 供电模式：【下拉框】设置接口电源供电管理方式，选项有{自动|关闭|强制}，默认自动。当选择“强制”时，支持配置自定义限值。
* 功率限值模式：【下拉框】当供电模式选择“自动”时，支持配置提供给接入设备的功率限值，选项有{Class模式| User模式}，默认Class模式，即根据接入设备分级自动配置功率限值，功率对照表见下表：

|  |  |
| --- | --- |
| 分级 | PD可用功率 |
| Class 0 | 15W |
| Class 1 | 4W |
| Class 2 | 7W |
| Class 3 | 15W |
| Class 4 | 30W |
| Class 5 | 45W |
| Class 6 | 60W |

当选择“User模式”时，由用户自定义限值。

* \*自定义限值 (W)：【text文本框】设置接口给PD设备配置的功率限值。当供电模式为802.3bt时，取值为1-60的整数，默认15W；当供电模式为802.3at时，取值为1-30的整数，默认15W；当供电模式为802.3af时，取值为1-15的整数，默认15W。
* 供电优先级：【下拉框】设置接口的PoE供电优先级，选项有{最高| 次高| 最低 }，默认最低。优先级管理策略：

（1）如果是由于正在被供电的某个PD功率需求增大造成PSE功率过载，则停止对该PD供电。

（2）如果PSE功率过载，比较各对应PoE接口的优先级来判断对各PD的断电或供电情况，优先级高的优先得到供电。相同优先级端口按上电时间计算优先级，上电越晚优先级越低；相同优先级端口且上电时间相同时(交换机软重启后)，接口编号小的优先级更高。

（3）未被供电且对应接口优先级相同的多个PD，接口编号小的优先得到供电。

（4）交换机软重启后，未断电的已供电设备的上电时间清除，所有已供电设备赋予相同上电时间。

* 断电时间(FP1D)：【下拉框】当且仅当供电模式选择“自动”或“强制”时支持配置。设置接口的断电时间，选项为已存在的时间策略，支持弹窗新建时间策略，具体配置详见[*系统→时间策略*](#_时间策略/Time_Policy)。在所选时间段内，PD设备无法上电。
* 供电告警：【开关】设置是否开启接口供电告警功能，默认关闭。开启后，需要设置功率消耗阈值。
* 功率消耗阈值 (mw)：【text文本框】设置接口供电功率消耗产生告警的阈值，取值范围为1-99，默认90。

注：开启LLDP端口的Power via MDI TLV或LLDP-MED端口的PoE-PSE TLV，可开启相应端口的LLDP协商供电功能，将会根据接收到的相应TLV调整端口供电优先级和功率限值。

接口PoE列表：

* 列表显示接口名称、供电标准、供电模式、供电优先级、断电时间、最大供电功率，以及当前接口上PD(受电设备)的相关信息：
* 当前电流，单位mA
* 当前功率，单位mW
* PD等级：系统自动根据PD设备的最大功率给PD的分类，共有0-4级。当接口下没有接PD时，显示“--”
* 温度，单位℃
* 供电状态(供电中|未供电)

# 维护

## 升级/Upgrade

GWN78XX交换机支持手动上传固件升级、固件服务器即时升级、预约升级。



新增当前版本号、新固件版本等信息，详见[[*4.5新固件升级提示*](#_新固件升级提示(FP1D))]模块。

手动上传升级

通过Grandstream官网或技术支持等渠道获取升级文件，在本地上传对交换机进行升级。

* 上传固件文件：点击<上传>按钮，将从当前管理设备上获取交换机升级文件。

固件上传过程中，不允许操作页面，直到上传成功，且需提示[固件上传中，请稍候…]。

上传成功后，进行固件的鉴权，判断是否是当前设备的固件，否则需要根据[安装失败，固件签名错误]。

固件鉴权通过后，判断固件版本。

* 若版本相同，则报错[安装失败，版本一致，无需升级]。
* 若版本不一致，则系统弹窗提示：

[固件上传成功，是否立即升级？

☑保存配置修改

取消 升级]

点击<取消>按钮不进行升级，点击<升级>按钮进入升级流程。

由于升级后设备自动重启，如有配置数据修改需要保存，则需要勾选“保存配置修改”。

网络升级

网络升级有2种方式：

方式一：手动配置网络升级的固件服务器设置。

通过配置升级方式、固件服务器路径、服务器用户名与密码，完成服务器升级的基本设置。

【配置参数】

* 固件升级方式：选择升级的固件服务器类型，选项有{FTP/FTPS(FP2) | TFTP｜HTTP｜HTTPS}，默认HTTP。
* 固件服务器路径：设置固件服务器的IP地址或URL，默认fm.grandstream.com/gs。
* HTTP/HTTPS用户名：输入HTTP/HTTPS服务器设置的用户名，若无则可为空
* HTTP/HTTPS密码：输入HTTP/HTTPS服务器设置的密码，若无则可为空

方式二：利用DHCP Option获取DHCP Server上的升级地址进行固件下载升级。

Smart Install功能，能够给用户提供零接触部署设备的能力。设备利用DHCP Option自动获取配置文件进行升级，非常适合对交换机进行二次升级功能，解决了出厂前设备的批量升级问题。

DHCP Option选项支持重写固件服务器地址。当使用DHCP Option提供的固件服务器地址下载失败时，支持使用配置的固件服务器地址重新请求固件。

【配置参数】

* 启动DHCP选项43、160和66设定服务器：选项有{否｜是｜优先使用，失败时回退}，默认为是。
* 设置为“否”，则默认使用配置的服务器路径请求固件信息
* 设置为“是”，则使用DHCP选项下发的服务器路径请求固件信息
* 若设置为“优先使用，失败时回退”，则优先使用DHCP选项下发的服务器路径请求固件信息。当请求失败时，则可以转而使用配置的服务器路径请求固件信息。

交换机支持启动时自动检测升级，支持跳过固件检查。(FP1D)

【配置参数】

* 启动时检查/下载新固件：默认开启，即每次设备启动，自动进行固件检测。若检测到有新固件，则下载升级。关闭后，每次启动跳过固件检查。

网络升级根据升级时间，分为两种：

1. 即时升级

当上述服务器升级设置完成后，支持交换机检测更新。

【配置参数】

* <升级>按钮：点击此按钮，弹出确认”确认立即升级？“，点击”OK“后，将会去向固件服务器地址请求固件。检测需要一定时间，界面需Loading提示。
* 若检测无新固件，则提示“已是最新版本，无需升级”。
* 若存在新版本固件，则提示“检测到新固件(版本号)，确定下载升级固件？ ☑保存配置修改”，提供<升级>按钮，点击以后进行新固件的下载，需显示固件下载进度，下载完成后自动进入升级界面。
* 若存在网络等问题，则提示“检测固件版本失败”，支持重新检测。

交换机升级流程：

交换机进入升级，界面需显示升级进度。此时，界面禁止操作。当升级完成后，设备需重启，此时界面需自动退出，并告知用户：

[设备升级成功，重启中…

您可以在重启后X分钟左右点击下方的链接，重新登录]，并提供<登录>按钮，跳转至登录界面。

注：1.升级过程中请勿断开交换机电源。

2.升级和重启过程中，下挂设备均无法连接到交换机。

升级过程中，若存在固件问题导致升级失败，则升级进度条暂停，提示[系统升级出错，错误码：XXXX]，告知具体错误原因，例如：固件签名出错、固件与硬件不匹配、固件不兼容、固件损坏、读取固件出错等。

1. 预约升级(FP1D)

支持预约时间进行升级，以避免网络瘫痪。在预约时间段内，随机进行固件检测下载。

【配置参数】

* 预约升级：设置是否开启预约升级，默认关闭。一旦开启，需要选择时间策略。
* 升级时间策略：选项有创建的时间策略。若未有时间策略可供选择，支持弹窗新建时间策略，具体配置详见***系统→时间策略***设置。
  + - 1. Secure Boot防降级(FP2)

为防止恶意软件，需支持Secure Boot。

* + - 1. 随机升级

后期交换机上云时，部署升级容易造成固件服务器压力，故交换机需支持随机升级功能。

## 诊断/Diagnostics(FP1B)

### 日志/Log

【功能概述】

日志等级（从高到低）：Emergency、Alert、Critical、Error、Warning、Notice、Information、Debug。

交换机的日志文件存储在2个地方，一部分存在RAM，一部分存在Flash。存储在RAM中的日志，设备重启不保存；存储在Flash中的日志，设备重启仍然保留。

* RAM：默认只打印Notice及以上等级日志
* Flash：仅保留Error及以上等级的日志
* Console：默认只打印Notice及以上等级日志，支持打开全部等级日志打印

交换机支持将日志存储到远程服务器中。

【配置参数】

1. 添加远程日志服务器：最多添加3个

* 日志服务器地址：【text文本框】设置远程日志服务器的地址，支持输入Hostname和IP地址（包括IPv4和IPv6），需要满足各类型的地址格式要求，否则需要报错提示。
* 端口：【text文本框】设置远程日志服务器使用的端口，取值范围为1-65535的整数，默认514。
* 最小日志等级：【下拉框】设置存储到远程日志服务器的最小日志等级，向上兼容，默认Notice。日志类型从高到低为Emergency、Alert、Critical、Error、Warning、Notice、Information、Debug。

远程日志服务器列表：

* 列表显示远程日志服务器地址、端口、~~Facility、~~最小日志等级
* 支持~~以服务器地址为索引，~~编辑远程日志服务器配置
* 支持删除单个远程日志服务器配置

2. 日志列表

* 日志列表倒序显示日志生成时间、日志等级、日志详情，即按照时间从远到近显示，时间最近的显示在最上面

日志等级从高到低分别为Emergency、Alert、Critical、Error、Warning、Notice、Information和Debug。

* 支持分页
* 支持刷新
* 支持清除现有所有日志
* 支持过滤和搜索日志
* 按8个等级过滤日志
* 支持选择时间范围来查询某一时段的日志
* 支持输入日志详情内容进行模糊搜索匹配

支持组合上述条件进行日志过滤

* 支持一键导出日志，默认导出所有日志，支持按搜索结果导出指定日志

### Ping

交换机支持Ping功能，来检查指定的地址是否可达，并输出相应的统计信息。

Ping配置：

* Ping：【text文本框】设置Ping的地址，可以是hostname，也可以是IP地址（包括IPv4地址和IPv6地址），需满足各类型的地址格式要求，否则需要报错提示。
* 发包数：【text文本框】设置发送ICMP/ICMPv6 ECHO-REQUEST报文的次数，取值范围为1-65535的整数，默认4次。
* 包长度 (字节/Bytes)：【text文本框】设置ICMP/ICMPv6 ECHO-REQUEST报文的长度，取值范围为0-65500字节，默认56字节。
* 接口：选择Ping包发往的指定VLAN接口，也可不选，默认无。

~~注：接口仅L3交换机支持。~~

配置完毕后，开启Ping。

Ping执行完毕后，将会显示结果，以大text文本框形式显示，内容包括：

* Ping的状态，包括未开启(N/A)、running、success、failed
* 发送报文数
* 接收报文数
* 丢包百分比
* 往返行程的最短时间，单位ms
* 往返行程的最长时间，单位ms
* 往返行程的平均时间，单位ms

### Traceroute

交换机支持路由跟踪功能，用于查看数据包从源端到目的端的路径信息，从而检查网络连接是否可用。当网络出现故障时，可使用此功能定位故障点。

Traceroute配置：

* Traceroute：【text文本框】设置路由跟踪的地址，可以是hostname，也可以是IP地址（包括IPv4地址和IPv6地址），需满足各类型的地址格式要求，否则需要报错提示。
* 接口：选择路由跟踪的指定接口。

注：接口仅L3交换机支持。

配置完毕后，开启Traceroute。

路由跟踪执行完毕后，将会显示结果，以大text文本框形式显示从本机地址到目的地址所经过的网关信息。

### 光模块/Fiber Module

显示光模块下，各光口在接入设备后的相关信息，包括：

* 接口名称
* OE Present
* Loss of signal
* Transceiver Type
* Connector Type
* Ethernet Compliance Code
* Transmission Media
* Wavelength
* Bitrate
* Vendor OUI
* Vendor Name
* Vendor PN
* Vendor Revision
* Vendor SN
* Temperature (℃)
* Voltage (V)
* Current (mA)
* Tx Power (dBm)
* Rx Power (dBm)

上述信息在各厂家存在出入。

支持刷新光口信息。

注：1.每个厂家的光模块显示信息存在不同，故建议采用大文本框的形式，直接从底层获取信息显示。

~~2.要求显示Output/Input Power的计算方式： (TX/RX power) \*0.1/1000~~

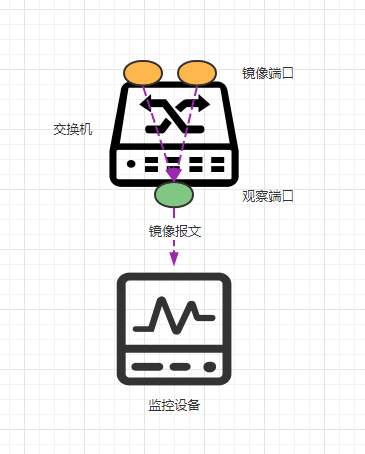
### 镜像/ Mirroring

#### 13.2.5.1 端口镜像/Port Mirroring(SPAN)(FP1B)

【功能概述】

镜像是指将指定源的报文复制一份到目的端口。指定源被称为镜像源，目的端口被称为观察端口，复制的报文被称为镜像报文。

镜像可以在不影响设备对原始报文正常处理的情况下，将其复制一份，并通过观察端口发送给监控设备，从而判断网络中运行的业务是否正常。



【配置参数】

【最终需求详见RSPAN部分】

~~端口镜像列表：~~

* ~~列表显示4组端口镜像，每组显示组、入方向镜像端口、出方向镜像端口、观察端口。~~
* ~~支持编辑端口镜像配置。~~
* ~~支持一键重置端口镜像配置。~~

编辑端口镜像：

* ~~组：显示选择的镜像组~~
* ~~入方向镜像端口：选择需要配置入方向镜像（针对端口接收的报文进行复制）的交换机接口，包括电口、光口和聚合接口。可多选。~~
* ~~出方向镜像端口：选择需要配置出方向镜像（针对端口发送的报文进行复制）的交换机接口，包括电口、光口和聚合接口。可多选。~~
* ~~观察端口：设置观察端口，包括电口、光口。有且仅能选择一个，且不能与镜像端口相同。不同组的观察端口不能相同。~~

~~注：观察端口默认支持发送/接收普通数据包。~~

#### 13.2.5.2 ACL镜像/ACL Mirroring (FP2)

适配ACL规则的高级镜像设置。

Web页面配置和端口镜像合并显示。优先级：ACL镜像>端口镜像

【最终需求详见RSPAN部分】

~~镜像组列表：~~

* ~~列表显示4组端口镜像，每组显示组、入方向镜像（显示配置的ACL类型+ACL名称+规则ID）、出方向镜像【暂不支持】、观察端口~~
* ~~支持编辑镜像配置。~~
* ~~支持一键重置镜像配置。一旦重置，相关联的ACL规则自动关闭镜像功能。~~

~~编辑镜像：~~

* ~~组：显示选择的镜像组~~
* ~~入方向镜像：显示配置的ACL类型+ACL名称+规则ID~~
* ~~观察端口：设置观察端口，包括电口、光口。有且仅能选择一个，且不能与ACL绑定的端口相同。不同组的观察端口不能相同。~~

~~注：观察端口默认支持发送/接收普通数据包。~~

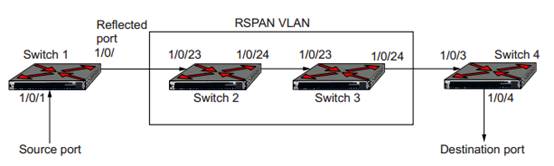
#### 13.2.5.4 RSPAN (FP2)

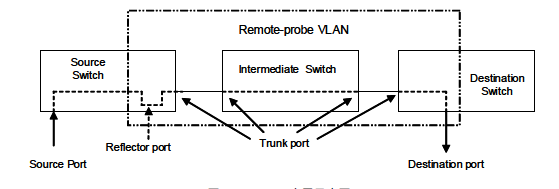
【功能概述】

将一个源接口或源VLAN的所有流量转发至另一个接口，称为SPAN（交换机接口分析），有时也称会话监控。SPAN会话的目的接口在本地交换机上。

RSPAN（Remote SPAN，远程镜像）是SPAN（镜像）的扩展，能够远程监控多台设备，每个RSPAN会话建立于用户指定的Remote VLAN内。RSPAN将所有的被镜像报文通过一个特殊的RSPAN VLAN（即Remote VLAN）传递到远端镜像设备的目的端口。远程镜像突破了被镜像端口和镜像端口必须在同一台设备上的限制，使被镜像端口和镜像端口间可以跨越多个网络设备，方便网管人员对远程交换机设备进行管理。

在RSPAN中，必须在源接口或源VLAN去往RSPAN的目的接口的整个交换路径上，配置一个特定的Remote VLAN，用于传输镜像流量。源交换机给端口流量打上对应的VLAN Tag，在源和目的交换机之间传输的镜像流量将会一直携带这个VLAN Tag，目的交换机收到带有这个VLAN Tag的镜像流量后，会去Tag，通过目的端口转发给流量采集设备。





**设备角色**：如上图所示，共分为3种角色。

* 源交换机：远程镜像源端口所在的交换机，负责将源端口的报文复制一份从源交换机的输出端口输出，通过Remote VLAN进行转发，传输给中间交换机或目的交换机。
* 中间交换机：网络中处于源交换机和目的交换机之间的交换机，通过Remote VLAN把镜像包文传输给下一个中间交换机或目的交换机。如果源交换机与目的交换机直接相连，则不存在中间交换机。
* 目的交换机：远程镜像目的端口所在的交换机，将从Remote VLAN接收到的镜像报文通过镜像目的端口转发给监控设备。

**RSPAN端口**

|  |  |  |
| --- | --- | --- |
| 交换机 | 参与镜像的端口 | 作用 |
| 源交换机 | 源端口 | 被监测的用户端口，通过本地端口镜像把用户数据报文复制到指定的输出端口或者反射端口，源端口允许多个 |
| 反射端口【暂不支持】 | 用于“一对多镜像”，从镜像源端口进入交换机的数据报文，通过反射端口的“反射”，从输出端口输出。反射端口无法作为正常的端口转发流量，所以建议用户将没有使用的处于shutdown状态的端口配置为反射端口，且不在该端口上添加其他配置 |
| 输出端口 | 将镜像报文发送到中间交换机或目的交换机 |
| 中间交换机 | 普通端口 | 将镜像报文发送到目的交换机。  建议中间交换机上配置2个Trunk端口，和两侧设备相连 |
| 目的交换机 | 源端口 | 接收远程镜像报文 |
| 镜像目的端口（观察端口） | 远程镜像报文的监控端口 |

**Remote VLAN**：只传输镜像报文，不能承载正常的业务数据。所有被镜像的报文通过该VLAN从源交换机传递到目的交换机的指定端口，实现在目的交换机上对源交换机的远程端口的报文进行监控的功能。

**注意点：**

（1）在源交换机、中间交换机和目的交换机上，RSPAN与本地SPAN功能可共存，互不冲突；

（2）远程镜像Remote VLAN内的报文不影响设备的CPU使用率；

（3）支持指定镜像目的端口（观察端口）允许或不允许对外通讯，默认允许对外通讯，即支持发送/接收普通数据包；

（4）建议将镜像源端口和反射端口设置在不同VLAN中；

（5）不支持聚合口设置为反射端口；

（6）Remote VLAN不建议是VLAN 1；

（7）Remote VLAN不参与GVRP。

RSPAN也支持基于流的配置，与端口镜像和ACL镜像同理。

（一）基于端口的RSPAN

源交换机配置：Remote VLAN、源端口、反射端口、输出端口（必须加入Remote VLAN）

中间交换机配置：Remote VLAN、普通端口设为Trunk且允许通过Remote VLAN

目的交换机配置：Remote VLAN、源端口、观察端口（必须加入Remote VLAN）

注：不建议与中间交换机或目的交换机相连的端口上配置镜像源端口，否则可能引起网络内的流量混乱。

（二）基于流的RSPAN

源交换机配置：Remote VLAN、源镜像根据ACL高级镜像设置显示（仅支持入方向）、反射端口、输出端口

中间交换机配置：Remote VLAN、普通端口设为Trunk且允许通过Remote VLAN

目的交换机配置：Remote VLAN、源端口、观察端口

【配置参数】

汇总SPAN/RSPAN，包括端口和ACL镜像的需求，具体如下：

全局设置：

* 远程VLAN：【多选】RSPAN功能使用时，设置用于镜像的远程VLAN。从已有VLAN中选择作为Remote VLAN，可多选。不建议选择VLAN 1，给出提示

镜像组列表：

* 列表显示4个镜像组，每个显示镜像组ID、模式、交换机角色（仅RSPAN才显示）、入方向镜像、出方向镜像、~~反射端口（仅RSPAN源交换机配置镜像端口才显示）、~~输出端口（仅RSPAN源交换机才显示）、观察端口（仅SPAN或RSPAN目的交换机才显示）、远程VLAN（仅RSPAN才显示）、收发普通数据报文开关
* 支持编辑镜像组配置
* 支持一键重置镜像组配置。一旦重置，相关联的ACL规则自动关闭镜像功能。

编辑镜像组：

* 组ID：显示选择的镜像组
* 模式：【单选】选择镜像组使用的镜像模式，选项有{SPAN|RSPAN}，默认SPAN。
* 角色：【下拉框】当且仅当模式选择“RSPAN”时支持配置。选择交换机角色，选项有{源交换机| 目的交换机}，默认源交换机。
* 入方向镜像：当且仅当①模式为“SPAN”；②模式为”RSPAN”且角色为“源交换机”时支持配置。选择需要配置入方向镜像（针对端口接收的报文进行复制）的交换机接口，包括电口、光口和聚合接口，可多选；若设置为ACL镜像，则显示关联的ACL类型+ACL名称+规则ID，且不支持更改
* 出方向镜像：当且仅当模式为“RSPAN”且角色为“源交换机”时支持配置。选择需要配置出方向镜像（针对端口发送的报文进行复制）的交换机接口，包括电口、光口和聚合接口。可多选。
* ~~反射端口：【单选】当且仅当交换机角色选择“源交换机”且出入方向镜像选择多个端口时支持配置，此时为必填项。需从交换机的电口、光口中选择，且该端口必须加入Remote VLAN。~~
* 输出端口：【单选】当且仅当模式为“RSPAN”且交换机角色选择“源交换机”时支持配置，选项为交换机的电口、光口和聚合口，不能与镜像端口或ACL绑定的端口相同，不同镜像组的输出端口也不能相同，且该端口必须加入Remote VLAN。
* 观察端口：【单选】当且仅当①模式为“SPAN”；②模式为“RSPAN”且交换机角色选择“目的交换机”时支持配置，选项为交换机的电口和光口。不能与镜像端口或ACL绑定的端口相同；不同镜像组的观察端口也不能相同；该端口必须加入Remote VLAN。

~~注：观察端口默认支持发送/接收普通数据包。~~

* 远程VLAN：【单选】从全局设置的远程VLAN中选择一个作为该镜像组的Remote VLAN。不同组的Remote VLAN不能相同。
* 发送/接收普通数据报文：【开关】设置镜像组是否允许发送/接收普通业务数据包，默认开启。

### sFlow/sFlow (FP3) 【待评审】

【功能概述】

采样流sFlow（Sampled Flow）是一种基于报文采样的网络流量监控技术，主要用于对网络流量进行统计分析。

监控局域网流量：将设备作为sFlow Agent，在局域网中对接口流量进行采样，并将采样结果发送给sFlow Collector用于流量分析，以达到监控网络的目的。

sFlow系统包含一个嵌入在设备中的sFlow Agent和远端的sFlow Collector。其中，sFlow Agent通过sFlow采样获取接口统计信息和数据信息，将信息封装成sFlow报文，当sFlow报文缓冲区满或是在sFlow报文缓存时间（缓存时间为1秒）超时后，sFlow Agent会将sFlow报文发送到指定的sFlow Collector。sFlow Collector对sFlow报文进行分析，并显示分析结果。

sFlow Agent提供了两种采样方式从不同的角度分析网络流量状况，分别为：

* Flow采样：sFlow Agent设备在指定接口上按照特定的采样方向和采样比对报文进行采样分析，用于获取报文数据内容的相关信息。该采样方式主要关注流量的细节，便于监控和分析网络上的流行为

工作原理：当一个报文通过某个接口时，sFlow Agent设备根据该接口下的采样率配置对报文进行flow采样，包括拷贝报文的头部、提取报文的以太网头部、IP头部、获得报文的路由信息等。最后sFlow Agent模块将flow采样结果封装成sFlow报文，发送到sFlow Collect进行分析。

* Counter采样：sFlow Agent设备周期性地获取接口上的流量统计信息。该采样只关注接口上流量的数量。

工作原理：sFlow Agent模块定时轮询接口，对于counter采样时间间隔到期的接口获得该接口的统计信息，然后将统计信息封装成sFlow报文，发送到sFlow Collector进行分析。

sFlow报文采用UDP封装，缺省目的端口号为6343。

sFlow版本号有2,4,5，暂仅支持v5。

【配置参数】

基于端口的sFlow。

全局配置：

* sFlow Agent：【下拉框】设置sFlow Agent的IP地址，选项为VLAN接口（不包括loopback接口）。选择后，在下方显示Agent的IP地址，即所选VLAN接口的IP地址，包括IPv4地址和IPv6全球单播地址。

Collecter设置：从Collector列表中指定进行设置

* ID：显示当前选择的sFlow Collector ID。
* \*IP地址：【text文本框，IP地址格式】设置Collector的IP地址，须与Agent的IP地址处于同一网段（IPv4地址或IPv6地址均可，二者选其一设置）
* ~~报文最大长度：【text文本框】设置Agent向Collector发送sFlow报文的最大长度，对采样数据进行尽可能的组合封装，使一个报文携带多个采样数据，减少发送报文的数量。取值范围为1024-8100，默认1400~~
* UDP端口：【text文本框】设置发送sFlow报文的UDP目的端口号，取值范围为1024-65535的整数，默认6343
* 自动删除时间 (秒)：【text文本框】设置Collector的自动删除时间，取值范围为0-3600的整数，默认0，即不删除
* 描述：【text文本框】设置对此Collector的说明，最长64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示

Collector列表：

* 列表显示Collector ID（默认从1-8排序）、IP地址、报文最大长度、UDP端口、自动删除时间、描述
* 支持单个编辑

接口设置：

* 接口：选择交换机物理端口，包括电口和光口，支持多选

~~Flow采样：~~

* ~~采样方向：【单选】设置接口在特定方向的Flow流量采样，选项有{入方向 | 出方向| 入方向&出方向}，默认入方向&出方向~~
* ~~截取的报文最大长度：【text文本框】设置接口上Flow采样截取的报文最大长度，取值范围为18-512字节，默认64字节~~
* ~~采样率：【text文本框】设置接口上Flow流量采样的采样率，取值范围为256-65535~~
* ~~Collector ID：【下拉框】选择接口发送Flow采样的目的Collector，选项为8个Collector~~

Counter采样：

* 采样间隔 (秒)：【text文本框】设置接口Counter采样即发送报文的时间间隔，取值范围为2-3600的整数，默认10秒
* Collector ID：【下拉框】选择接口发送Counter采样的目的Collector，选项为8个Collector

接口列表：

* 列表显示接口、~~Flow采样（包括采样方向、截取的报文最大长度、采样率、Collector ID、入方向样本数、出方向样本数）、~~Counter采样（包括采样间隔和Collector ID）
* 支持单个/批量编辑

### UDLD [TBD]

### 线缆检测/Copper Test (FP1C)

【GWN7832交换机不支持此功能】

【功能概述】

线缆检测能够检测与交换机相连的线缆是否有故障以及故障的位置，利用此功能可以辅助日常工程安装诊断。

注：1.进行线缆检测时，请确保电口为非UP状态，否则检测结果不可用。

2.检测结果可能存在误差，仅作为参考值。

【配置参数】

* 端口：【单选】选择交换机的接口，包括电口。建议加上端口状态。
* <线缆检测>按钮：点击进行所选端口连接的线缆检测。

检测结束后，显示线缆检测的结果，显示如下：

* 显示线缆的状态，包括OK(正常)、Open(开路)、Short(短路)、Mismatch(阻抗不匹配)、LineDriver(线路驱动)、Unknown(未知)
* 显示线缆的长度，有故障时为端口到故障位置的长度，无故障时为线缆的实际长度，未接线缆时默认为0米(根据芯片手册，可能有±3米的误差)

### 一键调试/OneClick Debug (FP1D)

【功能概述】

当设备发生故障时，支持对设备进行一键调试，获取相关调试信息，以便研发人员可以通过调试文件快速定位问题所在，帮助更好地分析和解决问题。

【配置参数】

* 一键调试：【开始/取消】按钮。调试开始后，显示“调试中”的状态，由于调试时间较短，系统自动调试完成即可。~~支持手动停止取消调试，且不保留调试文件。~~若时间长达30分钟，则会自动停止。

注：1.调试期间，不影响对设备的配置管理。但若触发设备的重启等操作，调试自动停止，设备内保留调试文件，仅保留最新的一份调试文件。

2.调试信息清单，支持对整个交换机信息的收集。

3.调试完成，自动生成设备调试信息，文件名为oneclickdebug年月日时分秒.log。调试完成后，显示调试文件及其大小和生成时间，支持下载和删除。点击下载会立即保存至本地PC浏览器指定的文件夹下。

4.【20230327】目前调试时间优化为1分钟左右，时间较短，可以去除“取消调试”功能。

### 云连接状态检测 (FP1D)

当交换机与GWN.Cloud/GWN Manager连接出现不稳定等问题时，用户可登录本地诊断页面进行云连接状态检测。

要求具备如下功能：

* 当且仅当与Cloud/Manager连接时，出现此功能。
* 增加与Cloud/Manager建立连接的检测功能。
* 增加在Cloud/Manager重连的日志显示，仅记录最近的500条日志，支持导出2000条日志。

1. 连接状态

* 连接状态：显示交换机与云端的实时连接状态，有{已连接|未连接}。

2. 连接检测

支持对交换机与云端的连接进行状态检测，主要分为6个阶段：

**阶段一：**准备阶段

查看是否开始尝试与云端建立连接。若无法与云端重新建连，需显示原因“交换机版本不支持”“设备异常”等。

**阶段二：**域名解析阶段

进行域名解析。若解析失败，需显示原因。

**阶段三：**TCP连接阶段

TCP三次握手过程检测。若失败，需显示原因。

**阶段四：**TLS连接阶段

TLS数据通道建立过程。若失败，需显示原因。

**阶段五：**HTTP(S) Transaction阶段

HTTP(S)请求发送及等待响应检测。若失败，需显示原因。

**阶段六：**WS(S) Upgrade阶段

HTTPS协议切换到Websocket协议的检测。若失败，需显示原因。

提供<检测>按钮触发连接状态检测。一旦开始检测，按照上述6个阶段逐步检测，并显示<检测中>的状态。任一阶段失败，即停止检测并显示失败原因（具体原因由底层上报），并支持重新检测。检测完成后，显示对应的检测结果，也支持重新检测（此时按钮显示<重新检测>），页面刷新按钮变回<检测>。

3. 日志

* 支持手动获取日志，点击<获取日志>后，仅显示近500条自动重连的简单日志。交互设计上建议采用大文本框形式。
* 支持一键导出详细日志，最多显示近2000条，自动下载至PC本地，文件名为“年月日时分秒.log”，时间以导出时间为准。

## 备份与恢复/Backup & Restore(FP1B)

【功能概述】

为防止设备意外损坏等情况，导致配置文件无法恢复，可以对设备进行备份配置文件。备份方式有：

* 备份配置文件至内部存储器中

在备份功能模块下，支持备份2类文件，一类是当前正在运行的配置文件，一类是保存的配置文件。

备份文件命名为“GWN78XX(型号)\_MAC\_config年月日时分秒.cfg”。备份文件至多8个，当数量达到8个后，新的备份文件将会覆盖最早的文件。

备份仅备份配置，数据不备份。

备份的安全性：基于设备型号进行加密处理，同型号的备份文件可以通用。

若用户进行了错误的配置，导致功能异常或未达到预期，可以执行备份恢复功能。备份恢复的方式有：

* 从内部存储器恢复配置文件
* 上传备份文件恢复配置

交换机还支持一键清除所有业务配置和数据文件，将设备恢复至出厂配置状态。恢复出厂的方式有：

* Web GUI软按钮恢复出厂
* Reset硬按键长按5秒恢复出厂

【配置参数】

1. 备份

提供一键备份的按钮，有<备份运行配置>和<备份保存配置>2种按钮。点击，即进行文件备份。备份完成后，备份文件自动保存至设备内部，并以列表形式呈现在Web端。

备份文件列表：

* 列表显示名称、备份时间
* 支持下载备份文件至当前管理PC本地
* 支持删除备份文件
* 支持选择某一备份文件进行配置还原

2. 备份恢复

交换机支持通过从内部存储器中选择某一时间节点的配置文件进行备份恢复，也支持上传备份文件进行备份恢复。

* 上传备份文件：点击<上传>按钮，从当前管理PC上选择备份文件。点击选中的文件进行上传前，需要对文件进行检查，判断是否适宜当前设备的备份文件，否则需要报错“此文件与设备不匹配，请重新上传”。

备份文件上传过程中，不允许操作页面，需提示“备份文件上传中，请稍候…”，且无法关闭提示，直至上传成功。

* 若使用内部存储器备份配置文件，支持从内部存储器的备份文件中选择某一备份文件进行恢复。

上传成功或选择完备份文件后，自动进行配置载入，备份文件中的配置将会覆盖当前交换机的现有配置信息。如果载入配置有误，可能会导致交换机无法正常使用，此时需长按设备上的Reset按键5秒来进行恢复出厂设置。

注：1.在载入备份文件过程中，请勿断开交换机电源。

2.载入配置结束后，交换机将会自动重启以生效配置。

3. 恢复出厂

恢复出厂有2种方式：

方式一：通过Web GUI进行恢复出厂

方式二：长按Reset硬按键5秒进行恢复出厂（启机和正常运行均支持）

* <恢复出厂>按钮：点击此按钮，页面弹出二次确认弹窗

[恢复出厂后，交换机所有配置都将恢复至出厂状态，请慎用! 建议您在恢复出厂前备份当前配置。

取消 确定]

点击“取消”关闭恢复出厂；点击“确定”执行恢复出厂设置，页面体会是“设备正在恢复出厂，请稍候…”。待设备恢复出厂完毕，交换机配置将恢复成出厂默认状态。

注：1.恢复出厂过程中，请勿断开交换机电源。

2.恢复出厂过程中，设备会断开与交换机的连接。

## 告警/Alert（适配Cloud端）(FP1D)

目前仅配合Cloud做如下告警支持：

* 性能告警：
* CPU使用率告警（含恢复） CPU使用率超过n%（75-100的整数，缺省为75）
* 内存使用率告警（含恢复） 内存使用率超过n%（75-100的整数，缺省为75）
* 端口丢包率告警（含恢复） 端口丢包率超过n %（0-100的整数，支持小数点后1位）
* 系统告警：
* 设备温度告警（含恢复）
* 设备硬件故障  电源、PoE模块、风扇
* 设备光模块loss 光模块信号丢失
* 设备光模块温度告警 仅支持GS的4款光模块（合理温度范围为0℃-70℃）(FP2) Alert等级（本地）
* 设备备份失败（启机时文件系统备份分区Flash损坏）
* 设备升级成功
* 设备升级失败
* 网络告警：
* 端口UP
* 端口Down
* PoE供电关闭（含恢复）（PSE功率过载+设备高温）
* 端口errdisable（含恢复） 原因为端口自动恢复10选项

## SNMP(FP1C)

【功能概述】

简单网络管理协议SNMP，广泛应用于TCP/IP网络的网络管理标准协议。其提供了一种通过运行网络管理软件的中心计算机（即网络管理工作站）来管理设备的防范。

SNMP管理模型：SNMP系统包括网络管理系统NMS、代理进程Agent、被管对象Management object和管理信息库MIB。NMS作为整个网络的网管中心，对设备进行管理。

每个被管理设备中都包含驻留在设备上的Agent进程、MIB和多个被管对象。NMS通过与运行在被管理设备上的Agent交互，由Agent通过对设备端的MIB的操作，完成NMS的指令。

**NMS：**在网络中扮演管理者角色，是一个采用SNMP协议对网络设备进行管理/监视的系统，运行在NMS服务器上。

* NMS可以向设备上的Agent发出请求，查询或修改一个或多个具体的参数值
* NMS可以接收设备上的Agent主动发送的Trap信息，以获知被管理设备当前的状态

**Agent：**被管理设备中的一个代理进程，用于维护被管理设备的信息数据并响应来自NMS的请求，把管理数据汇报给发送请求的NMS。

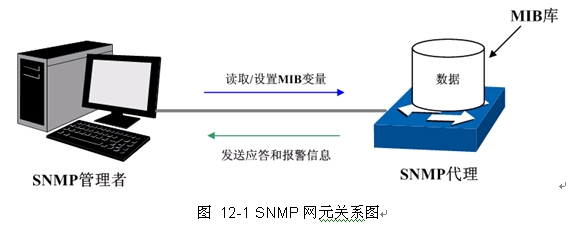
* Agent接收到NMS的请求信息后，通过MIB表完成相应指令后，并把操作结果响应给NMS
* 当设备发生故障或者其他事件时，设备会通过Agent主动发送信息给NMS，向NMS报告设备当前的状态变化

**Managed object：**被管理对象。每一个设备可能包含多个被管理对象，被管理对象可以是设备中的某个硬件，也可以是在硬件、软件（如路由选择协议）上配置的参数集合。

**MIB：**数据库，指明了被管理设备所维护的变量（即能够被Agent查询和设置的信息）。MIB在数据库中定义了被管理设备的一系列属性：对象的名称、对象的状态、对象的访问权限和对象的数据类型等。通过MIB，可以完成以下功能：

* Agent通过查询MIB，可以获知设备当前的状态信息
* Agent通过修改MIB，可以设置设备的状态参数

SNMP的管理信息库采用和域名系统DNS相似的树型结构，它的根在最上面，根没有名字。根的节点代表被管理对象，可以用从根开始的一条路径唯一标识，被管理对象可以用一串数字唯一确定，这串数字即被管理对象的对象标识符OID，如Grandstream的OID为1.3.6.1.4.1.42397。三者的关系如下图所示：



SNMP管理者是SNMP网络的管理者，SNMP代理是SNMP网络的被管理者，他们之间通过SNMP协议来交互管理信息。每个SNMP代理都有自己的MIB，SNMP管理者根据权限可以对MIB中的对象进行读/写操作。

交换机支持SNMPv1、SNMPv2c和SNMPv3三个协议版本，在选择SNMP协议时需要与网管站选择的协议版本保持一致。SNMPv1和SNMPv2c均采用团体名认证，团体名定义了SNMP管理者和SNMP代理的关系，起到类似密码的作用，用于限制SNMP管理者对SNMP代理的访问。如果SNMP报文携带的团体名没有得到设备的认可，该报文将被丢弃。SNMPv3采用VACM（基于视图的访问控制模型）和USM（基于用户的安全模型）认证机制，网络管理员可以设置认证和加密功能。认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对SNMP管理者和SNMP代理间的传输报文进行加密。以免被窃听。采用认证和加密功能，可以为SNMP管理者和SNMP代理间的通信提供更高的安全性。

通知管理功能是交换机主动向管理软件报告某些视图的重要事件（如设备重启等），便于管理员通过管理软件对交换机一些特定事件进行及时监控和处理。

通知报文共有2种方式：

* Trap：发送Trap报文通知SNMP管理者
* Inform：发送Inform报文通知SNMP管理者，并且要求SNMP管理者返回信息。交换机发送Inform报文后，若经过超时时间仍没有收到Inform回应报文，则会重发Inform报文。超过重传次数后，将不再重复发送该Inform报文。Inform具有更高的可靠性，仅在SNMPv2c和SNMPv3可以使用。

FP1暂仅支持公有MIB。

【配置参数】

**全局设置：**

* SNMP：【开关】设置是否开启交换机SNMP功能，默认关闭。
* 本地引擎ID：【text文本框】设置本地SNMP实体的引擎ID，本地用户建立在本地引擎之下。默认8000A59Dxxxxxxxx，其中，xxxxxxxx默认为设备MAC地址，支持用户修改，以十六进制表示，长度限制在2-56字符之间，字符个数必须为偶数。支持一键重置恢复成初始值。

远程引擎ID：支持添加多组，至多8组

* 远程引擎ID：【text文本框】设置SNMP管理端的引擎ID，远程用户建立在远程引擎之下。输入长度限制在10-64字符，以十六进制表示，字符个数必须为偶数
* 服务器地址：【text文本框】设置网管站服务器的地址，支持输入Hostname和IP地址（包括IPv4和IPv6），需要满足各类型的地址格式要求，否则需要报错提示。

远程引擎ID列表：

* 列表显示远程引擎ID、服务器地址
* 支持编辑，以远程引擎ID为索引，只能编辑服务器地址
* 支持删除远程引擎ID

**视图管理：**

* \*视图：【text文本框】设置SNMP视图的名称，最长32字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示。视图名称具有唯一性
* \*OID子树：【text文本框】设置该视图的管理变量OID，其标明了节点在MIB数中的准确位置，是MIB库中对象的唯一标识。只能是数字和点的组合，如1.3.6.1.2.1.1，最多支持15个数字，例如1个数字“.1”，2个数字“.1.3”，3个数字“.1.3.6”，每个数字最多8位
* 类型：【下拉框】设置该视图对MIB子树的访问权限，选项有{排除|包含}，默认包含。

视图列表：最多添加16个

* 列表显示视图、OID子树和类型。
* 默认存在一条视图，视图为all，OID子树为.1，类型为包含，不可删除和编辑
* 支持添加，以视图为标识符进行添加
* 支持删除视图（除默认all视图外）

**组管理：**

* \*组：【text文本框】设置SNMP组的名称，最长32字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示。组名称具有唯一性
* 安全模式：【下拉框】选择组的安全模式，选项有{SNMPv1|SNMPv2c|SNMPv3}，默认SNMPv1。选择SNMPv3时，需要配置安全级别。
* 安全级别：【下拉框】设置安全级别，选项有{不认证不加密|只认证不加密|既认证又加密}，默认不认证不加密。
* \*只读视图：【下拉框】从已有的视图中选择，对所选的视图只能被查看，不能被编辑。
* 读写视图：【下拉框】从已有的视图中选择，对所选的视图进行读写操作。如果不选择，则SNMP管理者不能对设备的所有MIB对象进行读写操作。
* 通知视图：【下拉框】从已有的视图中选择，管理软件可以接收到所选视图发送的异常告警信息。如果不选择，则SNMP代理不会向SNMP管理者发送Trap信息。

组列表：最多添加32个（组的添加受限于团体，1个基础团体系统会自动生成2个组。举例：若已添加基础团体2个，则此时可以手动添加的组为32-4=28个。）

* 列表显示组、安全模式、安全级别、只读视图、读写视图、通知视图
* 支持添加，以组为标识符进行添加
* 支持编辑。一旦被团体引用，只能编辑安全级别和视图
* 支持删除组。一旦被团体引用，将不能删除

**团体管理：**组内的用户通过只读、读写和通知视图来达到访问控制的目的。

* \*团体：【text文本框】设置SNMP团体的名称，最长32字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示。团体名称具有唯一性
* 类型：【下拉框】设置团体的类型，选项有{基础|高级}，默认基础。

当选择基础时，需要配置：

* 视图：【下拉框】从已有的视图中选择团体可访问的视图。
* 权限：【下拉框】设置团体对视图的访问权限，选项有{只读|读写}，默认只读。

当选择高级时，需要配置：

* 组：【下拉框】从已有的组（只能是安全模式为SNMPv1和SNMPv2c的组）中选择。

团体列表：最多添加8个

* 列表显示团体、类型、视图、权限、组
* 支持添加，以团体为标识符进行添加
* 支持编辑
* 支持删除团体

**用户管理：**SNMP管理软件可以通过用户的方式对交换机进行管理。用户建立在组之下，与其所属的组具有相同的安全级别和访问控制权限。

* \*用户：【text文本框】设置SNMPv3 用户的名称，最长32字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示。用户名称具有唯一性
* 组：【下拉框】设置用户所属组，从已有的组（只能是安全模式为SNMPv3的组）中选择。通过组来确定用户的安全级别。若无SNMPv3的组，支持新建。
* 安全级别：根据所选的组，来显示对应用户的安全级别和访问控制权限。

若选择的组的安全级别为不认证不加密，则无需设置认证和加密；

若选择的组的安全级别为只认证不加密，则需设置认证；

若选择的组的安全级别为既认证又加密，则需设置认证和加密。

* 认证模式：【下拉框】当组的安全级别为“只认证不加密”或“既认证又加密”时，需要设置认证模式，选项有{MD5|SHA}，默认MD5。
* 认证密码：【text文本框】设置认证密码，长度限制在8-32字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示
* 加密模式：【下拉框】当组的安全级别为“既认证又加密”时，需要设置加密模式，选项有{DES}，默认DES。
* 加密密码：【text文本框】设置加密密码，长度限制在8-32字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?,这5项，不支持字符以报错形式提示

用户列表：最多添加8个

* 列表显示用户、组、安全级别、认证模式、加密模式
* 支持添加，以用户为标识进行添加
* 支持编辑
* 支持删除用户

**通知管理：**通知管理功能是交换机主动向管理软件报告某些视图的重要事件（如设备重启等），便于管理员通过管理软件对交换机一些特定事件进行及时监控和处理。

* 服务器地址：【text文本框】设置管理主机的地址，支持输入Hostname和IP地址（包括IPv4和IPv6），需要满足各类型的地址格式要求，否则需要报错提示。
* UDP端口：【text文本框】设置管理主机上启用供通知过程使用的UDP端口，与IP地址共同作用，取值为1-65535的整数，默认162。
* 安全模式：【下拉框】设置安全模式，选项有{SNMPv1|SNMPv2c|SNMPv3}，默认SNMPv1。
* 通知类型：【下拉框】设置使用的通知报文类型，选项有{Trap|Inform}，默认使用Trap。当安全模式选择SNMPv1时，仅能使用Trap；当安全模式选择SNMPv2c或SNMPv3时，Trap和Inform可供用户自主选择。
* 团体：【下拉框】当且仅当安全模式选择SNMPv1或SNMPv2c时支持配置，从已有的团体中选择配置管理软件的团体名。
* 用户：【下拉框】当且仅当安全模式选择SNMPv3时支持配置，从已有的用户中选择配置管理软件的用户名。
* 安全级别：【下拉框】当且仅当安全模式选择SNMPv3时支持配置，选项有{不认证不加密|只认证不加密|既认证又加密}，默认不认证不加密。
* 超时时间 (秒)：【text文本框】当且仅当通知类型为Inform时支持配置。设置交换机等待Inform回应报文的时间。超过该时间后，将重新发送Inform报文，取值为1-300的整数，默认15秒。
* 最大重试次数：【text文本框】当且仅当通知类型为Inform时支持配置。设置Inform报文的最大重传次数。交换机发送Infrom报文后，若经过超时时间仍没有收到Inform回应报文，则会重发Inform报文。超过重传次数后，将不再重复发送Infrom报文。取值为1-255的整数，默认3次。

通知列表：最多添加8个

* 列表显示服务器地址、UDP端口、通知类型、安全模式、团体/用户、安全级别、超时时间、最大重试次数
* 支持添加
* 支持编辑
* 支持删除通知

**Trap事件：**设置Trap方式上报的事件

* 认证失败：【开关】设置是否将认证失败的事件发送给SNMP管理者。默认开启
* 端口Up/Down：【开关】设置是否将端口连接Up/Down的事件发送给SNMP管理者。默认开启
* 冷启动：【开关】设置是否将交换机冷启动的事件发送给SNMP管理者。默认开启
* 热启动：【开关】设置是否将交换机热启动的事件发送给SNMP管理者。默认开启

私有MIB (FP2)

## RMON(FP1C)

【功能概述】

RMON基于SNMP体系结构实现，与现存SNMP框架兼容，仍然是网管工作站NMS和运行在各网络设备商的代理Agent两部分组成，比SNMP更有效、更积极主动地监测远程网络设备，为监控网络的运行提供一种高效的手段。

RMON允许有多个监控者，监控者可用如下两种方法收集数据：

* 通过专用的RMON Probe（探测仪），NMS直接从RMON Probe获取管理信息并控制网络资源，这种方式可以获取RMON MIB的全部信息
* 将RMON Agent直接嵌入网络设备中，使它们成为带RMON Probe功能的网络设备。NMS使用SNMP与其交换数据信息，收集网络管理信息。这种方式受设备资源限制，一般无法获取RMON MIB的所有数据，基本上只收集四个组（告警、事件、历史和统计）的信息。

RMON主要实现了统计和告警功能，用于网络中管理设备对被管理设备的远程监控和管理。

RMON的统计功能可以通过RMON统计组或者RMON历史组来实现，分为以太网统计功能和历史统计功能。

* 以太网统计功能（对应RMON MIB中的统计组）：系统统计被监控的每个网络的基本统计信息。系统将持续统计某一网段的流量和各种类型包的分布，或者各种类型的错误帧数、碰撞次数等，统计对象包括网络冲突数、CRC校验错误报文数、过小（或超大）的数据报文数、广播、多播的报文数以及接收字节数、接收报文数等。
* 历史统计功能（对应RMON MIB中的历史组）：系统定期采样收集网络状态统计信息并存储，以便后续的处理。系统将按周期定时对各种流量信息进行统计，统计数据包括带宽利用率、错误包数和总包数等。

RMON告警功能包含事件定义功能和设置告警阈值功能，由这两个子功能的组合使用来实现RMON告警功能。

* 事件定义功能（对应RMON MIB中的事件组）：事件组控制从设备来的事件和提示，提供关于RMON Agent所产生的所有事件。当某事件发生时，可以记录日志或发送Trap到网管站。
* 设置告警阈值功能（对应RMON MIB中的告警组）：系统针对指定的告警变量（任意告警对象对应的OID）进行监控。在用于预先定义指定告警的一组阈值和采样时间后，系统会按照定义的时间周期去获取指定告警变量的值，当告警变量的值大于或等于上限阈值时，触发一次上限告警事件；当告警变量的值小于或等于下限阈值，触发一次下限告警事件。RMON Agent会将上述监控到的状态记录为日志或者把Trap发往网管站。

RMON规范中定义了多个RMON组，设备实现了公有MIB中支持的统计、历史、告警和事件4个组。

* 统计组：规定系统将持续地对以太网接口的各种流量信息进行统计，并将统计结果存储在以太网统计表中以便管理设备随时查看。统计信息包括网络冲突数、CRC校验错误报文数、过小（或超大）的数据报文数、广播、多播的报文数以及接收字节数、接收报文数等。在指定接口下创建统计表项成功后，统计组就对当前接口的报文数进行统计，它统计的结果是一个连续的累加值。
* 历史组：定期收集网络状态统计信息并存储，以便后续的处理。历史组包含两个表：
* 历史控制表：主要用来设置采样间隔时间等控制信息。
* 以太网历史表：主要用来存储历史组定期收集网络状态统计信息，为网络管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。
* 事件组：定义的事件用于告警组配置项。当监控对象达到告警条件时，就会触发事件。RMON事件管理即是在事件表的指定行添加事件，并定义事件的处理方式：
* Log：只发送日志。
* Trap：只向NMS发送Trap消息。
* Log-trap：既发送日志同时也向NMS发送Trap消息。
* None：不做任何处理。
* 告警组：允许针对告警变量（可以是本地MIB的任意对象）预先定义一组阈值进行监视。用户定义了告警表项后，系统会按照定义的时间周期去获取被监视的告警变量的值，当告警变量的值大于或等于上限阈值时，触发一次上限告警事件；当告警变量的值小于或等于下限阈值，触发一次下限告警事件，告警管理将按照事件的定义进行相应的处理。

各表的生存时间：

|  |  |  |
| --- | --- | --- |
| 表名称 | 表项容量（Bytes） | 最大生存时间（s） |
| 统计表 | 100 | 600 |
| 历史控制表 | 100 | 600 |
| 告警表 | 60 | 6000 |
| 事件表 | 60 | 600 |
| 事件日志表 | 600 | - |

说明：

1.历史控制表中的每一项控制信息在以太网历史表中最多可以有10条历史数据相对应。如果超过指定条数，将循环覆盖。

2.事件日志表没有最大生存时间，日志事件行对应的日志最多可以有10条，超过10条将循环覆盖。

【配置参数】

要使用RMON功能，必须先开启SNMP功能。

**统计组：**

统计组列表：

* 列表显示端口（包括电口、光口和聚合接口）、接收字节数、丢包事件数、接收报文数、广播报文数、组播报文数、CRC检验错误包数、过小报文数、超大报文数、分片数、网络冲突数、碰撞次数、64字节报文数、65-127字节报文数、128-255字节报文数、256-511字节报文数、512-1023字节报文数、1024-1518字节报文数
* 支持刷新，统计数据为累计值
* 支持清除单个/批量/全部端口的统计表数据

**历史组：**

* 历史组ID：历史索引ID，默认从1开始，自动往上累加。
* 端口：【单选】选择需要进行采样的交换机接口，包括电口、光口和聚合接口。
* \*最大采样条数：【text文本框】设置历史控制表项对应的历史表容量，即历史表最多可容纳的采样数据条目数，取值为1-50的整数，默认50。
* \*采样间隔 (秒)：【text文本框】设置端口采样的时间间隔，取值为1-3600秒，默认1800秒。
* 所有者：【text文本框】设置该条采样的创建者，最长32字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示

历史组列表：最多添加32个

* 列表显示历史组ID、端口、采样间隔、所有者、最大采样条数、实际采样数、采样统计信息
* 采样统计信息包括采样编号、丢包事件数、接收字节数、接收报文数、广播报文数、组播报文数、CRC检验错误包数、过小报文数、超大报文数、分片数、网络冲突数、碰撞次数、利用率

注：每次只显示50条采样统计信息（由最大采样条数决定）。当有新的统计信息时，最早的记录将被覆盖。

* 支持添加，每个端口支持添加多条
* 支持编辑，仅支持单条编辑，以历史组ID为索引进行编辑
* 支持删除单条/批量/全部历史组配置

**事件组：**

* 事件ID：事件索引ID，默认从1开始，自动往上累加。
* 描述：【text文本框】设置该事件的描述信息，最长32字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示
* 类型：【下拉框】设置事件发生时，系统所做的处理，选项有{None| Log| Trap| Log&Trap}，默认None。
* \*团体：【text文本框】当且仅当类型选择Trap或Log&Trap时支持配置。设置该事件所属的团体，当对应事件需要发送通知时，将会根据此团体名进行发送。最长32字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示
* 所有者：【text文本框】设置该事件的创建者，最长32字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示

事件组列表：最多添加32个

* 列表显示事件ID、描述、类型、用户、所有者和事件日志统计信息
* 事件日志统计信息包括日志ID、日志生成时间和日志描述
* 支持添加多条事件
* 支持编辑，仅支持单个编辑
* 支持删除单个/批量/全部事件组

**告警组：**

* 端口：【单选】选择需设置告警的交换机接口，包括电口、光口和聚合接口。
* 计数器：【下拉框】选择告警变量，选项有{丢包事件数| 接收字节数| 接收报文数| 接收的广播报文数| 接收的组播报文数| CRC校验错误包数| 过小报文数| 超大报文数| 分片数| 网络冲突数| 碰撞次数| 64字节报文数| 65-127字节报文数| 128-255字节报文数| 256-511字节报文数| 512-1023字节报文数| 1024-1518字节报文数}，默认丢包事件数。
* 采样类型：【下拉框】设置告警变量的采样方法，再将取样的值与阈值进行比较。选项有{绝对值|增量}，默认绝对值。绝对值，采样时间到达时直接提取变量的值；增量，采样时间到达时提取的是变量在采样间隔内的变化值。
* 采样间隔 (秒)：【text文本框】设置采样的时间间隔，取值为1-2147483647秒，默认100秒。
* \*所有者：【text文本框】设置该告警的创建者，最长32字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示
* 启动告警：【下拉框】设置告警触发的方式，选项有{上升|下降|上升&下降}，默认上升。

当选择上升或上升&下降时，需配置：

* 阈值上限：【text文本框】设置触发告警的阈值上限，取值为1-2147483647，默认100。
* 上升事件：【下拉框】设置超过阈值上限所执行的事件，从已有的事件组中选择。

当选择下降或上升&下降时，需配置：

* 阈值下限：【text文本框】设置触发告警的阈值下限，取值为1-2147483647，默认20。
* 下降事件：【下拉框】设置低于阈值下限所执行的事件，从已有的事件组中选择。

注：1.当告警变量的采样值在同一方向上连续多次超过阈值时，只会在第一次产生告警事件。即上升告警和下降告警是交替产生的，出现了一次上升告警，则下一次必为下降告警。2.芯片里有规定。若只选择“上升”告警，则下降阈值默认为20，上升阈值必须大于下降阈值；若只选择“下降”告警，则上升阈值默认为100，下降阈值必须小于上升阈值；当选择“上升&下降”告警，上升阈值必须大于下降阈值。

告警组列表：最多添加32个

* 列表显示端口、计数器及其值、采样类型、采样间隔、所有者、告警触发方式、上升的阈值和事件组、下降的阈值和事件组
* 支持添加多条，每个端口允许添加多条
* 支持编辑，仅支持单条编辑
* 支持删除单条/批量/全部告警组
* 支持刷新，刷新计数器的实际值

## TR-069(FP3)

GWN78XX交换机，既可以被GWN.Cloud/GWN Manager接管，也支持被TR-069管理。

无论GWN78XX是否被GWN.Cloud/GWN Manager管理，均支持TR-069功能，通过本地Web管理平台或CLI开启TR-069并进行相应配置。

当GWN78XX被TR-069管理后，本地仍可进行管理，不受到限制，即GWN78XX本地Web与CLI、TR-069、GWN.Cloud/GWN Manager可同时管理交换机，以 后配置的为准进行生效。

【配置参数】

* TR-069：【开关】设置是否启用TR-069功能，默认关闭。
* ACS源：【text文本框】设置TR-069自动配置服务器的地址。
* ACS用户名：【text文本框】设置交换机向ACS发起连接请求时ACS对TR-069客户端即交换机进行认证的用户名，必须与ACS侧的配置保持一致。
* ACS密码：【text文本框】设置ACS对交换机进行认证的密码，必须与ACS侧的配置保持一致。
* 开启定时连接：【开关】若启用定时连接，交换机将会定时向ACS发送连接通知包，默认开启。
* 定时连接间隔 (秒)：【text文本框】设置交换机向ACS定时发送连接通知包的时间间隔。取值范围为1- 2147483647的整数，默认64800。
* ACS连接请求用户名：【text文本框】ACS服务器向交换机发起连接请求时，交换机对ACS进行认证的用户名，必须与ACS侧的配置保持一致。
* ACS连接请求 (秒)：【text文本框】ACS服务器向交换机发起连接请求时，交换机对ACS进行认证的密码，必须与ACS侧的配置保持一致。
* ACS连接请求端口：【text文本框】ACS服务器向交换机发起连接请求时所使用的的端口号，取值范围为1-65535的整数，默认7547。
* CPE证书：【文本框】设置交换机通过SSL连接ACS时需要使用的证书文件。
* CPE证书密钥：【文本框】设置交换机通过SSL连接ACS时需要使用的证书密钥。

## LLDP & LLDP-MED(FP1C)

【功能概述】

链路层发现协议LLDP是一种标准的二层发现方式，可以将本端设备的管理地址、设备标识、接口表示等信息组织成不同的TLV（Type/Length/Value，类型/长度/值），并封装在LLDPDU中，发布给自己的邻居设备，邻居设备收到这些信息后将其以标准的管理信息库MIB的形式保存起来，以供网络管理系统查询及判断链路的通信状况。

工作原理：

1.LLDP模块通过LLDP代理与设备上物理拓扑MIB、实体MIB、接口MIB以及其他类型MIB的交互，来更新自己的LLDP本地系统MIB，以及本地设备自定义的LLDP扩展MIB。

2.将本地设备信息封装成LLDP帧发送给远端设备。

3.接收远端设备发过来的LLDP帧，更新自己的LLDP远端系统MIB，以及远端设备自定义的LLDP扩展MIB。

4.通过LLDP代理收发LLDP帧，设备就很清楚地知道远端设备的信息，包括连接的是远端设备的哪个接口、远端设备的MAC地址等信息。

LLDP本地系统MIB用来保存本地设备信息，包括设备ID、接口ID、系统名称、系统描述、接口描述、网络管理地址等信息。

LLDP远程系统MIB用来保存远端设备信息，包括设备ID、接口ID、系统名称、系统描述、接口描述、网络管理地址等信息。

LLDP代理完成以下任务：（1）维护LLDP本地系统MIB和远程系统MIB；（2）在本地状态发生变化的情况下，提取LLDP本地系统MIB信息并向远端设备发送。在本地设备状态信息没有变化的情况下，按照一定的周期提取LLDP本地系统MIB信息向远端设备发送；（3）识别并处理收到的LLDP帧；（4）LLDP本地系统MIB或远端系统MIB的状态发生变化的情况下，向网管发送LLDP告警。

基本概念：

1.LLDP报文

封装有LLDP数据单元LLDPDU的以太网报文称为LLDP报文。

2.LLDPDU

LLDPDU是封装在LLDP报文数据部分的数据单元。在组成LLDPDU之前，先将本地信息封装成TLV（Type/Length/Value）格式，再由拖杆个TLV组成一个LLDPDU封装在LLDP报文的数据部分进行传送。

3.LLDP工作机制

LLDP的工作模式：每个端口都可以分别配置LLDPDU的接收和发送功能，这样端口可以配置4种工作模式：

* TxRx：既发送也接收LLDP报文
* Tx：只发送不接收LLDP报文
* Rx：只接收不发送LLDP报文
* Disable：既不发送也不接收LLDP报文

当端口的 LLDP 工作模式发生变化时，端口将对协议状态机进行初始化操作。为了避免端口工作模式频繁改变而导致端口不断执行初始化操作，可配置端口初始化延迟时间，当端口工作模式改变时 延迟一段时间再执行初始化操作。

LLDPDU的传输机制：

* 当端口工作在发送接收模式或者只发送模式时，设备会周期性地向邻居设备发送LLDPDU以通告自己的信息。
* 当本地设备发生变化时，设备会发送变化通告。当本地设备在短时间内频繁变化时，为避免设备连续地发送LLDPDU而导致网络阻塞，NMS（Network Management System，网络管理系统）将会设定一个报文发送时延，以确保LLDPDU的发送有一个固定的最小时间差。
* 当端口的工作模式由禁用或者只接收模式切换为发送接收模式或者只发送模式时，该设备的快速启动机制将被激活，报文的发送间隔变为1s，快速发出一些LLDPDU之后，设备恢复正常的发送周期。

LLDPDU的接收机制：当端口工作在发送接收模式或只接收模式时，设备会对收到的LLDP报文及其携带的TLV进行有效性检查，通过检查后再将邻居信息保存到本地，并根据 TTL（Time To Live，生存时间） TLV中TTL的值来设置邻居信息在本地设备上的老化时间，若该值为零，则立刻老化该邻居信息。

4.TLV

TLV是LLDPDU的基本组成单位，是Type/Length/Value的简称，即类型/长度/值。

LLDP可以封装的TLV类型包括基本TLV、802.1组织定义的TLV、802.3组织定义的TLV和媒体终端发现MED TLV。基本TLV是一组对设备进行管理的基础TLV，802.1组织定义的TLV、802.3组织定义的TLV和MED TLV则是由标准组织或其他机构定义的TLV，用于增强对设备的管理功能，可根据实际需要选择是否在LLDPDU中发送。

基本TLV：

|  |  |  |
| --- | --- | --- |
| TLV名称 | 说明 | 是否必须发布 |
| Chassis ID TLV | 发送设备的桥MAC地址 | 是 |
| Port ID TLV | 标识LLDPDU发送端的端口，内容为端口名称 | 是 |
| Time to Live TLV | 本设备信息在邻居设备上的存活时间 | 是 |
| End of LLDPDU TLV | 标志LLDPDU结束 | 是 |
| Port Description TLV | 以太网端口的描述字符串 | 否 |
| System Name TLV | 设备名称 | 否 |
| System Description TLV | 系统描述 | 否 |
| System Capabilities TLV | 系统的主要功能以及有哪些主要功能被使能 | 否 |
| Management Address TLV | 供网管系统标识网络设备并进行管理的地址。管理地址可以明确地标识一台设备，有利于网络拓扑的绘制，便于网络管理 | 否 |

IEEE 802.1组织定义的TLV：

|  |  |
| --- | --- |
| TLV名称 | 说明 |
| Port VLAN ID TLV | 端口VLAN ID |
| Port And Protocol VLAN ID TLV | 端口的协议VLAN ID |
| VLAN Name TLV | 端口VLAN名称 |
| Protocol Identity TLV | 端口支持的协议类型 |

IEEE 802.3组织定义的TLV：

|  |  |
| --- | --- |
| TLV名称 | 说明 |
| EEE TLV | 端口是否支持EEE功能 |
| Link Aggregation TLV | 端口是否支持链路聚合以及是否已使能链路聚合 |
| MAC/PHY Configuration/Status TLV | 端口的速率和双工状态、是否支持端口速率自动协商、是否已使能自动协商功能以及当前的速率和双工状态 |
| Maximum Frame Size TLV | 端口支持的最大帧长度，取端口最大传输单元MTU |
| Power Via MDI TLV | 端口的供电能力，比如是否支持PoE，是供电设备还是受电设备 |

MED TLV：为VoIP提供了许多高级应用，包括基本配置、网络策略配置、地址信息以及目录管理等，满足了语音设备的不同生产厂商在成本有效、易部署性、易管理性等方面的要求，并解决了在以太网中部署语音设备的问题，为语音设备的生产商、销售者以及使用者提供便利。

|  |  |
| --- | --- |
| TLV名称 | 说明 |
| LLDP-MED Capabilities TLV | 当前设备的设备类型以及在LLDPDU中可封装的LLDP-MED TLV类型 |
| Inventory TLV | 设备的制造厂商 |
| Location Identification TLV | 位置标识信息，供其他设备发现设备的位置 |
| Network Policy TLV | Voice VLAN的VLAN ID、二层优先级以及DSCP值等 |
| Extended Power-via-MDI TLV | 当前设备的供电能力 |
| Hardware Revision TLV | 媒体终端ME设备的硬件版本 |
| Firmware Revision TLV | ME设备的硬件版本 |
| Software Revision TLV | ME设备的软件版本 |
| Serial Number TLV | ME设备的序列号 |
| Model Name TLV | ME设备的Model Name |
| Asset ID TLV | ME设备的资产标识符 |

5.管理地址

管理地址是供网络管理系统标识网络设备并进行管理的地址。管理地址可以明确地标识一台设备，从而有利于网络拓扑的绘制，便于网络管理。管理地址被封装在LLDP报文的Management Address TLV中向外发布。

**LLDP-MED：**

LLDP MED是LLDP的增强功能，提供其他功能以支持介质设备。LLDP MED具备功能有：实现实时应用（如语音和/或视频）的网络策略通告和发现；发现设备位置以让用户创建位置数据库，对于IP电话（VoIP）和紧急电话服务（911），则使用IP Phone电话位置信息；获取设备资产清单，了解设备相关信息；获取设备PoE/PSE供电情况信息。

通过LLDP MED实现对Voice VLAN的联动。依据TLV字段中包含的设备类型为IP Phone，交换机应答携带Voice VLAN的ID策略，并依据设备QoS优先级设置Voice VLAN的报文优先级。

【配置参数】

**1. LLDP：**

全局配置：

* LLDP：【开关】设置是否开启交换机的LLDP功能，默认开启。关闭后，需要配置LLDP报文处理机制。
* LLDP处理/LLDP Handling：【单选】当关闭LLDP功能时，交换设备收到LLDP报文的处理方式，选项有{过滤|桥接|泛洪}，默认泛洪。

注：如果开启STP，收到的端口STP功能属于转发或端口处于转发状态，才会生效。

过滤：交换机收到的LLDP报文，不会转给下游设备，直接丢弃。

桥接：交换机收到的报文直接转发给除了入口以外的相同VLAN域的端口。

泛洪：交换机收到的报文直接转发给除了入口以外的端口，不关注VLAN。

* TLV发送间隔 (秒)：【text文本框】设置本地设备向邻居设备发送LLDPDU的时间间隔，取值为5-32767的整数，默认30秒。
* TTL乘数：【text文本框】用于控制本地设备发送的LLDPDU中TTL字段的值，TTL即为本地信息在邻居设备上的存活时间。TTLTTL乘数\*发送间隔。取值为2-10的整数，默认4。
* 端口初始化延迟时间 (秒)：【text文本框】当端口LLDP工作模式改变时，将延迟一段时间再进行初始化，以避免端口LLDP工作模式频繁改变导致端口不断执行初始化。取值为1-10的整数，默认2秒。
* LLDPDU发送延迟时间 (秒)：【text文本框】设置本地设备向邻居设备发送LLDPDU的延迟时间。当本地配置发生变化时，将延迟指定时间再发送LLDPDU通知邻居设备，从而可以变由于本地配置频繁变化而导致LLDPDU的频繁发送。取值为1-8191的整数，默认2秒。

端口设置：

* 端口：选择进行LLDP设置的交换机接口，包括电口和光口。可多选
* 工作模式：【下拉框】设置端口的LLDP工作模式，选项有{发送接收|发送|接收|禁用}，默认发送接收。当选择禁用时，即表示关闭端口的LLDP功能。
* TLV：【多选】配置发送的LLDPDU中需要包含的TLV类型，选项有：
* 可选的基本TLV中有{Port Description TLV| System Name TLV| System Description TLV| System Capabilities TLV| Management Address TLV}
* IEEE 802.1组织定义的TLV中有{Port VLAN ID TLV | VLAN Name TLV}。选择VLAN Name TLV时，VLAN从端口已加入的VLAN中选择，可多选
* IEEE 802.3组织定义的TLV中有{MAC/PHY Configuration/Status TLV| Link Aggregation TLV| Maximum Frame Size TLV| Power via MDI TLV（仅电口支持）}

注：开启Power via MDI TLV，可开启端口的LLDP协商供电功能，将会根据接收到的相应TLV调整端口供电优先级和功率限值。

端口列表：

* 列表显示端口、工作模式、所选的TLV
* 支持编辑，支持多选端口进行批量编辑

**2. LLDP-MED**

全局配置：

* 快速报文个数：【text文本框】当LLDP-MED的快速发送机制启动时，会连续发送指定个数的包含LLDP-MED信息的LLDPDU。取值为1-10的整数，默认3。

MED网络策略：

* 自动语音网络策略：【开关】搭配“自动语音VLAN”模式功能使用，默认关闭。自动语音网络策略的开启与手动添加 应用为“语音”的网络策略互斥。

手动添加网络策略：

* \*策略ID：【text文本框】设置MED网络策略的ID，取值为1-32的整数。
* 应用：【下拉框】设置LLDP MED TLV发布的语音类型能力及内容值，选项有{语音| 语音信号| 访客语音| 访客语音信号| 软件电话语音| 视频会议| 流媒体视频| 视频信令}，默认语音。
* VLAN：【text文本框】设置需要发布指定语音的VLAN ID，取值为1-4094的整数。
* VLAN Tag：【下拉框】设置发布的VLAN Tag的属性，选项有{Tagged|Untagged}，默认Tagged。
* CoS：【下拉框】设置CoS（802.1p）优先级，选项有{0|1|2|3|4|5|6|7}，默认0。
* DSCP：【下拉框】设置DSCP优先级，选项有{0|1|2|3|…|63}，默认0。

策略列表：

* 列表显示策略ID、应用、VLAN、VLAN Tag、CoS、DSCP
* 支持添加，至多32条
* 支持编辑
* 支持删除单条/批量/全部策略。一旦网络策略被端口绑定，则无法删除，必须先解绑。

端口设置：

* 端口：选择需要配置MED的交换机接口，包括电口和光口。可多选
* LLDP MED：【开关】设置是否开启端口的LLDP MED功能。默认开启
* TLV：【可多选】配置发送的报文中需要包含的LLDP MED TLV类型，选项有{Network Policy TLV| Inventory TLV| Location Identification TLV| PoE-PSE TLV（仅电口支持） }，默认Network Policy TLV。

注：开启PoE-PSE TLV，可开启端口的LLDP协商供电功能，将会根据接收到的相应TLV调整端口供电优先级和功率限值。

* 网络策略：【可多选，也可不选】当且仅当选择Network Policy TLV时支持配置。从已有的网络策略中选择

注：支持选择不同应用类型的网络策略，但同一类型的有且仅能选择一个。

* 位置：当且仅当选择Location Identification TLV时支持配置。设置MED位置的配置信息
* 坐标/Coordinate：【text文本框】设置位置坐标，如经纬度、海拔等，必须以十六进制形式输入，且为16对
* 城市地址/Civic Address：【text文本框】设置具体的城市地址，如城市名称、邮政编码、街道、地标等，必须以十六进制形式输入，且为6-160对
* 紧急电话号码/ECS ELIN：【text文本框】设置紧急呼叫服务（ECS）ELIN。必须以十六进制形式输入，且为10-25对

端口列表：

* 列表显示端口、LLDP MED、Network Policy TLV及其应用、Location TLV、Inventory TLV、PoE-PSE TLV
* 支持编辑，可选多个端口进行批量编辑

**3. 设备信息**

本地设备信息：

* Chassis ID Subtype/机箱ID子类型：机箱ID的类型（如MAC地址）
* Chassis ID/机箱ID：机箱的标识符，如果机箱ID子类型为MAC地址，则显示设备MAC地址
* System Name/系统名称：设备名称
* System Description/系统说明：设备说明（采用字母数字格式）
* Supported Capabilities/支持的系统功能：设备的主要功能如网桥、路由器或WLAN AP
* Enabled Capabilities/已启用的系统功能：设备主要已启用功能
* Port ID Subtype/端口ID子类型：显示端口标识符的类型，通常为本地

本地端口信息：

每个端口（包括电口和光口）支持查看LLDP信息和LLDP-MED信息，具体信息包括但不限于下述内容：

注：每个端口信息存在差异，建议直接以大文本框形式直接显示相关内容。

* 基本TLV信息
* Chassis ID Subtype/机箱ID子类型：机箱ID的类型（如MAC地址）
* Chassis ID/机箱ID：机箱的标识符，如果机箱ID子类型为MAC地址，则显示设备的MAC地址
* System Name/系统名称：设备名称
* System Description/系统说明：设备说明（采用字母数字格式）
* Supported Capabilities/支持的系统功能：设备的主要功能如网桥、路由器或WLAN AP
* Enabled Capabilities/已启用的系统功能：设备主要已启用功能
* Port ID Subtype/端口ID子类型：显示端口标识符的类型
* Port ID/端口ID：端口的标识符
* Port Description/端口说明：有关端口的信息，包括制造商、产品名称和硬件/软件版本
* Management Address列表：包括
  + Address Subtype/地址子类型：管理IP地址类型，如IPv4
  + Address/地址：管理IP地址
  + Interface Subtype/接口子类型：用于定义接口编号的编号方法
  + Interface Number/接口号：管理地址关联的特定接口

或

* + IPv4地址：交换机管理IPv4地址
  + IPv6全球地址：交换机的IPv6全球地址
  + IPv6本地地址：交换机的IPv6本地链路地址
* IEEE 802.1组织定义的TLV信息
* PVID：端口PVID
* VLAN ID：端口的VLAN ID
* VLAN Name/VLAN名称：端口VLAN ID对应的名称
* IEEE 802.3组织定义的TLV信息
* MAC/PHY：包括
* Auto-Negotiation Supported/支持自动协商：端口速率自协商支持状态
* Auto-Negotiation Enabled/已启用自动协商：端口速率自协商活动状态
* Auto-Negotiation Advertised Capabilities/自动协商通告功能：端口速率自协商功能，如1000BASE-T半双工模式
* Operational MAU Type/运营MAU类型：中型附件单元（MAU）类型。MAU执行物理层功能，包括从以太网接口的冲突检测和比特注入到网络中的数字数据转换，如100BASE-T全双工模式
* Maximum Frame Size/最大帧大小：支持的IEEE 802.3最大帧大小
* Link Aggregation/链路聚合：包括
  + Aggregation Capability/链路聚合能力：表示接口是否支持链路聚合
  + Aggregation Status/链路聚合状态：表示接口是否已聚合
  + Aggregation Port ID/聚合端口ID：显示聚合接口ID
* Extended Power Via MDI/通过MDI供电：显示网络设备或终端设备的扩展供电能力，包括
  + MDI Power Support Port Class/MDI电源支持端口类别：显示电源支持端口类别
  + PSE MDI Power Support/PSE MDI电源支持：表示端口是否支持MDI电源
  + PSE MDI Power State/PSE MDI电源状态：表示端口上是否启用MDI电源
  + PSE Power Pair Control Ability/PSE电源对控制能力：表示端口是否支持电源对控制
  + PSE Power Pair/PSE电源对：端口支持的电源对控制类型
  + PSE Power Class/PSE电源类别：显示端口的电源类别
  + Power Type/电源类型：连接到端口的Pod设备类型
  + Power Source/电源：端口电源
  + Power Priority/电源优先级：端口电源优先级
  + PD Requested Power Value/PD请求功率值：PSE分配给PD的功率
  + PSE Allocated Power Value/PSE分配的功率值：分配给源设备（PSE）的功率
* MED TLV信息
* Capabilities Supported/支持的功能：端口支持的MED功能
* Current Capabilities/当前功能：端口上启用的MED功能
* Device Class/设备类别：LLDP-MED终端设备类，可能为通用终端类、媒体终端类、通信设备类
* PoE供电信息：包括
  + PoE Device Type/PoE设备类型：端口PoE类型，如PD
  + PoE Power Source/PoE电源：端口电源
  + PoE Power Priority/PoE电源优先级：端口电源优先级
  + PoE Power Value/PoE功率值：端口功率
* Hardware Revision/硬件修订版：硬件版本
* Firmware Revision/固件版本
* Software Revision/软件修订版：软件版本
* Serial Number/序列号：设备SN序列号
* Manufacturer Name/制造商名称：设备制造商名称
* Model Name/型号名称：设备型号名称
* Asset ID/资产ID
* Location：包括
  + Civic Address/城市地址
  + Coordinate/坐标
  + ECS ELIN/紧急电话号码
* Network Policy列表：包括
  + Application Type/应用类型
  + VLAN ID
  + VLAN Tag/VLAN 类型：分为已标记和无标记
  + CoS
  + DSCP

邻居信息：

显示交换机端口上获取到的邻居。支持点击端口查看其上的邻居信息，主要包括：

注：每个端口的邻居信息存在差异，建议直接以大文本框形式直接显示相关内容。

* 本地端口：显示交换机本地端口，包括电口和光口，以接口名称显示
* Time to Live
* 邻居基本信息
* Chassis ID Subtype /机箱ID子类型：机箱ID的类型（如MAC地址）
* Chassis ID /机箱ID：机箱的标识符，如果机箱ID子类型为MAC地址，则显示设备的MAC地址
* Port ID Subtype /端口ID子类型：显示端口标识符的类型
* Port ID /端口ID：端口的标识符
* Port Description /端口说明：有关端口的信息，包括制造商、产品名称和硬件/软件版本
* System Name /系统名称：设备名称
* System Description /系统说明：设备说明（采用字母数字格式）
* Supported Capabilities /支持的系统功能：设备的主要功能如网桥、路由器或WLAN AP
* Enabled Capabilities /已启用的系统功能：设备主要已启用功能
* Management Address列表：包括
  + Address Subtype /地址子类型：管理IP地址类型，如IPv4
  + Address/地址：管理IP地址
  + Interface Subtype /接口子类型：用于定义接口编号的编号方法
  + Interface Number/接口号：管理地址关联的特定接口
* IEEE 802.1组织定义的TLV信息
* PVID：端口PVID
* PPVIDs：包括
  + VID：协议VLAN ID
  + Supported/支持：支持的端口和协议VLAN ID
  + Enabled/已启用：已启用端口和协议VLAN ID
* VLAN IDs：包括
  + VID：端口和协议VLAN ID
  + VLAN Name/VLAN名称：显示VID对应的名称
* Protocol IDs/协议ID
* IEEE 802.3组织定义的TLV信息
* MAC/PHY：包括
  + Auto-Negotiation Supported/支持自动协商：端口速率自协商支持状态
  + Auto-Negotiation Enabled/已启用自动协商：端口速率自协商活动状态
  + Auto-Negotiation Advertised Capabilities/自动协商通告功能：端口速率自协商功能，如1000BASE-T半双工模式
  + Operational MAU Type/运营MAU类型：中型附件单元（MAU）类型。MAU执行物理层功能，包括从以太网接口的冲突检测和比特注入到网络中的数字数据转换，如100BASE-T全双工模式
* Maximum Frame Size /最大帧大小：支持的IEEE 802.3最大帧大小
* Link Aggregation/链路聚合：包括
  + Aggregation Capability/链路聚合能力：表示接口是否支持链路聚合
  + Aggregation Status/链路聚合状态：表示接口是否已聚合
  + Aggregation Port ID/聚合端口ID：显示聚合接口ID
* Power via MDI /通过MDI供电：包括
  + MDI Power Support Port Class/MDI电源支持端口类别：显示电源支持端口类别
  + PSE MDI Power Support/PSE MDI电源支持：表示端口是否支持MDI电源
  + PSE MDI Power State/PSE MDI电源状态：表示端口上是否启用MDI电源
  + PSE Power Pair Control Ability/PSE电源对控制能力：表示端口是否支持电源对控制
  + PSE Power Pair/PSE电源对：端口支持的电源对控制类型
  + PSE Power Class/PSE电源类别：显示端口的电源类别
  + Power Type/电源类型：连接到端口的Pod设备类型
  + Power Source/电源：端口电源
  + Power Priority/电源优先级：端口电源优先级
  + PD Requested Power Value/PD请求功率值：PSE分配给PD的功率
  + PSE Allocated Power Value/PSE分配的功率值：分配给源设备（PSE）的功率
* MED信息
* Capabilities Supported /支持的功能：端口支持的MED功能
* Current Capabilities /当前功能：端口上启用的MED功能
* Device Class /设备类别：LLDP-MED终端设备类，可能为通用终端类、媒体终端类、通信设备类
* PoE供电信息：包括
  + PoE Device Type/PoE设备类型：端口PoE类型，如PD
  + PoE Power Source/PoE电源：端口电源
  + PoE Power Priority/PoE电源优先级：端口电源优先级
  + PoE Power Value/PoE功率值：端口功率
* Hardware Revision /硬件修订版：硬件版本
* Firmware Revision /固件版本
* Software Revision /软件修订版：软件版本
* Serial Number /序列号：设备SN序列号
* Manufacturer Name/制造商名称：设备制造商名称
* Model Name /型号名称：设备型号名称
* Asset ID /资产ID
* Location：包括
  + Civic Address/城市地址
  + Coordinate/坐标
  + ECS ELIN/紧急电话号码
* Network Policy列表：包括
  + Application Type/应用类型
  + VLAN ID
  + VLAN Tag/VLAN 类型：分为已标记和无标记
  + CoS
  + DSCP

**4. 数据统计**

数据统计表：

* 列表显示端口，发送报文总数，接收的报文总数、丢弃数和错误数，接收的丢弃TLV数和未知TLV数、超时邻居数
* 支持刷新
* 支持清空指定端口的统计数据

## 节能管理/Energy Saving Management

节能管理中支持的特性包括：

* 风扇智能调速：采用智能风扇调速策略，监测设备关键器件温度。当设备内部温度敏感器件高于设定值时增加风扇转速，当设备内部温度敏感器件温度均低于设定值时则降低转速，最终控制设备保持在稳定的温度状态中，达到节能目的。具体策略详见[*16.风扇*](#_风扇/Fan(FP1D))。
* 激光器自动关断ALS：通过检测光口的LOS信号来控制光模块激光器的发光。ALS功能为用户提供安全保护的同时，也能为用户减少能源消耗。未使能ALS功能：当接口光纤不在位或光纤链路发生故障时，虽然数据通信中断，但设备的光接口没有被关闭，光模块激光器的发光功能是打开的。光模块激光器在数据通信中断时的持续发光不仅造成能源的浪费，激光射入人眼也会造成一定危害。使能ALS功能：当接口光纤不在位或光纤链路故障时，系统检测到光口的LOS信号后，将自动关闭光模块激光器；当接口插上光纤或光纤链路恢复后，系统检测到光口的LOS信号被清除，则会自动打开光模块激光器。
* 节能以太网EEE：一种根据网络流量动态调节电接口功率的节能方法。没有配置电接口的功率自调节功能时，系统以一定的功率为每个接口供电，即使接口处于业务空闲状态，也需要消耗同样的能量。配置电接口的功率自调节功能后，当接口处于业务空闲状态时，系统将会自动降低给该接口的供电，这样能够节省系统的总体能耗；当接口开始正常传输数据时，则恢复正常供电。
* 端口休眠：电口物理层芯片一种低功耗的工作状态。在没有网络连接的情况下，芯片的主要数据传输通道都会进入休眠状态，从而实现节能。当端口有网络连接且线缆上能量被检测到时，芯片正常开启。
* 设备休眠：设备的最低功耗工作状态，设备除CPU工作外其它芯片都进入到节能模式。可以通过设定休眠时间段定时唤醒或用户有输入信息时唤醒设备，使设备快速响应进入到正常使用模式。
* 节能模式：支持通过设置节能模式实现节能。具体有如下几种：
* 标准节能模式，即出厂模式，设备运行过程默认启用的节能技术。此时，ALS、EEE和端口休眠功能默认关闭。
* 基本节能模式，未配置业务或用户不在线时，对相关未用器件启用关闭、休眠操作。此时，ALS、EEE和端口休眠功能默认开启。
* 深度节能模式，对正常业务启动动态能耗调节，根据业务情况自动调整，对相关未用器件启用关闭、休眠操作。此时，ALS、EEE和端口休眠功能默认开启。
* Standby节能模式，不需要给PD进行PoE供电，进入低功耗工作状态，并关闭接口。若要开启接口，必须手动退出Standby模式。

本期暂仅支持绿色以太网功能。

### 节能以太网/EEE(FP1D)

【功能概述】

802.3az 节能以太网EEE功能，可在端口处于启用状态但没有流量时降低功耗。EEE仅电口支持。

EEE支持IEEE 802.3 MAC操作，速度为100Mbps和1000Mbps，即若端口协商速率为10Mbps时不支持EEE功能。

LLDP用于为两台设备选择最佳参数。如果端口链路不支持LLDP或已关闭LLDP，EEE仍可运行，但可能不会处于最佳运行模式。802.3az EEE TLV可查看相关本地和远程的EEE信息。

EEE功能通过交换机使用端口低功耗空闲LPI模式进行实现。若端口上没有流量但开启了此功能，则端口将被置于可大幅降低功耗的LPI模式。

EEE功能必须两端（交换机端口和连接终端）均支持才能运行生效。

自协商阶段，连接的设备可以检测链路另一端设备的支持程度，并配置自身设置以进行联调。但若端口上未开启自协商，EEE功能将被禁用。例外情况：如果链路速率达到1000Mbps，即使关闭自协商，EEE功能仍处于开启状态。

【配置参数】

**端口设置：**

* 端口：选择需要设置节能以太网功能的交换机接口，只包含电口。可多选
* 802.3 EEE：【开关】当且仅当全局EEE功能开启时支持配置。设置是否开启端口的EEE功能，默认关闭。

端口列表：

* 列表显示端口、802.3 EEE（配置状态）、802.3EEE（运行状态）
* 支持编辑

# 系统/System

## 基础设置/Basic Settings

【功能概览】

支持设备的基本系统配置，包括设备名称、系统位置、系统联系人、系统时间。系统时间是交换机工作时使用的时间，可以选择手动设置或自动同步NTP服务器的时间，也可以选择获取当前管理PC的时间作为交换机的系统时间，即为手动设置时间选择窗中的“此刻”。

【配置参数】

* \*设备名称：设置交换机名称，默认显示交换机型号，如GWN7811。允许输入最长64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示
* 系统位置：【text文本框】设置交换机实际所在的位置信息。允许输入最长64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示
* 系统联系人：【text文本框】设置交换机的联系人。允许最长64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示

系统时间：显示当前系统的日期和时间。

* 日期和时间：选择系统日期和时间的配置方式，选项有{手动设置|自动同步NTP服务器}，默认自动同步NTP服务器。
* 手动设置：需要设置具体日期（年月日）和时间（时分秒），支持直接选择“此刻”引用当前管理PC的时间来设置
* 年：2000-2035的整数
* 月：1-12的整数
* 日：1-31 的整数
* 时：0-23的整数
* 分：0-59的整数
* 秒：0-59的整数
* 自动同步NTP服务器：需要设置NTP服务器地址，默认pool.ntp.org
* 时区：选择系统所需要使用的时区。默认UTC（Universal Time Coordinated）时区
* 夏令时(FP2)：根据需要选择夏令时调整时钟，选项有{禁用|欧洲|美国|绝对夏令时|周期夏令时}，默认禁用。若开启，则需要配置如下：
* 偏移 (分钟)：【text文本框】当且仅当夏令时设置为非“禁用”选项时支持配置。设置当夏令时来临时，需要调整的时间额度，取值范围为1-1440的整数，默认60。

当选择“欧洲”时，默认3月最后一个星期天02:00至10月最后一个星期天02:00执行夏令时。

当选择“美国”时，默认3月第2个星期天02:00至11月第1个星期天02:00执行夏令时。

当选择“绝对夏令时”时，需要配置具体起始日期与时间：

* 开始：需要配置开始的年-月-日、时-分-秒
* 结束：需要配置结束的年-月-日、时-分-秒

当选择“周期夏令时”时，需要配置起始周期与时间：

* 开始：需要配置开始的第X月(X:1-12)、第Y个(Y:1-5)、星期几(星期一至星期日)、时-分-秒
* 结束：需要配置结束的第X月(X:1-12)、第Y个(Y:1-5)、星期几(星期一至星期日)、时-分-秒

交换机支持定时重启。通过选择某一个指定的时间策略，在时间策略的时间内随机选择一个时间点进行重启。

* 重启计划：【下拉框】设置重启生效的时间段，选项为{关闭|已存在的时间策略}，支持弹窗新建时间策略，具体配置详见[*系统→时间策略*](#_时间策略/Time_Policy_(FP1D))。默认关闭，即仅支持手动重启。

## 登录服务/Login Service

### ~~管理IP地址/Management IP Address~~ (FP1B) 【去除，不再支持20221122】

~~设备支持设置管理IP地址，作为设备Web访问地址。~~

~~管理IP地址默认采用缺省VLAN接口(VLAN 1)地址作为初始设备访问地址。~~

~~【配置参数】~~

* ~~管理VLAN：选择对应已存在的VLAN接口作为管理VLAN。缺省值为VLAN 1。~~

~~IPv4地址：设置管理VLAN使用的IPv4地址。~~

* ~~IPv4地址类型：设置IPv4地址的获取方式，选项有{DHCP|静态IP}，默认DHCP。~~
* ~~静态IP~~
* ~~\*IPv4地址：设置管理IPv4地址，输入格式为xxx.xxx.xxx.xxx(x：0-255)，以点分十进制形式表示。若输入格式错误，则提示“您输入的格式错误，请重新输入”。默认192.168.0.254。~~

~~注：管理IPv4地址不能与VLAN接口的IP网段相同，否则需要报错提示“IP地址网段已被其他VLAN接口使用，请重新输入”。~~

* ~~\*子网掩码：按照IPv4地址格式点分十进制输入~~
* ~~\*默认网关：按照IPv4地址格式点分十进制输入~~
* ~~DHCP：自动获取分配的IPv4地址。~~

~~注：若设备未接入DHCP，则可以使用192.168.0.254登录；若接在了DHCP服务器下，则需要以DHCP获取到的IP进行登录。~~

~~IPv6地址：配置管理VLAN使用的IPv6地址~~

* ~~IPv6地址类型：设置IPv6地址的获取方式，选项有{无状态自动配置|DHCP自动获取|静态IPv6}，默认无状态自动配置。~~
* ~~无状态自动配置：根据RA前缀自动生成全球单播地址。~~
* ~~静态IPv6：~~
* ~~IPv6地址：设置IPv6地址，按IPv6的冒号十六进制格式(IPv6地址共128bit，每16bit为一段，段之间用“:”分隔)输入IPv6地址，否则需要提示“您输入的IP地址格式错误，请重新输入”。管理IPv6地址不能与VLAN接口的IPv6地址网段相同，否则需要报错提示“IPv6地址网段已被其他VLAN接口使用，请重新输入”。~~
* ~~\*IPv6地址：以冒号十六进制形式设置管理VLAN的IPv6地址，若格式错误需要报错提示“您输入的IPv6地址格式不正确，请重新输入”。不同的VLAN接口，IPv6地址不能相同。~~
* ~~\*前缀长度：输入范围为1-128的整数，默认64。~~
* ~~\*默认网关：设置IPv6地址的网关地址，以IPv6地址格式输入。~~
* ~~DHCP：通过DHCPv6自动获取分配的IPv6地址。~~

~~注：若IP地址修改，保存时，需提示“IP地址变更，需要重新登录，确认修改？”，点击<确定>进行保存，并自动退出登录，用户需重新在浏览器输入新的管理IP地址进行访问。~~

### 访问控制/Access Control

交换机仅支持HTTPS浏览器登录访问，也支持Telnet、SSH访问。若使用HTTP方式访问Web，自动跳转至HTTPS方式。

支持设置Web闲置超时时间。

支持开启SSH远程访问功能。

交换机支持公有云GWN.Cloud和私有云GWN Manager的集中管理。(FP1D)

【配置参数】

Web服务管理：

* \*HTTPS端口：设置HTTPS端口，取值范围为443和1024-65535，默认443。
* Web闲置超时时间(分钟)：设置Web闲置时间，取值范围为1-1440分钟，默认15分钟。
* Telnet：设置是否允许Telnet方式访问交换机，默认关闭。
* SSH：设置是否允许SSH方式访问交换机，默认开启。
* SSH端口：【text文本框】设置SSH端口号，取值范围为22和1024-65535，默认22。

SSH/Telnet Client功能(FP1D)：

规格：838X芯片，同时支持4个；93XX芯片，同时支持8个

开启SSH/Telnet Client功能后，可以直接在交换机上通过SSH远程管理GWN系列设备，包括交换机、路由器和AP。鉴于管理配置的复杂性，考虑仅在CLI中进行支持。

前提：只有开启了SSH/Telnet功能，才可以开启SSH/Telnet Client功能。

开启后，通过在CLI中输入GWN设备的IP和管理密码或公钥/私钥，即可进行设备管理配置。路由器和AP进入的是gwnmenu，交换机仍是CLI命令行。

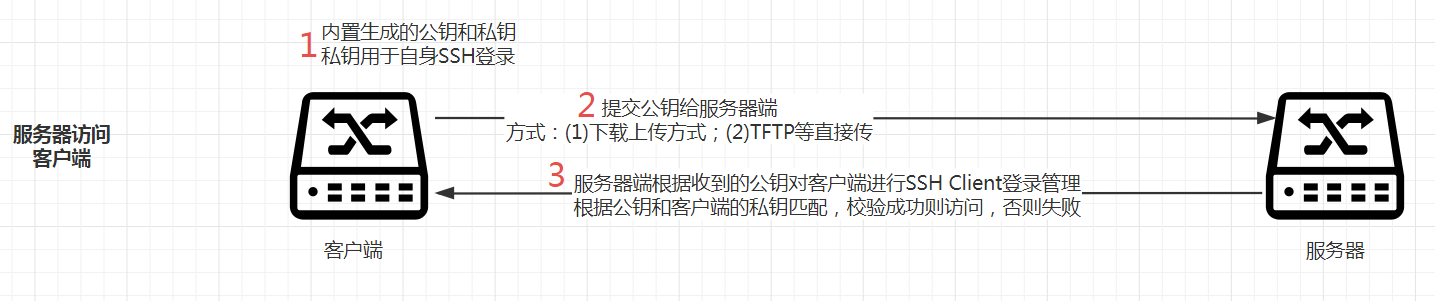
交换机支持设备管理密码和公有key。

1.设备管理密码方式

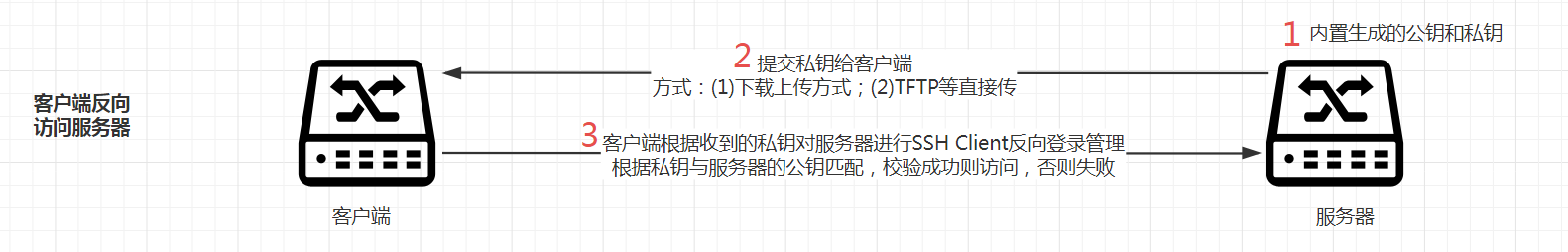
开启SSH Client后，选择简单密码方式，在CLI中输入GWN设备的IP和管理密码，即可进行设备管理配置。

2.公有Key方式

（1）GWN设备本地默认生成有密钥对（公钥和私钥），下载公钥证书或复制公钥并提交至相应服务器。设备开启SSH Client后，服务器利用设备IP地址和公钥对设备进行访问；公钥和设备上的私钥匹配校验通过后，方可进行设备管理配置。



（2）交换机本地默认生成有密钥对（公钥和私钥），下载私钥证书或复制私钥，提交至相应客户端（例如PC）。交换机开启SSH Client后，客户端可以通过设备IP地址和私钥对设备进行反向访问；私钥和设备上的公钥匹配校验通过后，方可进行设备管理配置。



~~由于GWN设备暂不支持公有key，暂不开放利用公有key的方式进行校验，仅支持使用设备管理密码。~~

SSH远程访问功能(FP1D)：

SSH远程访问功能。一旦开启，可以获取到设备公网IP和端口，用户可以通过任一一种SSH客户端软件进行连接访问，同时也会自动在cloud的admin管理平台上允许访问，内部开发人员可以直接通过此种形式访问用户设备进行问题查验。

* SSH远程访问：【开关】默认关闭。若要开启，需输入设备管理密码，即admin密码。
* 密码：输入设备管理密码。

保存后，校验密码正确性。验证通过后，用户可远程访问设备。访问有效期为48小时，开启后48小时自动关闭SSH远程访问。

交换机支持云管理(FP1D)。其中，针对Manager的管理，支持二层发现和三层发现。云管理的相关规则如下：

1. Cloud和Manager管理逻辑：

（1）Manager服务器将发送广播包给局域网内的所有交换机设备。支持多个Manager同时发送广播请求，交换机收到以后，将会携带上自己的信息响应请求，在Manager发现界面上即可呈现交换机信息（包括设备型号、MAC地址、固件版本、IP地址等，具体显示信息以Manager需求为准）。

（2）同局域网内可能存在多个Manager服务器，支持被多个Manager同时发现，但有且仅能被一个Manager接管/Cloud添加。

（3）若被Cloud添加或Manager接管，则其他Manager无法继续发现，其他Cloud也无法继续添加，必须先从Manager/Cloud侧删除确保其为非管状态。

（4）支持被指定的Manager服务器发现并接管，即Manager三层发现功能。此时，若先前已被二层Manager/Cloud管理，将会自动断开连接，设备列表显示离线。若后续关闭Manager三层发现，可重新被Manager/Cloud管理，设备列表显示在线。反之，亦然。

（5）交换机还支持跨VLAN被Manager服务器发现，即Manager三层发现，确保将网络环境中的交换机均接管到Manager上进行管理。

2. 管理优先级：

Manager三层发现>Cloud=Manager二层发现

三层发现需要本地提供Manager服务器的相关配置，支持用户手动配置，也支持Option 43下发，优先使用Option 43携带的Manager地址信息。

一旦开启Manager设置，则仅支持指定的Manager可以发现并管理交换机。

当且仅当Manager设置关闭时，支持Manager二层发现。

Manager设置：

* 启动DHCP选项43设定Manager服务器：【开关】设置是否开启Option43选项来覆写Manager服务器，默认开启。一旦开启，交换机将会从DHCP Option43中获取Manager地址，且无法手动修改，即Manager地址和端口禁用编辑。
* Manager服务器设置：【开关】设置是否开启GWN Manager服务器的配置，默认关闭。开启后，进行如下设置：
* \*Manager地址：【text文本框】设置Manager服务器地址，默认为空
* \*Manager端口：【text文本框】设置Manager服务器使用的端口，取值范围为1-65535的整数，默认8443

## 用户管理(FP1B)

【功能概述】

管理员根据管理需要，对登录交换机的用户进行认证和授权。细化用户管理，每个用户具有不同的权限与密码，默认可以使用console访问交换机，Web端默认支持使用HTTPS方式访问，其余Telnet、SSH访问方式支持与否取决于[***8.2.2访问控制***](#_访问控制/Access_Control)。每个用户最多允许在9个主机站点上登录Web，超过后无法登录，需提示“当前登录数已达限额，无法登录”。

用户共有3种等级，分别为administrator、operator和monitor。

* administrator
  + - 每台设备有且仅有1个administrator
    - 管理权限：权限最高，可执行任何命令
    - 不能修改用户名admin，仅支持修改密码
    - 支持增删~~改~~低级别的用户，包括operator和monitor
* Operator
* 由administrator添加，可有多个
* 管理权限：权限第二高，可执行除administrator关键操作和重要强制命令外的所有命令，不支持恢复出厂
* 不能修改自己的用户名，仅支持修改密码
* 支持增删~~改~~低级别的用户monitor
* monitor
* 由administrator/operator添加，可有多个
* 管理权限：权限最低，仅能查看交换机状态与统计信息，没有任何执行和配置权限
* 不能修改自己的用户名，仅支持修改密码

【配置参数】

添加用户：

* \*用户名：【text文本框】设置用户名名称。允许输入最长64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示
* \*密码：【text文本框，加密】设置密码。允许输入最长32字符，最小8字符，允许输入的字符由数字0-9、英文字符a-z/A-Z和特殊字符~~()<>,./’”;:[]{}\|=+-\_\*&^%$#@!~`（键盘半角全部支持，无需做特殊说明）~~
* \*确认密码：【text文本框，加密】重复上述密码，若不一致则提示“密码不一致，请重新输入”
* 用户等级：【单选】设置用户级别，选项有{ operator| monitor}。

注：需要对每个用户等级的权限进行说明。

用户列表：最多16个用户

* 显示用户名、用户等级、创建者、创建时间
* 支持删除单个/多个/全部用户（其中，不包含初始管理员用户）

注：1.administrator可以查看所有用户；

2.operator仅能查看自己与monitor用户；

3.monitor无用户管理模块。

## 时间策略/Time Policy (FP1D)

支持创建以周为单位的周期性时间策略，也支持创建以特殊节假日时间段的时间策略。时间策略可以用于PoE、ACL、重启和升级等功能模块。

允许最多添加32条时间策略。

【配置参数】

* 时间策略：设置时间策略的名称，限制长度为64字符，支持的字符为ASCII 0x20~0x7E，但不包含"\?/,这5项，不支持字符以报错形式提示。时间策略名称具有唯一性。
* 周期时间设置：
* 提供周期时间表，按照星期日、星期一、星期二、星期三、星期四、星期五、星期六，每天24小时，以半小时为间隔。由用户自主选择时间。
* 特殊时间设置：支持添加多条，至多8条，每条中日期不能重复，日期需显示法定节假日信息
* 日期：按年-月-日，只能选择今天及以后的日期，可多选。
* 时间：每天24小时，以半小时为间隔，由用户自主选择，可多选。

注：1.单条特殊时间设置里，每天的生效时间均相同；

2.同一天内，周期时间和特殊时间均有配置，优先生效特殊时间。

时间策略列表：

* 列表显示时间策略名称、点击支持查看详情
* 支持编辑和删除未被引用的时间策略
* 被引用的时间策略不能删除，且还需提示被引用的模块

## 1588v2 TC(FP2)

【功能概述】

精确时钟同步协议PTP（Precision Time Protocol）是一种对标准以太网终端设备进行时间和频率同步的协议，其本身只是用于设备之间的高精度时间同步，但也可用于设备之间的频率同步。

GWN78XX交换机仅支持1588v2协议。

1588协议是由IEEE定义的精确时间同步标准，分为1588v1和1588v2两个版本，1588v1只能达到亚毫秒级的时间同步精度，而1588v2可以达到亚微秒级同步精度。

**时钟同步原理**：应用网络时钟同步的网络，称为时钟同步网。时钟同步网分为2级，1级节点采用1级时钟同步设备，2级节点采用2级时钟同步设备，2级节点以下是客户端设备，即需要时钟同步的设备。

客户端时间同步链路是时钟同步网节点至客户端的时钟同步链路，因为这段链路需进行包括以太网时钟同步、NTP在内的多种同步方式，它包括NTP传送方式在内的各种传输链路。节点时间同步链路是时钟同步网节点之间的时钟同步链路，它包括除NTP传送方式以外的各种传输链路，主要采用DCLS传送方式的专线链路。

整个PTP网络中，所有时钟都会按照主从层次关系组织在一起，系统的最优时钟Grandmaster向各节点逐级同步时钟。整个同步的过程是通过交换PTP报文来完成的。从时钟通过PTP报文中携带的时间戳信息计算与主时钟之间的**偏移**和**延时**，据此调整本地时钟达到与主时钟的同步。

**PTP基本概念：**

（1）PTP域：应用了PTP协议的网络称为PTP域。网络中可能含有多个PTP域，PTP域是独立PTP时钟同步系统，一个PTP域内有且仅有一个时钟源，域内的所有设备都与该时钟源保持同步。

（2）1588v2时钟节点：PTP域中的节点称为时钟节点，PTP协议定义了三种类型的基本时钟节点：

* 普通时钟OC(Ordinary Clock)：同一个PTP域内，只存在单个物理端口参与PTP时间同步，设备通过该端口从上游节点同步时间，或者向下游节点发布时间；
* 边界时钟BC(Boundary Clock)：同一个PTP域内，可以存在两个或以上物理端口参与PTP时间同步，其中一个端口从上游设备同步时间，其余多个端口向下游设备发布时间。此外，当时钟节点作为时钟源，同时通过多个PTP端口向下游时钟节点发布时间，也称其为BC；
* 透传时钟TC(Transparent Clock)：TC有多个PTP端口，它只是在这些PTP端口之间转发PTP报文，对其进行转发时延校正，并不从任何一个端口同步时间。TC与OC、BC最大的不同是BC和OC都要保持本设备与其他设备的时间同步，但TC不需要。

（3）GWN78XX交换机支持的1588v2时钟类型

* 普通时钟OC
* 边界时钟BC
* Delay机制透传时钟E2ETC(End to End Transparent Clock)：一种延迟测量机制已经确定为Delay方式的透传时钟，使用时，不需要再配置设备的延迟测量机制类型
* Pdelay机制透传时钟P2PTC(Peer to Peer Transparent Clock)：一种延迟测量机制已经确定为pdelay的透传时钟，使用时，不需要再配置设备的延迟测量机制类型
* Delay机制透传时钟和普通时钟E2ETCOC：一种特殊的TC节点，其在时间同步方面和TC节点相同，但额外增加了根据PTP报文同步频率，实现与上游节点频率同步的功能。其中用作TC功能的端口使用Delay方式的延迟测量机制
* Pdelay机制透传时钟和普通时钟P2PTCOC：同上，其中用作TC功能的端口使用Pdelay方式的延迟测量机制
* 透传边界时钟TCandBC：设备的部分PTP端口用作BC功能，同步其他时钟，或向其他设备同步时钟，另有部分PTP端口用作TC功能，仅传输PTP报文，不进行延迟计算

（4）PTP端口

设备上运行了PTP协议的端口称为PTP端口，按角色可以分为3种：

* Master Port/主端口：发布同步时间的端口，可存在于T-BC、BC或OC上
* Slave Port/从端口：接收同步时间的端口，可存在于T-BC、BC或OC上
* Passive Port/被动端口：不接收同步时间，也不对外发布同步时间，闲置备用的端口，只存在于T-BC或BC上。该状态主要用于防止时钟成环

（5）主从关系

PTP域的节点设备按照一定的主从关系（Master-Slave）进行时钟同步。主从关系是相对而言的，同步时钟的节点设备称为从节点，发布时钟的节点设备称为主节点，一台设备可能同时从上层节点设备同步时钟，然后向下层节点设备发布时钟。对于相互同步的一对时钟节点来说，存在如下主从关系：

* 发布同步时间的节点称为主节点，接收同步时间的节点称为从节点
* 主节点上的时钟称为主时钟，从节点上的时钟称为从时钟
* 发布同步时间的端口称为主端口，接收同步时间的端口称为从端口

（6）最优时钟

PTP域中所有的时钟节点都按一定层次组织在一起，整个域的参考时钟就是最优时钟GMC(Grandmaster Clock)，即最高层次的时钟。通过各时钟节点间PTP报文的交互，最优时钟的时间最终将被同步到整个PTP域中，因此也称其为时钟源。最优时钟可以通过手动配置静态指定，也可以通过最优主时钟BMC算法动态选举。

（7）PTP报文

PTP通过主从节点间交互报文，实现主从关系的建立、时间和频率同步。根据报文是否携带时间戳，可以将PTP报文分为两类：

* 事件报文：时间概念报文，进出设备端口时打上精确的时间戳，PTP根据事件报文携带的时间戳，计算链路延迟。事件报文包含4种：Synv、Delay\_Req、Pdelay\_Req和Pdelay\_Resp
* 通用报文：非时间概念报文，进出设备不会产生时间戳，用于主从关系的建立、时间信息的请求和通告。通用报文包含6种：Announce、Follow\_Up、Delay\_Resp、Pdelay\_Resp\_Follow\_Up、Management和Signaling

各类报文均使用TLV格式以利于扩展，其作用具体如下：

* Sync：Master端发送到Slave端，携带Master端打的t1时间戳。Sync发送方式有2种：A.one-step/单步方式，Sync报文带有本报文发送时刻的时间戳；B.two-step/双步方式，Sync报文并不带有本报文发送时刻的时间戳，而是只记录本报文发送时的时间，由后续报文（Follow\_Up）带上该报文发送时刻的时间戳。
* Delay\_Req：Delay时间同步方式，Slave端发送到Master端，携带Slave端打的t3时间戳。
* Pdelay\_Req：Peer Delay时间同步方式，Slave端发送到Master端，携带Slave端打的t3时间戳。
* Pdelay\_Resp：Peer Delay时间同步方式，Master端发送到Slave端，携带Master端打的t4时间戳和请求的端口ID。
* Announce：用于时钟节点之间交换时间源信息，以确定主从结构。
* Follow\_Up：Delay时间同步方式，在two-step下出现，从Master端到Slave端发送Sync报文后会再发送一个Follow\_Up报文，携带Master端打的t1时间戳。
* Delay\_Resp：Delay时间同步方式，Master端发送到Slave端，携带Master端打的t4时间戳和请求的端口ID。
* Pdelay\_Resp\_Follow\_Up：Peer Delay时间同步方式，在two-step下出现，从Master端到Slave端发送Sync报文后会再发送一个Follow\_Up报文，携带Master端打的t1时间戳。
* Management：查询和设置PTP时钟的时钟数据。
* Signaling：用于PTP时钟之间的交互，如协商消息的周期等。

（8）报文封装方式

1588v2报文可以封装在二层和三层报文中进行传输。根据1588v2报文传输所采用的链路类型不同，可以分为2类：

* MAC封装方式：二层封装，对应的以太网Ethernet Type为0x88F7。此时，可以设置报文封装时携带的VLAN ID和802.1p优先级
* UDP封装方式：三层封装，对应的目的UDP端口号为319（非Announce报文）或320（Announce报文）。此时，可以设置报文封装时携带的VLAN ID、802.1p优先级和DSCP优先级

根据主从节点间的拓扑类型不同，可以分为2类：

* 单播封装：实现时钟信息点对点传输，实现单台设备同步主节点时钟。指定1588v2报文发送的目的MAC地址或IP地址为单播地址，则表示报文采用单播封装的方式。
* 组播封装：实现点到多点的时钟信号同步。对于同一个PTP域，同一个延时测量机制，默认加入同一个组播组，故采用组播封装时，无需配置目的MAC地址或IP地址。——GWN78XX交换机采用此种方式

（9）时间同步步骤

步骤1. 建立主从关系，选取最优时钟、协商端口主从状态等。

步骤2. 频率同步，实现从节点频率与主节点同步。

步骤3. 时间同步，实现从节点与主节点同步。

**（一）建立主从关系**

具体步骤：

PTP通过端口接收到和发送Announce报文，实现端口数据集和端口状态机信息的交互。BMC算法通过比较端口数据集和端口状态机，实现时钟主从跟踪关系。

（1）接收和处理来自对端设备端口的Announce报文

（2）利用BMC算法决策出最优时钟和端口的推荐状态，包括Master、Slave和Passive状态

（3）根据端口推荐状态，更新端口数据集

（4）按照推荐状态和状态决策事件，根据端口状态机决定端口的实际状态，实现时钟同步网络的建立。状态决策事件包括Announce报文的接收事件和接收Announce报文的超时时间结束事件。当接口接收Announce报文的时间间隔大于超时时间间隔时，将此PTP端口状态置为Master

BMC算法主要包括2部分：

* 数据比较算法：比较两个时钟以决定哪个作为最优时钟
* 状态决定算法：计算端口应该处于的状态

**（二）PTP时间同步**

PTP时间同步有两种不同的同步方式：Delay方式和Pdelay方式。

* 延时请求-请求响应机制E2E(End to End)：根据主从时钟之间的整体路径延时时间计算时间差，对应Delay时间同步方式
* 对端延时机制P2P(Peer to Peer)：根据主从时钟之间的每一条链路延时时间计算时间差，对应Pdelay时间同步方式

当前暂仅支持93XX平台的型号，包括GWN7806(P)/GWN7811(P)/12P/13(P)/GWN7831/30。~~暂仅先支持E2E TC。~~

PTP TC暂仅支持管理VLAN。

【配置参数】

全局设置：

* 1588v2 TC：【开关】设置是否开启设备PTP功能，默认关闭。开启后，需进行如下设置：
* 设备类型：【单选】设置设备的PTP类型，选项有{P2P TC | E2E TC}，默认E2E TC。

当且仅当设备类型选择“PTP TC”时，还需要支持如下三个配置（E2E TC完全采用硬件实现，故无）：

* 报文封装方式：【单选】设置1588v2报文的封装方式，选项有{MAC封装 | UDP封装}，默认MAC封装。通过报文进行时间同步的各设备接口发送出的报文封装方式必须一样，否则无法进行时间同步。

GWN78XX交换机采用组播封装方式，故无需配置目的MAC地址，也不带VLAN。

* \*PTP域：【text文本框】设置设备所在的PTP时钟域，取值范围是0-255的整数，默认0号PTP域。只有在同一个时钟域内的设备，才能通过PTP报文进行时间同步。
* 虚拟时钟ID：【text文本框】设置设备的虚拟时钟ID，默认根据设备MAC地址自动生成Clock ID信息，支持手动指定。

接口设置：

* 接口：选择交换机使用PTP时间同步的接口，仅支持电口。可多选
* 1588v2 TC：【开关】设置接口上的PTP功能，默认关闭。接收和发送PTP报文的端口均需使能PTP功能，才能正确计算设备的驻留时间，进行时间的修正。

列表：

* 列表显示接口名称、使能状态、工作状态（E2E TC的工作状态与使能状态一致）~~、端口状态（仅使能PTP功能的接口有，选项有{Master | Slave | Passive | Faulty | Disabled | Listening | Premaster | Initializing | Uncalibrated}）~~

# 堆叠/Stack(FP3)

【定义区分】

1.IRF：IRF2源于最早的堆叠技术，H3C称为IRF1。IRF1堆叠就是将多台盒式设备通过堆叠口连接起来形成一台虚拟的逻辑设备。用户对这台虚拟设备进行管理，来实现对堆叠中的所有设备的管理。这种虚拟设备既具有盒式设备的低成本优先，又具有框式分布式设备的扩展性以及高可靠性。IRF2既支持对盒式设备的堆叠虚拟化，同时也支持同系列框式设备的虚拟化。IRF2虚拟化功能模拟出虚拟的设备，设备管理同事管理IRF2的虚拟设备与真实的物理设备，屏蔽其差异。而对于运行在此系统上的上层应用软件来说，通过设备管理层的屏蔽，已经消除了IRF2系统中不同设备物理上的差异。因此，对于单一运行的物理设备或IRF2虚拟出来的设备，上层软件都不需要做任何的修改，并且对于上层软件系统新增的功能，可同步应用于所有硬件设备。IRF2虚拟化模块：自动进行IRF2系统的拓扑收集、角色选举，并将设备组虚拟成单一的逻辑设备，上层软件所见只是一台设备；IRF2作为通用的虚拟化技术平台，对不同形态的产品采用相同技术架构实现，便于整网运行特征一致性、升级能力一致性。

2.集群：随着网络规模的增加，网络边缘需要使用大量的接入设备，这使对这些设备的管理工作非常繁琐，同时要问这些设备逐一配置IP地址，在目前IP地址资源日益紧张的情况下无疑也是一种浪费。集群（Cluster）是一组网络通信设备的集合，集群管理的主要目的就是解决大量分散的网络设备的集中管理问题。其具备以下优点：

* 节省公网IP地址
* 简化配置管理任务。网络管理员只需在一台设备上配置公网IP地址，就可实现对集群中所有设备的管理和维护，而无需登录到每台设备上进行配置
* 提供拓扑发现和显示功能，有助于监视和调试网络
* 可同时对多台设备进行软件升级和参数配置，且不受网络拓扑和距离限制

3.堆叠：通过厂家提供的一条专用连接电缆，从一台交换机的UP堆叠端口直接连接到另一台交换机的DOWN堆叠端口，以实现单台交换机端口数的扩充。一般交换机能够堆叠4-9台。为了使交换机满足大型网络对端口的数量要求，一般在较大型网络中都采用交换机的堆叠方式来解决。要注意的是只有可堆叠交换机才具备这种端口。所谓可堆叠交换机，就是指一个交换机中一般同时具有UP和DOWN堆叠端口。当多个交换机连接在一起时，其作用就像一个模块化交换机一样堆叠在一起，交换机可以当作一个单元设备来进行管理。一般情况下，当有多个交换机堆叠时，其中存在一个可管理交换机，利用可管理交换机对此可堆叠式交换机中的其他“独立型交换机”进行管理。可堆叠式交换机可非常方便地实现对网络的扩充，是新建网络时最为理想的选择。

4.级联：级联既可使用普通端口也可使用特殊的MDI-II端口。当相互级联的两个端口分别为普通端（MDI-X）和MDI-II端口时，应当使用直通电缆。当相互级联的两个端口均为普通端口（MDI-X）或均为MDI-II端口时，则应当使用交叉电缆。无论是10/100/1000M以太网，级联交换机所使用的电缆长度均可达到100米，这个长度与交换机到计算机之间长度完全相同。因此，级联除了能够扩充端口数量外，还能快速延伸网络直径。当4台交换机级联时，网络跨度就可以达到500米，这样的距离对于位于同一座建筑物内的小型网络而言已经足够。

【功能概述】

堆叠是指将多台支持堆叠特性的交换机通过线缆连接后组合在一起，虚拟化成一台设备，是一种横向虚拟化技术，简化网络的配置和管理。结合跨设备链路聚合技术，不仅实现设备及链路的高可靠性备份，也避免二层环路。相比STP破环保护，逻辑拓扑更清晰、链路利用更高效。

可靠组网：

（1）VRRP+MSTP（传统）

（2）堆叠+链路捆绑（推荐），如：

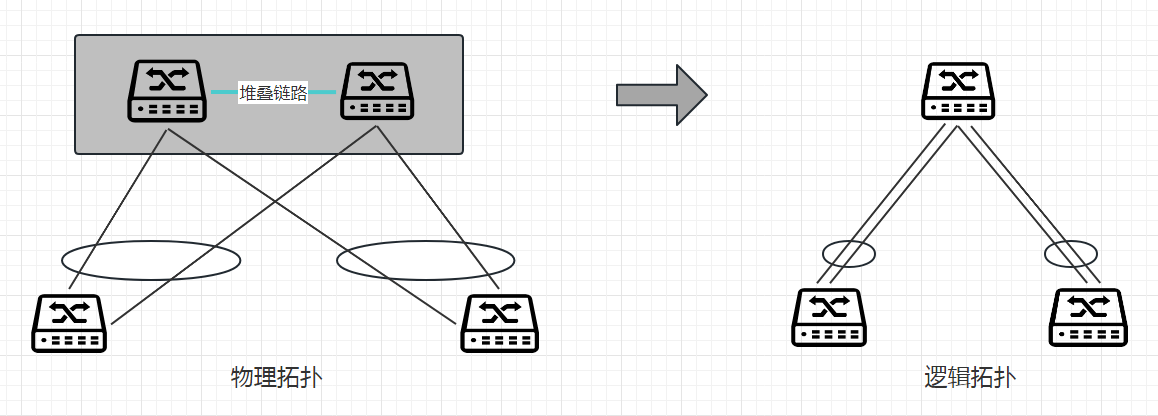
a.华为：CSS（框式）、iStack（盒式）

b.思科：VSS

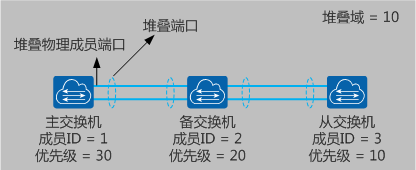
c.华三：IRF

d.锐捷：VSU

上述4种堆叠技术为各厂商私有，无法互通；用于堆叠的设备一般是同一系列，最好是同一型号。



**堆叠基本概念：**



1. 堆叠成员：

* 主交换机（Master）：负责管理整个堆叠。堆叠系统中只有一台主交换机。
* 备交换机（Standby）：主交换机的备份交换机。当主交换机故障时，备交换机接替原主交换机的所有业务。堆叠系统中只有一台备交换机。
* 从交换机（Slave）：主要用于业务转发，从交换机数量越多，堆叠系统的转发能力越强。除主交换机和备交换机外，堆叠系统中其他所有的成员交换机都是从交换机。当备交换机不可用时，从交换机承担备交换机的角色。

主交换机、备交换机和从交换机都可以进行业务流量的转发。添加、移除或替换堆叠成员交换机，都可能导致堆叠成员角色的变化。

2. 其余概念

* 堆叠域（Domain）：交换机通过堆叠链路连接在一起组成一个堆叠，这些成员交换机的集合就是一个堆叠域。为了适应各种组网应用，同一个网络里可以部署多个堆叠，堆叠之间使用域编号（Domain ID）进行区分。GWN78XX堆叠域暂统一为0，后续支持多个堆叠系统再开放。
* 堆叠成员ID（Member ID）：堆叠成员交换机的编号，用来标识和管理成员交换机。堆叠中所有成员交换机的堆叠成员ID都是唯一的。GWN78XX使用DevID来表示（DevID取值1-8，主交换机默认为1），最多支持8台设备组成一个堆叠系统（1主+1备+6从），且每台设备加入堆叠必须保证版本号一致。GWN78XX参与堆叠功能的型号涉及93XX芯片平台（GWN7806(P)/GWN7813(P)/GWN7816(P)/GWN7823P/GWN7831/GWN7832/GWN7830），相同型号设备才可以组成堆叠系统。
* 堆叠优先级：成员交换机的一个属性，主要用于角色选举过程中确定成员交换机的角色，优先级值越大表示优先级越高，当选为主交换机的可能性越大。
* 堆叠物理成员端口：被配置为堆叠模式的物理端口，用于堆叠成员交换机之间的连接。GWN78XX仅支持10G SFP+光口作为堆叠物理口。
* 堆叠端口：专用于堆叠的逻辑口，需要和堆叠物理成员端口绑定。一个堆叠端口可以与一个或多个堆叠物理成员端口绑定，以提高链路的带宽和可靠性。GWN78XX堆叠端口仅支持2个，stack port1和stack port2，最多支持4个堆叠物理口聚合。

3. 预留VLAN

堆叠系统预留VLAN（默认4093），用于堆叠协议通信。堆叠逻辑口会自动加入到预留VLAN4093中。

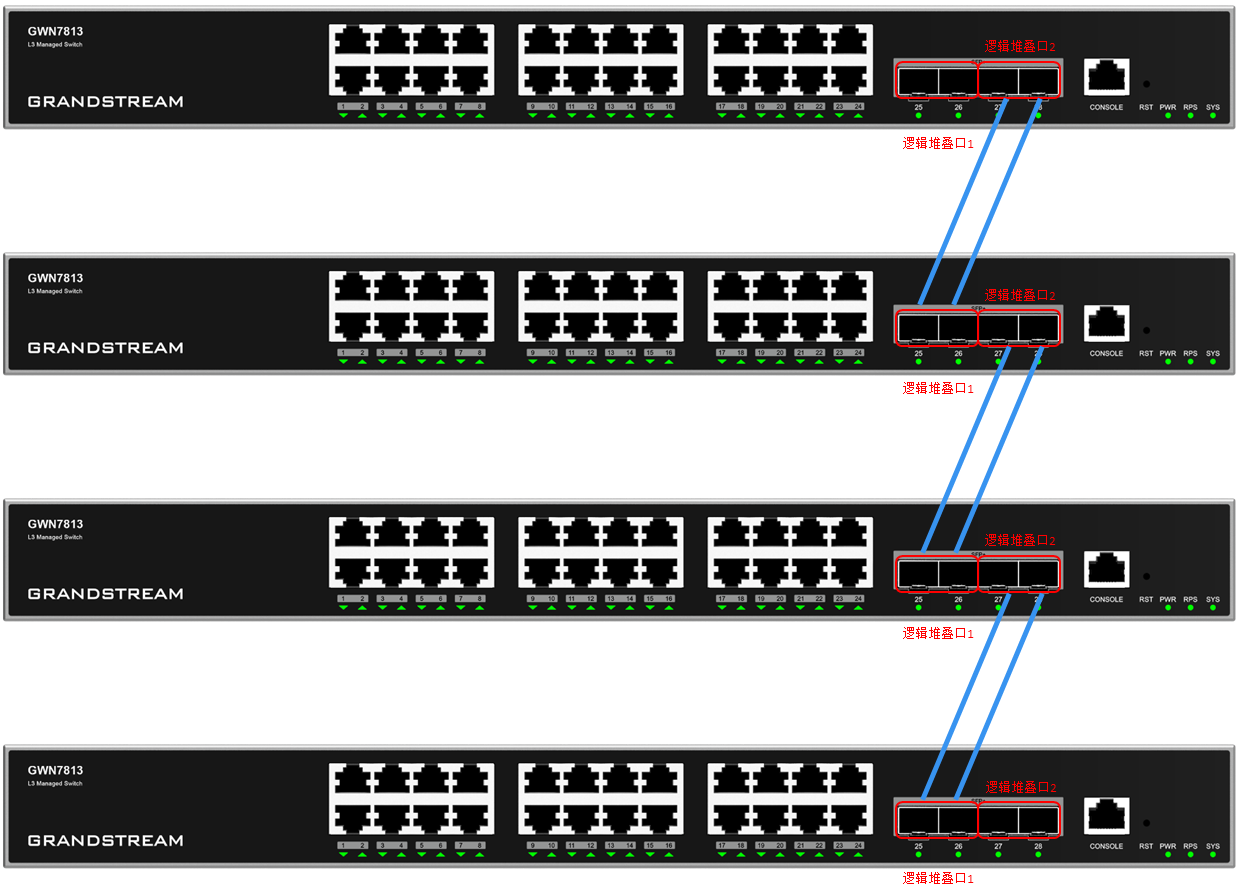
4. 接口编号规则（只针对盒式交换机）

堆叠ID决定堆叠成员交换机的接口编号。对于单台没有运行堆叠的交换机，接口编号采用：槽位号/0/端口号。对于单台没有运行堆叠的交换机，端口编号采用：1/0/端口号（槽位号统一取值为1）。交换机加入堆叠后，接口编号采用：堆叠号/0/端口号。槽位号与端口号的编号规则与单机状态下一致。

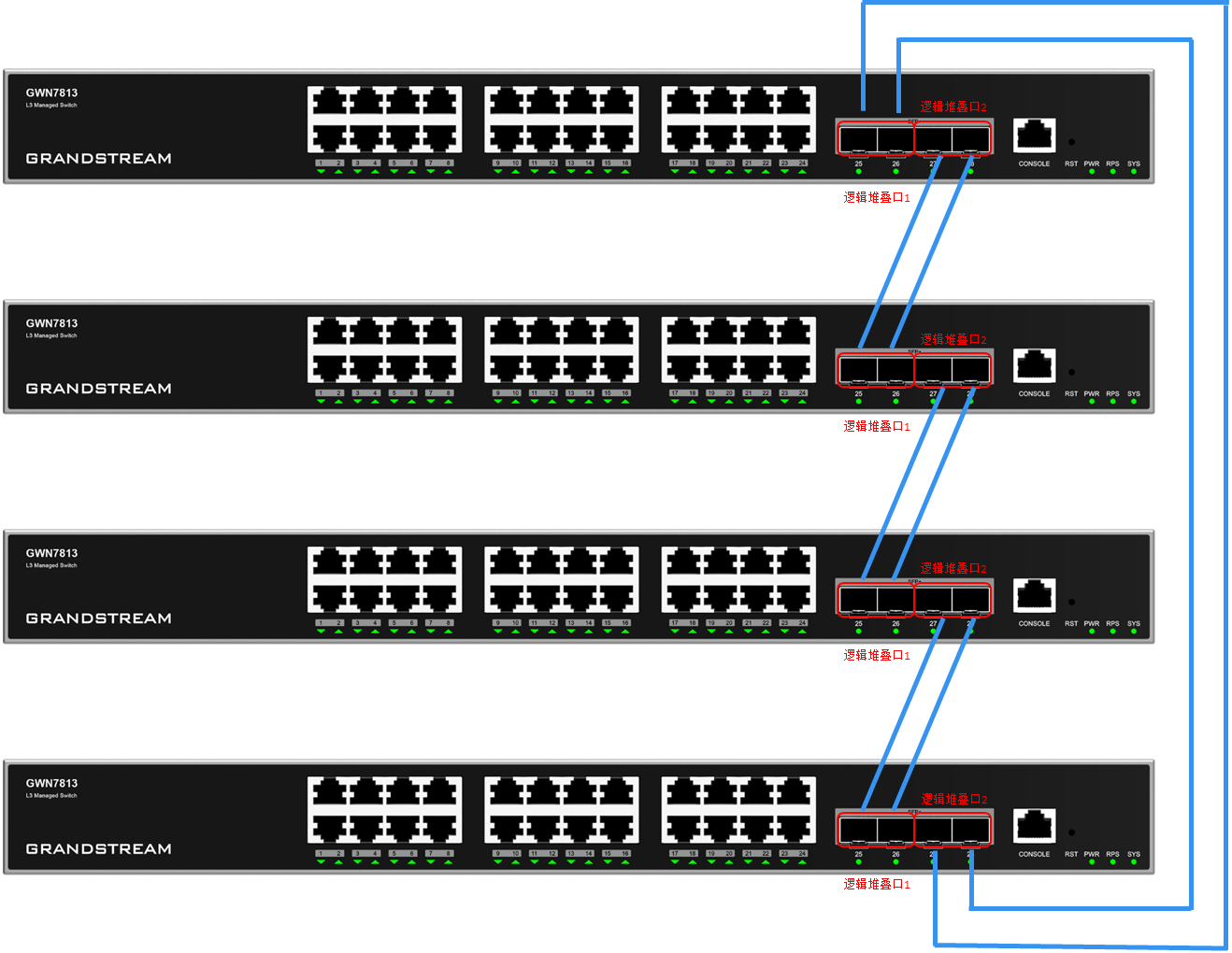
5. 堆叠形态

堆叠形态有链形、环形和星形3种【星形暂不支持】。

链形堆叠：



环形堆叠：



**堆叠原理：**

1. 堆叠建立流程，包括4个阶段：

* 物理连接和软件配置：根据网络要求，选择适当的连接拓扑，组建堆叠网络，并进行相关软件配置
* 主交换机选举：成员交换机之间相互发送堆叠竞争报文，并根据选举原则，选出堆叠系统主交换机
* 拓扑收集：主交换机收集所有成员交换机的信息并计算拓扑。如果成员交换机的堆叠成员ID冲突，主交换机将为冲突的成员交换机重新分配堆叠成员ID【暂不支持】
* 稳态运行：主交换机将整个堆叠系统的拓扑信息同步给所有成员交换机，并选举出一台备交换机

2. 角色选举

堆叠建立时，成员设备间相互发送堆叠竞争报文，选举出主交换机。主交换机选举规则如下：

* 堆叠优先级小的交换机为主交换机，次小的成为备交换机
* 堆叠优先级相同时，堆叠成员ID小的交换机优先竞争为主交换机，次小的成为备交换机
* 若堆叠成员ID仍相同时，需考虑MAC地址，MAC地址小的交换机优先竞争为主交换机，次小的成为备交换机【暂不支持，当前手动配置堆叠成员ID，ID相同无法加入堆叠系统】

3. 拓扑收集

主交换机选举完成后，主交换机会收集所有成员交换机的信息并计算拓扑。如果成员交换机的堆叠成员ID冲突，主交换机将为冲突的成员交换机重新分配堆叠成员ID。【暂不支持】

4. 稳态运行

主交换机计算出拓扑信息后，将整个堆叠系统的拓扑信息同步给所有成员交换机，并选举出一台备交换机。备交换机选举规则如下：

* 堆叠优先级比较，堆叠优先级高的交换机优先竞争为备交换机
* 堆叠ID比较，堆叠ID小的交换机优先竞争为备交换机
* MAC地址比较，MAC地址小的交换机优先竞争为备交换机

5. 版本一致

堆叠的前提必须是交换机具备相同的软件版本。若不相同，需提前升级至同一版本。

~~6. 私网IP分配~~

~~在堆叠系统预留VLAN（默认VLAN 4093）分配私网IP。需在主交换机上创建VLAN 4093的三层接口并配置静态IP地址，用于成员设备的堆叠业务通信。通过配置私网IP地址范围，在从设备加入堆叠时，主设备自动给从设备分配可用的IP地址，主设备可以通过远程登录每台从设备的私网IP地址进行调试和定位问题。~~

7. 配置同步

堆叠具有严格的配置文件同步机制，用来保证堆叠中的多台交换机能够像一台设备一样在网络中工作。

配置文件包括：（1）全局配置：例如IP地址、VLAN虚接口等，适用于所有堆叠成员交换机；（2）接口配置：例如端口所属VLAN，适用于接口所在成员交换机。

* 堆叠建立时，成员交换机在启动开始阶段使用各自的配置文件启动。启动完成后，备、从交换机会去主交换机批量同步配置。后续有新设备加入堆叠，也会按照此同步给新设备。
* 堆叠正常运行后，主交换机作为堆叠系统的管理节点，负责将用户的配置同步给其他交换机，从而使堆叠内各成员交换机的配置随时保持一致。

通过即时同步，堆叠中的所有交换机均保存有相同的配置文件，即使主交换机出现故障，其他交换机仍能按照相同的配置文件执行各项功能。

8. 环路阻塞（仅针对环形组网）

针对环形组网，需要设置环路阻塞点，避免广播流量在堆叠口之间形成风暴，尽可能均匀分布在成员设备上。

9. 虚拟化为一台设备

堆叠系统对外显示为一台主设备，其他从设备无法访问。需做操作如下：

* 成员设备的router-MAC配置为主设备的系统MAC，保证整个堆叠系统对外MAC一致
* 成员设备的ARP通过ACL在主设备处理，生成的主机路由同步到所有成员设备。保证堆叠系统的主机路由是一样的。
* 单台设备的虚接口状态、生成的直连路由同步到所有成员设备。保证堆叠系统的直连路由是一样的。
* 路由表trap to CPU设置为主设备，保证堆叠系统中的控制报文都由主设备进行处理。目的IP是本机，例如HTTP/ICMP/Telnet/SSH等协议报文会由主设备处理，达到无论从哪台成员设备进入，访问IP总是接入到主设备的目的。如果目的IP不是本机，此时主设备走完整的路由处理，得到ARP响应，并设置网络路由表action为forward，并同步到成员设备，保证堆叠系统的网络路由是一样的。

控制报文都由主设备处理；路由MAC、主机路由、直连路由、网络路由都需要同步，保持一致；数据报文由每台成员设备进行本地转发，不经过主设备。

10. 堆叠系统的登录

堆叠系统建立后，所有的成员设备组成一台虚拟设备存在于网络中，所有成员设备的资源由主交换机统一管理。用户可以通过任意一台成员设备登录堆叠系统，对整个堆叠系统进行管理和维护。无论使用什么方式，通过哪台成员交换机登录到堆叠系统，实际登录的都是主交换机。登录堆叠系统的方式有：

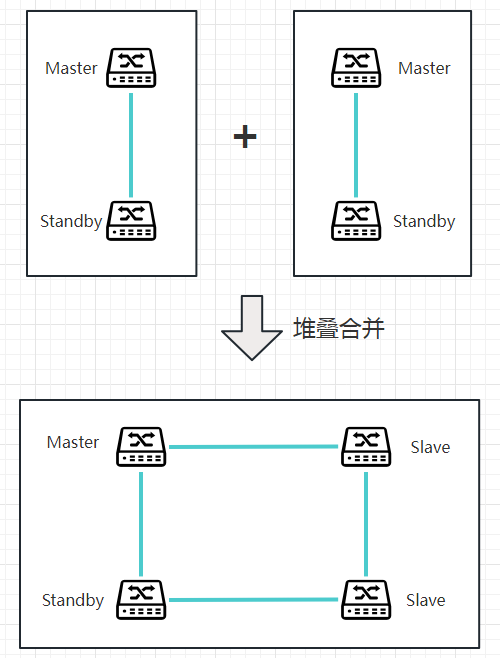
（1）本地登录：通过任意一台乘员设备的Console口登录

（2）远程登录：通过任意一台成员设备的三层接口，以HTTPS、Telnet、SSH等方式远程登录（注：需使用主交换机的IP地址）

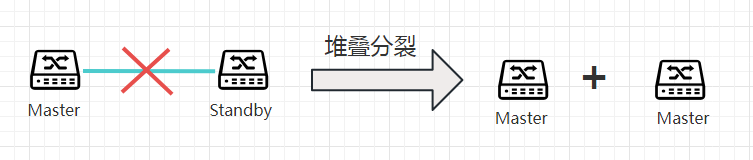
11. 堆叠合并与分裂：

堆叠合并：稳定运行的两个堆叠系统合并成一个新的堆叠系统。

堆叠系统合并时，两个堆叠系统的主交换机进行竞争，选举出一个更优的作为新堆叠系统的主交换机（选举规则与选举主交换机的规则一致）。竞争胜出的主交换机所在的堆叠系统将保持原有主、备角色和配置不变，业务也不会受到影响；而另一个堆叠系统的所有成员交换机将重新启动后加入到新堆叠系统。



堆叠分裂：堆叠建立后，主交换机和其他成员交换机之间定时发送心跳报文来维护堆叠系统的状态。当堆叠线缆或设备发生故障时，可能会导致交换机之间失去通信，堆叠系统分裂为多个堆叠系统。



堆叠分裂后，其全局配置完全相同，会以相同的IP地址和MAC地址（堆叠系统MAC）与网络中的其他设备交互，这样会导致IP地址和MAC地址冲突，引起整个网络故障，此时可以依靠堆叠的双主检测来避免堆叠分裂后出现双主。

12. 堆叠双主检测【暂不支持】

双主检测DAD（Dual-Active Detect）是一种检测和处理堆叠分裂的协议，可以实现堆叠分裂的检测、冲突处理和故障恢复，降低堆叠分裂对业务的影响。

配置双主检测后，主交换机在检测链路上发送DAD竞争报文。堆叠分裂后，分裂成多部分的堆叠系统互发竞争报文，并将接收到的竞争报文信息与本部分竞争信息做比较，如果本部分竞争胜出，则不做处理，保持Active状态（正常工作状态），正常转发业务报文；如果本部分竞争失败，则关闭除保留端口外的所有业务端口，转入Recovery状态（业务禁用状态），停止转发业务报文。

DAD竞争规则如下：

* 堆叠优先级比较，堆叠优先级高的交换机优先竞争胜出
* 堆叠ID比较，堆叠ID小的交换机优先竞争胜出

堆叠链路故障修复后，分裂成多部分的堆叠系统进行合并。处于Recovery状态的交换机将重新启动，同时将被关闭的业务端口恢复正常，整个堆叠系统恢复。

13. 跨设备链路聚合

堆叠支持的跨设备链路聚合技术，可以将不同成员交换机上的物理以太端口配置成一个聚合端口。如此，即使某台成员交换机故障或聚合链路其中一条链路出现故障，也不会导致聚合链路完全失效，从而保证了数据流量的可靠传输，不但解决了堆叠设备单点失效的问题，还极大提高了全网的可靠性。

14. 流量本地优先转发

跨设备链路聚合口会通过HASH算法选择转发出接口，从而进入堆叠的流量很可能会跨设备转发。但是由于堆叠设备间堆叠线缆的带宽有限，跨设备转发流量增加了堆叠设备之间的带宽承载压力，同时也降低了流量转发效率。此时，可以通过流量本地转发功能解决此问题，即从本设备进入的流量，优先从本设备的出接口转发出去；如果本设备的出接口故障，则流量从其它成员交换机的接口转发出去。

15.堆叠LED指示灯

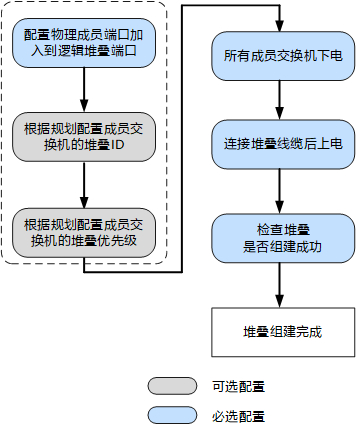
堆叠系统的成功建立与失败指示，借助系统指示灯可获知。具体使用如下：

|  |  |  |
| --- | --- | --- |
| **LED指示灯** | **指示灯状态** | **说明** |
| 系统指示灯（3色灯） | 黄色闪烁 | * 堆叠建立中，包括主从选举、首次配置同步等 |
| 白色常亮 | * 堆叠建立完成，表示主交换机 |
| 蓝色常亮 | * 堆叠建立完成，表示从交换机正常运行 |
| 蓝色闪烁 | * 后续从交换机同步配置 |
| 红色常亮 | * 从交换机堆叠建立失败 |

a.红灯（硬件控制）→b.启机绿灯常亮→c.主从黄灯闪烁，表示堆叠建立中→d.堆叠建立完成，主：白灯常亮，从：蓝灯常亮（成功加入堆叠系统）/红色常亮（加入堆叠系统失败），可登录其本地查看失败原因。

【配置参数】

组建堆叠流程图：



（一）堆叠设置：

单台堆叠成员交换机在组成堆叠系统前的设置。

* 堆叠：【开关】设置是否在交换机上开启堆叠功能，默认关闭。
* 预留VLAN：【text文本框】设置交换机的堆叠系统预留VLAN，取值范围为1-4094的整数，默认4093。
* 设备ID：【text文本框】设置交换机堆叠的设备ID，取值范围为1-8，默认1。
* 优先级：【text文本框】设置交换机堆叠的优先级，取值范围为1-255，默认1。优先级值越大优先级越高。

堆叠端口设置：设置前请需确保物理口处于shutdown状态

* 堆叠端口1：【多选框】从SFP+端口中选择物理口加入堆叠端口1，可单选也可多选，至多选4个
* 堆叠端口2：【多选框】从SFP+端口中选择物理口加入堆叠端口2，可单选也可多选，至多选4个

注：堆叠端口1/2内的物理端口不能重复，且2选1必填。

堆叠端口的命名跟随设备ID修改后的重启一并同步更新。

设置完并保存后，重启交换机以生效设置。在各成员交换机之间交叉连线，连好后上电（建议预设的主交换机先上电），即可形成堆叠系统。一旦堆叠系统建立后，无法再修改堆叠设备的配置，必须关闭并退出堆叠后才可编辑，然后再重新加入堆叠。

（二）堆叠系统：

在堆叠系统形成后，进入主交换机Web GUI页面，显示堆叠系统信息、成员交换机信息和拓扑图。  
1. 堆叠系统信息

需显示完整堆叠系统的MAC地址。

2. 成员交换机信息

成员交换机列表主要显示如下内容：

* 设备ID：显示各成员交换机的堆叠成员ID~~，包括当前设备ID、编辑过的新设备预设ID（新设备预设ID需重启以生效）~~
* 角色：显示各成员交换机的角色，包括{Master |Standby |Slave}
* MAC地址：显示各成员交换机的原MAC地址
* 优先级：显示成员交换机的堆叠优先级值
* 设备型号：显示成员交换机的交换机型号【暂不支持，考虑现仅支持同型号堆叠，无需显示】

列表显示顺序优先显示主交换机、备交换机，其余从交换机按照堆叠成员ID从小到大排序

~~支持对交换机修改设备ID。~~

备交换机和从交换机支持查看详情，具体包括系统资源状态。

3. 拓扑

显示成员交换机之间的拓扑关系图，展示出拓扑结构是链形还是环形，需包含：

* 成员交换机的堆叠成员ID~~（当前设备ID和新设备预设ID）~~、角色
* 成员交换机的堆叠端口1/2
* 成员交换机之间的连线，须关联上具体的堆叠物理端口

点击备交换机和从交换机支持查看系统资源状态。

（三）设备功能配置

堆叠建立后，所有成员交换机虚拟化为一台设备，在主交换机上进行功能配置。全文第4章-第14章Web GUI需求改动点如下表：

|  |  |
| --- | --- |
| **模块** | **修改点** |
| 概览 | |
| 系统信息 | 1.资源状态部分分设备查看（与拓扑里的查看资源状态为同一内容） |
| 接口信息 | 1.显示所有成员交换机的接口，接口编号规则详见上述功能概述（设备ID/0/端口ID），涉及接口编号的下同 |
| 以太网业务 | |
| 端口基本配置 | 1.显示所有成员交换机的端口进行配置，支持分页 |
| 流量统计 | 1.显示所有成员交换机的接口流量信息，支持分页 |
| 端口自动恢复 | 1.显示所有成员交换机的端口ErrDisable原因和剩余恢复时间，支持分页 |
| 链路聚合 | 1.链路聚合接口个数，按芯片上限+实测进行显示[TBD]  2.聚合组编辑，支持的端口需包括所有成员交换机的端口（不包括堆叠端口1/2里的物理口） |
| MAC表 | 1.MAC动态地址：可关联的端口包括所有成员交换机的端口  2.静态MAC地址：添加/编辑 端口包括所有成员交换机的端口  3.黑洞地址：添加/编辑 端口包括所有成员交换机的端口 |
| VLAN | 1.VLAN下tag和untag的端口包括所有成员交换机的端口  2.端口设置：显示所有成员交换机的端口，支持分页  3.端口成员：显示所有成员交换机的端口，支持分页  4.语音VLAN：显示所有成员交换机的端口进行设置，支持分页 |
| 生成树 | 1.端口设置：显示所有成员交换机的端口，支持分页  2.MST端口设置：显示所有成员交换机的端口，支持分页  3.PVST端口设置; 显示所有成员交换机的端口，支持分页 |
| IP业务 | |
| ARP表 | 1.ARP表里的接口支持显示所有成员交换机的端口 |
| 邻居发现 | 1.邻居表里的接口支持显示所有成员交换机的端口 |
| 组播业务 | |
| IGMP Snooping | 1.路由器端口：添加/编辑 静态/禁用路由器端口需包含所有成员交换机的端口  2.组播地址：添加/编辑 成员端口需包含所有成员交换机的端口  3.组播端口：显示所有成员交换机的端口，支持分页 |
| MLD Snooping | 1.路由器端口：添加/编辑 静态/禁用路由器端口需包含所有成员交换机的端口  2.组播地址：添加/编辑 成员端口需包含所有成员交换机的端口  3.组播端口：显示所有成员交换机的端口，支持分页 |
| QoS | |
| 端口优先级 | 1.显示所有成员交换机的端口，支持分页 |
| 队列调度 | 1.显示所有成员交换机的端口，支持分页 |
| 队列整形 | 1.显示所有成员交换机的端口，支持分页 |
| 端口限速 | 1.显示所有成员交换机的端口，支持分页 |
| 安全业务 | |
| 风暴控制 | 1.显示所有成员交换机的端口，支持分页 |
| 端口安全 | 1.端口安全：显示所有成员交换机的端口，支持分页  2.安全MAC地址：添加/编辑 端口需包含所有成员交换机的端口 |
| 端口隔离 | 1.需包含所有成员交换机的端口，支持分页和批量开启端口隔离 |
| ACL | 1.ACL绑定：端口需包含所有成员交换机的端口 |
| IP源防护 | 1.端口防护：需包含所有成员交换机的端口，支持分页  2.四元绑定表：添加/编辑/导入/导出需包含所有成员交换机的端口 |
| IPv6源防护 | 1.端口防护：需包含所有成员交换机的端口，支持分页  2.四元绑定表：添加/编辑/导入/导出需包含所有成员交换机的端口 |
| DAI | 1.DAI：显示所有成员交换机的端口，支持分页  2.端口数据统计表：显示所有成员交换机的端口，支持分页 |
| 802.1X | 1.端口模式：显示所有成员交换机的端口，支持分页  2.端口：显示所有成员交换机的端口，支持分页 |
| DHCP Snooping | 1.Option 82：添加/编辑Circuit ID的端口需包含所有成员交换机的端口  2.端口设置：显示所有成员交换机的端口，支持分页  3.端口数据统计表：显示所有成员交换机的端口，支持分页 |
| DHCPv6 Snooping | 1.Option设置：添加/编辑Option 18的端口需包含所有成员交换机的端口  2.端口设置：显示所有成员交换机的端口，支持分页  3.端口数据统计表：显示所有成员交换机的端口，支持分页 |
| PoE | |
| PoE（仅PoE型号支持） | 1.全局/电源信息：电源（如果有的话）、全局、芯片信息按成员交换机来显示，支持对成员交换机切换显示3部分内容，默认显示主交换机的电源信息  2.全局/设置：显示每个成员交换机的PoE预留功率设置  3.端口：需包含所有成员交换机的PoE端口。支持选择某一成员交换机的端口进行批量设置，默认显示所有成员交换机的端口。需在页面提示“供电优先级仅局限在单台物理交换机端口上生效” |
| 维护 | |
| 升级 | 1.升级方式不变，包括手动上传升级、网络升级、定时升级  2.主从交换机升级：整个堆叠系统升级完重启的方式 |
| 诊断 | 1.日志：需包含所有成员交换机的日志信息  ~~2.Ping：进行Ping之前需先指定成员交换机，默认主交换机~~  ~~3.路由跟踪：进行路由跟踪之前需先指定成员交换机，默认主交换机~~  4.光模块：需包含所有成员交换机的光口  5.镜像：出入方向端口需包含所有成员交换机的端口  6.线缆检测：需包含所有成员交换机的电口  7.一键调试：进行一键调试前需先指定成员交换机，默认主交换机 |
| 备份与恢复 | 1.恢复出厂：所有成员交换机执行恢复出厂操作  2.备份整个堆叠系统的功能配置  3.备份恢复：根据配置文件进行恢复，按照配置内容确定是否同步从交换机 |
| 告警 | 1.统一将告警信息记录到主交换机的日志中 |
| SNMP | 1.统一为堆叠系统整机受SNMP管理 |
| RMON | 1.统计组：需显示所有成员交换机的端口，支持分页  2.历史组：添加/编辑 端口需包含所有成员交换机的端口  3.告警组：添加/编辑 端口需包含所有成员交换机的端口 |
| LLDP/LLDP-MED | 1.LLDP全局设置/端口设置：需显示所有成员交换机的端口，支持分页  2.LLDP-MED端口设置：需显示所有成员交换机的端口，支持分页  3.设备信息：本地端口信息需包含所有成员交换机的端口  4.邻居信息：本地端口需包含所有成员交换机的端口，支持分页  5.数据统计/端口统计：需显示所有成员交换机的端口，支持分页 |
| 节能以太网 | 1.需显示所有成员交换机的电口，支持分页 |
| 系统 | |
| 1588v2（如果支持的话） | 1.需显示所有成员交换机的电口，支持分页 |

研发测试大体分为2阶段：

* 阶段一：堆叠设置+堆叠建立，先测二三层转发
* 阶段二：堆叠功能配置+测试

！！！状态机

# LED指示灯(FP1C)

GWN780X/11(P)/12P交换机指示灯分为三类：系统指示灯、端口指示灯、PoE指示灯。其中，系统指示灯为三色灯，端口指示灯、PoE指示灯为单色灯。其中，电口指示灯和PoE指示灯使用同一个灯口显示亮灯情况，均为单色灯，光口仅有端口指示灯，仍为单色灯。

GWN7813(P)交换机指示灯分为四类：系统指示灯、端口指示灯、PoE指示灯、电源指示灯。其中，系统指示灯为三色灯，端口指示灯、PoE指示灯为单色灯，电源指示灯为双色灯。其中，电口指示灯和PoE指示灯使用同一个灯口显示亮灯情况，均为三色灯，光口仅有端口指示灯，仍为单色灯，电源指示灯仅表示系统供电状态。

GWN7816(P)交换机指示灯分为四类：系统指示灯、端口指示灯、PoE指示灯和电源指示灯。其中，系统指示灯为三色灯，端口指示灯、PoE指示灯为单色灯，电源指示灯为双色灯。其中，电口指示灯和PoE指示灯使用同一个灯口显示亮灯情况，均为三色灯，光口仅有端口指示灯，仍为单色灯。

GWN7832交换机指示灯分为三类：系统指示灯、端口指示灯、电源指示灯。其中，系统指示灯为三色灯，端口指示灯、电源指示灯为双色灯。

GWN7830/31交换机指示灯分为三类：系统指示灯、端口指示灯、电源指示灯。其中，系统指示灯为三色灯，端口指示灯（包括电口、Combo口和光口）为单色灯，电源指示灯为双色灯。

相关指示灯颜色与状态变化如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| **型号** | **LED指示灯** | **指示灯状态** | **说明** |
| GWN78XX | 系统指示灯（三色） | Off | * 未上电 |
| 绿色常亮 | * 开机启动 |
| 绿色闪烁 | * 升级 |
| 蓝色常亮 | * 正常运行中 * 堆叠建立完成，表示从交换机正常运行 |
| 蓝色闪烁 | * 配置修改应用 * 堆叠从交换机，后续从主交换机同步配置 |
| 红色常亮 | * 升级失败 * 告警(FP2) * 从交换机堆叠建立失败 |
| 红色闪烁 | * 恢复出厂 |
| 白色闪烁 | * 【GWN780X(不包括7806(P))仅适用于产线升级】升级后自动重启变白色闪烁，二次重启后恢复蓝色 |
| 注：比上述新增堆叠说明  支持型号：GWN7806(P)/13(P)/16(P)/23P/32/31/30 | 黄色闪烁 | * 堆叠建立中，包括主从选举、首次配置同步等（仅限支持堆叠交换机） |
| 白色常亮 | * 堆叠建立完成，表示主交换机（仅限支持堆叠交换机） |
| GWN780X/1X | 端口指示灯（两个单色灯） | Off | * 端口关闭（电口&光口） * 光口故障 |
| 绿色常亮 | * 端口link（电口&光口） |
| 绿色闪烁，闪烁频率根据数据流量速率决定 | * 数据交换传输通信（电口&光口） |
| 黄色常亮 | * 端口link&PoE供电（仅电口） |
| 黄色闪烁，闪烁频率根据数据流量速率决定 | * 端口数据交换传输通信&PoE供电（仅电口） |
| 黄绿交替闪烁，1秒黄1秒绿 | * 故障（仅电口） |
| GWN7832 | 端口指示灯（双色灯） | Off | * 光口关闭或故障 |
| 绿色常亮 | * Link with 10Gbps |
| 绿色闪烁，闪烁频率根据数据流量速率决定 | * 数据交换传输通信with 10Gbps |
| 黄色常亮 | * Link with 1Gbps |
| 黄色闪烁，闪烁频率根据数据流量速率决定 | * 数据交换传输通信with 1Gbps |
| GWN7831/30 | 端口指示灯（单色灯） | Off | * 端口关闭（电口&光口） * 光口故障 |
| 绿色常亮 | * 端口link（电口&光口） |
| 绿色闪烁，闪烁频率根据数据流量速率决定 | * 数据交换传输通信（电口&光口） |
| GWN7813/13P/23P/32/31 | PWR/RPS电源指示灯（双色灯） | Off | * 电源未接入/故障 |
| 绿色 | * 电源使用中 * 电源已接入但未使用 |
| 红色 | * 电源过压或欠压（由硬件控制） |
| GWN7816(P) | PSU1/2电源指示灯 | Off | * 电源未接入 |
| 绿色常亮 | * 电源供电正常，使用中 |
| 绿色闪烁 | * 电源插入，AC供电正常，但I2C通信异常，输出正常，使用中 |
| 红色常亮 | * 电源故障，分为以下情况： * 电源AC供电正常，输出正常，但出现风扇异常/过温等电源告警 * 电源插入，无输入或无输出（前提：另一PSU正常） |
| 总结：  一个电源对应一个PSU指示灯；  1) 电源未插入, 对应LED灭；  2) 电源正常, 对应LED亮绿灯；  3) 电源插入，但无AC输入，或者无输出，对应LED显示红灯；  4) 单电源或双电源供电，电源输出正常，但出现过温过流等警告，对应LED也会显示红灯；  5) 若电源有输出，但I2C异常，对应指示灯闪烁 | |

注：系统指示灯的闪烁频率为：每1秒闪烁一次。

GWN780X(不包括7806(P))设备启机，系统指示灯在绿灯亮之前有一个不可控的红灯闪烁，一旦进入绿灯亮，后续均可控。

[xpfei]：红色灯的GPIO是直接由9301固化的，该GPIO在系统异常时就会闪烁 不需要软件做任何控制。当初做的时候出于这个考虑，现在产线出现异常很多都是借助这个红灯来判定设备是否正常起机的：

* 没烧写程序 亮红灯
* 设备在起机过程 亮红灯
* 设备没有完全起机 亮红灯
* 中途设备异常 亮红灯

这个I/O不管8382和9301都是本身固化好的

这个容易与恢复出厂搞混淆，建议启机不可控的状态保持红灯常亮。

# 风扇/Fan(FP1D)

GWN7802P有1个风扇，GWN7803P/12P/32/31有2个风扇，GWN7806/06P/13P/16/16P有3个风扇，无论是低转速运行还是高转速运行，风扇合力运作，不做单风扇主次策略。具体风扇运行策略详见表“[GWN78XX风扇策略](file:///C:\Users\Administrator\Desktop\GWN78XX风扇策略 -2023-08-07%20.xlsx)”。



Web端需求：

风扇个数不一，根据各型号支持情况进行显示。

* 风扇id
* 风扇类型[TBD]：固定 | 可拆除
* 工作状态：正常Normal | 故障Failure | 停止Stop

注：故障：指该转的时候发生故障导致无法正常运行

* 风扇转速：可借助此判断是低转速、中转速（仅GWN7806P支持）还是高转速
* 气流方向[TBD，暂不支持]：包括实际气流方向和首选气流方向

注：【yflu】GWN7802P/03P的风扇气流方向是固定的

补充建议：

1.GWN7803P是有2个风扇的，上述需求是直接默认2个一起转动降温，是否考虑做按照温度阶梯来，先转动1个，等温度往上再转动2个？

[yflu]：GWN7803P的风扇一起运作，不做单风扇主次的策略

2.风扇的反转告警与气流方向选择

[yflu]：GWN7802P/03P的风扇气流方向是固定的，接线方式限定不会反转

GWN781X/2X/3X是否考虑增加此部分？

3.增加蜂鸣器。当风扇反转、风扇故障或温度达到临界点时，采用蜂鸣器鸣叫警示。

4.增加风扇指示灯。查看竞品，TP-Link、NetGear、华为均有单独的指示灯。

后续若增加风扇指示灯，则指示灯亮灯逻辑如下：

建议考虑双色或三色灯

|  |  |  |
| --- | --- | --- |
| **LED指示灯** | **指示灯状态** | **说明** |
| 风扇指示灯 | Off | * 未运行 |
| 绿色常亮 | * 正常运行，且能正常通信 |
| 绿色闪烁 | * 正常运行，但通信异常 |
| 红色常亮 | * 风扇硬件故障，需要更换；同时，蜂鸣器响（若有的话） |
| 红色闪烁 | * 有相关告警，包括高温告警、风扇模组短路、堵转和风扇本身故障等；同时，蜂鸣器响（若有的话） |

或

|  |  |  |
| --- | --- | --- |
| **LED指示灯** | **指示灯状态** | **说明** |
| 风扇指示灯 | Off | * 未运行 |
| 绿色常亮 | * 正常运行 |
| 红色常亮 | * 风扇硬件故障，需要更换 * 相关告警，包括高温告警、风扇模组短路、堵转和风扇本身故障等；同时，蜂鸣器响（若有的话）风扇模组短路、堵转和风扇本身故障等 |

# 电源/Power Supply(FP1D)

GWN7813/13P/23P/31/32支持备用外置冗余电源，用RPS标识，内置主电源用PWR表示；

GWN7816/16P支持双电源，用PSU1/PSU2表示，PSU2内置热插拔且选配。

电源指示灯：7813/13P/32/31/23P/16/16P 红&绿

**（一）GWN7813P/23P的RPS电源**

1. 默认只支持一个内置电源，支持用户外置一个RPS电源应急使用。

2. 内置电源使用13V进行系统供电，56V（360W）进行PSE供电；RPS电源使用12V进行系统供电，54V（240W）进行PSE供电。当2个电源同时接入时，默认使用内置电源，当内置电源故障，系统自动切换至RPS备用电源使用。

3. 内置电源使用PWR指示灯，RPS电源使用RPS指示灯，均为双色灯，仅表示系统供电状态。

|  |  |  |  |
| --- | --- | --- | --- |
| GWN7813P/23P | PWR/RPS电源指示灯（双色灯） | Off | * 电源未使用/故障 |
| 绿色 | * 电源使用中 |
| 红色 | * 电源过压或欠压 |

4. 当连接上RPS电源时，默认仍然使用内置电源。当内置电源出现故障时，会进行供电切换，具体逻辑如下：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 供电场景 | 内置电源 | | RPS电源 | | PWR LED | RPS LED | 场景说明 |
| 系统供电 | PSE供电 | 系统供电 | PSE供电 |
| 场景一 | Yes | Yes | No | No | 绿色 | Off | RPS电源未接入，使用内置电源为系统和PSE供电 |
| 场景二 | Yes | Yes | No | No | 绿色 | 绿色 | RPS电源已接入但未使用，默认使用内置电源为系统和PSE供电 |
| 场景三 | No | No | Yes | Yes | Off | 绿色 | 内置电源故障，使用RPS电源为系统和PSE供电  *注：PSE供电功率从360W降至240W，需做PSE功率限制* |
| 场景四 | No | Yes | Yes | Yes | Off | 绿色 | 内置电源系统供电故障，使用RPS电源为系统供电，PSE供电虽然仍然使用内置电源，但功率需降至240W以提示内置电源有故障  *注：PSE供电功率从360W降至240W，需做PSE功率限制* |
| 场景五 | Yes | No | No | Yes | 绿色 | Off | 内置电源PSE供电故障，使用RPS电源为PSE供电，系统供电仍然使用内置电源  *注：PSE供电功率从360W降至240W，需做PSE功率限制* |
| 场景六 | No | Yes | Yes | No | Off | 绿色 | 内置电源系统供电故障，使用RPS电源为系统供电，PSE供电虽然仍然使用内置电源，但功率需降至240W以提示内置电源有故障  *注：PSE供电功率从360W降至240W，需做PSE功率限制* |

5. 只要内置电源故障，改用RPS电源为①系统 或 ②PSE 或 ③系统和PSE供电时，供电功率从360W降至240W，不满足所有PoE端口的供电需求，需做PSE供电限制。按照先到先得的机制，自动关闭后供电的PSE端口；当内置PSE供电恢复时，需要将强制关闭PSE供电的端口自动恢复供电。

6. 由于RPS电源同时支持PSE供电，会影响PoE模块。故需要PoE模块中新增电源相关内容，且PoE预留功率取值范围改为0-240W。具体需求详见[*[PoE]*](#_PoE(FP1B))。

7. [概览/系统信息]处需显示内置电源和RPS电源的相关状态，具体需求详见[*[概览/系统信息]*](#_系统信息/System_Info.)。

**（二）GWN7813/32/31的RPS电源**

1. 默认只支持一个内置电源，支持用户外置一个RPS电源应急使用。

2. 内置电源使用13V进行系统供电；RPS电源使用12V进行系统供电。当2个电源同时接入时，默认使用内置电源，当内置电源故障，系统自动切换至RPS备用电源使用。

3. 内置电源使用PWR指示灯，RPS电源使用RPS指示灯，均为双色灯，仅表示系统供电状态。

|  |  |  |  |
| --- | --- | --- | --- |
| GWN7813/32/31 | PWR/RPS电源指示灯（双色灯） | Off | * 电源未使用/故障 |
| 绿色 | * 电源使用中 |
| 红色 | * 电源过压或欠压 |

4. 当连接上RPS电源时，默认仍然使用内置电源。当内置电源出现故障时，会进行供电切换，具体逻辑如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 供电场景 | 内置电源 | RPS电源 | PWR LED | RPS LED | 场景说明 |
| 场景一 | Yes | No | 绿色 | Off | RPS电源未接入，使用内置电源为系统供电 |
| 场景二 | Yes | No | 绿色 | 绿色 | RPS已接入但未使用，默认使用内置电源为系统供电 |
| 场景三 | No | Yes | Off | 绿色 | 内置电源故障，使用RPS电源为系统供电 |

5. [概览/系统信息]处需显示内置电源和RPS电源的相关状态，具体需求详见[*[概览/系统信息]*](#_系统信息/System_Info.)。

**（三）GWN7816(P)的CRPS电源**

1. 默认只支持一个PSU电源，支持用户再加装一个PSU电源使用。

2. GWN7816P：PSU1和PSU2规格完全相同，使用12V（60W）进行系统供电，54.5V（740W）进行PSE供电。GWN7816：PSU1和PSU2规格完全相同，使用12V（60W）进行系统供电。双PSU接入时，同时为交换机供电，各提供整机功耗的一半；当某个PSU故障/掉电时，由另一个PSU对整机完全供电。

3. PSU1使用PSU1指示灯，PSU2电源使用PSU2指示灯，均为双色灯，仅表示系统供电状态。

|  |  |  |  |
| --- | --- | --- | --- |
| GWN7816(P) | PSU1/2电源指示灯 | Off | * 电源未接入 |
| 绿色常亮 | * 电源供电正常，使用中 |
| 绿色闪烁 | * 电源插入，AC供电正常，但I2C通信异常，输出正常，使用中 |
| 红色常亮 | * 电源故障，分为以下情况： * 电源AC供电正常，输出正常，但出现风扇异常/过温等电源告警 * 电源插入，无输入或无输出（前提：另一PSU正常） |
| 总结：  一个电源对应一个PSU指示灯；  1) 电源未插入, 对应LED灭；  2) 电源正常, 对应LED亮绿灯；  3) 电源插入，但无AC输入，或者无输出，对应LED显示红灯；  4) 单电源或双电源供电，电源输出正常，但出现过温过流等警告，对应LED也会显示红灯；  5) 若电源有输出，但I2C异常，对应指示灯闪烁 | |

4. PSU供电的具体逻辑如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 供电场景 | PSU 1供电 | PSU2供电 | PSU1 LED | PSU2 LED | 场景说明 |
| 场景一 | Yes | No | 绿色 | Off | PSU2未接入，使用PSU1为整机供电 |
| 场景二 | No | Yes | Off | 绿色 | PSU1未接入，使用PSU2为整机供电 |
| 场景三 | Yes | Yes | 绿色 | 绿色 | PSU1/2同时为整机供电，每个PSU提供整机功耗的一半 |
| 场景四 | Yes→No | Yes | 绿色→红色 | 绿色 | PSU1损坏故障或掉电，PSU2输出功率从原来分担整机的一半升高至整机全部功率 |
| 场景五 | Yes | Yes→No | 绿色 | 绿色→红色 | PSU2损坏故障或掉电，PSU1输出功率从原来分担整机的一半升高至整机全部功率 |

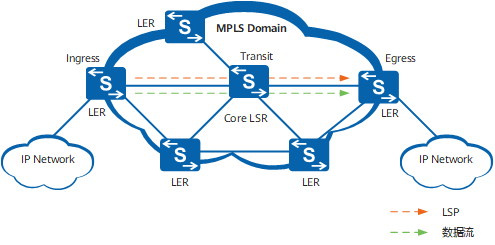
5. 单PSU供电，提供整机功耗；双PSU供电，每个PSU平均功耗提供；一旦某个PSU故障，另一个PSU提供完整整机供电，不影响设备使用。

6. [概览/系统信息]处需显示PSU1/2的相关状态，具体需求详见[*[概览/系统信息]*](#_系统信息/System_Info.)。

# MPLS [TBD]

多协议标签交换MPLS（Multiprotocol Label Switching）是一种IP骨干网技术。MPLS在无连接的IP网络上引入面向连接的标签交换概念，将第三层路由技术和第二层交换技术相结合，充分发挥了IP路由的灵活性和二层交换的简捷性。

MPLS基于标签进行转发。进行MPLS标签交换和报文转发的网络设备称为标签交换路由器LSR；由LSR构成的网络区域称为MPLS域。位于MPLS域边缘、连接其他网络的LSR称为边缘路由器LER，区域内部的LSR称为核心LSR。

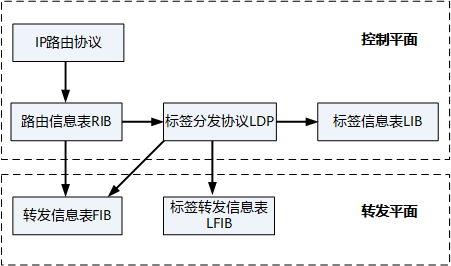


IP报文进入MPLS网络后，MPLS入口的LER分析IP报文的内容并且为这些IP报文添加合适的标签，所有MPLS网络中的LSR根据标签转发数据。当该IP报文离开MPLS网络时，标签由出口LER弹出。

IP报文在MPLS网络中经过的路径称为标签交换路径LSP。LSP是一个单向路径，与数据流的方向一致。其中，LSP的入口LER称为入节点（Ingress）；位于LSP中间的LSR称为中间节点（Transit）；LSP的出口LER称为出节点（Egress）。一条LSP可以有0个、1个或多个中间节点，但有且仅有一个入节点和一个出节点。

**体系结构**

MPLS的体系结构由控制平面、转发平面组成。



* 控制平面：负责产生和维护路由信息以及标签信息。
* 路由信息表RIB：由IP路由协议生成，用于选择路由
* 标签分发协议LDP：负责标签的分配、标签转发信息表的建立、标签交换路径的建立、拆除等工作
* 标签信息表LIB：由标签分发协议生成，用于管理标签信息
* 转发平面：即数据平面，负责普通IP报文的转发以及带MPLS标签报文的转发。
* 转发信息表FIB：从RIB提取必要的陆游信息生成，负责普通IP报文的转发
* 标签转发信息表LFIB：简称标签转发表，由标签分发协议在LSR上建立LFIB，负责带MPLS标签报文的转发

**MPLS标签**

转发等价类：MPLS将具有相同特征的报文归为一类，称为转发等价类FEC。属于相同FEC的报文在转发过程中被LSR以相同方式处理。FEC可以根据源地址、目的地址、源端口、目的端口等要素进行划分。

标签：一个短而定长的、只具有本地意义的标识符，用于唯一标识一个分组所属的FEC。在某些情况下比如负载分担时，对应一个FEC可能会有多个入标签。但是一台设备上，一个标签只能代表一个FEC。

**LSP的建立**

MPLS需要为报文事先分配好标签，建立一条LSP，才能进行报文转发。LSP分为静态LSP和动态LSP。

（1）静态LSP的建立：用户通过手工为各个转发等价类分配标签而建立的。由于静态LSP各节点上不能相互感知到整个LSP的情况，因此静态LSP是一个本地的概念。

静态LSP不使用标签发布协议，不需要交互控制报文，因此消耗资源比较小，适用于拓扑结构简单并且稳定的小型网络。但通过静态方式分配标签建立的LSP不能根据网络拓扑变化动态调整，需要管理员干预。

（2）动态LSP的建立

动态LSP的标签发布协议：