1.Introdução a ACL

Uma ACL é uma série de comandos do IOS usadas para filtrar pacotes com base nas informações encontradas no cabeçalho do pacote. Por padrão, um roteador não tem nenhuma ACL configurada, porém, quando uma ACL for aplicada a uma interface, o roteador executará a tarefa adicional de avaliar todos os pacotes de rede que passam pela interface para determinar se o pacote pode ser enviado.

Ela usa uma lista sequencial de instruções de permissão ou negação, conhecidas como entradas de controle de acesso (ACEs). Quando o tráfego da rede passa através de uma interface configurada com uma ACL, o roteador compara as informações no pacote com cada ACE, em ordem sequencial, para determinar se o pacote corresponde a uma das ACEs. Esse procedimento é chamado de filtragem de pacotes.

A filtragem de pacotes controla o acesso a uma rede analisando os pacotes de entrada e/ou saída, encaminhando-os ou descartando-os com base nos critérios fornecidos. A filtragem de pacotes pode ocorrer na camada 3 ou camada 4.

Os roteadores Cisco suportam 2 tipos de ACLs.

- **ACLs padrão:** As ACLs filtram apenas na camada 3 usando apenas o endereço IPv4 de origem
- **ACLs estendidas:** Os ACLs filtram na camada 3 usando o endereço IPv4 de origem e/ou destino. Eles também podem filtrar na camada 4 usando TCP, portas UDP e informações de tipo de protocolo opcional para controle mais fino.

Uma ACL de entrada filtra pacotes antes de serem roteados para a interface de saída. Ela é eficiente porque salva a sobrecarga de pesquisas de roteamento se o pacote é descartado. Se o pacote for permitido pela ACL, ele será processado para roteamento. As ACLs de entrada são mais usadas para filtrar pacotes quando a rede conectada a uma interface de entrada é a única origem dos pacotes que precisa ser examinada.

Uma ACL de saída filtra pacotes após seu roteamento, independentemente da interface de entrada. Pacotes de entrada são roteados para a interface de saída e são processados através da ACL de saída. As ACLs de saída são mais usadas quando o mesmo filtro é aplicado aos pacotes que vêm de várias interfaces de entrada antes de saírem da mesma interface de saída.

Uma ACL IPv4 usa uma máscara curinga de 32 bits para determinar quais bits do endereço examinar para uma correspondência. As máscaras curingas também são usadas pelo protocolo de roteamento OSPF.

Uma máscara curinga é semelhante a uma máscara de sub-rede na vez que usa o processo de ANDing para identificar quais bits em um endereço IPv4 devem

corresponder. No entanto, eles diferem na forma como combinam 1s e 0s, onde na máscara de sub-rede 1s são correspondência e 0s não, o inverso é verdadeiro.

As máscaras curinga utilizam as seguintes regras para corresponder ao binário 1s e 0s.

- **Máscara curinga bit 0:** Corresponde ao valor do bit correspondente no endereço
- **Máscara curinga bit 1:** Ignora o valor do bit correspondente no endereço

Máscara curinga	Último octeto (em binário)	Significado
0.0.0.0	00000000	Combine todos os octetos
0.0.0.63	00111111	Combine os três primeiros octetos Combine os dois restantes bits do último octeto Ignore os últimos 6 bits
0.0.0.15	00001111	Combine os três primeiros octetos Combine os quatro restantes bits do último octeto Ignora os últimos 4 bits do último octeto
0.0.0.252	11111100	Combine os três primeiros octetos Ignora os seis restantes bits do último octeto Combina os últimos dois bits
0.0.0.255	11111111	Combine os três primeiros octetos Ignora o último octeto

Um método para calcular as máscaras é subtrair a máscara de sub-rede de 255.255.255.255.

Exemplo 1: Suponha que você desejasse uma ACE na ACL 10 para permitir o acesso a todos os usuários na rede 192.168.3.0/24. Para calcular a máscara de curinga, subtraia a máscara de sub-rede de 255.255.255.255. A solução produz a máscara curinga.

Valor início	255.255.255.255
Subtrair a máscara de sub-rede	255.255.255.0
Máscara curinga resultante	0.0.0.255

Exemplo 2: Suponha que você desejasse uma ACE na ACL 10 para permitir o acesso à rede para os 14 usuários na sub-rede 192.168.3.32/28. Subtraia a sub-rede 255.255.255.255. Esta solução produz a máscara curinga 0.0.0.15.

Valor inicial	255.255.255.255
Subtrair a máscara de sub-rede	255.255.255.240
Máscara curinga resultante	0.0.0.15

Exemplo 3: Suponha que você precisava de uma ACE na ACL 10 para permitir somente redes 192.168.10.0 e 192.168.11.0. Essas duas redes podem ser resumidas como 192.168.10.0/23, que é uma máscara de sub-rede de 255.255.254.0. Novamente, subtrair a máscara de sub-rede 255.255.254.0 de 255.255.255.255. Esta solução produz a máscara curinga 0.0.1.15.

Valor inicial	255.255.255.255
Subtrair a máscara de sub-rede	255.255.254.0
Máscara curinga resultante	0.0.1.255

1.1 Curinga para corresponder a um host

A máscara curinga é usada para corresponder a um endereço IPv4 de host específico e é necessário uma máscara que consiste em todos os zeros. A máscara curinga 0.0.0.0 estipula que cada bit corresponder exatamente, portanto, quando a ACE é processada, a máscara curinga permitirá apenas o endereço 192.168.1.1

	Decimal	Binário
Endereço IPv4	192.168.1.1	11000000.10101000.00000001.00000001
Máscara curinga	0.0.0.0	00000000.00000000.00000000.00000000
Endereço IPv4 permitido	192.168.1.1	11000000.10101000.00000001.00000001

1.2 Máscara curinga para corresponder a uma sub-rede IPv4

A ACL precisa de uma ACE que permita todos os hosts na rede 192.168.1.0/24. A máscara curinga 0.0.0.255 estipula que os três primeiros octetos devem corresponder exatamente, mas o quarto octeto não. A tabela lista em binário, o endereço IPv4 do host, a máscara curinga e os endereços IPv4 permitidos. Quando processado, a máscara curinga 0.0.0.255 permite todos os hosts na rede 192.168.1.0/24.

	Decimal	Binário
Endereço IPv4	192.168.1.1	11000000.1010100.00000001.00000001
Máscara curinga	0.0.0.255	00000000.00000000.00000000.11111111
Endereços IPv4 hosts permitidos	192.168.1.1. para 192.168.1.254	11000000.10101000.00000001.00000000 11000000.10101000.00000001.11111111

1.3 Máscara curinga para corresponder a um intervalo de endereços IPv4

A ACL precisa de uma ACE que permita todos os hosts nas redes 192.168.16.0/24, 192.168.17.0/24,..., 192.168.31.0/24. A máscara curinga 0.0.15.255 filtraria corretamente esse intervalo de endereços. A tabela lista em binário, o endereço IPv4 do host, a máscara curinga e os endereços IPv4 permitidos. Os bits de máscara curinga realçados identificam quais bits do endereço IPv4 devem corresponder. Quando processada, a máscara curinga 0.0.15.255 permite que todos os hosts nas redes 192.168.16.0/24 a 192.168.31.0/24.

	Decimal	**Binário**
Endereço IPv4	192.168.16.0	1100000000.10101000.00010000.00000000
Máscara curinga	0.0.15.255	00000000.00000000.00001111.11111111
Endereço IPv4 do host permitido	192.168.16.1 para 192.168.31.254	1100000000.10101000.00010000.00000000 11000000.10101000.00011111.11111111