مبانی اولیه سیسکو

CCNA

CISCO CERTIFIED
CCNA
Security

جلسه نهم : Access - List

✓ آموزش کامل Routing & Switching

✓ به همراه سناریو

نویسنده: مهندس امیرحسین خالقی

فهرست

Akhaleghi.ir

پیشگفتار

سپاس پروردگار را که این امکان را داد که تا باز بتوانیم مجموعه ای پر مطلب و پر فهم را کمتر از یک سال بنویسیم.

این کتاب با توجه به سرفصل های کتاب CCNA ICND 1 & ICND 2 برای علاقه مندان به شبکه و سیسکو نوشته شده است. در تهیه این کتاب سعی بر آن شده است تا فهم مطالب و مباحث به صورت روان و گیرا مطرح گردد.

در ابتدای کتاب سر فصل مطالب قید شده است. در انتهای هر فصل سناریویی طراحی شده که می تواند در فهم و یادگیری سریع تر شما کمک کند. توصیه می شود که این سناریو ها حتما کار شود. در انتهای کتاب به بررسی نمونه سوالات آزمون Cisco پرداخته ایم.

درصورت هرگونه مشکل در این کتاب میتوانید با ایمیل نویسنده (info@akhaleghi.ir) تماس حاصل فرمایید تا با بررسی آن بتوانیم کتابی کامل و با زبان فارسی در اختیار شما دوستان و همکاران ارجمند قرار دهیم.

در پایان از تمامی عزیزانی که ما را در تهیه و تنظیم این کتاب یاری نموده اند کمال تشکر را داریم.

باشد که موثر باشیم ....

امیرحسین خالقی

Akhaleghi.ir

Access-List :

خب... تا اینجای کار با روتینگ پروتکل ها آشنا شدیم. حال نوبت به کنترل ترافیک شبکه و تعیین مجوز های دسترسی برای ترافیک هاست. مثلا آیا شبکه ۱۰,۱۰,۱۰,۲ اجازه دارد برای ما ترافیک بفرستد یا خیر؟

ما در Access List ها یاد میگیریم چطور ترافیک شبکه را مدیریت کنیم و اعمال فیلترینگ داشته باشیم. ما میتوانیم با استفاده از Access List برای یک روتر تعریف کنیم چه ترافیک هایی اجازه ورود به روتر و چه ترافیک هایی اجازه خروج از روتر را دارند.

Access-List ها به دو صورت قابل پیاده سازی هستند :

- Standard Access-List
- Extended Access-List

Standard Access-List

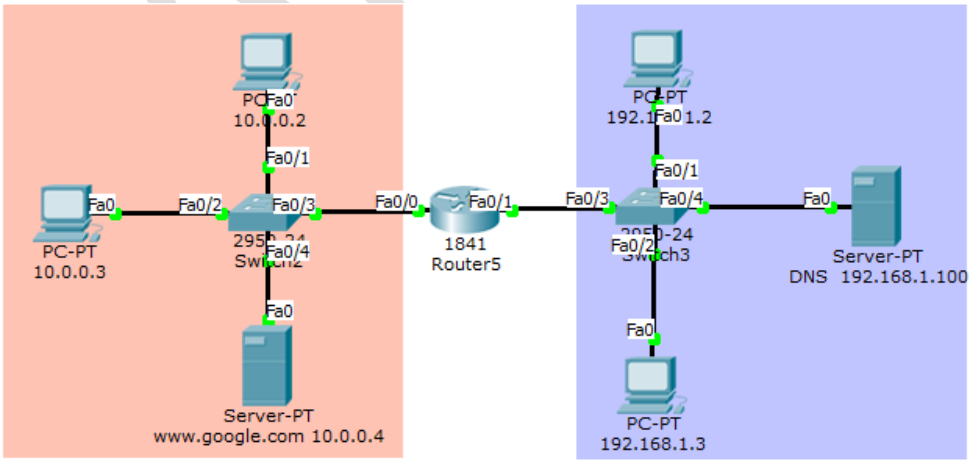
خصوصیات Access List های استاندارد:

- ✓ این نوع Access-List این اجازه را به ما می دهد که در لایه سه (لایه نتورک) برحسب Logical Address ها (همون آدرس IP) اعمال فیلترینگ داشته باشیم.
- ✓ برای متمایز کردن Access-List های استاندارد از همدیگر از یک رینج عدد استفاده می کنیم. رینج عددی که برای این Access-List ها در نظر گرفته شده از ۱ تا ۹۹ هست.

نکته : چون Range این اعداد کم بود، از IOS ورژن ۱۱,۲ به بعد رینج عددی ۱۳۰۰ تا ۱۹۹۹را برای Access List استاندارد اضافه کردند. یعنی با این اعداد هر Access List ی نوشته شود، هم مشخص می کند چه نوع Access List هست (چون بین ۱۳۰۰ تا ۱۹۹۹ هست پس Access List استاندارد هست)، هم اینکه این عدد، اسم آن Access-List به حساب می آید.

- ✓ Access- List های استاندارد بنابر Source قابل تعریف هستند نه بنابر Destination.

نحوه پیاده سازی Access-List Standard به چه صورت هست؟



فرض کنید در شکل فوق نمی خواهیم 10.0.0.3 Network به شبکه 192.168.1.100 دسترسی داشته باشد. برای این کار می خواهیم از access-list استاندارد استفاده کنیم. جهت این کار در محیط کانفیگ ترمینال دستوری هست به نام Access-list .

```
Router(config)#access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
Router(config)#access-list 1 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
Router(config)#access-list 1 deny ?
  A.B.C.D  Address to match
  any      Any source host
  host     A single host address
```

پس از تایپ این دستور از ما می خواهد که شماره آن را مشخص کنیم . خب چون ما می خواهیم access-list استاندارد تعریف کنیم پس باید بین رینج ۱ تا ۹۹ بگذاریم. همینطور میتونیم بین رینج ۱۳۰۰ تا ۱۹۹۹ نیز بگذاریم. حال بعنوان مثال ۱ را انتخاب می کنیم که مشخص کنیم که می خواهیم اکسس لیست استاندارد تعریف کنیم. اگر همینجا ؟ بگیریم میبینیم :

- ✓ Deny: بواسطه این دستور ما جلوی دسترسی را می گیریم.
- ✓ Permit: بواسطه این دستور ما اجازه دسترسی می دهیم.
- ✓ Remark: بواسطه این دستور ما می تونیم Description یا توضیح بنویسیم. یعنی بعنوان مثال بنویسم این access-list به شماره یک از دسترسی فلان شبکه جلوگیری می کند.

خب ما اینجا Deny را انتخاب می کنیم. اگر اینجا ؟ بگیریم مجددا سه گزینه در جلوی راه ما قرار می گیرد.

- ✓ Hostname: می توانیم از دسترسی یک Network جلوگیری به عمل آوریم. مثلا می توانیم بگوییم کلا 10.0.0.0 Network نتواند به آدرس شبکه 192.168.1.100 دسترسی داشته باشد. البته بعد از تایپ Network باید wildcard را هم مشخص کنیم.
- ✓ Any: اگر بخواهیم از دسترسی همه به شبکه خاصی جلوگیری کنیم.
- ✓ Host: اگر بخواهیم از دسترسی یک نفر یا یک هاست مشخص جلوگیری کنیم از این دستور استفاده می کنیم.

همانطور که در بالا مشاهده کردید ، این access-list یعنی Access-List Standard بر اساس source هست، یعنی ما به آن آدرس مقصد ندادیم و فقط گفتیم که فلان آدرس در این روتر اجازه دسترسی ندارد. حالا به کجا اجازه دسترسی ندارد را دیگر تعریف نمی کنیم.

نکته مهمی که در اینجا باید توجه داشته باشید این هست که نوشتن Access-List به خودی خود کاری انجام نمی دهد و به عبارتی نوشتن یک قانون هست، برای پیاده سازی آن باید حتما شماره اکسس لیست نوشته شده را به یکی از اینترفیس ها Assign کنیم. بعنوان مثال در مثال بالا به یکی از اینترفیس ها بگیم که از آدرس 10.0.0.3 پکتی اومد جلوی آن را بگیر

اما نحوه Assign کردن یک Access-List به یک interface :

۱. وارد interface مورد نظر می شویم. بعنوان مثال وارد interface Fastehternet 0/0 می شویم.

۲. حال از دستور روبه رو استفاده می کنیم.

```
Router(config-if)#ip access-group ?
  <1-199>  IP access list (standard or extended)
  WORD     Access-list name
Router(config-if)#ip access-group 1 ?
  in   inbound packets
  out  outbound packets
Router(config-if)#ip access-group 1 in
```

اگر در اینجا ؟ بگیریم به ما می گوید که از کدام access-list ها می خواهی استفاده کنی که ما در مثال بالا access-list به شماره یک را تعریف کردیم.

حال مجدد ؟ می گیریم. از ما می پرسد in یا out . یعنی موقع ورود عمل کند یا موقع خروج؟ یعنی از ورد پکت هایی که آدرس source آنها 192.168.1.100 هست جلوگیری کنم یا از خروج پکت هایی که آدرس source آنها 192.168.1.100 هست؟ بسته به نیاز یکی از کلمه های in یا out را انتخاب می کنیم.

حال پکتی که آدرس source 192.168.1.100 باشد، بخواهد به interface Fastehternet 0/0 این روتر وارد شود از ورودش جلوگیری به عمل می آید. یعنی کلا پکت از طرف آن آدرس Network این روتر دریافت نمی کند و همه را Drop می کند.

چند قانون

- با یک شماره Access-List می توانیم بی نهایت قانون تعریف کنیم.
- به هر interface فقط می توان یک شماره Access-list ورود اختصاص داد یا اصطلاحا Assign کرد ویک Access-List خروج و اگر دو تا Access-List assign کنیم Access-List جدید بر روی قبلی overwrite و جایگزین می شود. دقت کنید که روی In و Out یک interface هرکدام می توان یک Access-List اختصاص داد.
- در IOS های قبل از 12.1 می توانستیم In و Out را مشخص نکنیم. که به طور پیش فرض Out در نظر می گرفت.
- ترتیب نوشتن Access لیست ها مهم است (مخصوصا روی IOS های قدیمی). وقتی ترافیکی می آید روتر به داخل Access-List می رود و هرجا ترافیک با match Access-List شود (مثلا گفته باشد که ترافیک را deny کن و از ورودش جلوگیری کن) دیگر سراغ Access-List های بعدی نمی رود و همون جا ترافیک را Deny می کند.

هر Access-List که نوشته می شود یک خط هم به آخر آن اضافه می شود که عبارت است از :

```
Router(config)#access-list 1 deny any
```

این خط در انتهای هر شماره Access-List وجود دارد و به صورت transparent و نامرئی وجود دارد که دیده نمی شود و همه را deny می کند. مثلا اگر دستور زیر را نوشته باشیم که فقط یک هاست را deny کنیم:

```
Router(config)#access-list 1 deny host 192.168.1.100
```

آن خط بالا هم زیر آن قرار می گیرد و همه را deny می کند. یعنی اگر 192.168.1.101 هم بیاید باز deny می شود در صورتی که ما آن را نگفته بودیم! جهت حل این مشکل کافی است آخر دستوری که می دهیم دستور زیر را بدهیم:

```
Router(config)#access-list 1 permit any
Router(config-if)#ip access-group 1 in
```

Access-List Extended

خصوصیات Access-List Extended:

- ✓ قابل پیاده سازی در لایه ۳ و لایه ۴ می باشد. **(یعنی هم بر** اساس Logical Address و هم بر اساس Port Number یا شماره پورت ها می توانیم اعمال محدودیت داشته باشیم)
- ✓ رینج عددی Access-List های extended از ۱۰۰ تا ۱۹۹ هست و در IOS های 12.1 به بعد رینج عددی 2000 تا 2699 به بعد نیز اضافه شده اند.

✓ این نوع از Access-List هم بنا بر Source و هم بنابر Destination عمل می کنند.

حال باهم به بررسی مثال بالا می پردازیم:

فرض بگیرید یک Access-List می خواهیم بنویسیم و جلوی دسترسی 10.0.0.3 را به آدرس 192.168.1.100 بگیریم:

```
Router(config)#access-list 100 deny ?
  ahp    Authentication Header Protocol
  eigrp  Cisco's EIGRP routing protocol
  esp    Encapsulation Security Payload
  gre    Cisco's GRE tunneling
  icmp   Internet Control Message Protocol
  ip     Any Internet Protocol
  ospf   OSPF routing protocol
  tcp    Transmission Control Protocol
  udp    User Datagram Protocol
Router(config)#access-list 100 deny ip ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
Router(config)#access-list 100 deny ip host ?
  A.B.C.D  Source address
Router(config)#access-list 100 deny ip host 10.0.0.3 ?
  A.B.C.D  Destination address
  any      Any destination host
  host     A single destination host
Router(config)#access-list 100 deny ip host 10.0.0.3 host 192.168.1.100
```

ابتدا قانون کلی را تعریف می کنیم و سپس آن Access-List را به Assign interface می کنیم.

اگر ؟ بگیریم از ما می پرسد که بر حسب IP می خواهی ببندی یعنی همان Logical Address یا برحسب پروتکل؟ بعنوان مثال ما Ip را می زنیم:

حال اگر ؟ را بگیریم از ما Source Address را می پرسد. سه گزینه زیر را در اختیار ما قرار می دهد:

- Source Address: که ما در اینجا آدرس سورس را 10.0.0.3 میگذاریم.
- Any Source Host:
- A single Source Host:

دو گزینه دیگر هم که در قبل توضیح داده شد و مشخص است.

مجدد ؟ می گیریم، باز سه گزینه اما این بار برای Destination و مقصد در اختیار ما قرار می دهد.که طبق سناریو ما باید مجدد در این جا host را انتخاب کنیم و آدرس مقصد را 192.168.1.100 بدهیم.

خب. به همین سادگی ما یک extended Access-List نوشتیم که از دسترسی آی پی آدرس 10.0.0.3 به آدرس 192.168.1.100 جلوگیری می کند.

یک نکته را دقت داشته باشید بهترین جا برای Assign کردن یک Extended Access-List نزدیک ترین جا به Source هست .چون مبدا و مقصد مشخص است ، ترافیک بیخود در شبکه در گردش نباشد و اگر به مقصد خاصی است به جای اینکه در مقصد drop شود همان در مبدا drop اش می کنیم که بیخود ترافیک در شبکه در جریان نیوفتد و بار را زیاد نکند.

برعکس بهترین جا برای Assign کردن یک Access-List استاندارد نزدیک ترین جا به Destination هست .

حال چگونه یک Extended Access-List بنویسیم بر اساس پورت بنویسیم؟(لایه چهارم)

حال فرض بگیریم که بخواهیم جلوی دسترسی آی پی آدرس 192.168.10.10 را به صفحات وب 172.16.0.1 بگیریم یعنی پورت ۸۰ آنرا ببندیم.

جهت این کار کافی است دستور زیر را تایپ کنیم:

```
Router(config)#ACCess-list 100 deny tcp host 10.0.0.3 host 192.168.1.100 eq 80
```

همانطور که می بینید در دستور بالا به جای IP از پروتکل TCP استفاده کردیم. Source و Destination را مشخص کردیم و در پایان با استفاده از دستور EQ یک شماره پورت را مشخص کنیم. یعنی بگیم فقط پورت ۸۰ را deny کن.

نکات!

اگر بخواهیم بگیم که به هیچ چیز دسترسی نداشته باشد و فقط به پورت 80 دسترسی داشته باشد کافی است به جای eq کلمه neq را به کار ببریم.

```
Router(config)#ACCess-list 100 deny tcp host 10.0.0.3 host 192.168.1.100 neq 80
```

اگر بخواهیم بگیم که یک رینج پورت را ببندیم به جای EQ از دستور Range استفاده می کنیم . مثلا از رینج ۸۰ تا ۱۰۰

```
Router(config)#ACCess-list 100 deny tcp host 10.0.0.3 host 192.168.1.100 range 8
0 100
```

و اگر بخواهیم از یک پورت به بعد را ببندیم می توانیم به جای eq از gt استفاده کنیم و همینطور بخواهیم از یک پورت به پایین را ببندیم به جای eq از lt استفاده می کنیم.

تمرین:

اگر بخواهیم فقط آی پی آدرس 192.168.10.10 اجازه داشته باشد به روتر از طریق پورت کنسول دسترسی داشته باشد چه Access-list ی باید بنویسیم؟

```
Router(config)#access-list 1 permit 192.168.10.10
Router(config)#line vty 0
Router(config-line)#access-class 1 in
Router(config-std-nacl)#permit host 192.168.10.10
```

سه خط دستور بیشتر نیاز ندارد. هر سه خط هم در روتر نوشته می شود .

دقت کنید همانطور که می بینید ما حتی می توانیم بر روی پورت کنسول هم Access-list بنویسیم. فقط تنها تفاوتش این هست که برای Assign کردن باید به جای استفاده از دستور Access-group از دستور Access-class استفاده کنیم.

چطور به Access-list ها نام اختصاص دهیم؟

ما در نوشتن Access-list ها باعدد یک سری محدودیت ها داشتیم: اول اینکه تعدادش محدود بود و دوم اینکه اگر چندتا Access-list بنویسیم و بهش عدد اختصاص بدیم دیگه شناسایی اینکه کدوم عدد کدوم Access-list بود سخت می شه.

سیسکو از IOS های 12.1 به بعد گفت می توانید Access-list ها را با اسم تعریف کنید و استفاده کنید. دیگه هم محدودیت در تعداد Access-list ها برطرف میشه و هم شناسایی Access-list ها بسیار ساده تر میشه. **اما چطور این کار را انجام دهیم؟**

حالا وارد Access-list استاندارد میشیم و داخلش می تونیم به سادگی قوانین رو بنویسیم . مثلا:

```
Router(config)#ip access-list standard Cisco
```

همینطور اگر بخواهیم extended Access-list تعریف کنیم به صورت زیر عمل می کنیم:

```
Router(config)#ip access-list extended Cisco
```

به همین سادگی ما Access-list را با نام تعریف کردیم.

نکته آخر اینکه اگر بخواهیم Access-list را برداریم کافی است مثل همیشه از no قبل از دستور استفاده کنیم. یعنی بنویسیم

```
Router(config)#no access-list 1
```

Akhalegh.ir