M系列交换机

CLI 配置手册

目录

第 1 章 系统状态命令

1.1 命令模式

命令描述

如何进入退出各种模式状态（特权模式、全局模式、接口模式等）

参数

无

缺省

无

命令模式

无

示例

Switch Login: admin

password: admin（隐藏）

switch>

//进入用户模式

switch>enable

switch#

//进入特权模式

switch# configure terminal

switch(config)# exit

switch#

//进入全局模式，exit 退出全局模式回到特权模式

switch# configure terminal

switch(config)# interface G1

switch(config-if)# exit

switch(config)#

//在全局模式下，进入 G1 接口模式，exit 退出接口模式

switch(config)# vlan1

switch(config-vlan)# exit

switch(config)#

//在全局模式下，进入 vlan1 接口模式，exit 退出 vlan1

1.2 System information

此模块可以查询软件版本、编译时间、设备名称、设备序列号、mac 地址、CPU 利用率、内存利用率、系统当前时间等信息。

1.2.1 show system

命令描述

此命令可以查询软件版本、编译时间、设备名称、设备序列号、mac 地址、等信息

参数

无

缺省

无

命令模式

用户模式（ 连接串口，输入设备用户名和密码进入用户模式,使用 exit 退出当前模式）

示例

Switch Login: admin

password: admin（密码为隐藏状态）

switch> show system

```
Switch> show system
Product Model     :  switch
Hardware Version  :  V1
Serial Number     :  SN20210220
MAC Address       :  AC:90:00:3F:3A:60
Firmware Version  :  V1.0.0.1-gd06e45122
Compile Time      :  Mar 23 2021 08:04:22
System Uptime     :  0 Day 0 Hours 56 Minutes 12 Seconds
System Time       :  1970-01-10 09:18:30
```

1.3 Log information

此模块可查看设备运行过程中的一些系统日志信息，方便维护人员分析问题。

1.3.1 show logging

命令描述

查看交换机当前日志信息

参数

无

缺省

无

命令模式

用户模式

示例

Switch> show logging

1.4 Port statistics

在端口统计模块中，可以查看全局端口发送/接收的数据包报文数、字节数，以及端口过滤掉的报文数。

1.4.1 show interface

命令描述

查看交换机端口统计信息

参数

<cr>	查看所有端口的统计信息
G<1-24>	查看某端口的统计信息

缺省

无

命令模式

特权模式

示例

switch# show interface G1

```
switch# show interface G1
G1 is down
  Hardware address is 22-00-00-55-11-23
  Media type is MEDIUM_COPPER, loopback not set
  Autonegotiation enable, Flow control is on
  Speed: 1000, Duplex-auto, Max frame size: 1518
  Ifindex: 0x2010001
  Port link-type: access, PVID is 1
    Untag vid: 1
   0 packets input, 0 bytes
   0 broadcast, 0 multicast
   0 jabber, 0 pause
   0 input errors, 0 CRC, 0 drops
   0 packets output, 0 bytes
   0 broadcast, 0 multicast
   0 output errors, 0 drops
   0 late collision, 0 pause
```

1.5 View route

此功能模块用于查看交换机全局路由信息

1.5.1 show ip route

命令描述

查看交换机当前路由信息

参数

bgp	查看 bgp 路由信息
connected	查看直连路由信息
ospf	查看 ospf 路由信息

rip	查看 rip 路由信息
static	查看静态路由信息
A.B.C.D	查看包含特定 ip 的路由信息
A.B.C.D/M	查看某网段的路由信息
summary	查看所有路由汇总信息

缺省

无

命令模式

用户模式

示例

switch# show ip route

```
Switch> show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       V - VRRP, D - DHCP, M - MRIB, D - PTP,
       > - selected route, * - FIB route

S   10.1.1.0/24 [1/0] via 10.0.0.1 inactive
S   10.1.2.0/24 [2/0] via 10.0.0.2 inactive
C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.10.0/24 is directly connected, vlanif1
Switch>
```

第 2 章 系统设置命令

2.1 IP config

IP 配置命令有：

ip address

ip address dhcp

ip address old_ip A.B.C.D/M new_ip A.B.C.D/M

show ip interface

注意：A.B.C.D/M，格式例如：192.168.1.1/24

ip 配置模块可添加修改或查看交换机的接口 ip 信息；

2.1.1 ip address

命令描述

配置端口 ip 为 A.B.C.D/M

no ip address A.B.C.D/M，表示删除端口 ip A.B.C.D/M

参数

无

缺省

vlan 接口模式

命令模式

在端口配置模式下配置该命令。

示例

switch(config)# interface vlanif1

switch(config-vif)#ip address 192.168.100.1/24

switch(config-vif)#no ip address 192.168.100.1/24

2.1.2 ip address dhcp

命令描述

配置端口 ip 为自动获取方式（ 网络中 dhcp server 会为交换机端口分配一个动态 ip）

no ip address dhcp，表示禁用接口的 ip 为自动获取方式

参数

无

缺省

启用端口

命令模式

在接口配置模式下配置该命令。

示例

switch(config)# interface vlanif1

switch(config-vif)#ip address dhcp

switch(config-vif)#no ip address dhcp

2.1.3 ip address old_ip

命令描述

ip address old_ip A.B.C.D/M new_ip A.B.C.D/M

修改接口的 ip 配置（将 old_ip 修改为 new_ip）

参数

无

缺省

无

命令模式

接口模式

示例

switch(config)# interface vlanif1

switch(config-vif)#ip address old_ip 192.168.255.1/24 new_ip 192.168.10.1/24

2.1.4 show interface

命令描述

查看接口的 ip 配置

参数

无

缺省

启用接口

命令模式

特权模式或全局模式

示例

switch(config)#show interface vlanif1

switch#show interface vlanif1

```
Switch(config)# show  interface vlanif1
Interface vlanif1 is up, line protocol is up
  Link ups:       2  last: Sat, 10 Jan 1970 10:47:27 +0800
  Link downs:     1  last: Sat, 10 Jan 1970 10:47:24 +0800
  vrf: 0
  index 3 metric 0 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  Type: Unknown
  HWaddr: ac:90:00:3f:3a:60
  inet 192.168.10.15/24 broadcast 192.168.10.255
  inet6 fe80:fe00::1/64
  inet6 fe80::ae90:ff:fe3f:3a60/64
Switch(config)#
```

2.2 User config

用户配置命令有：

username

show user

注意：name 表示用户名，最大支持 32 个字符；passwd 表示密码，最大支持 32 个字符；

功能介绍

此功能模块可查看修改或添加用户信息、可达到保护交换机配置的目的

2.2.1 username name

命令描述

username name password passwd

修改一个用户的密码

参数

缺省

命令模式

全局模式

示例

switch(config)#username admin password simple 123456
//修改用户 ：admin，密码为：123456，

show user

命令描述

查看交换机当前所有用户配置信息；

参数

无

缺省

无

命令模式

特权模式

示例

Switch#show user

2.3 Time setting

该配置命令有：

sntp enable|disable

sntp unicast-server

sntp auto-sync timer

sntp connect

sntp timezone

可此功能开启可使交换机自动同步网络时间

2.3.1 sntp enable|disable

命令描述

sntp enable，启用 ntp 功能；

sntp disable，禁用 ntp 功能；

参数

无

缺省

禁用

命令模式

在全局模式下使用该命令

示例

switch(config)#sntp enable

switch(config)#sntp disable

2.3.2 sntp unicast-server

命令描述

sntp unicast-server A.B.C.D

配置 sntp 服务器地址

no sntp unicast-server A.B.C.D，为删除一个 ntp 服务器地址

参数

无

缺省

无

命令模式

全局模式

示例

Switch(config)#sntp unicast-server 210.21.196.6

2.3.3 sntp auto-sync timer

命令描述

配置 sntp 同步时间间隔

参数

sntp auto-sync timer time，time 取值范围 5-65535s，默认值 300s；

缺省

300s

命令模式

全局模式

示例

Switch(config)#sntp auto-sync timer 5

2.3.4 sntp connect

命令描述

sntp connect A.B.C.D

使用该命令选择当前需要连接的 sntp 服务器。

参数

无

缺省

无

命令模式

在全局模式下使用该命令

示例

switch(config)#sntp connect 210.21.196.6

2.3.5 timezone

命令描述

switch(config)# timezone

使用该命令选择当前交换机所处地区的时区

参数

缺省

0

命令模式

全局模式

示例

switch(config)# timezone UTC-8

//修改时区为东八区

第 3 章 端口配置命令

3.1 Port config

端口配置命令有

duplex

speed

flow-control

shutdown

Description

此模块配置交换机端口相关的各项基本参数。端口基本参数将直接影响端口的工作方式。

3.1.1 speed

命令描述

speed {10-(auto/full) | 100-(auto/full/half) | 1000-(auto,full,half)|10000|auto }

设置端口的速率及双工模式

参数

参数	参数命令模式
1000M-auto	设置端口速率为 1000M，双工模式为自动
1000M-full	设置端口速率为 1000M，双工模式为全双工
100M-auto	设置端口速率为 100M，双工模式为自动
100M-full	设置端口速率为 100M，双工模式为全双工
100M-half	设置端口速率为 100M，双工模式为半双工

10G	设置端口速率为 10G
10M-auto	设置端口速率为 10M，双工模式为自动
10M-full	设置端口速率为 10M，双工模式为全双工
10M-half	设置端口速率为 10M，双工模式为半双工
auto	设置端口速率为自协商

缺省

所有接口都是自动协商（auto），

命令模式

接口模式

注：

示例

将 G1 的端口速率设定为 100M 全双工。

Switch(config)# interface G1

switch(config-if)# speed 100M-full

3.1.2 flow-control

命令描述

flowctrl

no flowctrl

配置端口的流量控制功能。

参数

无

缺省

流控功能开启。

命令模式

接口模式

示例

打开端口的流控功能。

switch(config-if)# flowctrl

3.1.3 shutdown

命令描述

shutdown

no shutdown

配置端口的开启关闭。

缺省

端口默认开启。

命令模式

接口模式

示例

关闭端口。

switch(config-if)# shutdown

3.1.4 description

命令描述

配置端口的描述信息，便于管理(由字母、数字和下划线组成)。

缺省

无

命令模式

接口模式

示例

switch(config-if)# description A1

3.2 Rate limit

可配置端口的限速策略，限制所有数据包进出端口的速率。

3.2.1 rate-limit

命令描述

rate-limit {1-10000000 } {1-65535}{1-10000000 }{1-65535 }

no rate-limit

配置端口出口/入口限速功能，使用 no 形式，端口恢复缺省设置。

参数

1-10000000	端口限速速率范围 1-10000000kbps
1-65535	端口限速突发尺寸范围 1-65535kbits

缺省

限速为 0。

命令模式

接口模式

示例

出口限速 10000kbps 突发尺寸 1000kbits，入口不限

switch(config-if)# rate-limit 10000 1000 0 0

3.3 Port mirroring

端口镜像也叫端口监控。端口监控是一种数据包获取技术，通过配置交换机，可以实现将一个/几个端口（镜像源端口）的数据包复制到一个特定的端口（镜像目的端口），在镜像目的端口接有一台安装了数据包分析软件的主机，对收集到的数据包进行分析，从而达到了网络监控和排除网络故障的目的。

3.3.1 monitor

命令描述

mirror to <IFNAME>

mirror sources direction {both|egress|ingress}

no mirror

配置端口镜像功能，使用该命令的 no 形式，删除镜像设置

参数

参数	参数命令模式
IFNAME	端口号，如 G1，X1

缺省

无

命令模式

在全局配置模式下配置目的端口

在接口配置模式下配置源端口

示例

配置目的端口为 G3，源端口为 G1、G2，

switch(config)# monitor to G3

switch(config)# interface G1

switch(config-if)# mirror source direction both

switch(config-if)#exit

switch(config)# interface G2

switch(config-if)# mirror source direction both

3.4 Link aggregation

端口静态聚合配置命令有：

Trunk

端口动态聚合的配置命令有：

lacp enable | disable

lacp active | passive

lacp key

lacp port-priority

链路聚合是将交换机的多个物理端口形成一个逻辑端口，属于同一汇聚组内的多条链路可视为一条更大带宽逻辑链路。

链路聚合可以实现通信流量在聚合组中各个成员端口之间分担，以增加带宽。同时，同一聚合组的各个成员端口之间彼此动态备份，提高了链路的可靠性。

属于同一个汇聚组中的成员端口必须有一致的配置，这些配置主要包括 STP、QoS、VLAN、端口属性、MAC 地址学习、ERPS 配置、loop Protect 配置、镜像、802.1x、IP 过滤、Mac 过滤、端口隔离等。

3.4.1 trunk

命令描述

interface trunk [聚合组 ID]

配置聚合组。

trunk [聚合组 ID]

缺省

无

命令模式

在全局配置模式下配置该命令

示例

switch(config)# interface trunk 1

switch(config)# interface G1

switch(config-if)# trunk 1

3.4.2 load-balance

命令描述

trunk load-balance 设置静态聚合的负载均衡模式

参数

srcdst-mac	基于源目 mac 的负载均衡

dst-mac	基于目的 mac 的负载均衡
src-mac	基于源 mac 的负载均衡

缺省

禁用

命令模式

接口模式

示例

设置负载均衡模式为基于源目的 mac

switch(config)# trunk load-balance both-mac

3.4.3 lacp enable | disable

命令描述

lacp enable，配置端口动态汇聚使能

lacp disable，禁用端口动态汇聚

参数

无

缺省

禁用

命令模式

接口模式

示例

switch(config-if)# lacp disable

3.4.4 lacp active | passive

命令描述

lacp activity-mode active，*设置端口为主动状态*

lacp activity-mode passive，*设置端口为被动状态*

参数

无

缺省

被动

命令模式

接口模式

示例

switch(config-if)# lacp activity-mode active

3.4.5 lacp port-key

命令描述

Lacp key，指动态汇聚端口的管理 key 值 ，是端口能添加到一个汇聚组的标识之一。LACP 协议根据端口的配置（即速率、双工、基本配置、管理 Key）生成的一个操作 key，对于动态汇聚组而言，同组成员一定有相同的操作 Key 才可汇聚成功。

参数

<1-65535>

手动指定范围 1-65535；

缺省

命令模式

端口模式

示例

switch(config)# interface G1

switch(config-if)# lacp port-key 100

3.4.6 lacp port-priority

命令描述

lacp port-priority *<1-32768>* ，配置 lacp 端口优先级

参数

<1-32768> ，优先级范围，数值越小优先级越高

缺省

0

命令模式

接口模式

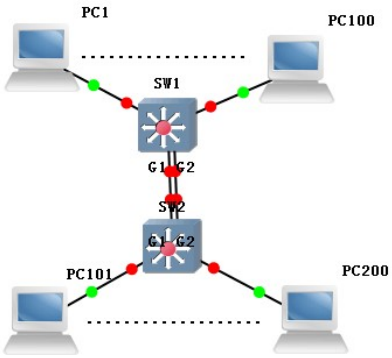
示例

switch(config)# interface G1

switch(config-if)# lacp port-priority 100

3.4.7 example

使用链路聚合增加设备级联端口带宽并且实现基于源目 MAC 的负载分担



SW1/SW2:

switch# configure terminal

switch(config)#trunk load-balance both-mac

switch(config)# interface G1

switch(config-if)# trunk 1

switch(config-if)# exit

switch(config)# interface G2

switch(config-if)# trunk 1

现象

聚合后两条链路形成一条逻辑链路，增加一倍带宽，且根据源或者目的 MAC 进行负载分担，当汇聚组其中一条链路断掉时，数据会走汇聚组其他链路，不会造成通信中断。

第 4 章 高级配置命令

4.1 VLAN config

Vlan 配置命令有：

switchport mode

switchport pvid

switchport trunk|hybrid| access

show vlan

以太网是一种基于 CSMA/CD（带冲突检测的载波侦听多路访问）技术的共享通讯介质。采用以太网技术构建的局域网，既是一个冲突域，又是一个广播域，当网络中主机数目较多时会导致冲突严重，广播泛滥、性能显著下降，甚至网络不可用等问题。通过在以太网中部署网桥或二层交换机，可以解决冲突严重的问题，但仍然不能隔离广播报文。在这种情况下出现了 VLAN（Virtual Local Area Network，虚拟局域网）技术，这种技术可以把一个物理 LAN 划分成多个逻辑的 LAN——VLAN。处于同一 VLAN 的主机能直接互通，而处于不同 VLAN 的主机则不能直接互通。这样，广播报文被限制在同一个 VLAN 内，即每个 VLAN 是一个广播域。

VLAN 的优点如下：

1) 提高网络性能。将广播包限制在 VLAN 内，从而有效控制网络的广播风暴，节省了网络带宽，从而提高网络处理能力。

2) 增强网络安全。不同 VLAN 的设备不能互相访问，不同 VLAN 的主机不能直接通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发。

3) 简化网络管理。同一个虚拟工作组的主机不会局限在某个物理范围内，简化了网络的管理，方便了不同区域的人建立工作组。

4.1.1 switchport mode

命令描述

switchport mode {access | trunk | hybrid }

配置端口模式

参数

参数	参数命令模式
access	访问模式
trunk	中继模式
Hybrid	混合模式

缺省

访问模式

命令模式

端口配置模式

使用命令模式

交换机端口支持以下几种模式：访问模式、中继模式、混合模式

访问模式表示该端口只从属于一个 VLAN，并且只发送和接收无标签的以太网帧

中继模式表示该端口与其它交换机相连，可以发送和接收带标签的以太网帧

混合模式表示该端口既可以连电脑，也可以连交换机和路由器（是 access 模式和 trunk 模式的集合）

示例

将端口配置为 VLAN 中继模式/混合模式/访问模式

Switch(config)# interface G1

Switch(config-if)#switchport mode trunk /hybrid/access

4.1.2 switchport pvid

命令描述

switchport pvid { vlan-id}

参数

参数	参数命令模式
Vlan-id	Vlan 号.取值范围:1-4094.

缺省

Vlan1

命令模式

端口配置模式

使用命令模式

本命令可以改变端口的默认 vlan

示例

将端口的默认 vlan 设置为 vlan2

Switch(config)# interface G1

Switch(config-if)# switchport pvid 2

4.1.3 switchport trunk|hybrid| access

命令描述

switchport trunk tag {vlan-id}

switchport hybrid tag|untag|unpvid {vlan-id}

switchport access {vlan-id}

参数

参数	参数命令模式
Vlan-id	Vlan 号,取值范围:1-4094.

缺省

所有端口都是 vlan1 成员,不属于其它 vlan

命令模式

端口配置模式

使用命令模式

本命令可以将端口设置加入到一个或者多个 vlan

示例

下面命令是将 trunk 模式端口加入到一个 vlan 或者多个 vlan

switch(config)# interface G1

switch(config-if)# switchport mode trunk

switch(config-if)# switchport trunk tag 2

switch(config-if)# switchport trunk tag 3-4

下面命令是将 hybrid 模式端口加入到一个 vlan 或者多个 vlan

switch(config-if)# switchport mode hybrid

switch(config-if)# switchport hybrid tag|untag 2

switch(config-if)# switchport hybrid tag| untag 3-4

下面命令是将 access 模式端口加入到 vlan2

switch(config-if)# switchport access 2

4.1.4 show vlan

命令描述

show vlan [vlan-id]

参数

参数	参数命令模式
vlan-id	显示给定的 VLAN。取值范围：1－4094。

缺省

无

命令模式

用户模式

使用命令模式

本命令可以查看 vlan 成员

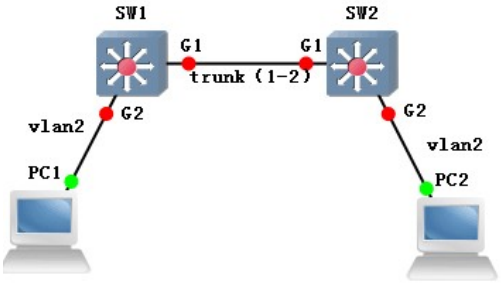
示例

显示所有 VLAN 信息

```
Switch#show vlan
Vid  Status Name      Ports
---- ------ --------- ---------------------------------
1    static vlan1    G1 G2 G3 G4 G5 G6 G7 G8 G9 G10 G11 G12 G13 G14
                     G15 G16 G17 G18 G19 G20 G21 G22 G23 G24 X1 X2
                     X3 X4
2    static vlan2
3    static vlan3
```

4.1.5 example

实现跨交换机的 vlan 通信（pc1 与 pc2 能正常访问）



SW1/SW2：
```
switch# configure terminal
switch(config)# interface G1
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk tag 2
switch(config-if)# exit
switch(config)# interface G2
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 2
```

现象

pc1（192.168.222.107）与 pc2（192.168.222.94）互相 ping 通

4.2 QinQ config

该配置命令有：

Qinq

Qinq otpid

QinQ 技术通过在以太帧中堆叠两个 802.1Q 报头，有效地扩展了 VLAN 数目，使 VLAN 的数目最多可达 4096x4096 个。

4.2.1 qinq

命令描述

使能端口 qinq 功能

no qinq 表示禁用该功能

参数

无

缺省

无

命令模式

接口模式

示例

switch(config)# interface g1

switch(config-if)# qinq

4.2.2 qinq otpid

命令描述

配置 QinQ 层 tag 协议类型

参数

<0x0000-0x9999>	QinQ 层 tag 协议类型

缺省

0x8100

命令模式

接口模式

示例

switch(config-if)# qinq otpid 0x88a8

4.3 MAC config

该配置命令有：

mac-address aging-time

show mac-addres

交换机之所以能够直接对目的节点发送数据包，而不是像集线器一样以广播方式对所有节点发送数据包，最关键的技术就是交换机可以识别连在网络上的节点的网卡 MAC 地址， 并把它们放到一个叫做 MAC 地址表的地方。这个 MAC 地址表存放于交换机的缓存中，并记住这些地址，这样一来当需要向目的地址发送数据时，交换机就可在 MAC 地址表中查找这个 MAC 地址的节点位置，然后直接向这个位置的节点发送。所谓 MAC 地址数量是指交换机的 MAC 地址表中可以最多存储的 MAC 地址数量，存储的 MAC 地址数量越多，那么数据转发的速度和效率也就就越高。

4.3.1 mac-address aging-time

命令描述

mac-address aging-time {10-1000000}

no mac-address aging-time

配置 Mac 老化时间，使用该命令的 no 形式，恢复到缺省设置

参数

参数	参数命令模式
time	以秒为单位的 MAC 地址老化时间。

缺省

300

命令模式

全局配置模式

使用命令模式

在全局配置模式下配置 mac 地址的老化时间

示例

将 MAC 地址老化时间配置为 100 秒

Switch(config)# mac-address aging-time 100

将 MAC 地址老化时间恢复默认 300 秒

Switch(config)# no mac-address aging-time

4.3.2 show mac-address

命令描述

show mac-addres{ aging-time}

参数

无

缺省

无

命令模式

用户模式或全局模式

使用命令模式

使用本命令后，可以查看 mac 地址和 mac 地址的老化时间

示例

下面的命令可以查看 mac 地址和 mac 地址的老化时间

```
switch# show mac-address
MAC                    Vlan Port                    Type
-------------------------------------------------------------------------------
94-de-80-dc-cf-38    1       G4                      dynamic
60-92-17-9d-30-c3    1       G4                      dynamic
Switch# show mac-address aging-time
Mac address aging-time : 100
```

4.4 ARP config

该配置命令有：

show arp

arp static

arp timeout

此功能模块，可查看交换机学习到的 arp 条目信息，可添加 arp 静态条目防止非法主机访问、可修改 arp 条目老化时间。

4.4.1 show arp

命令描述

show arp

如果希望查看动态 ARP 表项，可以通过此命令。

参数

无

缺省

无

命令模式

在全局配置模式下配置该命令。

示例

查看动态 ARP 表项。

Switch(config)# show arp

4.4.2 arp static

命令描述

arp static ip_addr mac_addr

no arp static ip_addr

如果希望添加静态 ARP，可以通过此命令配置。使用该命令的 no 形式取消此配置。

参数

参数	参数命令模式
ip_addr	ip 地址，取值范围 X.X.X.X。
mac_addr	mac 地址，取值范围：H.H.H

缺省

无

命令模式

在全局配置模式下配置该命令。

示例

添加静态 ARP 表项。

switch(config)# arp static 192.168.111.1 00-00-a1-b2-c3-d4

4.4.3 arp timeout

命令描述

arp timeout seconds

no arp timeout

如果希望设置 ARP 老化时间，可以通过此命令配置。使用该命令的 no 形式取消此配置。

参数

参数	参数命令模式
seconds	单位：秒，取值范围 1-2147483。

缺省

无

命令模式

在接口模式下配置该命令。

示例

设置 ARP 老化时间为 3000 秒。

switch(config)# interface vlanif1

switch(config-vlanif1)# arp timeout 3000

4.5 MSTP config

该配置命令有：

spanning-tree

spanning-tree mode

spanning-tree max-age

spanning-tree hello-time

spanning-tree forward-delay

spanning-tree max-hop

spanning-tree instance

show spanning-tree

show spanning-tree interface brief

STP（Spanning Tree Protocol，生成树协议）是根据 IEEE 802.1D 标准建立的，用于在局域网中消除数据链路层物理环路的协议。运行该协议的设备通过彼此交互信息发现网络中的环路，并有选择的对某些端口进行阻塞，最终将环路网络结构修剪成无环路的树型网络结构，从而防止报文在环路网络中不断增生和无限循环，避免设备由于重复接收相同的报文所造成的报文处理能力下降的问题发生。

4.5.1 spanning-tree

命令描述

spanning-tree

no spanning-tree

配置开启 STP 设置，使用该命令的 no 形式，关闭 STP。

参数

无

缺省

缺省开启 STP 模式

命令模式

全局模式

示例

switch(config)# spanning-tree

switch(config)# no spanning-tree

4.5.2 spanning-tree mode

命令描述

spanning-tree mode {stp|rstp|mstp}

参数

Stp	开启STP模式
rstp	开启RSTP模式。
mstp	开启MSTP模式。

缺省

缺省开启 STP 模式

命令模式

全局模式

使用命令模式

配置 spanning-tree 运行模式

示例

下面的命令将开启 STP 模式：

switch(config)# spanning-tree mode rstp

4.5.3 spanning-tree max-age

命令描述

spanning-tree max-age {6-40}

参数

seconds	BPDU最大生存时间。取值范围：6-40s。

缺省

20s

命令模式

全局模式

使用命令模式

配置 STP BPDU 的最大生存时间

示例

下面的命令将配置 STP 的最大生存时间为 24 秒：

Switch(config)# spanning-tree max-age 24

4.5.4 spanning-tree hello-time

命令描述

spanning-tree hello-time｛1-10｝

参数

Time	hello报文发送间隔,取值范围：1-10s。

缺省

2s

命令模式

全局配置模式

示例

下面的命令将配置 STP hello 报文发送间隔时间为 10 秒：

Switch(config)# spanning-tree hello-time 10

4.5.5 spanning-tree forward-delay

命令描述

spanning-tree forward-delay｛4-30｝

参数

time	转发时延时间。取值范围：4-30s。

缺省

15 seconds

命令模式

全局配置模式

示例

下面的命令将配置 STP 的转发延时为 20 秒：

Switch(config)# spanning-tree forward-delay 20

4.5.6 spanning-tree max-hop

命令描述

spanning-tree max-hop｛1-40｝

参数

跳数	BPDU 协议包有效的最大跳数。取值范围：1-40。

缺省

20

命令模式

全局配置模式

示例

下面的命令将配置 BPDU 协议包有效的最大跳数为 40：

Switch(config)# spanning-tree max-hop 40

4.5.7 spanning-tree instance

命令描述

spanning-tree instance 配置 MSTP 的 vlan 与实例的映射关系

参数

缺省

无

命令模式

全局配置模式

示例

switch(config)# spanning-tree instance 44 vid 4

4.5.8 spanning-tree mstp name

命令描述

spanning-tree mstp name 配置 mstp 的域名

参数

缺省

无

命令模式

全局配置模式

示例

switch(config)# spanning-tree mstp name 2

4.5.9 spanning-tree mstp revision

命令描述

spanning-tree mstp revision 配置 mstp 的修订号

参数

缺省

无

命令模式

全局配置模式

示例

switch(config)# spanning-tree mstp revision 2

4.5.10 show spanning-tree

命令描述

show spanning-tree

参数

无

缺省

无

命令模式

特权模式/全局模式

使用命令模式

使用本命令后，可以查看 mstp 信息

示例

下面的命令可以查看 mstp 信息：

switch# show spanning-tree

Spanning-tree is disable:

max age 20 bridge forward delay 20

forward delay 15 max hops 20

hello time 2 orce protocol version mstp

4.5.11 show spanning-tree interface brief

命令描述

show spanning-tree interface brief

参数

无

缺省

无

命令模式

特权模式/全局模式

使用命令模式

使用本命令后，可以查看 mstp 信息

示例 switch(config)# show spanning-tree interface brief

```
switch(config)# show spanning-tree interface brief
MSTID Port        Role              State
----------------------------------------
0     G1          Disabled          discarding
0     G2          Disabled          discarding
0     G3          Disabled          discarding
0     G4          Disabled          discarding
0     G5          Disabled          discarding
0     G6          Disabled          discarding
0     G7          Designated        forwarding
0     G8          Disabled          discarding
```

4.6 IGMP-snooping

该配置命令有：

igmp-snooping

igmp-snooping host-age-time

igmp-snooping fast-leave

igmp-snooping static-group

show igmp-snooping group

IGMP Snooping 是 Internet Group Management Protocol Snooping（互联网组管理协议窥探）的简称，它是运行在二层设备上的组播约束机制，用于管理和控制组播组。

4.6.1 igmp-snooping

命令描述

igmp-snooping

no igmp-snooping

配置开启 IGMP 侦听功能，使用该命令的 no 形式，关闭该功能。

参数

无

缺省

关闭

命令模式

全局模式

示例

下面的命令将配置开启和关闭 igmp-snooping：

Switch(config)# igmp-snooping

Switch(config)#no igmp-snooping

4.6.2 igmp-snooping host-age-time

命令描述

igmp-snooping host-age-time｛200-1000｝

参数

参数	参数命令模式
time	主机老化时间。取值范围：200-1000s。

缺省

300

使用命令模式

配置主机老化时间

命令模式

全局配置模式

示例

下面的命令将配置主机老化时间为 200s：

Switch(config)# igmp-snooping host-age-time 200

4.6.3 igmp-snooping fast-leave

命令描述

igmp-snooping fast-leave

no igmp-snooping fast-leave

配置开启端口快速离开功能，使用该命令的 no 形式，关闭该功能。

参数

无

缺省

关闭

命令模式

接口模式

示例

switch(config)# vlan 1

switch(config-vlan)# igmp-snooping fast-leave

4.6.4 igmp-snooping static-group

命令描述

igmp-snooping static-group 添加静态组播组

no igmp-snooping static-group 删除已添加的静态组播组

参数

无

缺省

关闭

命令模式

接口模式

示例

switch(config)# interface G1

switch(config-if)# igmp-snooping static-group 224.1.1.1 vlan 2

switch(config-if)# no igmp-snooping static-group 224.1.1.1 vlan 2

4.6.5 show igmp-snooping group

命令描述

show igmp-snooping group

参数

无

缺省

无

命令模式

用户模式

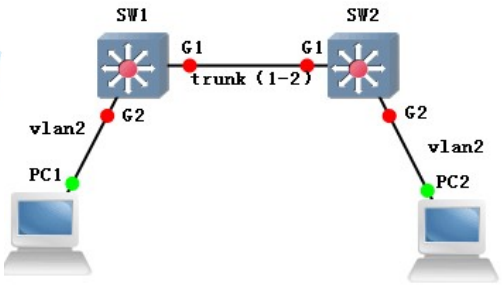
示例

下面的命令将查看组播组信息：

```
switch# show igmp-snooping  group
VID   SOURCE          GROUP          interFACE
---------------------------------------------- ----------------------
1     0.0.0.0         233.45.18.88       G4
1     0.0.0.0         239.255.255.250    G4 G2
1     0.0.0.0         224.0.0.252        G2 G4
```

4.6.6 example

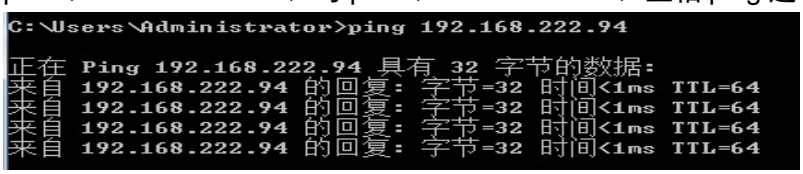
实现跨交换机的 vlan 通信（pc1 与 pc2 能正常访问）



SW1/SW2：switch# configure terminal
switch(config)# interface G1
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk tag 2
switch(config-if)# exit
switch(config)# interface G2
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 2

现象

pc1（192.168.222.107）与 pc2（192.168.222.94）互相 ping 通



4.7 DHCP server

该配置的命令有：

dhcp-server

network

default-router

dns-server

static

lease

domain-name

netbios-name-server

DHCP Server ：指在一个特定的网络中管理 DHCP 标准的一台计算机。DHCP 服务器的职责是当工作站登录进来时分配 IP 地址，并且确保分配给每个工作站的 IP 地址不同，DHCP 服务器极大地简化了以前需要用手工来完成的一些网络管理任务。

4.7.1 ip dhcpd

命令描述

dhcp-server enable 开启 DHCP Server 功能

dhcp-server disable 关闭 DHCP Server 功能

参数

无

缺省

关闭

使用命令模式

使用本命令后，可以

命令模式

全局模式

示例

开启 DHCP Server 功能

switch(config)# dhcp-server enable

4.7.2 pool

命令描述

dhcp-server pool <NAME>建立 DHCP 地址池

no dhcp-server pool <NAME>删除 DHCP 地址池

参数

参数	参数命令模式
NAME	地址池名字，如 dizhichi

缺省

无

命令模式

全局模式

示例

建立名为 1 的地址池

switch(config)# dhcp-server pool 1

4.7.3 network

network A.B.C.D/M vlanif-id 设置 DHCP 下发的地址网段

参数

参数	参数命令模式
A.B.C.D/M	地址池地址范围，如 192.168.1.0/24
vlanif-id	需要从哪个 vlan 下发配置 ID

缺省

无

命令模式

dhcp-server 配置模式

示例

设置 DHCP 下发地址网段为 192.168.1.0/24

switch(config-dhcps)#Network 192.168.1.0/24

4.7.4 default-router

命令描述

default-router A.B.C.D 用于设置 DHCP 下发的地址的网关

参数

参数	参数命令模式
A.B.C.D	DHCP 下发的网关地址

缺省

无

命令模式

dhcp-server 配置模式

示例

switch(config-dhcps)#Default-router 192.168.1.1

设置 DHCP 下发地址的网关

4.7.5 dns-server

命令描述

dns-server A.B.C.D 可以设置 DHCP 的 DNS

参数

参数	参数命令模式
A.B.C.D	DHCP 下发的 DNS 地址

缺省

无

命令模式

dhcp-server 配置模式

示例

设置 DNS 服务器地址为 192.168.1.1 114.114.114.114

switch(config-dhcps)#dns-server 192.168.1.1 114.114.114.114

4.7.6 static

命令描述

static A.B.C.D MAC

no static A.B.C.D

设置静态绑定条目，使用该命令的 no 形式，删除静态绑定条目。

参数

参数	参数命令模式
A.B.C.D	静态绑定的 IP 地址
MAC	静态绑定的 MAC 地址

缺省

无

命令模式

dhcp-server 配置模式

示例

静态绑定 192.168.1.1 与 11-11-11-11-11-11，然后删除该条目

switch(config-dhcps)#static 192.168.1.1 11-11-11-11-11-11

switch(config-dhcps)#no static 192.168.1.1

4.7.7 lease

命令描述

lease <0-31536000>/infinite

设置 dhcp 地址的租期时间

参数

参数	参数命令模式
<0-31536000>	时间范围 单位：秒
infinite	租期时间无限

缺省

Infinite

命令模式

dhcp-server 配置模式

示例

配置 dhcp 地址池租期时间为 3600 秒

switch(config-dhcp)# lease 3600

4.7.8 domain-name

命令描述

domain-name domain

设置 dns 服务器的域名

参数

参数	参数命令模式
domain	域名 ，如：www.dahua.com

缺省

无

命令模式

dhcp-server 配置模式

示例

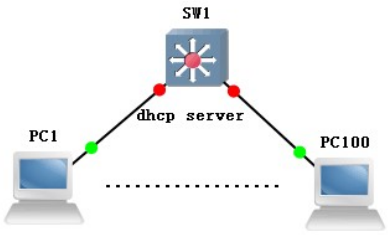
设置主 DNS 服务器域名为 www.dahua.com

switch(config)# dhcp pool 1

switch(config-dhcp)# domain-name www.dahua.com

4.7.9 example

配置交换机为 dhcp 服务器，客户端 ip 信息由服务器统一分配



switch# configure terminal

switch(config)# dhcp-server enable

switch(config)# dhcp-server pool a

switch(config-dhcps)# default-router 192.168.1.1

switch(config-dhcps)#dns-server 8.8.8.8

switch(config-dhcps)# lease 1000

switch(config-dhcps)# network 192.168.1.0/24

现象

pc1-pc100 等客户端可从 dhcp server（sw1）获取到正确的 ip 信息。

注：配置 vlan 的 dhcp server 时，需配置同 vlan 的三层接口，dhcp server 才能给相应 vlan 下的客户端下发 ip 信息

4.8 DHCP relay

功能介绍

如果 DHCP 客户机与 DHCP 服务器在同一个物理网段，则客户机可以正确地获得动态分配的 ip 地址。如果不在同一个物理网段，则需要 DHCP Relay Agent(中继代理)。用 DHCP Relay 代理可以去掉在每个物理的网段都要有 DHCP 服务器的必要,它可以传递消息到不在同一个物理子网的 DHCP 服务器，也可以将服务器的消息传回给不在同一个物理子网的 DHCP 客户机。

4.8.1 dhcp-relay

命令描述

dhcp-relay

参数

无

缺省

禁用

命令模式

特权模式，接口模式

示例

开启 DHCP 服务器中继功能。

switch(config)# dhcp-relay enable

在 vlan1 开启 192.168.1.1DHCP 服务器中继功能。

switch(config-vif)# dhcp-relay remote-server 192.168.1.1

4.9 DHCP snooping

该配置的命令有：

dhcp-snooping

4.9.1 dhcp-snooping

命令描述

dhcp-snooping

no dhcp-snooping

开启 DHCP 侦听功能，使用该命令的 no 形式，关闭该功能。

参数

无

缺省

禁用

命令模式

全局模式

示例

无

4.9.2 dhcp-snooping

命令描述

dhcp-snooping untrust

no dhcp-snooping untrust

设置端口的模式为不信任，使用该命令的 no 形式，端口模式配置为信任。

参数

无

缺省

非信任

命令模式

端口模式

示例

设置端口 1 的模式为信任

Switch(config-if)# no dhcp-snooping untrust

4.9.3 show dhcp-snooping

命令描述

show dhcp-snooping

参数

无

缺省

无

命令模式

特权模式

示例

switch# show dhcp-snooping

4.10 QoS config

该配置的命令有：

qos

cos default

cos map

dscp map

scheduler police

功能介绍

QoS（Quality of Service，服务质量）指一个网络能够利用各种基础技术，为指定的网络通信提供更好的服务能力，是网络的一种安全机制， 是用来解决网络延迟和阻塞等问题的一种技术。 在正常情况下，如果网络只用于特定的无时间限制的应用系统，并不需要 QoS，比如 Web 应用，或 E-mail 设置等。但是对关键应用和多媒体应用就十分必要。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。

4.10.1 QOS

命令描述

Qos remask<all/cos/dscp>

更改 QoS 信任模式权重。

参数

无

缺省

cos

命令模式

接口模式

示例

修改优 G1 端口的 qos 信任模式为 dscp

switch(config)# interface G1

switch(config-if)# qos trust dscp

4.10.2 cos default

命令描述

cos default<0-7>

参数

无

缺省

0

命令模式

接口模式

示例

修改 G1 端口的默认 cos 优先级

switch(config)# interface g1

switch(config-if)# cos default 6

4.10.3 cos map

命令描述

cos map

设置 cos 优先级与队列的映射关系

参数

无

缺省

优先级与队列一一映射

命令模式

全局模式

示例

将 cos 优先级 0 映射到队列 3

switch(config)# cos map 0 3

4.10.4 dscp map

命令描述

dscp map

设置 dscp 优先级与 cos 优先级的映射关系

参数

无

缺省

Dscp 优先级	Cos 优先级
0-7	0

8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

命令模式

全局模式

示例

将 dscp 优先级 45 映射到 cos 优先级 7

switch(config)# dscp map 45 7 7

4.10.5 scheduler policy

命令描述

scheduler police

设置 Qos 调度算法

参数

sp	严格优先级方式：首先为最高优先级的队列进行服务，直到这个优先级为空，然后为下一个次高优先级的队列服务，以此类推。
wrr	加权轮询调度算法：支持不同的带宽需求，可以为不同的队列分配不同比例的输出带宽。

缺省

sp

命令模式

全局模式

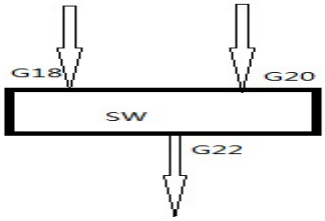
示例

switch(config)# scheduler policy wrr 1 2 3 4 5 6 7 8

4.10.6 example

测试拓扑（测试基于端口的 QoS）

Ixia 测试仪的 1-3 口分别对应交换机的 G18-G22



（一）配置

//当入端口的数据包不带任何优先级标志，会带上端口设置的优先级进入到相应队列

设置交换机 18 口入的数据包打上优先级 7，20 口入的数据包打上优先级 6。

switch(config)#interface G18

switch(config-if)cos default 7

switch(config-if)no qos trust

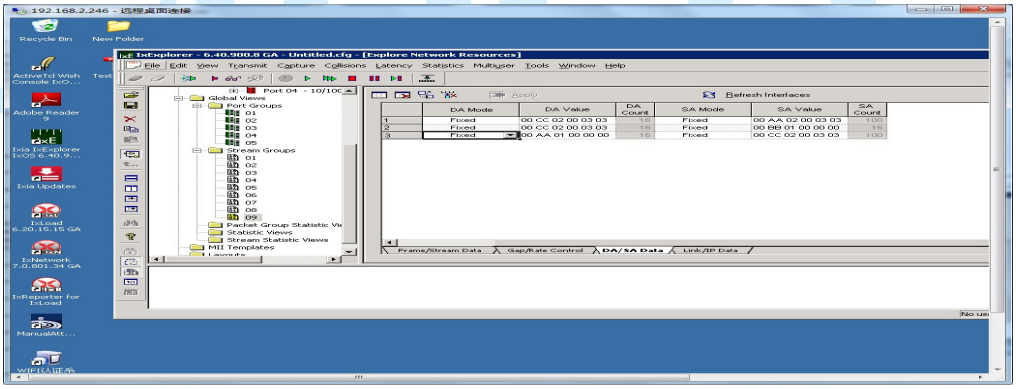
switch(config-if)exit

switch(config)#interface G20

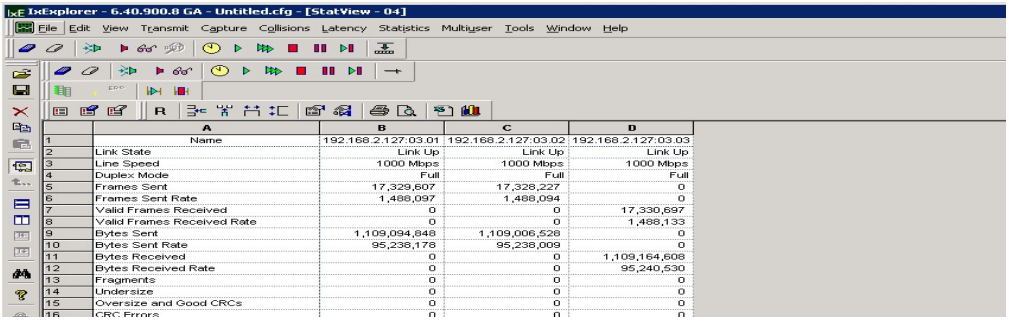
switch(config-if)cos default 6

switch(config-if)no qos trust

b、设置 Ixia1-2 口的目的地址为 Ixia3 口



c、学习 MAC 地址后开始 1-2 口的发包动作



	A	B	C	D
1	Name	192.168.2.127:03.01	192.168.2.127:03.02	192.168.2.127:03.03
2	Link State	Link Up	Link Up	Link Up
3	Line Speed	1000 Mbps	1000 Mbps	1000 Mbps
4	Duplex Mode	Full	Full	Full
5	Frames Sent	17,329,607	17,328,227	0
6	Frames Sent Rate	1,488,097	1,488,094	0
7	Valid Frames Received	0	0	17,330,697
8	Valid Frames Received Rate	0	0	1,488,133
9	Bytes Sent	1,109,094,848	1,109,006,528	0
10	Bytes Sent Rate	95,238,178	95,238,009	0
11	Bytes Received	0	0	1,109,164,608
12	Bytes Received Rate	0	0	95,240,530
13	Fragments	0	0	0
14	Undersize	0	0	0
15	Oversize and Good CRCs	0	0	0
16	CRC Errors	0	0	0

（二）测试结果

结论：pass

在 3 端口抓包观察原 MAC 地址可以看到接收到的数据包是来自端口 1

先队列高的数据包通过

第 5 章 网络安全命令

5.1 Anti-attack

防攻击配置命令有：

system ignore icmp-echo

system protection syn-ack

system rate-limit

功能介绍

防攻击配置用于忽略目的为本设备的 ICMP 请求、防御对本设备的 TCP SYN 攻击以及控制 CPU 接收数据的阀值。

5.1.1 system ignore icmp-echo

命令描述

如果希望忽略目的为本设备的 ICMP 请求，可以通过此命令配置。使用该命令的 no 形式取消此配置。

system ignore icmp-echo

no system ignore icmp-echo

参数

无

缺省

无

命令模式

在全局配置模式下配置该命令。

示例

配置忽略目的为本设备的 ICMP 请求。

switch(config)# system ignore icmp-echo

5.1.2 system protection ddos

命令描述

如果希望防御对本设备的 ddos 攻击，可以通过此命令配置。使用该命令的 no 形式取消此配置。

system protection ddos

no system protection ddos

参数

缺省

无

命令模式

全局模式

示例

配置防御对本设备的 ddos 攻击。

switch(config)# system protection ddos

5.1.3 system rate-limit

命令描述

如果希望控制 CPU 接收数据的阀值，可以通过此命令配置。使用该命令的 no 形式取消此配置。

system rate-limit value

no system rate-limit

参数

参数	参数命令模式
value	<0-100000> pps，默认值 0 :disable limited。

缺省

无

命令模式

全局模式

示例

配置 CPU 接收数据的阀值为 1000。

switch(config)# system rate-limit 1000

关闭 CPU 接收数据的阀值控制功能。

switch(config)# no system rate-limit

5.2 MAC binding

MAC 绑定配置命令有：

mac-address static

5.2.1 mac-address static

命令描述

mac-address static mac-addr vlan vlan-id interface interface-id

no mac-address static mac-addr vlan vlan-id

如果希望添加一个静态 MAC 地址，可以通过此命令配置。使用该命令的 no 形式取消此配置。

参数

参数	参数命令模式
mac-addr	MAC 地址。取值范围：H.H.H。
vlan-id	该 MAC 地址所属 VLAN。取值范围：1－4094。
interface-id	该 MAC 地址所属物理端口。

缺省

无

命令模式

在全局配置模式下配置该命令。

示例

配置 MAC 地址 00-00-0 0-00-00-01 绑定到属于 VLAN2 的端口 G10 上。

switch(config)# mac-address static 00-00-00-00-00-01 vlan 2 interface G10

5.3 ARP binding

该配置的命令有：

arp

功能介绍

为了更好的对网络中的计算机进行管理，您可以通过 ARP 绑定功能来控制网络中计算机间的访问(IP 绑定)。

5.3.1 arp static

命令描述

arp static

参数

缺省

无

命令模式

在全局配置模式下配置该命令。

示例

switch(config)# arp static 192.168.1.1 50-46-5D-E2-D5-50

5.3.2 show arp

命令描述：

查看该 arp 地址的绑定

show arp

参数：

缺省

无

命令模式

在特权配置模式下配置该命令。

示例

显示 ARP 绑定列表

switch(config)# show arp

5.4 ACL config

该配置的命令有：

mac acl

ip acl

rule

ip/mac access-group

功能介绍

访问控制列表（Access Control List，ACL） 用来控制端口进出的数据包。

信息点间通信和内外网络的通信都是企业网络中必不可少的业务需求，为了保证内网的安全性，需要通过安全策略来保障非授权用户只能访问特定的网络资源，从而达到对访问进行控制的目的。简而言之，ACL 可以过滤网络中的流量，是控制访问的一种网络技术手段。

配置 ACL 后，可以限制网络流量，允许特定设备访问，指定转发特定端口数据包等。如可以配置 ACL，禁止局域网内的设备访问外部公共网络，或者只能使用 FTP 服务。ACL 既可以在路由器上配置，也可以在具有 ACL 功能的业务软件上进行配置。

ACL 是物联网中保障系统安全性的重要技术，在设备硬件层安全基础上，通过对在软件层面对设备间通信进行访问控制，使用可编程方法指定访问规则，防止非法设备破坏系统安全，非法获取系统数据。

5.4.1 mac acl

命令描述

mac acl <1-99>

no mac acl <1-99>

如果希望添加一个 mac acl 组，可以通过此命令配置。使用该命令的 no 形式删除该组。

参数

参数	参数命令模式
<1-99>	mac acl 组编号，范围：1-99

缺省

无

命令模式

全局模式

使用命令模式

使用本命令后，可以添加一个 mac acl 组

示例

switch(config)#mac acl 1

5.4.2 ip acl

命令描述

ip acl <100-999>

no ip acl <100-999>

如果希望添加一个 ip acl 组，可以通过此命令配置。使用该命令的 no 形式删除该组。

参数

参数	参数命令模式
<100-999>	ip acl 组编号，范围：100-999

缺省

无

命令模式

全局模式

示例

switch(config)#ip acl 100

5.4.3 rule

命令描述

rule <1-127> deny/permit <source mac> <destination mac> cos <0-7>/vlan <1-4094>/eth_type ETHTYPE

rule <1-127> deny/permit icmp/igmp/tcp/udp/ip <source ip> <destination ip> ip_pri<0-7> / tos_pri<0-15>/ dscp_pri<0-63>

no rulel <1-127>

如果希望添加一个 acl 规则，可以通过此命令配置。使用该命令的 no 形式删除该组。

参数

参数	参数命令模式
<1-127>	规则编号，范围：1-127
source mac	源 mac 地址，any 表示任意
destination mac	目的 mac 地址，any 表示任意
1-4094	vlan 号，范围：1-4094
ETHTYPE	以太网类型，范围 0x0000-0xFFFF; 0x0000 或者不填表示不匹配以太类型字段，
source ip	源 ip 地址，any 表示任意
destination ip	目的 ip 地址，any 表示任意
<0-7>	要匹配的 IP 优先级，范围 0-7
<0-15>	要匹配的 TOS，范围 0-15
<0-63>	要匹配的 DSCP，范围 0-63

缺省

无

命令模式

全局模式

使用命令模式

使用本命令后，可以添加一个 acl 规则

示例

添加一条 mac acl 1 的 rule 1

switch(config)#mac acl 1

switch(config-acl-mac)#rule 1 deny any any

5.4.4 ip/mac access-group

命令描述

ip access-group <100-999>

no ip access-group <100-999>

mac access-group <1-99>

no mac access-group <1-99>

使用本命令后，可以绑定端口使用的 acl 规则

参数

参数	参数命令模式
<100-999>	ip acl 组编号，范围：100-999
<1-99>	mac acl 组编号，范围：1-99

缺省

无

命令模式

端口模式

示例

Switch(config-if)# ip access-group <100-999>

5.5 802.1X config

该配置的命令有：

dot1x auth-port system-auth-ctrl

dot1x initialize interface IFNAME

dot1x radius-client source-interface HOSTNAME PORT

dot1x radius-server deadtime MIN

dot1x radius-server host HOSTNAME auth-port PORTNO key STRING retransmit RETRIES timeout SEC

dot1x re-authenticate interface IFNAME

功能介绍

802.1x 协议是基于 Client/Server 的访问控制和认证协议。它可以限制未经授权的用户/设备通过接入端口(access port)访问 LAN/WLAN。在获得交

换机或 LAN 提供的各种业务之前，802.1x 对连接到交换机端口上的用户/设备进行认证。在认证通过之前，802.1x 只允许 EAPoL（基于局域网的扩展认证协议）数据通过设备连接的交换机端口；认证通过以后，正常的数据可以顺利地通过以太网端口。

5.5.1 dot1x auth-port system-auth-ctrl

命令描述

dot1x auth-port system-auth-ctrl

no dot1x auth-port system-auth-ctrl

开启关闭基于端口的 Dot1x 功能。

参数

无

缺省

无

命令模式

全局模式

使用命令模式

使用本命令后，可以开启 802.1X 功能，使用该命令的 no 形式，关闭该功能。

示例

switch(config)# dot1x auth-port system-auth-ctrl

5.5.2 dot1x initialize interface IFNAME

命令描述

dot1x initialize interface IFNAME

初始化端口的 802.1X 认证。

参数

参数	参数命令模式
IFNAME	指定接口名称，如 G1，X1 等

缺省

无

命令模式

全局模式

使用命令模式

使用本命令后，初始号认证，已连接的会话将会断开。

示例

switch(config)# dot1x initialize interface G1

5.5.3 dot1x radius-client source-interface HOSTNAME PORT

命令描述

dot1x radius-client source-interface HOSTNAME PORT

参数

参数	参数命令模式
HOSTNAME	RADIUS 客户端（主机名或 IP）
PORT	客户端端口号（默认为 1812）

缺省

无

命令模式

全局模式

使用命令模式

使用本命令后，可以设置 radius 客户端的 IP 和端口号

示例

Switch(config)#dot1x radius-client source-interface 192.168.200.200 1812

5.5.4 dot1x radius-server deadtime MIN

命令描述

dot1x radius-server deadtime MIN

配置计费服务器的 IP 地址及备用服务器 IP 地址和秘钥。

参数

参数	参数命令模式
MIN	RADIUS 服务器死亡时间（以分钟为单位）<0-1440>，默认为 0

缺省

无

命令模式

全局模式

使用命令模式

使用本命令后，可以设置 Radius 服务器的死亡时间

示例

switch(config)# dot1x radius-server deadtime 5

5.5.5 dot1x radius-server

命令描述

dot1x radius-server host HOSTNAME auth-port PORTNO key STRING retransmit RETRIES timeout SEC

配置认证服务器的更新间隔/保持认证时间。

参数

参数	参数命令模式
HOSTNAME	RADIUS 服务器（主机名或 IP）
PORTNO	Radius 服务器端口号（默认 1812）
STRING	RADIUS 服务器密钥串
RETRIES	重传次数（范围 1-100）
SEC	RADIUS 服务器超时（以秒为单位）<1-1000>

缺省

无

命令模式

全局模式

使用命令模式

使用本命令后，可以设置 Radius 服务器相关参数

示例

switch(config)#Dot1x radius-server host 192.168.200.1 auth-port 1812 key 123456 retransmit 3 timeout 5

5.5.6 dot1x re-authenticate

命令描述

dot1x re-authenticate interface IFNAME

手动对指定端口进行重认证。

参数

IFNAME	指定接口名称，如 G1，X1 等

缺省

无

命令模式

全局模式

使用命令模式

使用本命令后，对指定端口进行重认证

示例

配置端口 G1 的重认证

Switch(config)# dot1x re-authenticate interface

5.5.7 dot1x initialize

命令描述

dot1x initialize

对指定端口进行初始化，即禁用端口并尝试重新验证。

参数

无

缺省

无

命令模式

端口模式

使用命令模式

使用本命令后，对指定端口进行重认证

示例

端口 G1 初始化

Switch(config)# interface G1

Switch(config-if)# dot1x initialize

5.5.8 dot1x keytxenabled

命令描述

dot1x keytxenabled enable/disable

使能/去使能指定端口的密码传输开关。

参数

无

缺省

无

命令模式

端口模式

使用命令模式

使用本命令后，使能指定端口的密码传输开关

示例

端口 G1 初始化

Switch(config)# interface G1

Switch(config-if)# dot1x keytxenabled enable

5.5.9 dot1x port-control

命令描述

dot1x port-control auto

dot1x port-control dir both/in

dot1x port-control force-authorized

dot1x port-control unforce-authorized

配置指定端口的认证模式。

参数

无

缺省

无

命令模式

端口模式

使用命令模式

使用本命令设置指定端口的认证模式

示例

配置 G1 口认证模式为自动，控制方向为双向

Switch(config)# interface G1

Switch(config-if)#dot1x port-control auto

Switch(config-if)# dot1x port-control dir both

5.5.10 dot1x protocol-version

命令描述

dot1x protocol-version 1/2

配置指定端口的认证协议版本，默认为 2。

参数

无

缺省

无

命令模式

端口模式

使用命令模式

使用本命令设置指定端口的认证协议版本

示例

配置 G1 口认证协议版本为 1

Switch(config)# interface G1

Switch(config-if)#dot1x protocol-version 1

5.5.11 dot1x quiet-period

命令描述

dot1x quiet-period <1-65535>

认证失败后处于无提示状态的时间，默认为 60s。

参数

无

缺省

无

命令模式

端口模式

使用命令模式

使用本命令设置认证失败后处于无提示状态的时间

示例

配置 G1 口静默时间为 60s

Switch(config)# interface G1

Switch(config-if)#dot1x quiet-period 60

5.5.12 dot1x re-authenticate

命令描述

dot1x re-authenticate

对指定端口进行重认证。

参数

无

缺省

无

命令模式

端口模式

使用命令模式

使用本命令对指定端口进行重认证

示例

配置 G1 重认证

Switch(config)# interface G1

Switch(config-if)#dot1x re-authenticate

5.5.13 dot1x reauthMax

命令描述

dot1x reauthMax <1-10>

未授权前的重新验证尝试次数（默认 2）。

参数

无

缺省

无

命令模式

端口模式

使用命令模式

使用本命令设置指定端口未授权前的重新验证尝试次数

示例

配置 G1 重认证次数为 5

Switch(config)# interface G1

Switch(config-if)#dot1x reauthMax 5

5.5.14 dot1x reauthentication

命令描述

dot1x reauthentication

使能指定端口的重认证，前面加 no 命令去使能。

参数

无

缺省

无

命令模式

端口模式

使用命令模式

使用本命令设置指定端口重认证开关

示例

启用 G1 重认证

Switch(config)# interface G1

Switch(config-if)#dot1x reauthentication

5.5.15 dot1x timeout

命令描述

dot1x timeout re-authperiod <1-4294967295>

重新授权尝试之间的秒数（默认 3600 秒）

dot1x timeout server-timeout <1-65535>

认证服务器响应超时（默认 30 秒）

dot1x timeout supp-timeout <1-65535>

请求方响应超时（默认 30 秒）

dot1x timeout tx-period <1-65535>

连续请求 id 尝试之间的秒数（默认 30 秒）

参数

无

缺省

无

命令模式

端口模式

使用命令模式

使用本命令设置超时时间

示例

无

5.6 Port isolation

端口隔离配置命令有：

switchport protected

功能介绍

端口隔离是为了实现报文之间的二层隔离，可以将不同的端口加入不同的 VLAN，但会浪费有限的 VLAN 资源。采用端口隔离特性，可以实现同一 VLAN 内端口之间的隔离。用户只需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。

5.6.1 switchport protected

命令描述

switchport protected

no switchport protected

如果希望配置端口隔离，可以通过此命令配置。使用该命令的 no 形式取消此配置。

参数

无

缺省

无

示例

配置 G1 端口隔离。

switch(config)# interface G1

switch(config-if)# switchport protected

5.7 Storm control

该配置命令有：

storm-control broadcast pps

storm-control multicast pps

storm-control unicast pps

功能介绍

风暴抑制是指用户可以限制端口上允许接收的广播流量大小，当该类流量超过用户设置的阈值后，系统将丢弃超出流量限制的数据帧，防止风暴的发生，从而保证网络的正常运行。

5.7.1 storm-control broadcast pps

命令描述

storm-control broadcast pps vlaue

no storm-control broadcast

如果希望抑制端口的广播报文，可以通过此命令配置。使用该命令的 no 形式取消此配置。

参数

参数	参数命令模式
Value	取值范围：0-1000000 单位 pps，默认值 0,表示不抑制。

缺省

无

命令模式

在端口模式下配置该命令。

示例

抑制 G1 号端口下的广播报文速率为 1000pps。

switch(config)# interface G1

switch(config-if)# storm-control broadcast pps 1000

5.7.2 storm-control multicast pps

命令描述

storm-control multicast pps vlaue

no storm-control multicast

如果希望抑制端口的组播报文，可以通过此命令配置。使用该命令的 no 形式取消此配置。

参数

参数	参数命令模式
value	取值范围：0-1000000 单位 pps，默认值 0，表示不抑制。

缺省

无

命令模式

在端口模式下配置该命令。

示例

抑制 G1 号端口下的组播报文速率为 1000pps。

switch(config)# interface G1

switch(config-if)# storm-control multicast pps 1000

5.7.3 storm-control unicast pps

命令描述

storm-control unicast pps vlaue

no storm-control unicast

如果希望抑制端口的单播报文，可以通过此命令配置。使用该命令的 no 形式取消此配置。

参数

参数	参数命令模式
value	取值范围：0-1000000 单位 pps，默认值 0，表示不抑制。

缺省

无

命令模式

在端口模式下配置该命令。

示例

抑制 G1 号端口下的单播报文速率为 1000pps。

switch(config)# interface G1

switch(config-if)# storm-control unicast pps 1000

5.8 ERPS config

功能介绍

ERPS（Ethernet Ring Protection Switching）：以太网多环保护技术，协议标准为 ITU-TG.8032 多环标准 。ERPS 追求更高性能、更加安全是网络永远的发展方向，以太环网技术成为二层网络中重要的冗余保护手段。

在二层网络中，对于网络可靠性一般采用 STP 协议，还有上节提到的环路保护协议，STP 协议是由 IEEE 开发的一种标准的环网保护协议，已得到广泛应用，但实际应用中受到网络大小的限制，收敛时间受网络拓扑影响。STP 一般收敛时间为秒级，网络直径较大时收敛时间更长，采用 RSTP/MSTP 虽然可以减少收敛时间，达到毫秒级，但是对于 3G/NGN 语音等高服务质量要求的业务仍然不能满足要求。为更大缩短收敛时间，消除网络尺寸的影响，ERPS 协议应运而生。

ERPS 是一个专门应用于以太网环的链路层协议，它在以太网环中能

够防止数据环路引起的广播风暴；当以太网环上一条链路断开时，能迅速启用备份链路以恢复环网上各个节点之间的通信。和 STP 协议相比，ERPS 协议具有拓扑收敛速度快（低于 20ms） 和收敛时间与环网上节点数无关的特点。

5.8.1 erps

命令描述

Erps enable/disable

参数

无

缺省

关闭

命令模式

全局

使用命令模式

使用本命令后，可以对 erps 进行全局模式

示例

Switch(config)# erps enable

Switch(config)# erps disable

5.8.2 erps xx

命令描述

erps physical-ring Ring ID east-interface PORT(A) west-interface PORT(B)

erps instance Instance ID

ring type major-ring/sub-ring

raps-cannel-vlan VLAN ID

node-role owner/neighbour/normal/interconnection

data-traffic-vlan reference-stg STG ID

参数

参数	参数命令模式
Ring ID	1-255
PORT(A)	任意端口
PORT(B)	除上面填写的端口

Instance ID	1-64
VLAN ID	协议 vlan，范围 2-4094，不能和业务 vlan 重复
node-role	一个 ERPS 环当中有且仅有一个 Owner 节点
STG ID	业务 vlan 实例

缺省

关闭

命令模式

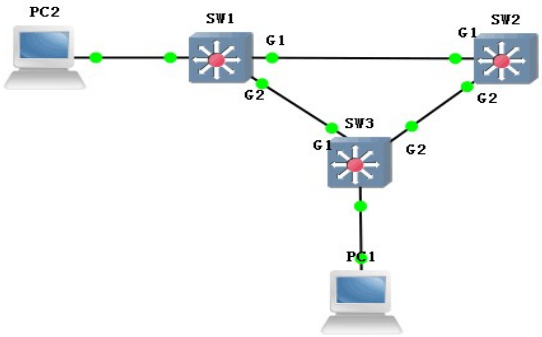
全局模式

5.8.3 example

三台设备组 erps 环，设置 sw1 上 G1 为主端口（负责控制转发状态，即存在环路时会阻塞此端口）

环路时 pc1 与 pc2 正常访问

当阻塞端口所在链路以外的其他链路出现故障时，erps 能实现较快速切换



sw1：switch(config)#erps enable

switch(config)#erps physical-ring 1 east-interface G1 west-interface G2

swtich(config)#erps instance 1

swtich(config-erps-instance)#physical-ring 1

swtich(config-erps-instance)#ring-type major-ring

swtich(config-erps-instance)#node-role owner east-interface

swtich(config-erps-instance)#raps-channel-vlan 3001

swtich(config-erps-instance)#data-traffic-vlan reference-stg 0

swtich(config-erps-instance)#erps enable

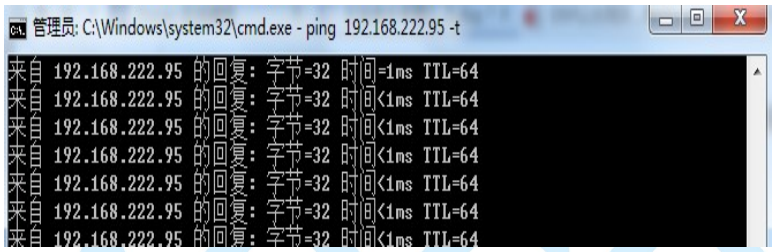
sw2/sw3：switch(config)#erps enable

switch(config)#erps physical-ring 1 east-interface G1 west-interface G2
swtich(config)#erps instance 1
swtich(config-erps-instance)#physical-ring 1
swtich(config-erps-instance)#ring-type major-ring
swtich(config-erps-instance)#node-role normal
swtich(config-erps-instance)#raps-channel-vlan 3001
swtich(config-erps-instance)#data-traffic-vlan reference-stg 0
swtich(config-erps-instance)#erps enable

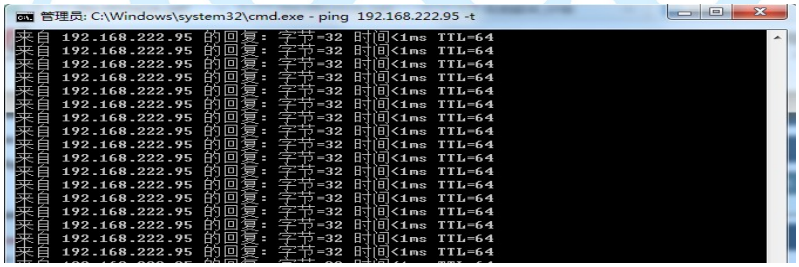
现象

阻塞 SW1 上的 G1 端口

pc1（192.168.222.107） ping pc2（192.168.222.95）



手动切断阻塞端口所在链路外的链路，能实现快速切换，ping 未中断



5.9 IP source guard

该配置命令有：

ip source-guard
ip source-guard trust<0/1/2/3>
ip dhcp-snooping binding

功能介绍

通过 IP 源保护功能，可以对端口转发的报文进行过滤控制，防止非法报文通过端口，从而限制了对网络资源的非法使用（比如非法主机仿冒合法用户 IP 接入网络），提高了端口的安全性。

如果交换机的端口配置了 IP 源保护，则当报文到达该端口时，设备会检

查 IP 源保护的表项，符合表项的报文则可以转发或者进入后续流程，不符合表项的报文将被丢弃。绑定功能是针对端口的，一个端口被绑定后，仅该端口被限制，其他端口不受该绑定影响。

5.9.1 ip source-guard

命令描述

ip source-guard

no ip source-guard

配置开启 IP 源保护功能，使用该命令的 no 形式，关闭该功能 S

参数

无

缺省

禁止

命令模式

全局模式

使用命令模式

使用本命令后，可以开启 IP 源保护功能

示例

Switch(config)#Ip source-guard

5.9.2 ip source-guard trust

命令描述

ip source-guard trust<0/1/2/3>

no ip ip source-guard trust

参数

参数	参数命令模式
0/1/2/3	动态客户端最大数量为 0/1/2，3 表示无限制

缺省

禁止

命令模式

端口模式

使用命令模式

使用本命令后，可以开启端口 IP 源保护功能，使用该命令的 no 形式，端口恢复缺省值。

示例

Switch(config-if)#Ip source-guard trust 1

5.9.3 ip dhcp-snooping binding

命令描述

ip dhcp-snooping binding <MAC> vlan <VLANID> ip <A.B.C.D> mask <Msak> interface < IFNAME>

no ip dhcp-snooping binding <MAC> vlan <VLANID> ip <A.B.C.D> interface < IFNAME>

参数

参数	参数命令模式
MAC	静态绑定的 MAC 地址
VLANID	静态绑定的 VLAN 号
A.B.C.D	静态绑定的 IP 地址
Msak	静态绑定的 IP 地址的掩码
IFNAME	端口号

缺省

命令模式

用户模式

使用命令模式

使用本命令后，可以开启 IP 源保护静态绑定功能，使用该命令的 no 形式，解除绑定。

示例

switch(config)#ip dhcp-snooping binding 40-50-11-11-11-11 vlan 1 ip 192.168.1.1 mask 255.255.255.0 interface G1

第 6 章 网络管理命令

6.1 HTTP config

该配置命令有：

ip http-server http

ip http-server https

功能介绍

描述了 HTTP 配置命令。本命令可以配置交换机在指定的端口接受 HTTP/HTTPS 服务请求，处理该请求并向浏览器返回处理结果。

6.1.1 ip http-server http

命令描述

ip http-server http

no ip http-server

如果希望启动交换机 http 服务，可以通过此命令配置。使用该命令的 no 形式取消此配置，此时将无法使用 http 方式管理交换机

参数

无

缺省

无

命令模式

在全局配置模式下配置该命令。

示例

启动交换机 http 服务。

Switch(config)# ip http-server http

6.1.2 ip http-server https

命令描述

ip http-server https

no ip http-server

如果希望启动交换机 https 服务，可以通过此命令配置。使用该命令的 no 形式取消此配置，此时将无法使用 https 方式管理交换机

参数

无

缺省

无

命令模式

在全局配置模式下配置该命令。

示例

启动交换机 https 服务。

Switch(config)# ip http-server https

6.2 SNMP config

该配置命令有：

community

syscontact

syslocation

sysname

trap

trap2sink

trapsink

user

功能介绍

简单网络管理协议（SNMP），由一组网络管理的标准组成，包含一个应用层协议（application layer protocol）、数据库模型（database schema）和一组资料物件。该协议能够支持网络管理系统，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。该协议是互联网工程工作小组（IETF，Internet Engineering Task Force）定义的 internet 协议簇的一部分。

6.2.1 snmp

命令描述

snmp

no snmp

如果希开启 snmp 功能，可以通过此命令配置。使用该命令的 no 形式禁用此功能。

参数

无

缺省

启用

命令模式

全局模式

示例

启动交换机 snmp 功能。

switch(config)# snmp

6.2.2 snmp-server trap2sink

命令描述

snmp-server trap2sink ip

snmp-server trapsink ip

选择 snmp 的版本，以及接收地址的的配置，可以通过此命令配置。

参数

无

缺省

snmp

命令模式

全局模式

示例

配置交换机 snmp 协议版本。

switch(config)# snmp-server trap2sink 192.168.1.1

6.2.3 snmp-server trap

命令描述

snmp-server trap

no snmp-server trap

开启/关闭 snmp trap 功能。

参数

无

缺省

关闭

命令模式

全局模式

示例

switch(config)# snmp-server trap

6.2.4 snmp-server community

命令描述

community

// 设置认证名和权限

参数

ro；只读

rw：读写

缺省

public

命令模式

全局模式

示例

配置交换机

switch(config)#snmp-server community ro 111

//认证名为 111，权限为只读

6.2.5 snmp host

命令描述

snmp-server sysname

// 设置主机名

参数

无

缺省

无

命令模式

全局模式

示例

switch(config)#snmp-server sysname 1111 //主机名为 1111

6.2.6 snmp-server user

命令描述

snmp-server

参数

无

缺省

无

命令模式

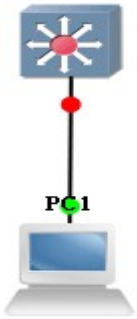
全局模式

示例

switch(config)#snmp-server user ro 111

6.2.7 example

交换机开启 snmp，pc1 上安装 MIB Browser，用于获取交换机节点信息



sw： switch(config)# snmp-server

switch(config)#snmp-server version v2c

switch(config)#snmp-server community v2c 123 RO

switch(config)#snmp-server community v2c 123 RW

//snmp 版本以及读写团体配置

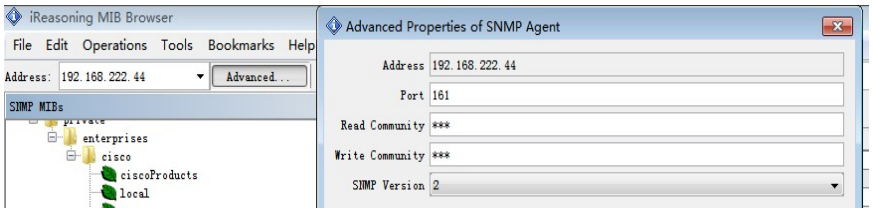
switch(config)# snmp-server host aa

switch(config-snmps-host)# no shutdown

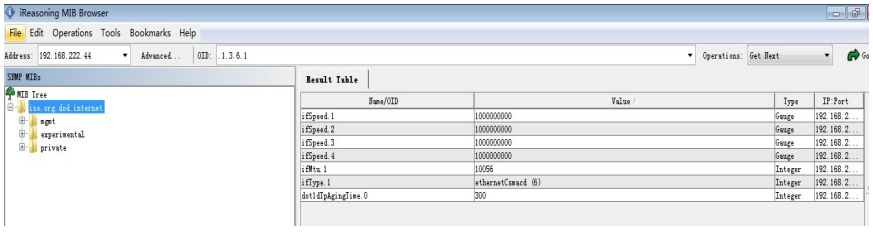
switch(config-snmps-host)# host 192.168.222.107

//snmp trap 信息配置

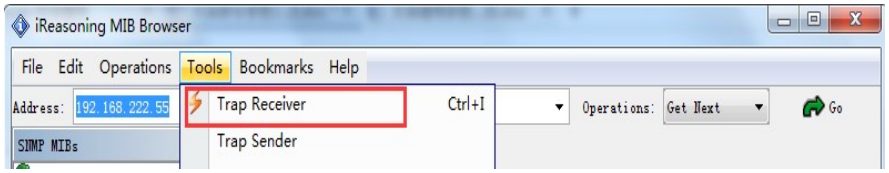
pc： pc 上打开 MIB Browser，并添加交换机 ip，与对应团体名称



右键单击 iso.org.dod.internet,点击 work,在信息显示页面就会显示相关信息。



点击 tools 下的 trap receive 可查看上传的 trap 信息



第 7 章 系统维护命令

7.1 Reboot

命令描述

如果希望重启设备，可以通过此命令配置。

reboot

参数

无

缺省

无

命令模式

特权模式下配置该命令。

示例

保存配置后重启设备。

switch# system config save

switch# reboot

7.2 System config restore

命令描述

如果希望对交换机进行恢复出厂操作，可以通过此命令配置，重启后生效。

参数

无

缺省

无

命令模式

特权模式下配置该命令。

示例

恢复出厂配置并重启后生效。

switch# system config restore

swtich# reboot

7.3 System config save

命令描述

如果希望保存交换机的配置，可以通过此命令配置。

参数

无

缺省

无

命令模式

特权模式

示例

保存交换机配置

switch# system config save

7.4 PING test

功能介绍

PING (Packet Internet Groper)，因特网包探索器，用于测试网络连接量的程序。Ping 发送一个 ICMP(Internet Control Messages Protocol）即因特网信报控制协议；回声请求消息给目的地并报告是否收到所希望的 ICMP echo（ICMP 回声应答）。它是用来检查网络是否通畅或者网络连接速度的命令。

命令描述

Ping ip

测试与主机的可到达性。

参数

无

缺省

无

命令模式

在特权模式下可使用该命令。

示例

测试交换机与主机的可到达性

```
switch# ping 192.168.1.100
```