身份证 130425198708092057，210181199209046813，222302197312260017，350128197311050034 ，410611197403020058

联通手机号 18575414999 ，13026844666

电信手机号 18919628498 ， 18919628499

移动手机号 18756500265 ，18555918746 15665541872

邮箱 zhangsan@163.com ，lisi@qq.com

银行卡 6216610200016587010 ， 6221882600114166800

财务报表

内部数据

内部资料

保密

秘密

机密

密码口令

超级用户

家庭地址

第十二章 ACL访问控制列表 188

12.1 ACL的工作方式 188

12.2 标准访问控制列表 188

12.3 扩展访问控制列表 190

12.4 访问控制列表的显示 194

12.5 动态访问控制列表 195

12.6 命名的访问控制列表 197

12.7 CCIE\_lab中的ACL 197

Chapter 12 ACL访问控制列表

12．1 ACL的工作方式

访问控制列表时一些列自上而下按顺序逐条执行的控制条件，其设置方式和很久以前的行号 Basic

类似。访问控制列表的种类如下

router(config)#access-list ?

<1–99>IP standard access list

<100–199>IP extended access list

<1000–1099>IPX SAP access list

<1100–1199>Extended 48-bit MAC address access list

<1200–1299>IPX summary address access list

<1300–1999>IP standard access list (expanded range)

<200–299>Protocol type-code access list

<2000–2699>IP extended access list (expanded range)

<300–399>DECnet access list

<400–499>XNS standard access list

<500–599>XNS extended access list

<600–699>Appletalk access list

<700–799>48-bit MAC address access list

<800–899>IPX standard access list

<900–999>IPX extended access list

访问控制列表的过滤基于地址匹配的条件，最终对给定的地址一个 permit 或者 deny 的判断，配置

ACL 需要注意以下规则

1． 所有的访问控制列表最后都存在一个隐含的 deny all 的条件，但配置文件不显示出来

2． 访问控制列表为顺序执行方式，满足某条后，停止执行

3． 访问控制列表应按一定的顺序，从特殊到一般配置，先拒绝特定主机，然后组或一般条件的

过滤操作

4． 表中新的列表项总是加在访问控制列表的最后，可以使用 no accees-list x 删除整个列表，

但不能有选择的删除或者添加条目

5． 没有任何定义的访问控制列表可以 permit 所有数据

6． 配置访问控制列表，应先配置好列表再加载到相应的进程上

7． IP 访问控制列表会发送一个 ICMP 主机不可达的消息到数据包的发送者，然后丢弃数据包

8． 采用的过滤规则与所过滤得数据源要尽量接近，安全过滤通常是阻止入站访问，数据过滤一

般采用出站过滤或者禁止通过某条链路

9． 删除访问控制列表需要注意，如果某个列表挂接在实际接口上，删除列表后，默认的 deny any

规则会阻断那个接口的所有数据流量

12．2 标准访问控制列表

在 cisco IOS12.0 中，标准访问控制列表在 1~99 和 1300~1999 范围内，可以在列表后加 log 关

键字，匹配信息可以在控制台显示出来，其用法如下

Access-list x {deny | permit} a.b.c.d wildcard\_mask {log}

标准访问控制列表用于如下方式：

1． 数据包过滤

2． 路由过滤

3． 为 NAT 或 DDR 等链路定义期望数据流

CCIE R/S & Service Provider Exam Certification Guide

P a g e | 189

如下拓扑结构，将禁止 jefferson 具有到 172.16.2.0/24 的路由，允许用户 172.16.1.129 通过 telnet 访

问 henry，但拒绝其他任何访问方式，同时禁止 172.16.1.0/24 访问令牌环网

过滤前 jefferson 的路由表

jefferson#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default

U - per-user static route, o - ODR

T - traffic engineered route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 2 subnets

D 172.16.1.0 [90/297728] via 128.200.1.2, 00:00:31, TokenRing0

D 172.16.2.0 [90/323328] via 128.200.1.2, 00:00:18, TokenRing0

128.200.0.0/24 is subnetted, 1 subnets

C 128.200.1.0 is directly connected, TokenRing0

jefferson#

配置路由过滤

paine(config)#router eigrp 2001

paine(config-router)#distribute-list 1 out to1

paine(config-router)#exit

paine(config)#access-list 1 deny 172.16.2.0 0.0.0.255

paine(config)#access-list 1 permit any

paine(config)#exit

paine#

过滤后的路由表

jefferson#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default

U - per-user static route, o - ODR

T - traffic engineered route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 2 subnets

CCIE R/S & Service Provider Exam Certification Guide

P a g e | 190

D 172.16.1.0 [90/297728] via 128.200.1.2, 00:00:31, TokenRing0

C 128.200.1.0 is directly connected, TokenRing0

jefferson#

允许telnet访问路由器

henry#conf t

Enter configuration commands, one per line. End with CNTL/Z.

henry(config)#access-list 1 permit 172.16.1.129 0.0.0.0

henry(config)#line 2 6

henry(config-line)#access-class 1 in

henry(config-line)#^Z

控制网络访问

paine#conf t

Enter configuration commands, one per line. End with CNTL/Z.

01:42:01: %SYS-5-CONFIG\_I: Configured from console by console

paine(config)#access-list 5 deny 172.16.1.0 0.0.0.255

paine(config)#access-list 5 permit any

paine(config)#int to1

paine(config-if)#ip access-group 5 out

paine(config-if)#^Z

12．3 扩展访问控制列表

扩展 IP 访问控制列表的范围为 100~199 和 2000~2699，通过如下命令配置

access-list {100-199 | 2000-2699} {permit | deny} protocol\_type Source\_address

Source\_address\_wildcard destination\_address destination\_address\_wildcard

[protocol specific options] [precedence precedence][tos tos][log][established]

支持的 Protocol\_type 类型

Value What It Means

<0– 255> An IP protocol number

ahp Authentication Header Protocol

eigrp Cisco's EIGRP routing protocol

esp Encapsulation Security Payload

gre Cisco's GRE tunneling

icmp Internet Control Message Protocol

igmp Internet Gateway Message Protocol

igrp Cisco's IGRP routing protocol

ip Any Internet protocol

ipinip IP in IP tunneling

nos KA9Q NOS-compatible IP over IP tunneling

ospf OSPF routing protocol

pcp Payload Compression Protocol

pim Protocol Independent Multicast

tcp Transmission Control Protocol

udp User Datagram Protocol

支持的 TCP 端口号列表

CCIE R/S & Service Provider Exam Certification Guide

P a g e | 191

Value What It Means

<0– 65535> Port number

bgp Border Gateway Protocol (179)

chargen Character generator (19)

cmd Remote commands (rcmd, 514)

daytime Daytime (13)

discard Discard (9)

domain Domain Name Service (53)

echo Echo (7)

exec Exec (rsh, 512)

finger Finger (79)

ftp File Transfer Protocol (21)

ftp-data FTP data connections (used infrequently, 20)

gopher Gopher (70)

hostname NIC host name server (101)

ident Ident Protocol (113)

irc Internet Relay Chat (194)

klogin Kerberos login (543)

kshell Kerberos shell (544)

login Login (rlogin, 513)

lpd Printer service (515)

nntp Network News Transport Protocol (119)

pim-auto-rp PIM Auto-RP (496)

pop2 Post Office Protocol v2 (109)

pop3 Post Office Protocol v3 (110)

smtp Simple Mail Transport Protocol (25)

sunrpc Sun Remote Procedure Call (111)

Syslog Syslog (514)

Tacacs TAC Access Control System (49)

Talk Talk (517)

telnet Telnet (23)

Time Time (37)

Uucp UNIX-to-UNIX Copy Program (540)

Whois Nicname (43)

www World Wide Web (HTTP, 80)

支持的 UDP 端口号列表

Value What It Means

<0– 65535> Port number

biff (mail notification, comsat, 512)

bootpc Bootstrap Protocol (BOOTP) client (68)

bootps Bootstrap Protocol (BOOTP) server (67)

discard Discard (9)

dnsix DNSIX security protocol auditing (195)

domain Domain Name Service (DNS, 53)

echo Echo (7)

CCIE R/S & Service Provider Exam Certification Guide

P a g e | 192

isakmp Internet Security Association and Key Management Protocol

(500)

mobile-ip Mobile IP registration (434)

nameserver IEN116 name service (obsolete, 42)

netbiosdgm NetBIOS datagram service (138)

netbios-ns NetBIOS name service (137)

netbios-ss NetBIOS session service (139)

ntp Network Time Protocol (123)

pim-auto-rp PIM Auto-RP (496)

rip Routing Information Protocol (router, in.routed, 520)

snmp Simple Network Management Protocol (161)

snmptrap SNMP Traps (162)

sunrpc Sun Remote Procedure Call (111)

syslog System Logger (514)

tacacs TAC Access Control System (49)

talk Talk (517)

tftp Trivial File Transfer Protocol (69)

time Time (37)

who Who service (rwho, 513)

xdmcp X Display Manager Control Protocol (177)

支持的 ICMP 报文类型列表

<0-255> ICMP message type

administratively-prohibited Administratively prohibited

alternate-address Alternate address

conversion-error Datagram conversion

dod-host-prohibited Host prohibited

dod-net-prohibited Net prohibited

dscp Match packets with given dscp value

echo Echo (ping)

echo-reply Echo reply

fragments Check non-initial fragments

general-parameter-problem Parameter problem

host-isolated Host isolated

host-precedence-unreachable Host unreachable for precedence

host-redirect Host redirect

host-tos-redirect Host redirect for TOS

host-tos-unreachable Host unreachable for TOS

host-unknown Host unknown

host-unreachable Host unreachable

information-reply Information replies

information-request Information requests

log Log matches against this entry

log-input Log matches against this entry, including input interface

mask-reply Mask replies

mask-request Mask requests

mobile-redirect Mobile host redirect

CCIE R/S & Service Provider Exam Certification Guide

P a g e | 193

net-redirect Network redirect

net-tos-redirect Net redirect for TOS

net-tos-unreachable Network unreachable for TOS

net-unreachable Net unreachable

network-unknown Network unknown

no-room-for-option Parameter required but no room

option-missing Parameter required but not present

packet-too-big Fragmentation needed and DF set

parameter-problem All parameter problems

port-unreachable Port unreachable

precedence Match packets with given precedence value

precedence-unreachable Precedence cutoff

protocol-unreachable Protocol unreachable

reassembly-timeout Reassembly timeout

redirect All redirects

router-advertisement Router discovery advertisements

router-solicitation Router discovery solicitations

source-quench Source quenches

source-route-failed Source route failed

time-exceeded All time exceededs

time-range Specify a time-range

timestamp-reply Timestamp replies

timestamp-request Timestamp requests

tos Match packets with given TOS value

traceroute Traceroute

ttl-exceeded TTL exceeded

unreachable All unreachables

其中经常用到的为 echo，和 echo-reply， echo 为 ping 包，后者为 ping 包的回复报文，一方面有些简单

的 DDOS 攻击采用 ping 包，另一方面在 CCIE lab 中也经常考到

如上拓扑结构，在接口上定义访问控制列表进行接入访问控制如下：

CCIE R/S & Service Provider Exam Certification Guide

P a g e | 194

access\_router(config)#access-list 199 permit tcp any any established

access\_router(config)#access-list 199 deny ip 206.191.241.40 0.0.0.7 any

access\_router(config)#access-list 199 deny ip host 206.191.194.42 host 206.191.194.42

access\_router(config)#access-list 199 permit icmp any any echo

access\_router(config)#access-list 199 permit icmp any any echo-reply

access\_router(config)#access-list 199 permit tcp any 206.191.241.40 0.0.0.7 eq www

access\_router(config)#access-list 199 permit tcp any 206.191.241.40 0.0.0.7 eq smtp

access\_router(config)#access-list 199 permit tcp any 206.191.241.40 0.0.0.7 eq domain

access\_router(config)#access-list 199 permit udp any 206.191.241.40 0.0.0.7 eq domain

access\_router(config)#access-list 199 deny tcp any 206.191.241.40 0.0.0.7 lt 1024

access\_router(config)#access-list 199 deny tcp any 206.191.241.40 0.0.0.7 gt 1023

access\_router(config)#access-list 199 permit udp any 206.191.241.40 0.0.0.7 gt 1023

access\_router(config)#access-list 199 deny udp any 206.191.241.40 0.0.0.7 gt 50000

access\_router(config)#access-list 199 deny udp any 206.191.241.40 0.0.0.7 lt 1024

access\_router(config)#int bri 0

access\_router(config-if)#ip access-group 199 in

对于如上访问控制列表的解释如下：

1． 第一行调用关键字 establish 路由器会在 TCP 报头中寻找 ACK 或者 RESET 报文，这样就使

得已建立的数据流通过访问控制列表时产生匹配

2． 第二，三行用来防止电子欺骗，2 用于防止外部冒充 lan 地址访问，3 防止电子欺骗

3． 第四，五行用于 ping 的收发

4． 后面则是允许 www,smtp 和 DNS 流量，注意 DNS 同时存在 TCP 和 UDP2 种方式

5． 后续则是对一些端口进行处理 lt 小于 eq 等于 gt 大于

12．4 访问控制列表的显示

可以使用 show access-list 查看访问控制列表，同时可以调用 clear access-list counter 清除计数

对于某些带有 log 参数的 acl，可以通过 logging buffered 捕获所有的控制台消息，然后 show log

可以看到相应的记录

access\_router# show ip access-lists

Standard IP access list 69

permit 206.191.241.0, wildcard bits 0.0.0.255 log

Extended IP access list 101

deny udp host 172.16.16.2 host 204.221.151.211 eq domain

permit tcp any any established (15992 matches)

permit ip any 192.168.5.0 0.0.0.255 (43 matches)

permit ip any 204.221.151.0 0.0.0.255 (169 matches)

permit icmp any any echo (78 matches)

permit icmp any any echo-reply (9 matches)

permit tcp any any eq www (216 matches)

permit udp any any

Extended IP access list 110

permit ip any any (37779 matches)

permit tcp any any established

Extended IP access list 199

permit tcp any any established (175 matches)

deny ip 206.191.241.40 0.0.0.7 any

deny ip host 206.191.194.42 host 206.191.194.42

permit icmp any any echo

permit icmp any any echo-reply

permit tcp any 206.191.241.40 0.0.0.7 eq www

permit tcp any 206.191.241.40 0.0.0.7 eq smtp

permit tcp any 206.191.241.40 0.0.0.7 eq domain

permit udp any 206.191.241.40 0.0.0.7 eq domain

deny tcp any 206.191.241.40 0.0.0.7 lt 1024

deny tcp any 206.191.241.40 0.0.0.7 gt 1023

permit udp any 206.191.241.40 0.0.0.7 gt 1023 (13 matches)

deny udp any 206.191.241.40 0.0.0.7 gt 50000

CCIE R/S & Service Provider Exam Certification Guide

P a g e | 195

deny udp any 206.191.241.40 0.0.0.7 lt 1024

access\_router#

12．5 动态访问控制列表

动态访问控制列表能够允许用户在通过路由器认证之后进行临时性的访问，例如实际上可能需要cisco

TAC的工程师远程登录来检查网络故障时，可以使用这种方式。配置方式如下：

1． 定义一个用户名和密码

2． 定义用户名时加上 autocommand 和 timeout 参数；这些参数必须和动态访问控制列表中指定的

超时值匹配

3． 定义一个仅一行的动态访问控制列表，指定用户在通过认证后才能传输数据，同时此行设置一个超

时值，应和如上值匹配。

4． 定义一个扩展访问控制列表，其范围和动态访问控制列表一样，用这表对接口进行常规数据流量过

滤，其中必须允许该接口的telnet访问，因为是用telnet认证的，最后将此访问控制列表加到接口

5． 将 login local 加到vty线路号中去，这些线路信息可以通过show line 显示

定义用户名和密码：

username franklin password ben

username franklin autocommand access-enable timeout 5

access-enable是一条隐藏命令，后面的时间单位为分钟，此超时为空闲超时

定义动态访问控制列表如下：

access-list 101 dynamic allowben timeout 5 permit ip 172.16.1.0 0.0.0.255 any

access-list 101 permit tcp 172.16.1.0 0.0.0.255 host 172.16.1.2 eq telnet

CISCO对于配置动态访问控制列表有如下规则和建议：

1． 对于超时，可以通过autocommand 后加 access-enable 来定义，也可以用 acl中的timeout

来定义，空闲超时和绝对超时(ACL的那个时间)必须定义，否则，临时性的访问控制列表

将无限期的常住在接口上

2． 如果要配置一个空闲超时，其值应等于拨号空闲超时值

3． 空闲超时应小于绝对超时

上图中路由器Paine的配置如下

hostname paine

!

CCIE R/S & Service Provider Exam Certification Guide

P a g e | 196

enable password 7 02050D480809

!

username franklin password 7 02040155

username franklin autocommand access-enable timeout 5

!!

interface Ethernet0

no ip address

shutdown

media-type 10BaseT

!

interface Ethernet1

ip address 172.16.1.2 255.255.255.0

ip access-group 101 in

media-type 10BaseT

!

<<<text omitted>>>

!

interface TokenRing1

ip address 128.200.1.2 255.255.255.0

ring-speed 16

!

router eigrp 2001

network 128.200.0.0

network 172.16.0.0

no auto-summary

!

ip classless

!

access-list 101 dynamic allowben timeout 5 permit ip 172.16.1.0 0.0.0.255 any

access-list 101 permit tcp 172.16.1.0 0.0.0.255 host 172.16.1.2 eq telnet

!!

line con 0

line aux 0

line vty 0 4

login local

!

end

测试动态访问控制列表如下

washington#

washington#ping 128.200.1.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 128.200.1.5, timeout is 2 seconds:

U.U.U

Success rate is 0 percent (0/5)

washington#

washington#

washington#telnet 172.16.1.2

Trying 172.16.1.2 ... Open

User Access Verification

Username: franklin

Password:

[Connection to 172.16.1.2 closed by foreign host]

washington#

washington#

washington#ping 128.200.1.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 128.200.1.5, timeout is 2 seconds:

!!!!!

CCIE R/S & Service Provider Exam Certification Guide

P a g e | 197

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

washington#

<<<After 5 minutes expires>>>

washington#ping 128.200.1.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 128.200.1.5, timeout is 2 seconds:

U.U.U

Success rate is 0 percent (0/5)

washington#

12．6 命名的访问控制列表

Cisco IOS 11.2以后出现带命名的访问控制列表，配置方式如下

ip access-list {standard | extended} access\_list\_name

然后进入控制列表条目，输入方式如下,前者为标准访问控制列表使用，后者为扩展访问控制列表使用

{permit | deny} a.b.c.d [wildcard\_mask]

{permit | deny} protocol\_type source\_address source\_address\_wildcard

destination\_address destination\_address\_wildcard [protocol specific options] {log}

然后将这个访问控制列表使用 access-group 挂接在某个接口上，

Screening\_router(config)#ip access-list standard allow\_net\_172

Screening\_router(config-std-n)#permit 172.0.0.0 0.255.255.255

Screening\_router(config-std-n)#exit

Screening\_router(config)#int e0/0

Screening\_router(config-if)#ip access-group allow\_net\_172

12．7 CCIE试验中的ACL

CCIE试验中对ACL的考察十分细致，例如计算wildcard\_mask来精确控制访问网段

ACL中匹配计算方法为，将ACL中的地址和反掩码进行逻辑或进行运算，得出A值，将实际IP和反掩码进

行逻辑或运算，得到B值，若A=B，访问控制列表条件为真。

1．仅允许偶数字网访问

state\_patrol(config)#ip access-list standard alloweven

state\_patrol(config-std-nacl)#permit 150.100.0.0 0.0.254.255

state\_patrol(config-std-nacl)#exit

state\_patrol(config)#router eigrp 2001

state\_patrol(config-router)#distribute-list alloweven out s0

state\_patrol(config-router)#^Z

2。仅允许奇数字网访问

state\_patrol(config)#ip access-list standard allowodd

state\_patrol(config-std-nacl)#permit 150.100.1.0 0.0.254.255

state\_patrol(config-std-nacl)#exit

state\_patrol(config)#router eigrp 2001

state\_patrol(config-router)#distribute-list allowodd out s0

state\_patrol(config-router)#^Z

3． 在sw1 F0/17端口下作MAC-ADDRESS-LIST,DENY ETHERNET TYPE 6000 的帧。

CCIE R/S & Service Provider Exam Certification Guide

P a g e | 198

mac access-list extended BLOCK\_ETH6000

deny any any etype-6000

permit any any

int f0/17

mac access-group BLOCK\_ETH6000 in

4． 在R2以内的区域为clean区域，从R2到 BB1之间的区域是 Dirty区域，在R2的子接口上配置：

两个域之间都允许routing和ICMP包通过，外出包允许TCP、 UDP，进入的包不允许有其它访问。

ip access-list extended outacl

permit eigrp any any

permit icmp any any

permit tcp any any eq bgp

permit udp any any reflect flow

permit tcp any any reflect flow

ip access-list extended inacl

permit eigrp any any

permit icmp any any

permit tcp any any eq bgp

evaluate flow

int e0.2

ip access-group inacl in

ip access-group outacl out

5．Tcp intercept

VlanA有PC对BB1的服务器150.100.1.240进行syn flooding close, the tcp connection

even the legitimate which open after 2.5 minuts.In TCP intercept,the original

file said the server is 150.100.1.24, but in his lab,the attack is it.

Access-list 110 permit tcp 148.1.X.0 0.0.0.255 150.100.1.240

Ip tcp intercept list 110

Ip tcp intercept mode intercept

Ip tcp intercept connection-timeout 150

//show tcp intercept connections show tcp intercept statisics

6．ICMP flooding

怀疑ICMP 来自R5 与R2 连接的帧中继链路上,use access-list 日志跟踪出发送大量

无效数据报的攻击源地址。ACL命名为ICMPTRACKER，但不能阻断任何正常报文

Ip access-list extended ICMPTRACKER

Permit icmp any any log-input

Permit ip any any

Inter s0/0

Ip access-group ICMPTRACKER in

7．要求只能YY.YY.28.0 网段telnet 至R4，用户名：joe，密码：joeshowbgp，telnet 上

来后自动显示show ip bgp summary 后断掉

Access-list 110 permit tcp 1.1.28.0 0.0.0.255 any eq 23

Username joe password joeshowbgp

Username joe autocommand show ip bgp summary

Line vty 0 4

Login local

Access-class 110 in

8．DF(DATA FRAGMENT)

管理员发现有大量的设置了ＤＦ位的超大的数据包攻击BB2 上某个web－server,ip 为

150.100.2.4, 非初始分段包到此服务器拒绝，初始包到此服务器允许.

Access-list 110 deny ip any 150.100.2.4 0.0.0.0 fragments

CCIE R/S & Service Provider Exam Certification Guide

P a g e | 199

Access-list 110 permit ip any any

Inter s0/0

Ip access-group 110 in

9. Time-Ranges ACL.

在VlanB上，每周8：00~18：00 不准www流量通过，同时周末，从中午到16：00不准UDP

流量通过，在R5 的F0/0 做access-list, 过滤RFC1918 规定的三个网段的私有地址和

127.0.0.0/8 这个地址。

Clock timezone GMT +8

Clock set xx:xx:xx day month year //可以考虑不加

time-range weekdays

period weekdays 8:00 to 18:00

time-range weekend

period weekend 12:00 to 16:00

access-list 110 deny tcp 135.1.57.0 0.0.0.255 any eq www time-range weekdays

access-list 110 deny upd any any time-range weekend

access-list 110 deny ip 10.0.0.0 0.255.255.255 any

access-list 110 deny ip 127.0.0.0 0.255.255.255 any

access-list 110 deny ip 172.16.0.0 0.15.255.255 any

access-list 110 deny ip 192.168.0.0 0.0.255.255 any

//没说哪个是目的哪个是源，需不需要any

access-list 11p permit ip any any

inter fa0/0

ip access-group 100 in

10．在R2以内的区域为clean区域，从R2到 BB1之间的区域是 Dirty区域，在R2的子接口上

配置：两个域之间都允许routing和ICMP包通过，外出包允许TCP、UDP，进入的包不允

许有其它访问.(fa0/0是单臂路由，fa0/0.1 rip连bb1----150.100.1.0 fa0/0.2是

eigrp------133.1.12.0)当你配完以上的访问列表后你发现从R2上不再能TELNET到R1

上,请解决此问题

Ip access-list extended outband

Permit icmp any any

Permit eigrp any any

Permit tcp any any eq bgp

Permit tcp any any reflect ccie

Permit udp any any reflect ccie

Ip access-list extended inbound

Permit eigrp any any

Permit tcp any any eq bgp

Permit icmp any any

Evaluate ccie

Inter fa0/0.1

Ip access-group inbound in

Ip access-group outbound out

Ip access0list extended inbound

Permit tcp 133.1.12.1 eq 23 any //reflexive acc不支持从本地路由器发起的

11. Support engineers who come in through vlan\_d must be given occasional access

to the rest of your yy.yy.0.0 net they will telnet from sw1 to r4 e0/0 and

give their crendentials once this is done

they will have unrestricted access to the rest of the network .Use local

authentication on r4 allows unrestricted access for 10 minutes and 2 minutes

idle.make sure the existing feature of this link(connectivity,route)is not

compromise.User name is ccie,password is cisco

R4:

CCIE R/S & Service Provider Exam Certification Guide

P a g e | 200

Username ccie password cisco

Username ccie autocommand access-enable timeout 2

Access-list 101 permit tcp 1.1.13.0 0.0.0.255 1.1.13.4 0.0.0.0 eq 23

Access-list 101 permit ospf any any

Access-list 101 permit icmp 1.1.13.7 0.0.0.0 any

Access-list 101 dynamic-list ccie timeout 10 ip 1.1.13.7 0.0.0.0 1.1.0.0 0.0.255.255

Inter e0/0

Access-group 101 in

Line vty 0 4

Login local