对通过SNMP访问S8500交换机的用户进行ACL控制的配置

罗淳榕   2006-08-28 发表

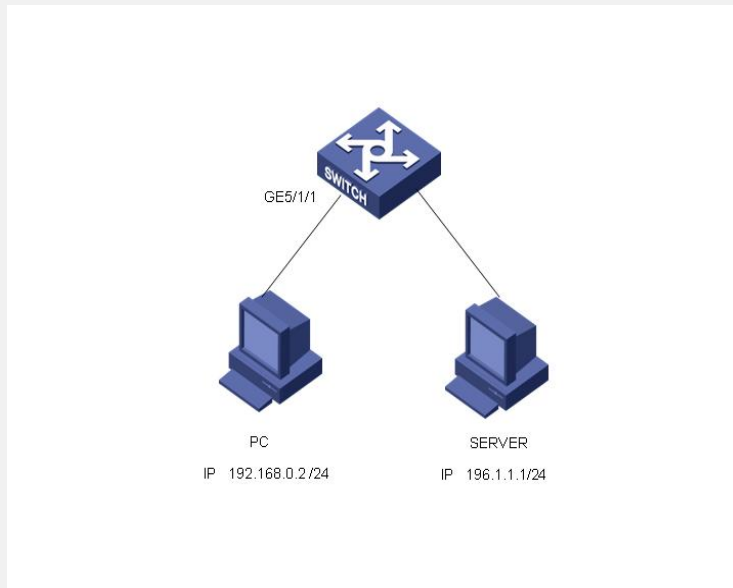**对通过SNMP访问H3C S9500交换机用户**
进行的ACL控制的配置

一、简单介绍

H3C S9500系列路由交换机支持通过网管软件进行远程管理。网管用户可以通过SNMP访问交换机，对这些用户的ACL控制功能可以过滤掉不合法的网管用户，使其不能登录本交换机。

二、S8500设备配置实例

1．组网需求

仅允许来自10.110.100.52和10.110.100.46的SNMP用户访问交换机。

2．组网图

GE5/1/1

PC
IP 192.168.0.2 /24

SERVER
IP 196.1.1.1/24

对Switch的SNMP用户进行ACL控制

3. 配置步骤

定义基本访问控制列表和子规则。

<H3C> system-view

System View: return to User View with Ctrl+Z.

[H3C] acl number 2000 match-order config

[H3C-acl-baisc-2000] rule 1 permit source 10.110.100.52 0

[H3C-acl-baisc-2000] rule 2 permit source 10.110.100.46 0

[H3C-acl-basic-2000] rule 3 deny source any

[H3C-acl-baisc-2000] quit

引用访问控制列表。

[H3C] snmp-agent community read test acl 2000

[H3C] snmp-agent group v3 testgroup acl 2000

[H3C] snmp-agent usm-user v3 testuser testgroup acl 2000

snmp-agent community、**snmp-agent group**、**snmp-agent usm-use**三个命令中引用的访问控制列表可以是不同的访问控制列表。网管用户的ACL控制功能只能引用基于数字标识的基本访问控制列表。

三、正确配置状态显示

[H3C]dis snmp-agent sys-info

  The contact person for this managed node:

     R&D Hangzhou, H3C Technology co.,Ltd.

  The physical location of this node:

     Hangzhou China

  SNMP version running in the system:

     SNMPv3

[H3C]dis snmp-agent usm-user

```
  User name: testuser
  Group name: testgroup
     Authencation Mode: no
     Privacy Mode: no
     Engine ID: 800007DB00E0FC2989796877 active
     Acl:2000

[H3C]dis snmp-agent statistic
  0 Messages delivered to the SNMP entity
  0 Messages which were for an unsupported version
  0 Messages which used an unknown SNMP community name
  0 Messages which represented an illegal operation for the community supplied
  0 ASN.1 or BER errors in the process of decoding
  0 Messages passed from the SNMP entity
  0 SNMP PDUs which had badValue error-status
  0 SNMP PDUs which had genErr error-status
  0 SNMP PDUs which had noSuchName error-status
  0 SNMP PDUs which had tooBig error-status (Maximum packet size 2000)
  0 MIB objects retrieved successfully
  0 MIB objects altered successfully
  0 GetRequest-PDU accepted and processed
  0 GetNextRequest-PDU accepted and processed
  0 GetBulkRequest-PDU accepted and processed
  0 GetResponse-PDU accepted and processed
  0 SetRequest-PDU accepted and processed
  0 Trap PDUs accepted and processed
  0 Alternate Response Class PDUs droped silently
  0 Forwarded Confirmed Class PDUs droped silently
[H3C]dis snmp-agent community
  Community name:test
     Group name:test
     Acl:2000
     Storage-type: nonVolatile

[H3C]dis snmp-agent group

  Group name: testgroup
     Security model: v3 noAuthnoPriv
     Readview: ViewDefault
     Writeview: <no specified>
     Notifyview :<no specified>
     Storage-type: nonVolatile
     Acl:2000
[H3C]dis cu
#
acl number 2000
 rule 1 permit source 10.110.100.52 0
 rule 2 permit source 10.110.100.46 0
 rule 3 deny
#
 snmp-agent
 snmp-agent local-engineid 800007DB00E0FC2989796877
 snmp-agent community read  test acl 2000
 snmp-agent sys-info version v3
 snmp-agent group v3 testgroup acl  2000
 snmp-agent usm-user v3 testuser testgroup acl 20
```