

CISCO中IP访问控制列表思科认证 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/638/2021\\_2022\\_\\_EF\\_BC\\_A31SCO\\_E4\\_B8\\_AD\\_c101\\_638597.htm](https://www.100test.com/kao_ti2020/638/2021_2022__EF_BC_A31SCO_E4_B8_AD_c101_638597.htm) 本实验对IP访问控制列表进行配置和监测，包括标准、扩展和命名的IP访问控制列表。

1.实验目的 通过本实验，读者可以掌握以下技能： 配置标准IP访问控制列表. 配置扩展IP访问控制列表. 配置命名的标准IP访问控制列表. 配置命名的扩展IP访问控制列表. 在网络接口上引用IP访问控制列表. 在VTY上引用IP访问控制列表. 查看和监测IP访问控制列表。

2.设备需求 本实验需要以下设备： Cisco路由器3台，分别命名为R1、R2和R3。要求R1具有1个以太网接口，R2具有1个以太网接口和1个串行接口，R3具有1个串行接口. 1条交叉线序的双绞线，或2条正常线序双绞线和1个Hub. 1条DCE电缆和1条DTE电缆，或1条DCE转DTE电缆. 1台终端服务器，如Cisco 2509路由器，及用于反问Telnet的相应电缆. 1台带有超级终端程序的PC机，以及Console电缆及转接器。

3.拓扑结构及配置说明 本实验拓扑结构如图10-1所示，R1的E0接口与R2的E0接口通过以太网连接起来，R2的S0接口与R3的S0接口通过串行电缆连接起来。各路由器相关接口的IP地址分配如图10-1中的标注。

4.实验配置及监测结果 首先配置各路由器，并且通过路由选择协议的配置实现了整个拓扑的IP连通性，在此基础上进行IP访问控制列表的配置和监测。在R1上设置enable口令为cisco，VTY口令为cisco1，用于Telnet测试。以上配置在以前章节中已进行过实验，在本实验中不再给出配置清单。我们主要在R2路由器上配置访问控制列表，R1和R3用于测试目的。

第1部分:配置和引用标准IP访问控制列表 配置清单10-1列出了在R2路由器上配置和引用标准IP访问控制列表的操作。配置清单10-1 配置和引用标准IP访问控制列表

```
R2#conf t Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny 30.1.1.0 0.0.0.255
R2(config)#access-list 1 permit any R2(config)#int s0
R2(config-if)#ip access-group 1 in R2(config-if)#^Z R2#sh
14:34:20: %SYS-5-CONFIG_1: Configured from console by console
R2#sh ip access-list 1 Standard IP access list 1 deny
30.1.1.0, wildcard bits 0.0.0.255 check=2 permit any(2 matches)
R2#sh ip int s0 Serial0 is up, line protocol is up Internet address is
20.1.1.2/24 Broadcast address is 255.255.255.255 Address
determined by setup command MTU is 1500 bytes Helper address is
not set Directed broadcast forwarding is disabled Multicast reserved
groups joined: 224.0.0.9 Outgoing access list is not set Inbound
access list is 1 Proxy ARP is enabled Security level is default ... (输出
省略) R2#clear access-list counters R2#sh ip access-1 1 Standard IP
access list 1 deny 30.1.1.0 wildcard bits 0.0.0.255 permit any R2#
Term_Server#3 [Resuming connection 3 to R3 ... ] R3#ping 10.1.1.1
Type escape sequence to abort. Sending 5, 100-byte ICMP Echoes to
10.1.1.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5).
round-trip time/ min/avg/max = 32/37/48 ms R3#ping Protocol [ip]: Target
IP address: 10.1.1.1 Repeat count [5]: Datagram size [100]: Timeout
in seconds [2]: Extended commands [n]: y Source address or
interface: 30.1.1.3 Type of service [0]: Set DF bit in IP header? [no]:
Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict,
```

Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: Type escape sequence to abort. Sending 5,100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds: U.U.U Success rate is 0 percent (0/5)  
R3#^Z Term\_Server#2 [Resuming connection 3 to R2 ... ] R2#sh ip access-1 1 Standard IP access list 1 deny 30.1.1.0, wildcard bits 0.0.0.255 (5 matches) checks 15 permit any (5 matches) (1)在定义访问控制列表时，要特别注意语句输入的先后顺序，因为路由器在执行该列表时的顺序是自上而下的。另一个应注意的问题是路由器不对由自身产生的IP进行过滤，在实验时应由其他的设备发包进行测试。(2)配置标准IP访问控制列表1时，定义了除30.1.1.0/24网段外的所有网段都被接受。(3)在R2路由器S0接口的进入方向引用了访问控制列表1,目的是过滤来自30.1.1.0/24网段的数据包，允许其他所有网段的数据包通过。在接口上引用访问控制列表时，使用in或out子命令。这里的in和out是指以路由器本身为参考点，数据包是进入(in)还是离开(out)路由器。(4)show ip access-list命令列出了所定义的访问控制列表的情况，可以看到"permit any"一行有2个匹配包的报告，表示已经有2个匹配此行条件的数据包被S0接口接收。(5)show ip int s0命令列出的信息中加阴影的2行是关于访问控制列表引用情况的信息，表明在进入路由器的方向(而)引用了访问控制列表1。(6)接下来用clear access-list counters指令清空了访问控制列表的计数器。以便观察实验结果。所谓清空计数器，就是把访问控制列表各行的匹配数清空。再次使用show ip access-list命令查看显示了我们想得到的结果。(7)使用ping和扩展的ping命令测试访问控制列表1的定义和引用情况，结果为:从20.1.1.3发往10.1.1.1的IP包被R2接收和路由。

从30.1.1.3发往10.1.1.1的IP包被R2过滤掉。测试结果符合访问控制列表的设置。(8)再次查看访问控制列表的匹配情况，可以看到，在访问控制列表1中，2条语句各有5个相匹配的包，即5个ICMP Echo包。第2部分:配置和引用扩展IP访问控制列表 接下来是有关扩展IP访问控制列表的实验。配置清单10-2列出了在R2路由器上配置和引用扩展IP访问控制列表的操作。

配置清单10-2配置和引用扩展IP访问控制列表

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 101 deny icmp 20.1.1.0 0.0.0.255 10.1.1.0
0.0.0.255 echo
R2(config)#access-list 101 permit ip any any
R2(config)#int e0
R2(config-if)#ip access-group 101 out
R2(config-if)#int s0
R2(config-if)#no ip access-group 1 in
R2(config-if)#^Z
R2#
R2#sh ip access-list Standard IP access list 1
deny 30.1.1.0, wildcard bits 0.0.0.255 (8 matches) check=20 permit
any (20 matches) permit ip any any
R2#
Term_Server#3 [Resuming
connection 3 to R3 ...]
R3#ping 10.1.1.1 Type escape sequence to
abort. Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2
seconds: U.U.U Success rate is 0 percent(0/5)
R3#telnet 10.1.1.1
Trying 10.1.1.1... Open User Access Verification Password: (键入
cisco1 )
R1>.en Password: (键入 cisco )
R1#
R1#exit [Connection
to 10.1.1.1 closed by foreign host]
R3#
Term_Server#2 [Resuming
connection 2 to R2 ... ]
R2#sh ip access-list 101 Extended IP access
list 101 deny icmp 20.1.1.0 0.0.0.255 10.1.1.0.0.0.0.255 echo(8
matches) permit ip any any (40 matches)
R2#
```

(1)首先定义了一个扩展的IP访问控制列表101。列表的第1句拒绝从20.1.1.0/24网段发往10.1.1.0/24网段的ICMP Echo包，即希望从20.1.1.0/24网

段到10.1.1.0/24网段的ping失败。列表的第2句允许所有的  
100Test 下载频道开通，各类考试题目直接下载。详细请访问  
[www.100test.com](http://www.100test.com)