CCNA 2 – Conceitos Básicos de Roteadores e Roteamento

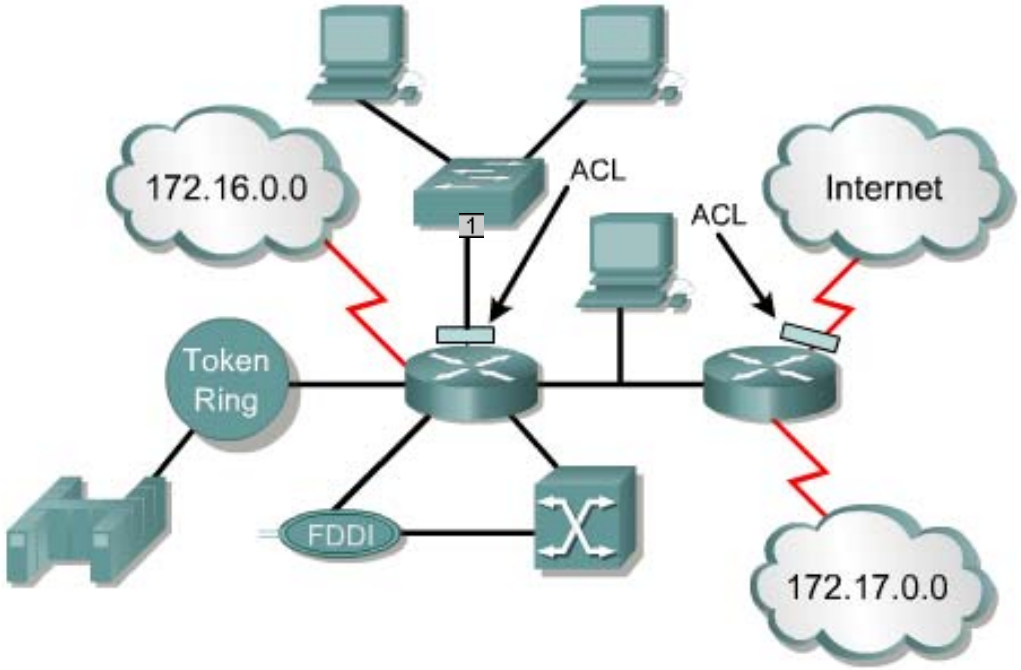
Capítulo 11 - Listas de Controle de Acesso (ACLs)

Objetivos do Capítulo

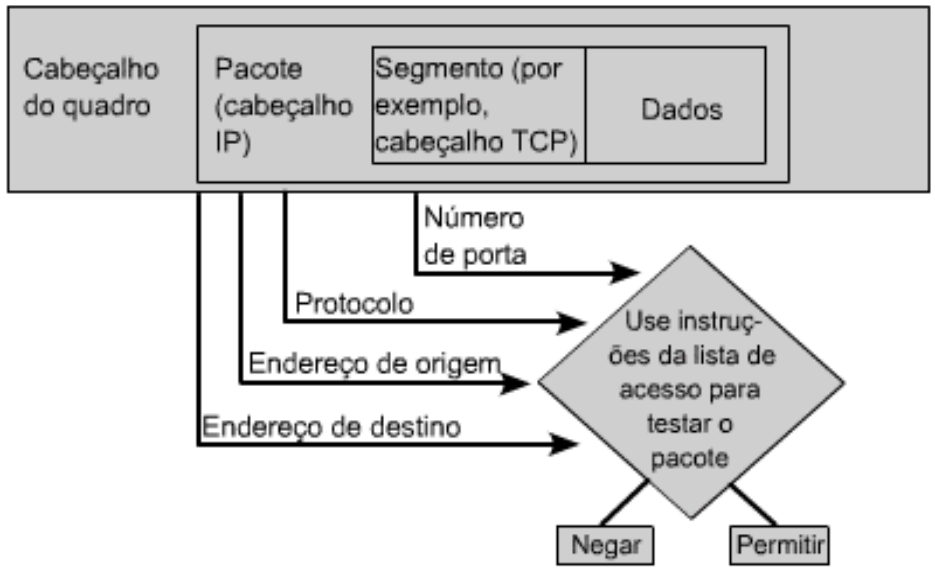
- Descrever as diferenças entre ACLs padrão e estendidas;
- Explicar as regras de posicionamento das ACLs;
- Criar e aplicar ACLs com nomes;
- Descrever a função dos firewalls;
- Usar as ACLs para restringir o acesso via terminal virtual.

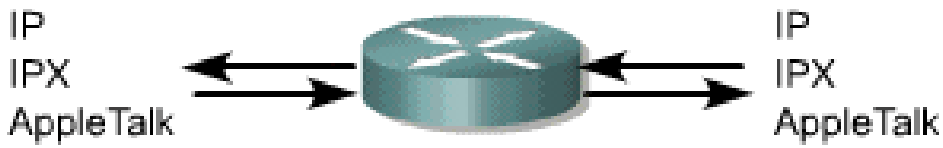
O que são ACLs

- **ACLs**: São listas de controle de acesso, aplicadas na interface do roteador, que filtram o tráfego.
- Essas listas contém informações sobre os tipos de pacotes que o roteador deve aceitar ou recusar.
- Elas gerenciam o tráfego aumentando a segurança da rede.



ACLs Cisco IOS





- Nas interfaces dos roteadores, os pacotes são filtrados com base nos endereços de origem e destino, protocolos e números de portas de camadas superiores.
- Nesse caso, seriam necessárias 12 **ACLs**. Uma por porta, uma por direção e uma por protocolo.

Funcionamento das ACLs

- Instruções da **ACL** operam em ordem seqüencial e lógica.
- O IOS testa o pacote com cada instrução, de cima para baixo.
- Quando uma correspondência é encontrada na lista, a ação de aceitação ou rejeição é realizada e nenhuma outra instrução da ACL é verificada.
- No final da ACL existe **deny any** oculto, não permitindo que nenhum pacote sem correspondência na ACL seja aceito.

Criando ACLs

- **ACLs** são criadas no modo de configuração global.
- Cada ACL deve receber um número exclusivo de acordo com o seu tipo.

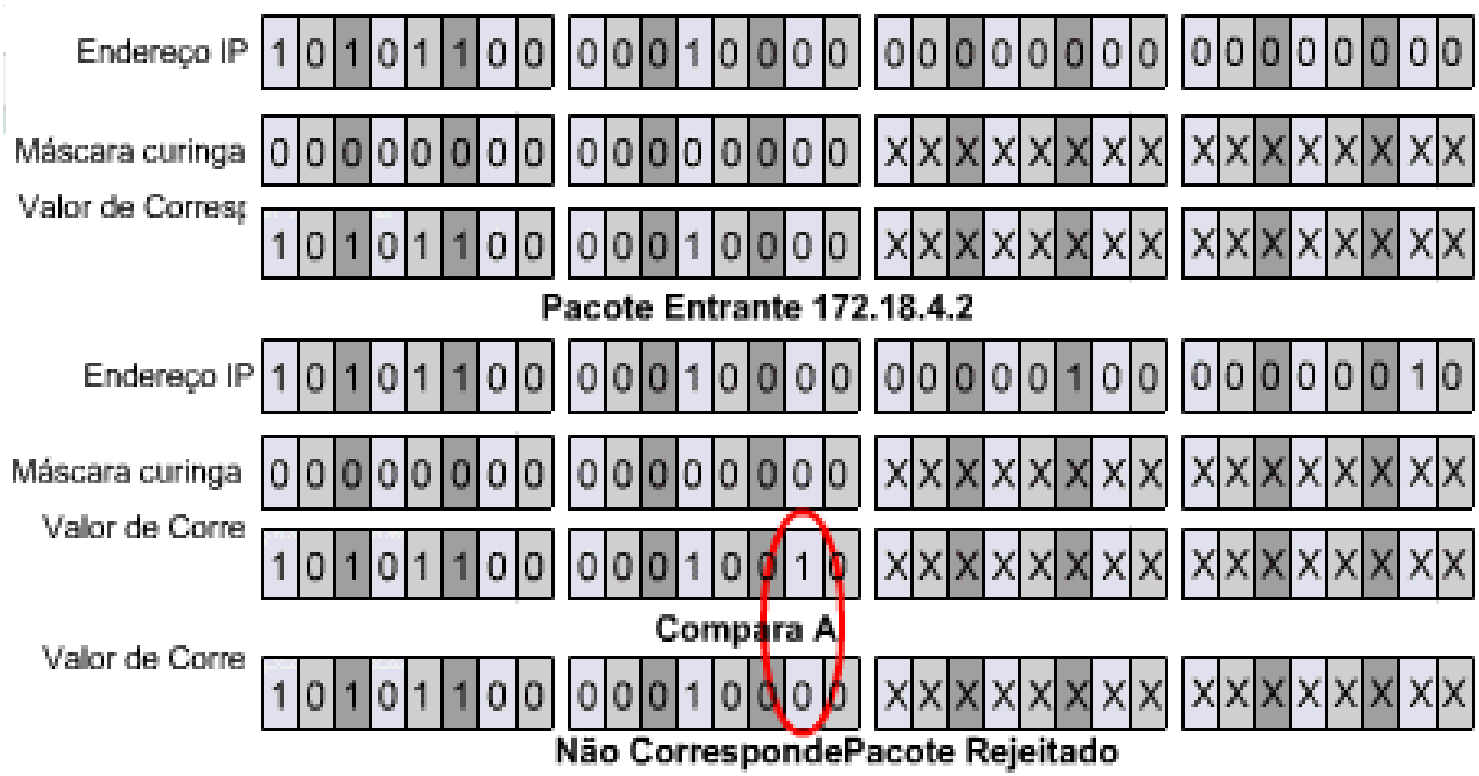
Protocolo	Intervalo
IP	1-99, 1300-1999
IP Estendido	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
IPX Estendido	900-999
Protocolo de Anúncio de Serviço IPX	1000-1099

- Utiliza-se o comando **access-list**, seguido dos parâmetros adequados: **permit**: permite, **deny**: nega, etc....
- Após criada a ACL, ela deve ser atribuida à interface do roteador.

Função da Máscara Curinga

- **Máscara curinga**: Composta de 32 bits divididos em 4 octetos. Ela é emparelhada com um endereço IP para identificar como lidar com os bits correspondentes.
- **Bit 0**: verifica o bit correspondente;
- **Bit 1**: ignora o bit correspondente.
- A palavra **any**, substitui o endereço IP por 0.0.0.0 e a máscara curinga por 255.255.255.255. E **host**, substitui a máscara por 0.0.0.0.
- Router (config) # access-list 1 permit 0.0.0.0 255.255.255.255
- Router (config) # access-list 1 permit any
- Router (config) # access-list 1 permit 172.30.16.29 0.0.0.0
- Router (config) # access-list 1 permit host 172.30.16.29

Aplicação da Máscara Curinga



- Neste caso os valores não correspondem e o pacote é rejeitado.

ACLs Padrão

```
access-list 2 deny   172.16.1.1
access-list 2 permit 172.16.1.0  0.0.0.255
access-list 2 deny   172.16.0.0  0.0.255.255
access-list 2 permit 172.0.0.0   0.255.255.255
```

- **ACLs Padrão** verificam o endereço de origem dos pacotes IP que são roteados.
- Router(config)#access-list *access-list-number* {deny | permit | remark} source [*source-wildcard* **]**
- A palavra-chave **remark**, pode ser utilizada para adicionar um comentário de até 100 caracteres.
- Removendo uma ACL padrão:
  - Router(config)#no access-list *access-list-number*
- Associar uma ACL padrão a uma interface:
  - Router(config-if)#ip access-group {access-list-number | access-list-name} {in | out}

ACLs Estendidas

- **ACLs Estendidas v**erificam os endereços de origem e destino dos pacotes e são capazes de verificar protocolos e números de portas.

Access-list *access-list-number* {deny| permit|remark} protocol source source-wildcard destination destination-wildcard {operator operand} {port port number or name}

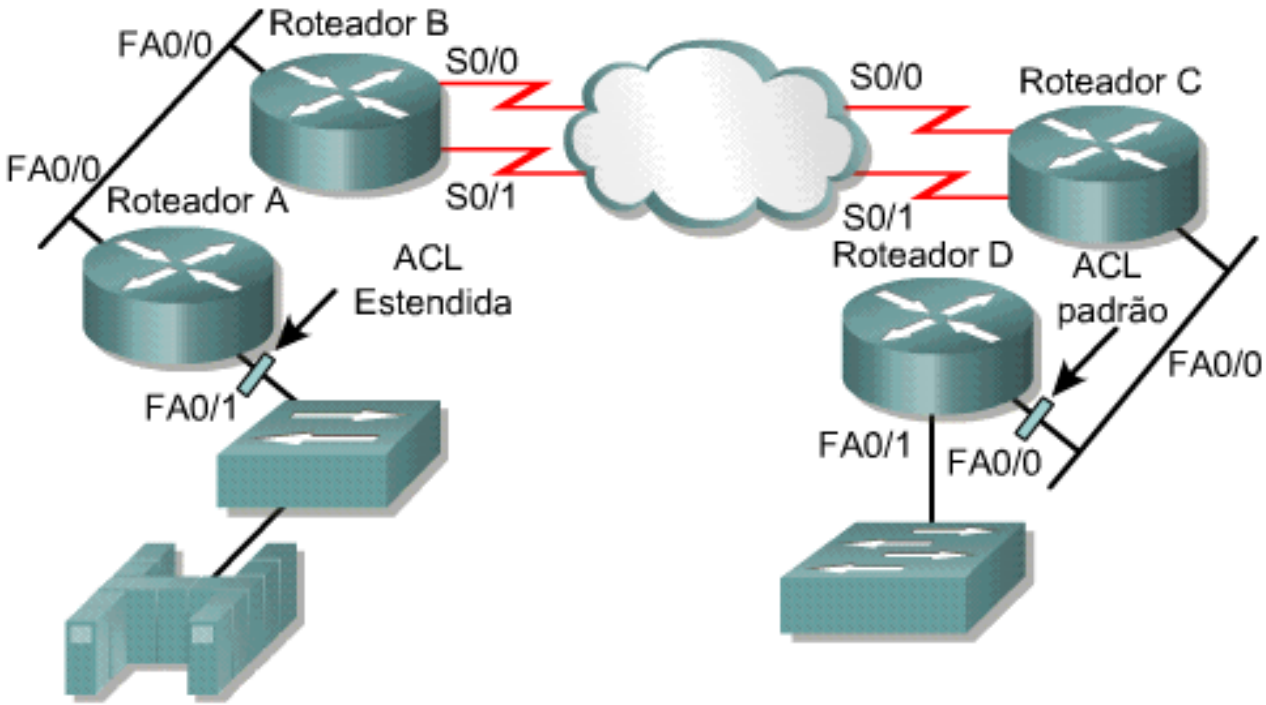
- Operações lógicas: **eq**: igual, **neq**: diferente, **gt**: maior do que, **lt**: menor do que.

```
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data
```

ACLs Nomeadas

- **ACLs Nomeadas** permitem atribuir nomes as ACLs Padrão e Estendidas.
- **Vantagens:**
  - Identificar intuitivamente uma ACL pelo nome;
  - O IOS não limita o número de ACLs nomeadas;
  - Podem ser modificadas sem ser excluídas, e em seguida, podem ser reconfiguradas.
- Router(config) # ip access-list {extended|standard} name
- Router(config)# ip access-list extended ainet
- Router(config-ext-nacl)# permit tcp host 1.1.1.1 host 5.5.5.5 eq smtp

Posicionando ACLs



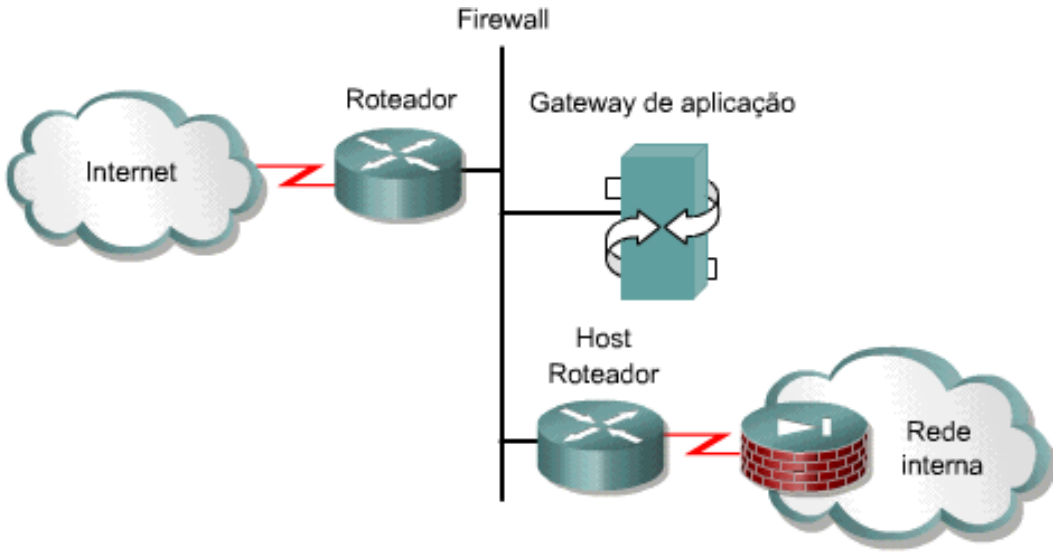
- Como regra geral: **ACLs Estendidas** devem ser colocadas próximo da origem do tráfego negado. As **ACLs Padrão** não especificam os endereços de destino, portanto devem ser posicionadas próximo ao destino.

Verificando as ACLs

- **show ip interface**: exibe as informações da interface IP e indica se há alguma ACL definida.
- **show access-lists**: exibe o conteúdo de todas as ACLs do roteador. Para ver uma lista específica, adicione o nome ou número da ACL.
- **show running-config**: revela as listas de acesso de um roteador e as informações de atribuição de interface.

Firewalls

- **Firewall**: Serve para proteger a rede interna de ataques externos.
- ACLs devem ser usadas em roteadores de firewall, posicionados entre a rede interna e a rede externa.
- Para maior segurança, ACLs devem ser configuradas em roteadores de borda, que são roteadores situados nos limites da rede.



Restringindo Acesso ao Terminal Virtual

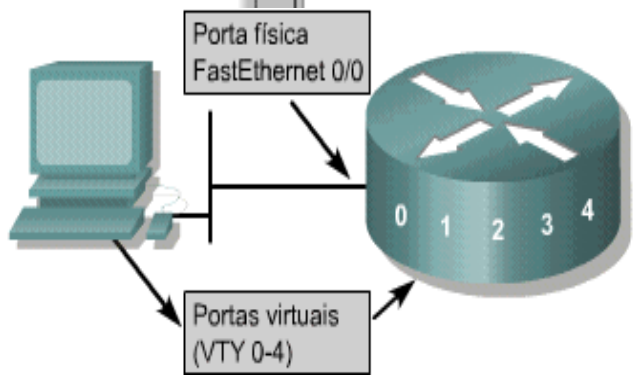
Cisco - Hyperterminal

```
Creating the standard list:

Rt1(config)#access-list 2 permit 172.16.1.0 0.0.0.255
Rt1(config)#access-list 2 permit 172.16.2.0 0.0.0.255
Rt1(config)#access-list 2 deny any

Applying the access list:

Rt1(config)#line vty 0 4
Rt1(config-line)#login
Rt1(config-line)#password secret
Rt1(config-line)#access-class 2 in
```



- Existem 5 portas virtuais no roteador numeradas de 0 a 4, chamadas de **linhas vty**.
- Pode-se permitir ou negar o acesso do usuário aos terminais virtuais, através de **lista de acesso vty**.
- A aplicação da ACL a uma linha de terminal, requer o comando **access-class** em vez do comando **access-group**.