Listas de Controlo de Acesso (ACLs)

- Permitem filtrar tráfego (efectuam testes aos pacotes de dados. Ex: negam ou permitem em função do endereço ou tipo de tráfego)
- Permitem restringir a utilização da rede para certos serviços e/ou dispositivos
- Cada interface do router, pode ter duas listas de acesso por protocolo, uma para entrada e outra para saída de tráfego
- Não se pode apagar uma linha da ACL (Apenas toda a lista)

REGRAS:

- É efectuado de uma forma sequencial: linha1, linha2, linha3, etc. (Colocar as linhas mais restritivas no topo da lista!)
- A procura é feita até que uma linha faça matching (as outras linhas serão ignoradas)
- Existe um **"deny" implícito no fim de todas as listas de acesso** (se não for efectuado *matching* até essa linha, então o pacote de dados será descartado).

Tipos de ACLs

- **Standard (1-99, 1300-1999)**
    - Usado para filtrar pacotes de uma dada origem (permite ou nega o tráfego a um conjunto de protocolos baseado no endereço de rede/subrede/máquina)
    - Devem ser colocadas o mais próximo possível do "destino"
- **Extended (100-199, 2000-2699)**
    - Usado para filtrar pacotes baseados na sua origem e destino
    - Filtra pelo tipo de protocolo (Ex: IP, TCP, UDP, etc.) e pelo número da porta
    - Também permite ou nega o tráfego com mais granularidade
    - Devem ser colocadas o mais próximo possível da "origem"

Nota: Também podem ser utilizados nomes para fazer referência às listas (em "substituição" dos números)

Comandos para manuseamento de ACLs

- **Standard**
  - Acrescentar uma linha a uma lista:

```
access-list número-lista {permit | deny} endereço_origem {máscara} {log}
```

  - Activar uma lista de acesso numa interface do router (para "entrada" ou "saída"):

```
ip access-group número-lista {in | out}
```

- **Extended**
  - Acrescentar uma linha a uma lista:

```
access-list número-lista {permit | deny}  protocolo  endereço_origem {máscara} endereço-destino {máscara} {log}
```

  - Activar uma lista de acesso numa interface do router (para "entrada" ou "saída"):

```
ip access-group número-lista {in | out}
```

- **Listas com nome**
  - `ip access-list standard|extended nome_lista` (depois colocar as linhas necessárias para a lista)
  - Activar uma lista de acesso numa interface do router (para "entrada" ou "saída"):

```
ip access-group nome-lista {in | out}
```

- **Remoção de uma lista de acesso:**
  - `no access-list número-lista`

- `no ip access-group número-lista in|out` (remove uma ACL de uma interface)

- **Comandos para consulta de listas:**
  - `show ip interfaces`
  - `show access-lists [número]`
  - `show ip access-list [número]`

Máscaras nas ACLs

São utilizadas para identificar os intervalos de endereços IP. Funcionam de forma contrária às máscaras de subrede (Cada 0 deve fazer matching, cada 1 deve ser ignorado).

Para calcular a máscara da lista faz-se o seguinte:

- Identificar o valor decimal de cada byte da máscara de subrede
- Subtrair a 255 o valor encontrado

Exemplo: Obter a máscara utilizada numa lista para a máscara de subrede 255.255.248.0

Primeiro byte: 255-255=0

Segundo byte: 255-255=0

Terceiro byte: 255-248=7

Quarto byte: 255-0=255

A máscara a utilizar na lista será: **0.0.7.255**

Nota: ***Atente aos valores obtidos:***

Máscara da subrede (255.255.248.0): **11111111.11111111.11111000.00000000**

Máscara da lista (0.0.7.255): **00000000.00000000.00000111.11111111**

Exemplos de Listas *Standard*

Exemplo 1: Cria uma lista de acesso que permite todo o tráfego excepto da rede 10.0.0.0. A lista é aplicada à interface Ethernet0.

```
Router(config)#access-list 1 deny 10.0.0.0 0.255.255.255
Router(config)#access-list 1 permit any
Router(config)#interface Ethernet0
Router(config-if)#ip access-group 1 out
```

Exemplo 2: Rejeita todo o tráfego excepto da máquina 10.12.12.14 e aplica a lista à interface Serial0

```
Router(config)#access-list 2 permit 10.12.12.16
Router(config)#interface Serial0
Router(config-if)#ip access-group 2 in
```

Exemplo 3: Restringir o acesso via telnet ao router

Numa ligação via telnet ao router, este associa a ligação com uma linha para terminal virtual (VTY). Por defeito suporta 5 telnets (0-4).

```
Router(config)# access-list 99 permit 192.168.1.0 0.0.0.255
Router(config)# line vty 0 4
Router(config-line)# access-class 99 in
```

Neste exemplo, apenas é permitido tráfego da rede 192.168.1.0/24

Exemplos de Listas *Extended*

Exemplo 1: Não encaminha tráfego TCP de qualquer host da rede 10.0.0.0 para a rede 11.12.0.0. Aplica a lista à interface Serial0

```
Router(config)#access-list 111 deny tcp 10.0.0.0 0.255.255.255
11.12.0.0 0.0.255.255
```

```
Router(config)#access-list 111 permit ip any any
Router(config)#int Serial0
Router(config-if)#ip access-group 111 in
```

Exemplo 2: Esta lista impede todos os telnets do host 192.168.1.25

```
Router(config)# access-list 102 deny tcp host 192.168.1.25 any eq 23
Router(config)# access-list 102 permit tcp any any
```

Exemplo 3: Qual o objective deste exemplo?

```
Router(config)# access-list 101 permit tcp
                  host 199.199.199.1
                  host 200.200.200.1 eq dns
Router(config)# access-list 101 permit udp
                  any host 200.200.200.1 eq dns
Router(config)# access-list 101 permit tcp
                  any host 200.200.200.2 eq www
Router(config)# access-list 101 permit icmp
                  any 200.200.200.0 0.0.0.255
Router(config)# access-list 101 permit tcp
                  any host 200.200.200.3 eq smtp
Router(config)# access-list 101 permit udp
                  host 201.201.201.2
                  host 201.201.201.1 eq rip
Router(config)# interface Ethernet0
Router(config-if)# ip address 201.201.201.1 255.255.255.0
Router(config-if)# ip access-group 101 in
```

Exemplo de ACL com nome

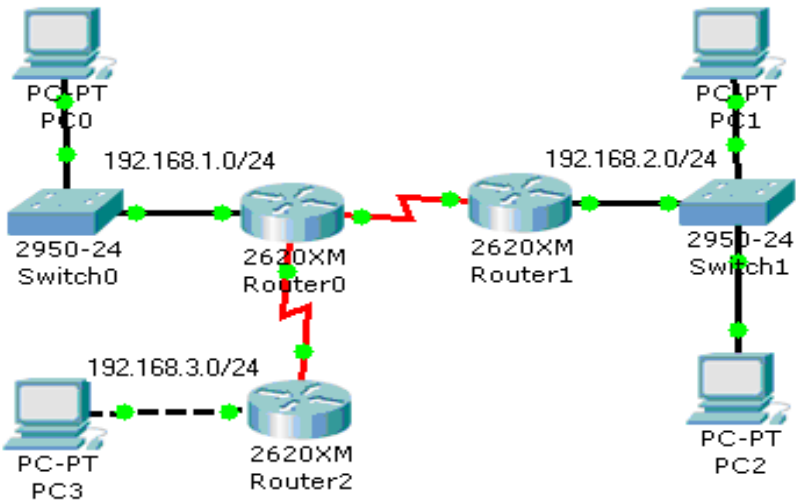
```
Router(config)# ip access-list extended fica_de_fora
Router(config-ext-acl)# permit tcp
```

```
                              any 172.16.0.0 0.0.255.255
                              established log
Router(config-ext-acl)# permit udp
                              any host 172.16.1.1 eq dns log
Router(config-ext-acl)# permit tcp
                              172.17.0.0 0.0.255.255
                              host 176.16.1.2 eq telnet log
Router(config-ext-acl)# permit icmp
                              any 176.16.0.0 0.0.255.255
                              echo-reply log
Router(config-ext-acl)# deny ip any any log

Router(config)# interface Ethernet0
Router(config-if)# ip access-group fica_de_fora
```

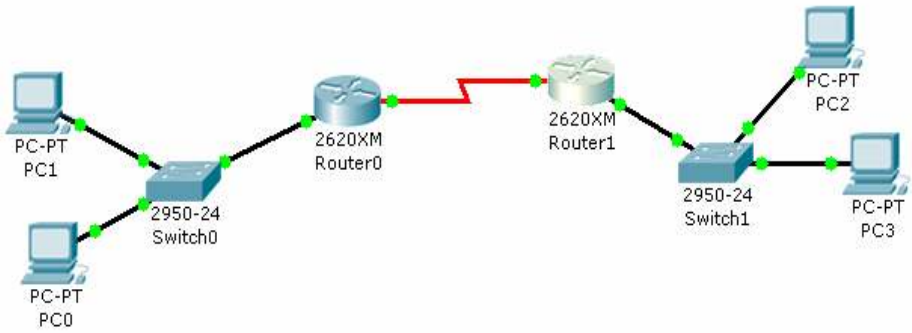
Exercícios

1- Considere a seguinte figura:



a) Verifique as configurações e teste a conectividade entre todos os pcs.
b) Através da utilização de ACLs, configure a rede de modo a que o PC1 não consiga aceder a todas as máquinas da rede 192.168.1.0/24. Aplique a lista construída à interface mais adequada.
c) Teste a conectividade de modo a confirmar a configuração da alínea anterior.

2- Considere a seguinte figura:



a) Configure os routers:
Clock rate 56000 em ambos os routers

Router0: fa0/0 172.16.10.1/24
Router0: s0/0 192.168.4.5/30

Router1: fa0/0 172.30.10.1/24
Router1: s0/0 192.168.4.6/30

b) Configure os PCs (IP e *default gateway*):

PC0 172.16.10.5/24
PC1 172.16.10.6/24

PC2 172.30.10.20/24
PC3 172.30.10.21/24

c) Configure RIP V2 de modo a que exista conectividade entre todas as redes. Teste a conectividade de/para todas as máquinas.

d) Utilizando ACLs, faça com que o PC2 não consiga efectuar *TELNET* para a interface série do Router0, mas permita que o PC2 o faça para a interface fa0/0 do mesmo router. Aplique a ACL no local mais adequado. Teste a configuração.

3- Considere a figura do exercício 2.

a) Remova a ACL criada no exercício anterior da interface onde a aplicou.
b) Remova a ACL do exercício anterior do router onde a aplicou
c) Crie a ACL com nome **Limita_Acesso**. Essa ACL deve:

- Negar pings da rede 172.30.10.0/24 para a interface Fa0/0 do Router0 e para a rede 172.16.10.0/24;
- Permitir *TELNET* da rede 172.30.10.0/24 para a interface Fa0/0 do Router0, mas negue todos os outros *TELNETS* com origem nessa rede
- Permita o "resto" do tráfego

.Aplique a ACL no local mais adequado. Teste a configuração.

4- Faça o exercício:

CCNA2\ Skillbuilder_NACLs\ CCNA2 Skills Activity lab handout_NACL.doc

5- Considere a seguinte figura da página seguinte.

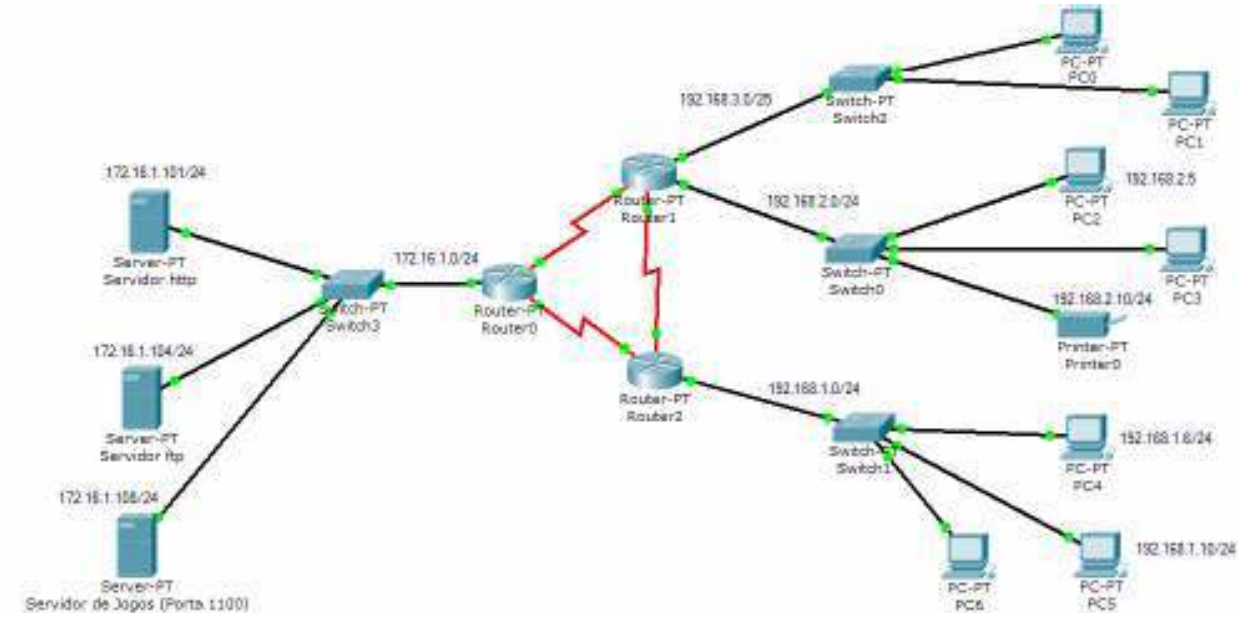
a) Configure todo o sistema de modo a que exista conectividade entre todas as redes. Utilize RIP V2.

b) Configure o sistema de modo a satisfazer os seguintes requisitos:

- A subrede 172.16.1.0/24 não aceita "pings" do exterior
- A subrede 172.16.1.0/24 não aceita tráfego da subrede 192.168.3.0/25
- Apenas as máquinas 192.168.2.5 e 192.168.1.6 acedem ao servidor de jogos
- A rede 192.168.2.0 acede ao servidor http
- Na rede 192.168.1.0 apenas a máquina 192.168.1.6 não acede ao servidor http

- Apenas a rede 192.168.1.0 acede ao servidor ftp
- A impressora apenas pode ser utilizada por máquinas que se encontrem em

192.168.2.0/24 e 192.168.3.0/25



Referências:

IBM Redbook : TCP/IP Tutorial and Technical Overview

http://www.redbooks.ibm.com/abstracts/gg243376.html

Internetworking Technology Handbook

http://www.cisco.com/en/US/tech/tk1330/tsd_technology_support_technical_reference_book09186a00807594e5.html

Access Control Lists and IP Fragments

http://www.cisco.com/warp/public/105/acl_wp.html