احتمالا تا حالا برای شما پیش آمده باشد که بخواهید دسترسی یک کلاینت را به یک سرور خاص محدود کنید یا بخواهید استفاده از یک برنامه خاص مثل telnet را مسدود کنید و یا به طور کلی بخواهید بروی عملکرد شبکه کنترل و نظارت داشته باشید. با استفاده از Access Control List که به آن Access list نیز گفته می شود می توانید تمام موارد ذکر شده و بسیاری قابلیت های دیگر را داشته باشید. در این مقاله سعی بر آن شده که ACLs را مورد بررسی قرار گیرد و نحوی عملکرد آن شرح داده شود.

Access Control List یا ACL یک فیلتر است که به وسیله آن می توانیم جریان ترافیک را کنترل کنیم که چه بسته هایی اجازه ورود یا خروج به شبکه را دارند یا خیر. این فیلتر معمولا توسط مدیر شبکه تعیین و مورد استفاده قرار می گیرند تا به این وسیله بتواند کنترل و امنیت بیشتر را برای شبکه خود فراهم کند. این فیلترها را می توان روی بسیاری از دستگاه های شبکه مانند روتر و سوئیچ مورد استفاده قرار داد.

ACLs ها یک روش قدرتمند برای کنترل ترافیک ورودی یا خروجی به شبکه می باشد این کنترل می تواند به صورت ساده براساس آدرس IP انجام شود یا براساس بررسی آیتم ها متفاوت و پیچیده انجام گیرد. ACLs را میتوان برای پروتکل متفاوت مانند IP، AppleTalk و ... استفاده کرد.

مهمترین دلیل استفاده از ACLs ها فراهم کردن امنیت برای شبکه می باشد هرچند که برای مقاصد دیگری مانند کنترل ترافیک نیز استفاده می شود.

نحوی عملکرد ACLs :

برای اینکه نحوی عملکرد ACLs ها را بهتر درک کنیم یک نگهبان که جلوی یک در بسته مستقر است را تصور کنید. نگهبان براساس دستورالعملی که به او داده شده اجازه عبور به افراد را می دهد به طور مثال به او یک لیست داده شده که فقط این افراد اجازه ورود دارند. افراد که می خواهند از این در عبور کنند نام آنها توسط نگهبان با لیست خود مطابقت داده می شود و در صورتی که نام آنها در لیست بود به آنها اجازه عبور از در را می دهد در غیر اینصورت فرد اجازه عبور از در را نخواهد داشت .
ACLsها با استفاده از آیتم های مختلف مانند آدرس مبدا و مقصد ، پورت مبدا و مقصد ، نوع پروتکل و ... می تواند عمل فیلترینگ را روی بسته های ورودی یا خروجی یک پورت برای ما انجام دهد. زمانی که یک بسته به دستگاه می رسد در صورت وجود ACLs ، اطلاعات موجود در Header بسته را بررسی می کند و با آیتم های تعریف شده در ACLs مقایسه می کنند و نسبت به آن اجازه یا عدم اجازه عبور به بسته را می دهد .

چه زمانی از ACLs استفاده می کنیم:

- جهت مقاصد امنیتی
- محدود کردن ترافیک برای افزایش کارایی شبکه
- جهت کنترل بسته های مربوط به پروتکل های مسیریابی
- چه نوع ترافیکی اجازه عبور یا عدم عبور دارند
- جداسازی برخی ترافیک های خاص به منظور عملیات خاص مانندQoS
- اعمال محدودیت های زمانی
- و...

انواع: Access Control List

- Standard ACLs
- Extended ACLs
- Reflexive ACLs
- Time-Base ACLs
- Established ACLs

ACLs را می توان به دو صورت تعریف کرد یکی براساس نام و دیگری براساس عدد. که هر کدام می تواند یکی از دو نوع Extended یا Standard باشد.

زمانی که یک ACLs با استفاده از نام ایجاد می کنیم قبل از مشخص کردن نام نوع آنرا مشخص می کنیم مانند مثال زیر:

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

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

زمانی که یک ACLs با استفاده از عدد ایجاد می کنیم شماره عددی که انتخاب می کنیم نشان دهنده نوع آن می باشد. یک نمونه از ACL با نام گذاری عددی:

```
Router(config)#access-list 101 deny tcp host 192.168.1.1 eq www host 10.1.1.1
```

جدول زیر نشان دهنده محدوده این اعداد و نوع آنها می باشد.

Type	Range
IP Standard	1–99
IP Extended	100–199
IP Standard Expanded Range	1300–1999
IP Extended Expanded Range	2000–2699

نحوی تخصیص ACLs :

زمانی که یک ACLs تعریف می شود برای عمل کردن باید به یک پورت اختصاص داد شود که می تواند در دو جهت زیر ترافیک را کنترل کند:

Inbound : منظور ترافیکی است که وارد یک پورت می شود.

Outbound : ترافیک است که از یک پورت خارج می شود.

با انتخاب هر کدام از این دو جهت ترافیک توسط ACLs ترافیک شروع به کنترل می شود.

ACLs Action :

زمانی که یک ACLs تعریف می شود دو نوع اقدام زیر را می توان نسبت به ترافیک که بررسی می کند می توان در نظر گرفت :

Deny : اجازه عبور به بسته را نمی دهد.

Permit : اجازه عبور به بسته را می دهد.

سیسکو دو نوع Access list با نام های Standard ACL و Extended ACL معرفی کرده است. Standard ACL قدیمی ترین و ساده ترین نوع Access List است که در نسخه IOS 8.3 سیسکو ارائه شده است. Standard ACL ترافیک را به وسیله مقایسه آدرس مبدا بسته ها با آدرس تعریف شده در ACL کنترل می کند. در همه نسخه ها ، برای Standard ACL می توان یک عدد از ۱ تا ۹۹ در نظر گرفت. از نسخه IOS 11.2 سیسکو امکان تعریف Standard ACL به وسیله نام فراهم شد و همچنین از نسخه IOS 12.0.1 سیسکو محدود عددی بین ۱۳۰۰ تا ۱۹۹۹ برای Standard ACL اضافه شد.

نحوی تعریف Standard ACL در حالت عددی:

```
access-list access-list-number {permit|deny} {host|source-wildcard|any}
```

access-list-number : عدد بین ۱ تا ۹۹ یا ۱۳۰۰ تا ۱۹۹۹

permit|deny : عملی که در هنگام تطبیق بسته با ACL نسبت با آن گرفته می شود(اجازه عبور یا عدم اجازه)

host-source-wildcard-any : مشخص کردن IP به یکی از سه روش زیر:

Host : یک ادرس IP مشخص می کنیم مانند Host 192.168.1.1

Any : هر IP آدرسی

source source-wildcard : تعیین یک IP به همراه Wildcard Mask

نحوی تعریف Standard ACL با استفاده از نام :

```
IP Access-list {standard|extended} name
{permit|deny} {host|source source-wildcard|any}
```

نحوی تخصیص به Standard ACL اینترفیس:

```
Ip access-group {number|name} {in|out}
```

Extended ACL نوعی دیگری از ACL است که برخلاف Standard ACL می تواند ترافیک را براساس فیلدها و پارامترهای مختلف برای ما کنترل کند. وجود پارامترهای فراوان به ما این امکان را می دهد که بتوانیم ترافیک ها را به صورت دقیق تر و بهتر کنترل کنیم. در Standard ACL ما تنها می توانیم براساس آدرس مبدا ، بسته ها را کنترل کنیم ولی Extended ACL می تواند کنترل را براساس آدرس مبدا و مقصد ، شماره پورت مبدا و مقصد ، نوع پروتکل و ... انجام دهد در نتیجه Extended ACL به عنوان یک ابزار قدرتمند برای مدیران برای کنترل ترافیک محسوب می شود.

در همه نسخه ها ، برای Extended ACL می توان یک عدد از ۱۰۰ تا ۱۹۹ در نظر گرفت. از نسخه IOS 11.2 سیسکو امکان تعریف Extended ACL به وسیله نام فراهم شد و همچنین از نسخه IOS 12.0.1 سیسکو محدود عددی بین ۲۰۰۰ تا ۲۶۹۹ برای Extended ACL اضافه شد.

پارامترهای که می توان توسط Extended ACL کنترل کرد :

- آدرس IP مبدا
- آدرس IP مقصد
- شماره پورت مبدا
- شماره پورت مقصد
- نوع پروتکل

نحوی تعریف Extended ACL در حالت عددی:

```
access-list access-list-number {permit|deny} protocol source [Source port]destinat
                                                                ion [destination port]
```

access-list-number : عدد بین ۱۰۰ تا ۱۹۹ یا ۲۰۰۰ تا ۲۶۹۹

permit|deny : عملی که در هنگام تطبیق بسته با ACL نسبت با آن گرفته می شود(اجازه عبور یا عدم اجازه)

Protocol : مشخص کردن نوع پروتکل مثل TCP، UDP، IP و ...

Source : مشخص کردن IP مبدا به یکی از سه روش زیر:

Host : یک ادرس IP مشخص می کنیم مانند Host 192.168.1.1

Any : هر IP آدرسی

source source-wildcard : تعیین یک IP به همراه Wildcard Mask

Source port : شماره پورت مبدا بسته

destination: مشخص کردن IP مقصد به یکی از سه روش زیر:

Host : یک ادرس IP مشخص می کنیم مانند Host 192.168.1.1

Any : هر IP آدرسی

source source-wildcard : تعیین یک IP به همراه Wildcard Mask

destination port : شماره پورت مبدا بسته

نحوی تعریف Extended ACL با استفاده از نام :

```
IP Access-list {standard|extended} name
{permit|deny} protocol source [Source port] destination [destination port]
```

نحوی تخصیص Extended ACL به اینترفیس :

```
Ip access-group {number|name} {in|out}
```