Cisco
Access Control List

آشنایی با ACLهای سیسکو

writen By: ??!!! | Spread and Edited by Esh.Blackhat

در این جلسه خواهیم آموخت :

- انواع Access-List های سیسکو کدامند؟
- Access-List چه کاربرد هایی دارد؟

مقدمه

معنای کلی Access-Control-List:

لیستی از مجوزهای دسترسی کنترل شده که به یک منبع مربوط باشد

Cisco ACL ، دستوارتی هستند که در سیستم عامل سیسکو (IOS)، به منظور های مختلف بکار گرفته میشود ، که یکی از پرکاربرد ترین دستورات میباشد

در ادامه با کاربردهای مختلف این لیست های دسترسی بطور اجمالی آشنا خواهیم شد.

انواع Access-List کدامند ؟

شماره ACL مشخص کننده نوع آن است !

جدول زیر ، انواع معمول Access-List را نمایش میدهد:

ACL Type :	ACL Number :
IP Standard	1-99
IP Extended	100-199
AppleTalk	600-699
IPX Standard	800-899
IPX Extended	900-999
IPX SAP	1000-1099

معرفی IP Access-Lists

یکی از وظایف معمول Access-List ها Packet Filtering است

Standard: تنها بر روی Source و یا مبدا کنترل دسترسی انجام میدهد

Standard ACL Template :
access-list list# [permit/deny] source-ip wildcard-mask

Extended: بر روی Source-IP و Destination IP کنترل دسترسی انجام میدهد

و همچنین Source Port و Destination Port کنترل دسترسی دارد

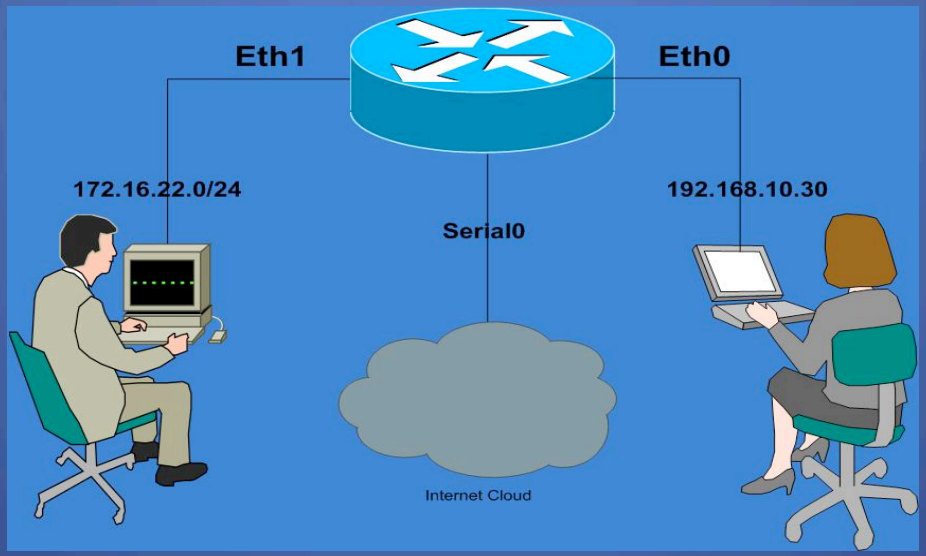
Extended ACL Template :
access-list list# [permit/deny] protocol src src-wildcard dst dst-wildcard operator [port]

IP Standard Access-List

همانطور که گفته شد، در ACL استاندارد ، تنها میتوان بر روی مبدا مدیریت داشت .

به مثال زیر توجه کنید :

با توجه به شکل زیر میخواهیم کاربر192.168.10.30 به شبکه 127.16.22.0 دسترسی نداشته باشد



پس مینویسیم :

access-list 10 deny host 192.168.10.30

چگونگی اعمال Access-List

Acess-List ها بتنهایی قادر به انجام کاری نیستند و تنها بعنوان یک لیست ، گروهی را با سیاستهای تعریف شده در خود جای داده است .

با استفاده از قالب دستوری زیر ، بایستی قانون و سیاست نوشته شده خود را در قالب یک گروه ، به درگاه خاصی اختصاص دهیم .

Interface port #

Ip access-group [acl#] [in/out]

پس برای اتمام عملیات در مثال قبل مینویسیم :

Interface ethernet 1

Ip access-group 10 [out]

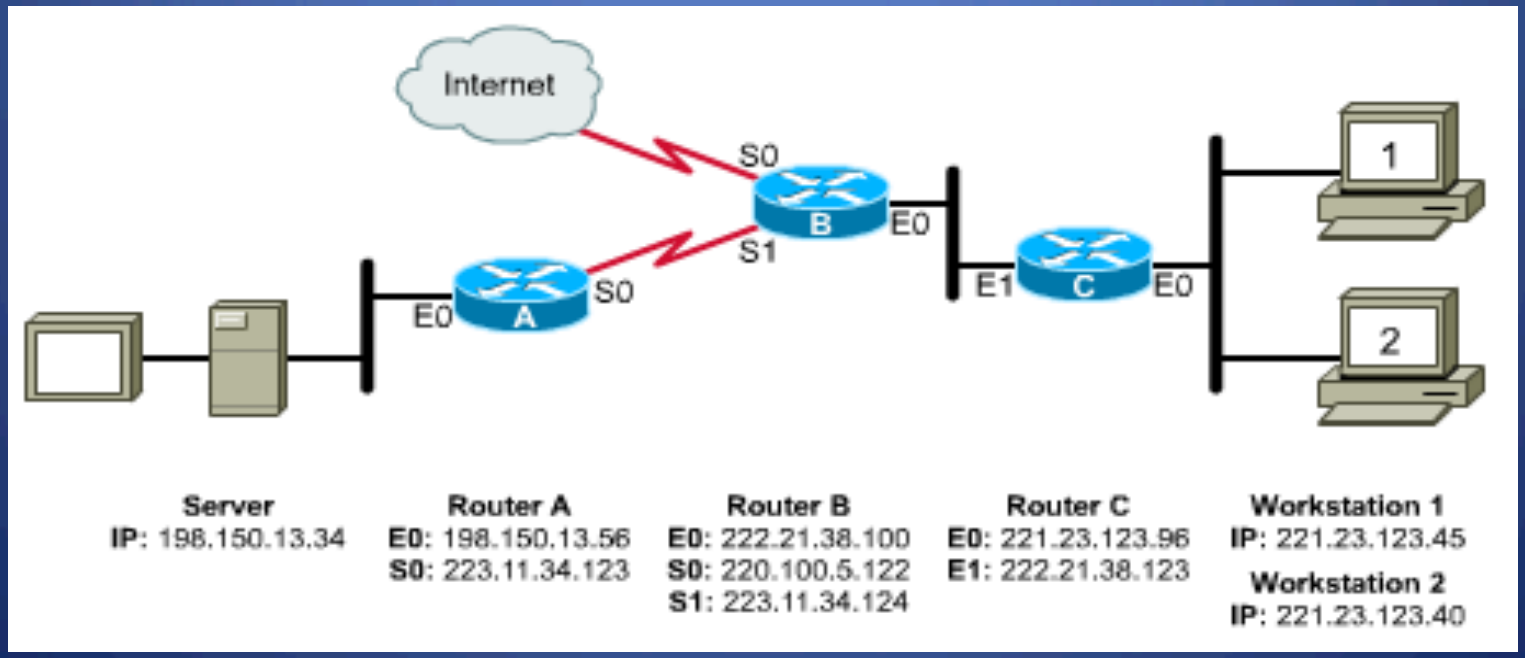
با توجه به قرارگیری این قانون در درگاه ethernet 1 ، کاربر192.168.10.30 ، بجز عدم ارتباط با شبکه 127.16.22.0/24 ، قادر است با اینترنت ارتباط خود را حفظ کند .

IP Extended ACL

از آنجایی که Extended-ACL بر روی مقصد و درگاهها نیز کنترل دارد ، میتوان در قوانین خود ، محدودیتهای دقیقتری را در نظر گرفت .

در سناریوی زیر میخواهیم ، شبکه 221.23.123.0 را به سرور 198.150.13.34 مسدود کنیم .

در کدام روتر و کدام interface باید Access-List بکار رود ؟



ابتدا یک ACL در روتر C مینویسیم و آن را در اینترفیس ethernet 0 روتر بکار میبریم .

access-list 101 deny ip 221.23.123.0 0.0.0.255 host 198.150.13.34

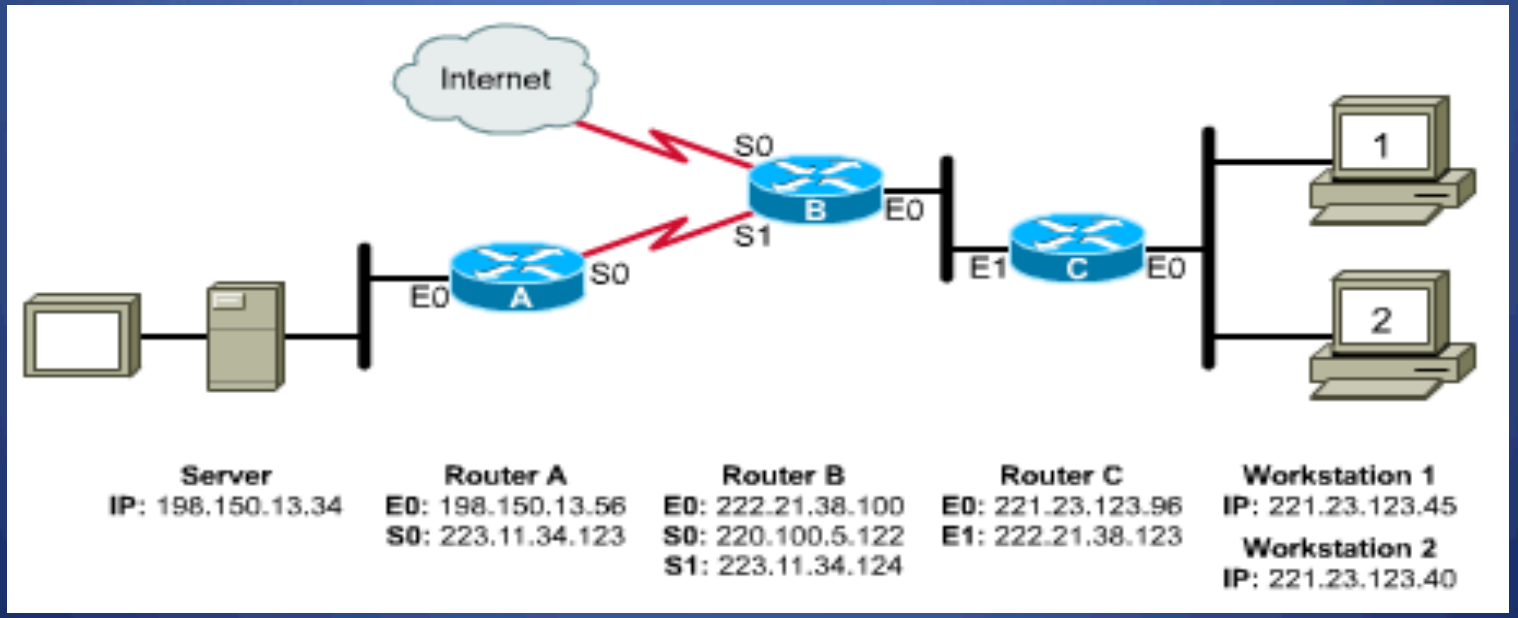
با توجه به اینکه ترافیک یک ترافیک ورودیست ، باید با استفاده از دستور

Interface eth0#

ip access-group acl101 in

کنترل دسترسی را انجام داد .

با این عمل ، اجازه خواهیم داد که شبکه 221.23.123.0 به جز آدرس 198.150.13.34 به هر جای دیگر دسترسی داشته باشد .



Wildcard Mask

جهت درک مفهوم Wildcard Mask با مثال کوچکی پیش خواهیم رفت :

میخواهیم شبکه 192.168.32.0/28 را از دسترسی به یک شبکه یا سیستم مسدود کنیم ...

مرحله اول :

Wildcard Mask را محاسبه میکنیم

همانطور که میدانیم 28/ یعنی 255.255.255.240

باینری آن برابر است با :

11111111.11111111.11111111.11110000

برای Wildcard Mask تنها بیت های 0 مورد توجه قرار میگیرد .

128/64/32/16/8/4/2/1 => 1+2+4+8 = 15

بنابراین Wildcard Mask برابر است با 0.0.0.15

access-list را هم از قرار زیر مینویسیم

access-list 1 deny 192.168.32.0 0.0.0.15

access-list 1 permit any

Wildcard Mask Example

مثال :

access-list مینویسیم که دسترسی شبکه 210.93.105.0 را به هر جا ، بر روی سریال 0 مسدود کرده و به دیگران اجازه ی عبور دهیم

```
access-list 4 deny 210.93.105.0 0.0.0.255
access-list 4 permit any
Interface serial 0
ip access-group 4 [out]
```

مثال مشابه با این تفاوت که تنها نیمه 128 تایی اول شبکه را در نظر میگیریم :

```
access-list 4 deny 210.93.105.0  0.0.0.127
```

و نیمه 128 تایی دوم شبکه از قرار زیر :

```
access-list 4 deny 210.93.105.128  0.0.0.127
```

مثال مشابه با این تفاوت که تنها ip های زوج در نظر گرفته شود : (بیت آخر ip برابر 0)

```
access-list 4 deny 210.93.105.0  0.0.0.254
```

مثال مشابه با این تفاوت که تنها ip های فرد در نظر گرفته شود : (بیت آخر ip برابر 1)

```
access-list 4 deny 210.93.105.1  0.0.0.254
```

Don’t Forget to Permit others

از آنجایی که access-list ها دارای یک عبارت deny any بصورت پیشفرض در آخر هر لیست میباشند ، لذا پس از نوشتن سطح دسترسی های مختلف باید متوجه اعطای مجوز permit به گروه های دیگر باشیم ...

بعنوان مثال اگر شبکه را از دسترس منع کردیم ، بایستی با نوشتن دستوری دیگر ، سطح دسترسی را برای دیگران باز گذاشت، چرا که همانطور که گفته شد بصورت پیشفرض، دستور deny any در آخر لیست موجود است که بعد از چک کردن تمامی قوانین، دسترسی همه را قطع خواهد نمود . لذا اگر میخواهیم deny any وجود داشته باشد، پس قبل از آن قوانین اجازه دسترسی کاربران و شبکه ها را در آن لیست تعیین میکنیم تا با دستور پیشفرض مذکور با مشکل مواجه نشویم .

به مثال زیر توجه کنید :

access-list 1 deny 192.168.10.0 0.0.0.128

access-list 1 permit any

با استفاده از این دستور ، deny any خنثی میگردد (البته اگر بصورت دستی deny any را قبل از آن وارد نکرده باشیم !)

مورد عکس نیز وجود دارد ، بدین معنی که میتوان ابتدا شبکه ها و یا گره هایی از شبکه را به لیست سفید (permit) اختصاص دهیم و در آخر deny any را اضافه کنیم .

Filtering بر مبنای Protocol Type & Port Number

access-list 110 deny tcp host 10.10.10.1 any neq 22
access-list 110 permit tcp any any eq 22
access-list 110 deny udp any host 192.168.10.1 eq 53

ip access-list extended 120
deny tcp any any gt 1024
permit tcp host 10.10.2.10 any lt 23
deny tcp 10.10.10.128 0.0.0.127 host 172.16.1.20 range 20 23

Named-ACL
ip access-list extended Logging-ACL
permit tcp host 10.10.10.11 host 192.168.1.10 eq 23 log
permit tcp host 10.10.10.11 host 192.168.1.10 eq 23 log-input

TCP header fields

access-list 106 permit udp any any

ack Match on the ACK bit
established Match established connections
fin Match on the FIN bit
fragments Check non-initial fragments
psh Match on the PSH bit
rst Match on the RST bit
syn Match on the SYN bit
urg Match on the URG bit
eq Match only packets on a given port number
gt Match only packets with a greater port number
log Log matches against this entry
log-input Log matches against this entry, incl. input interface
lt Match only packets with a lower port number
neq Match only packets not on a given port number
precedence Match packets with given precedence value
range Match only packets in the range of port numbers
tos Match packets with given TOS value

Verifying ACLs

Show commands:

- **`show access-lists`**
  - shows all access-lists configured on the router
- **`show access-lists {`*`name`*` | `*`number`*`}`**
  - shows the identified access list
- **`show ip interface`**
  - shows the access-lists applied to the interface--both inbound and outbound.
- **`show running-config`**
  - shows all access lists and what interfaces they are applied on

Enhanced Access Lists

Time-Based

ACL ها در ساعت خاصی از روز و یا روز خاصی در هفته فعال شده و ایفای نقش میکنند

```
(conf)# time-range APA
(conf-time-range)# periodic daily 10:00 to 13:00
(conf-time-range)# ip access-list  TimeACL in

 (conf-time-range)#ip access-list extended TimeACL
(config-ext-nacl)# deny tcp any any eq www time-range  APA
(config-ext-nacl)# permit ipv6 any any
```

Reflexive

```
! create the named extended access list that "sees" the outbound packets
      ip access-list extended outbound-packet-watch
        permit tcp any any reflect tcp-reflexive-temporary-list
        permit udp any any reflect udp-reflexive-temporary-list

! create the named extended access list that evaluates the inbound packets
      ip access-list extended inbound-packet-catcher
        evaluate tcp-reflexive-temporary-list
        evaluate udp-reflexive-temporary-list

interface serial 1/0
        ! apply the named access list to watch packets leaving the secure network
        ! as they go out serial 1/0
        ip access-group outbound-packet-watch out
        ip access-group inbound-packet-catcher in
```

http://www.commandsource.org/