Redes de Dados II

3º Ano

Licenciatura em Engenharia Informática

acunha@utad.pt

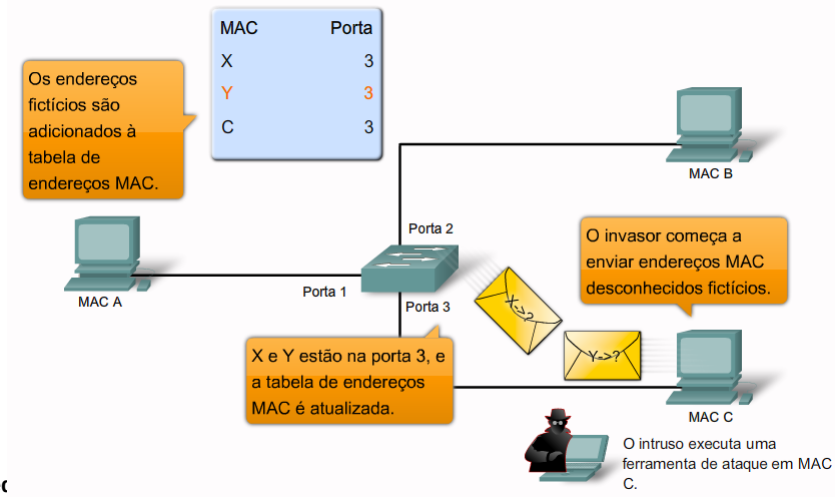
1

Ataques a Switchs

2

Ataques a Switchs

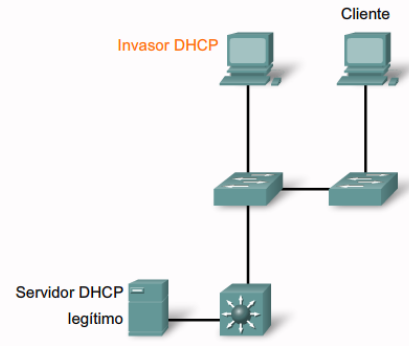
- Esgotamento da Tabela de MAC



Ataques a Switchs

Ataque ao DHCP (DHCP Snooping)

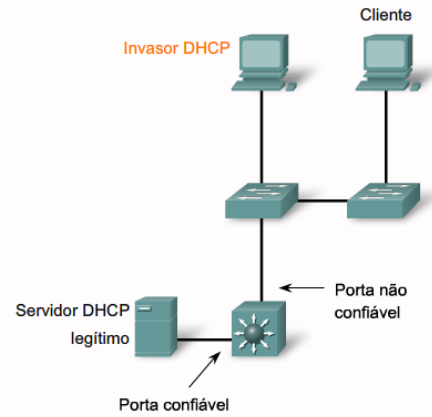
1) Um invasor ativa um servidor DHCP em um segmento de rede.
2) O cliente difunde uma solicitação para obter informações de configuração DHCP.
3) O servidor DHCP invasor responde antes que o servidor DHCP legítimo possa responder, atribuindo informações de configuração IP definidas pelo invasor.
4) Os pacotes de host são redirecionados para o endereço do invasor à medida que ele emula um gateway padrão para o endereço DHCP fornecido para o cliente.



Ataques a Switchs

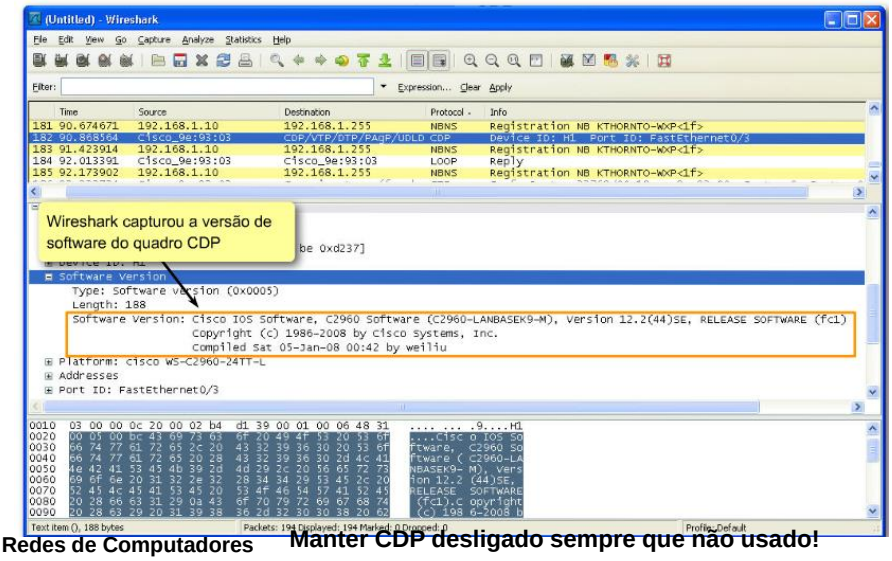
Defesa ao Ataque ao DHCP

- A opção DHCP Snooping permite a configuração de portas como confiáveis ou não confiáveis.
  - As portas confiáveis podem enviar solicitações DHCP e confirmações.
  - As portas não confiáveis só podem encaminhar solicitações DHCP.
- A opção DHCP Snooping permite ao switch criar uma tabela de associação DHCP que mapeia um endereço MAC de cliente, endereço IP, VLAN e ID de porta.
- Use o comando **`ip dhcp snooping`**.



Ataques a Switchs

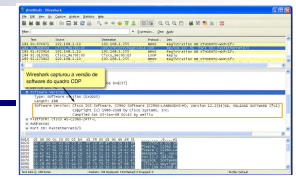
Ataque ao CDP CDP spoofing



 Manter CDP desligado sempre que não usado!

Ataques a Switchs

Ataque ao CDP CDP spoofing



Tipos de ataques CDP :

- Spoofing CDP:
  Os atacantes podem fazer-se passar por um dispositivo Cisco confiável, enviando pacotes CDP forjados. Isto pode ser usado para obter acesso não autorizado à rede ou lançar mais ataques.
- Flood CDP:
  Os atacantes podem inundar a rede com um grande número de pacotes CDP, sobrecarregando a infraestrutura da rede e causando negação de serviço.
- Recolha de Informações CDP:
  Os atacantes podem usar o CDP para recolher informações sobre a rede, como tipos de dispositivos, endereços IP e versões de plataforma. Estas informações podem ser usadas para fins de reconhecimento em preparação para futuros ataques.

Para se proteger :

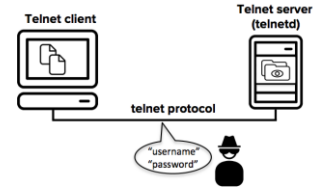
- Desativar o CDP em interfaces de rede não essenciais.
- Implementar listas de controlo de acesso (ACLs) para filtrar pacotes CDP.
- Ativar mecanismos de autenticação, como autenticação MD5, para verificar a autenticidade dos pacotes CDP.
- Atualizar regularmente os dispositivos Cisco com o firmware mais recente para corrigir quaisquer vulnerabilidades conhecidas.

Manter CDP desligado sempre que não usado!

Ataques a Switchs

Ataque ao Telent

Tipos de ataques Telnet:
-Ataques de força bruta de senha
-Ataques DoS



Protegendo-se contra um ataque de força bruta de senha:
-altere as suas senhas sempre
-use senhas fortes
-limite quem pode se comunicar usando linhas vty

Protegendo-se contra um ataque DoS:
-Atualize para a versão mais nova do software Cisco IOS

Ferramentas de segurança

As ferramentas de segurança da rede desempenham estas funções:

-As auditorias de segurança da rede ajudam a

- Revelar que tipo de informação um invasor pode obter simplesmente monitorando o tráfego da rede.
- Determinar a quantidade ideal de endereços MAC falsificados (spoofed) a serem removidos.
- Determinar o período de expiração da tabela de endereços MAC.

Ferramentas de segurança

As ferramentas de segurança da rede desempenham estas funções:

-As auditorias de segurança da rede ajudam a

- Revelar que tipo de informação um invasor pode obter simplesmente monitorando o tráfego da rede.
- Determinar a quantidade ideal de endereços MAC falsificados (spoofed) a serem removidos.
- Determinar o período de expiração da tabela de endereços MAC.

-Testes de penetração da rede ajudam a

- Identificar deficiências na configuração de seus dispositivos de rede.
- Iniciar vários ataques para testar a sua rede.
- Cuidado: Planeje testes de penetração para evitar impactos sobre o desempenho da rede.

Recursos de segurança

Entre os recursos comuns de uma ferramenta de segurança da rede moderna estão:

-Identificação de serviço
-Suporte de serviços SSL
-Testes destrutivos e não destrutivos
-Banco de dados de vulnerabilidades

Recursos de segurança

É possível usar ferramentas de segurança de rede para:

-Capturar mensagens de bate-papo
-Capturar arquivos do tráfego NFS
-Capturar solicitações HTTP no Formato de Log Comum
-Capturar mensagens de email no formato Berkeley mbox
-Capturar senhas
-Exibir URLs capturados em tempo real no Netscape ou outro navegador
-Inundar uma rede local comutada com endereços MAC aleatórios
-Forjar respostas para consultas de endereço e apontador DNS
-Interceptar pacotes em uma rede local comutada

Configurando segurança Porta

- Implemente segurança em todas as portas do switch
  - Especifique um grupo de end. MAC válidos permitidos em cada porta
  - Permita apenas um endereço MAC aceder à porta
  - Especifique que a porta será desativada automaticamente se forem detetadas endereços MAC não autorizados.

Tipos de endereço MAC seguro

- Endereços MAC seguros **estáticos**
  - os MAC são configurados manualmente
  - os MAC configurados são armazenados na tabela de endereços
- Endereços MAC seguros **dinâmicos**
  - os MAC são aprendidos dinamicamente e armazenados apenas na tabela de endereços.
  - os MAC assim configurados são removidos quando o switch reinicia.
- Endereços MAC seguros **fixos**
  - é possível configurar uma porta para saber endereços MAC dinamicamente e
  - salvar esses endereços MAC na configuração de execução.

Modos de violação da segurança

- **É uma violação** de segurança quando :
  - O número máximo de endereços MAC seguros foi adicionado à tabela de endereços e uma estação cujo endereço MAC não está na tabela de endereços tenta aceder à interface.
  - Um endereço aprendido ou configurado em uma interface segura
    - é visto em outra interface segura na mesma VLAN.

- Modos de violacão

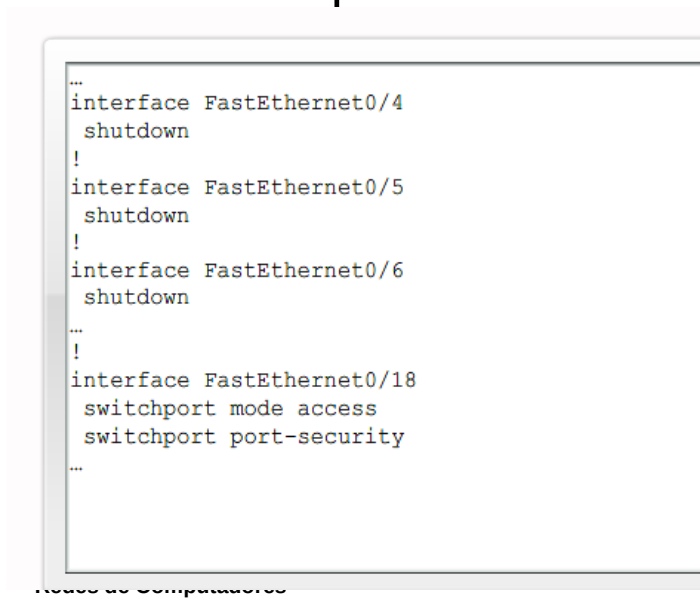
Modo de violação	Encaminha tráfego	Envia mensagem Syslog	Exibe mensagem de erro	Aumenta o contador de violação	Desativa a porta
Proteger (protect)	Não	Não	Não	Não	Não
Restringir (restrict)	Não	Sim	Não	Sim	Não
Desabilitar (shutdown)	Não	Sim	Não	Sim	Sim

Verificar segurança porta


```
switch#show port-security interface fastEthernet 0/18
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

```
switch#show port-security address
        Secure Mac Address Table
------------------------------------------------------------------------
Vlan  Mac Address       Type              Ports     Remaining Age (mins)
99    0050.BAA6.06CE    SecureConfigured  Fa0/18    -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8320
```

Desabilitar portas não usadas




```
…
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
…
!
interface FastEthernet0/18
 switchport mode access
 switchport port-security
…
```

17

Switchs

Comandos de IOS

18

Configuração básica switch

Segurança

- Configuração senha modo EXEC

Sintaxe de comando da CLI do Cisco IOS	
Alterne do modo EXEC privilegiado para o modo de configuração global.	`S1#configure terminal`
Configura o **`enable password`** para entrar no modo EXEC privilegiado.	`S1(config)#enable password senha`
Configura a senha **`enable secret`** para entrar no modo EXEC privilegiado.	`S1(config)#enable secret senha`
Saia do modo de configuração de linha e volte ao modo EXEC privilegiado.	`S1(config)#end`

Configuração básica switch

Segurança

- Configuração senha Criptografadas

```
…
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 no login
line vty 5 15
 password cisco
 no login
!
end
S1#config terminal
S1(config)#service password-encryption
S1(config)#end
S1#Show running-config
…
control-plane
!
line con 0
 password 7 030752180500
 login
line vty 0 4
 password 7 1511021F0725
 no login
line vty 5 15
 password 7 1511021F0725
 no login
!
end
```

Banner de login / Banner MOTD

Sintaxe de comando da CLI do Cisco IOS	
Alterne do modo EXEC privilegiado para o modo de configuração global.	`S1#configure terminal`
Configure um banner de login.	`S1(config)#banner login "Authorized Personnel Only!"`

Sintaxe de comando da CLI do Cisco IOS	
Alterne do modo EXEC privilegiado para o modo de configuração global.	`S1#configure terminal`
Configure um banner de login MOTD.	`S1(config)#banner motd "Device maintenance will be occurring on Friday!"`

Telnet vs SSH

Telnet

-Método de acesso mais comum

-Envia fluxos de mensagens de texto sem formatação

-Não é seguro

SSH

-Ele deve ser o método de acesso comum

-Envia o fluxo de mensagem criptografado

-É seguro

Telent / SSH

- Telnet:

```
S1(config)#line vty 0 15
S1(config-line)#transport input telnet
```

- SSH:

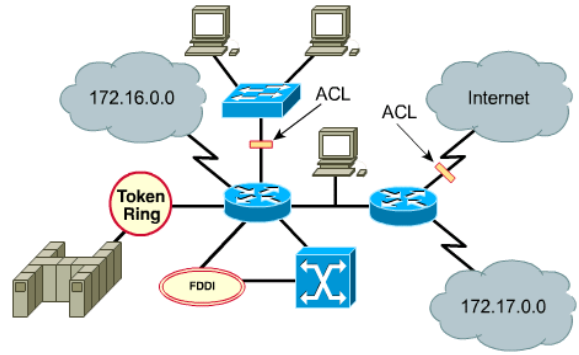
```
(config)#ip domain-name mydomain.com
(config)#crypto key generate rsa
(config)#ip ssh version 2
(config)#line vty 0 15
(config-line)#transport input SSH
```


Listas de Controlo de Acesso (ACLs)

Redes de computadores
Acunha@utad.pt

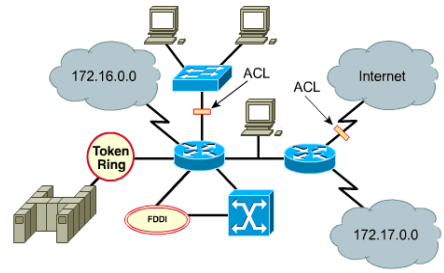
Definição

- Precisamos de ACLs para
  - Negar certos acessos, permitindo outros
  - São mais flexibilidade comparado com a verificação de Palavras passe
- Lista de controlo de acesso – ACL
  - É coleção sequencial de frases do tipo “permita” ou “negue”



Definição

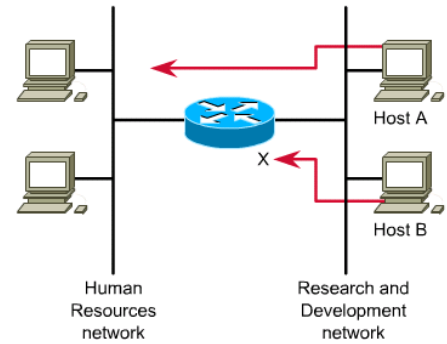
- Há 2 tipos ACLs
  - Standard
  - Estendidas



- Características gerais das ACL
  - Aplicam-se às portas dos routers
  - O tráfego é confrontado com as condições ACL
  - Baseadas no protocolo: IP, IPX, ...
  - Condições: origem, destino, porto, ...
    - Uma ACL para cada protocolo

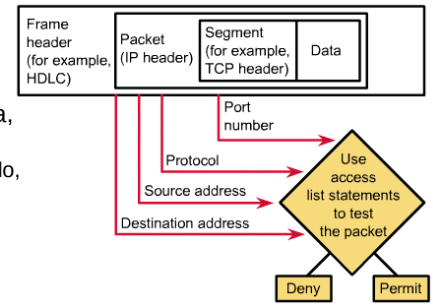
Motivação

- Limitar o tráfego e aumentar o desempenho da rede
  - Permite, p. ex designar pacotes a serem processados, com base no protocolo.
- Controlo do fluxo de tráfego
  - Pode restringir-se por exemplo atualizações
- Nível de segurança
  - Ex: permitir uns aceder a uma parte da rede e outros não
- Definir tipo de tráfego possível
  - Ex: permitir encaminhar *email*, bloqueando *telnet*



Como funciona uma ACL (1)

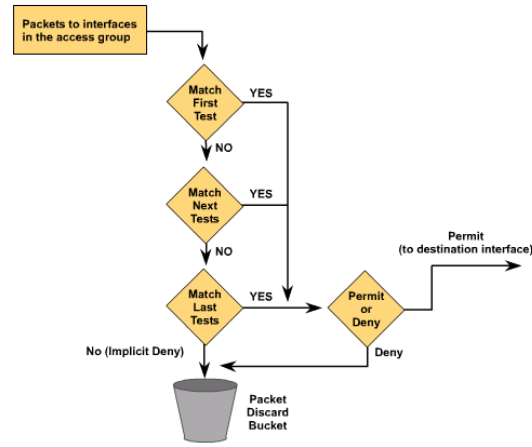
- A verificação das regras das ACLS são feitos por ordem
  - **Por isso a sua ordem é importante**
- Logo que uma condição seja verdadeira, **não se testa mais nenhuma**
  - Ex: se uma condição permite passar tudo, não se testa mais nada !!!
- Alteração de ACLs
  - Apagar toda a ACL e recriá-la de novo!
  - usar editor de texto antes de configurar
- Para alguns protocolos,
  - pode criar-se uma ACL para filtrar tráfego de entrada e
  - uma ACL para filtrar o de saída



Como funciona uma ACL (2)

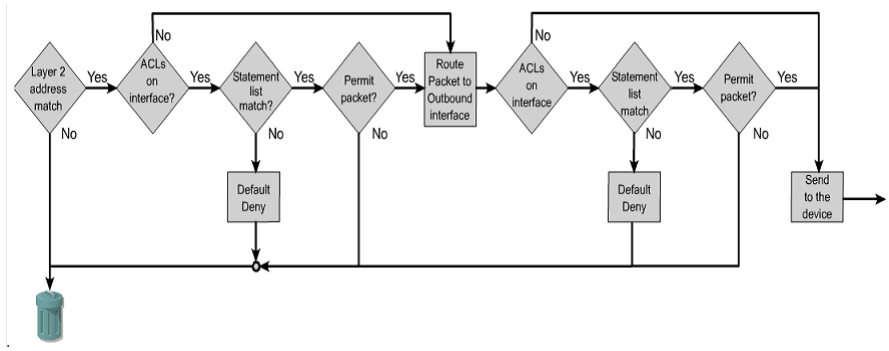
- Se nenhuma condição é verdadeira?
  - Existe implícita (como se estivesse escondida) a seguinte condição:
  - ***deny any***

- **Conclusão**:
  - Se há uma ACL
    - Para que o pacote passe, tem de haver uma condição explícita para tal!



Como funciona uma ACL (3)

Como fica agora a sequência passo-a-passo num router com ACL?



Configuração de uma ACL (1)

Step 1	Define the ACL by using the following command: `Router(config)# access-list access-list-number {permit | deny} {test-conditions}` A global statement identifies the ACL. Specifically, the 1-99 range is reserved for standard IP. This number refers to the type of ACL. In Cisco IOS Release 11.2 or newer, ACLs can also use an ACL name, such as education_group, rather than a number. The **permit** or **deny** term in the global ACL statement indicates how packets that meet the test conditions are handled by Cisco IOS software. **permit** usually means the packet will be allowed to use one or more interfaces that you will specify later.The final term or terms specifies the test conditions used by the ACL statement.

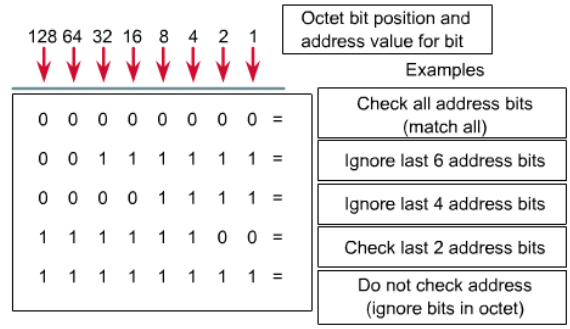
- Se nº da ACL entre 0 e 99: ACL IP ***standard***
- ACL entre 100 e 199: ACL IP ***extended***
- É obrigatório especificar os protocolos IP permitidos. Restantes devem ser negados

Configuração de uma ACL (2)

Step 2	Next, you need to apply ACLs to an interface by using the **access-group** command, as in this example: `Router(config-if)# {protocol} access-group access-list-number` All the ACL statements identified by *access-list-number* are associated with one or more interfaces. Any packets that pass the ACL test conditions can be permitted to use any interface in the access group of interfaces.

O uso de máscaras de bits – *Wildcards*

- um **0** <u>significa</u>
  - verificar bit correspondente
- um **1** <u>significa</u>
  - ignorar o bit correspondente
- Ver diferenças com a conhecida *Subnet Mask*



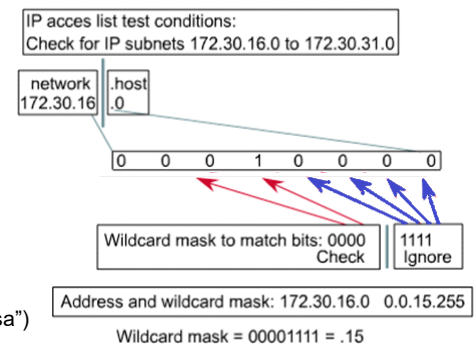
O uso de máscaras de bits – *Wildcards*

<u>Exemplo:</u> Verificar a subrede 172.30.16.0 até 172.30.31.0

- Os bits variáveis que não interessam, têm 1 na máscara

<u>Ou seja</u>:

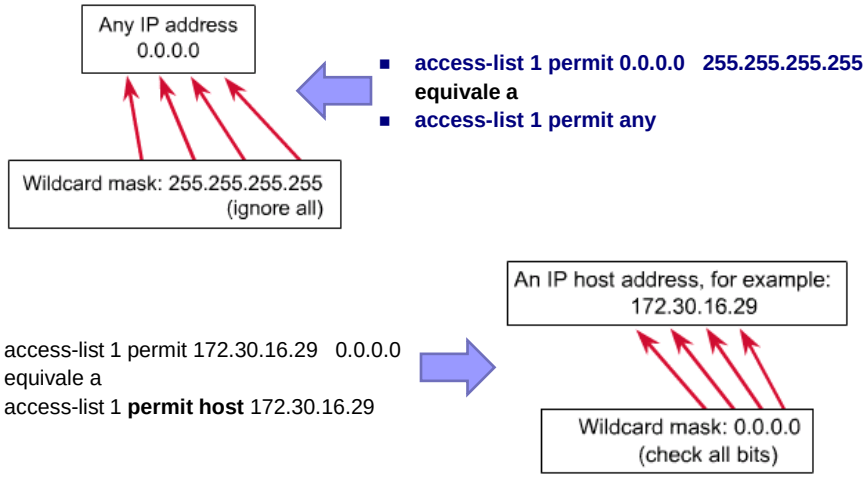
- Os bits que permanecem fixos, têm 0 na máscara
- Os bits que vão variando, têm 1 na máscara
  ("podem variar, que não interessa")



<u>Para permitir passar tráfego vinda destes endereços:</u>

→ **Router(config)#access-list 1 permit 172.30.16.0 0.0.15.255**

Wildcards específicos e abreviados

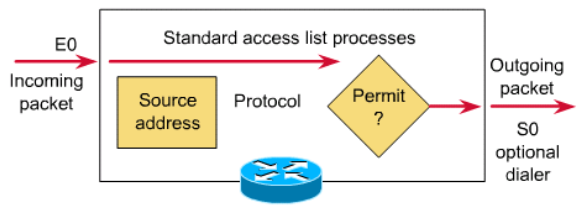


- **access-list 1 permit 0.0.0.0 255.255.255.255**
  equivale a
- **access-list 1 permit any**

- access-list 1 permit 172.30.16.29 0.0.0.0
  equivale a
- access-list 1 **permit host** 172.30.16.29

ACLs *Standard*

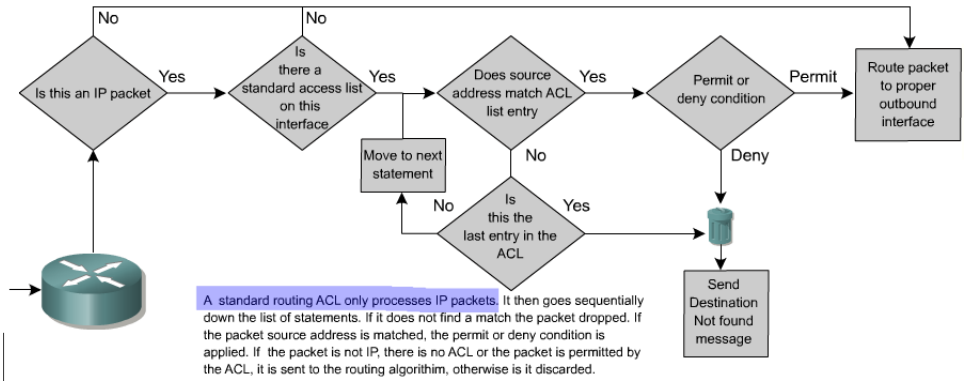
- Verificam os endereços (rede, sub-rede, *host*) de origem dos pacotes que podem ser encaminhados
- Como resultado permite ou nega (todo um *protocol suite*)



Sintaxe duma ACL *standard*:

→ **Router(config)#access-list access-list-number {deny | permit} source [source-wildcard] [log]**

ACLs *Standard*



A standard routing ACL only processes IP packets. It then goes sequentially down the list of statements. If it does not find a match the packet dropped. If the packet source address is matched, the permit or deny condition is applied. If the packet is not IP, there is no ACL or the packet is permitted by the ACL, it is sent to the routing algorithim, otherwise is it discarded.

```
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
```

- Access list number range of 1-99
- Filter only on source IP address
- Wildcard masks
- Applied to port closest to destination

Sintaxe duma ACL *Standard*

→ **Router(config)#access-list access-list-number {deny | permit} source [source-wildcard] [log]**

Parameter	Description
access-list-number	Number of an ACL. This is a decimal number from 1 to 99 (for a standard IP ACL).
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
source	Number of the network or host from which the packet is being sent. There are two ways to specify the *source*: ·Use a 32-bit quantity in four-part, dotted- decimal format. ·Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.55.
source-wildcard	(Optional) Wildcard bits to be applied to the source. There are two ways to specify the *source-wildcard*: ·Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. ·Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.

Sintaxe duma ACL *Standard* *(2)*

Parameter	Description
`log`	The message includes the ACL number, whether the packet was permitted or denied, the source address, and the number of packets. The message is generated for the first packet that matches, and then at five-minute intervals, including the number of packets permitted or denied in the prior five-minute interval.
`in | out`	Selects whether the ACL is applied to the incoming or outgoing interface. If `in` or `out` is not specified, `out` is the default.

Alguns Comandos

Mostrar os conteúdos de todas as ACLs

→ **Router(config)#show access-lists**

Mostrar os conteúdos de uma dada ACL

→ **Router(config)#show access-lists {nome | número}**

A seguinte ACL permite acesso a hosts das 3 redes especificadas

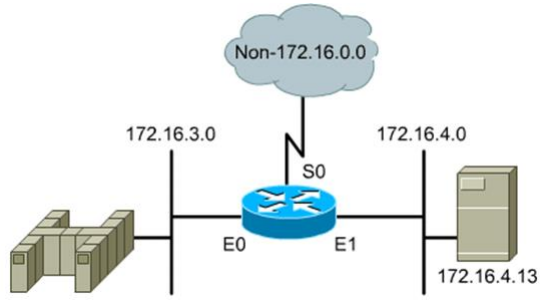
- **access-list 1 permit 192.5.34.0 0.0.0.255**
  access-list 1 permit 128.88.0.0 0.0.255.255
  access-list 1 permit 36.0.0.0 0.255.255.255
  !(Nota: Todas os restantes acessos, negados)
- **access-list 1 permit 36.48.0.3 0.0.0.0**

  é equivalente a
- **access-list 1 permit host 36.48.0.3**

Agrupar a ACL a um interface:

- **Router(config-if)#ip access-group access-list-number {in | out}**

Exemplo 1: Permissão da rede 172.16.0.0/16

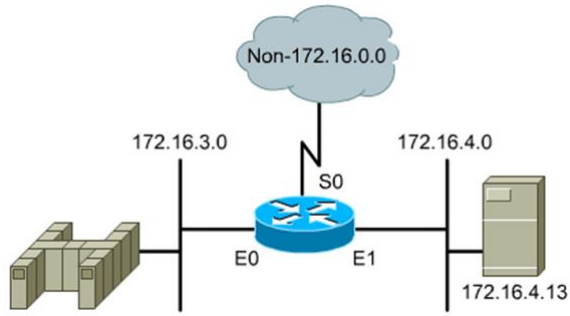


Command Output

```
access-list 1 permit 172.16.0.0  0.0.255.255
(implicit deny any - not visible in the list)
(access-list 1 deny 0.0.0.0  255.255.255.255)

interface ethernet 0
ip access-group 1 out
interface ethernet 1
ip access-group 1 out
```

Field	Description
1	ACL number; indicates that this is a simple list.
permit	Traffic that matches selected parameters will be forwarded.
172.16.0.0	IP address that will be used with the wildcard mask to identify the source network.
0.0.255.255	Wildcard mask; zeros indicate positions that must match and ones indicate "don't care" positions.

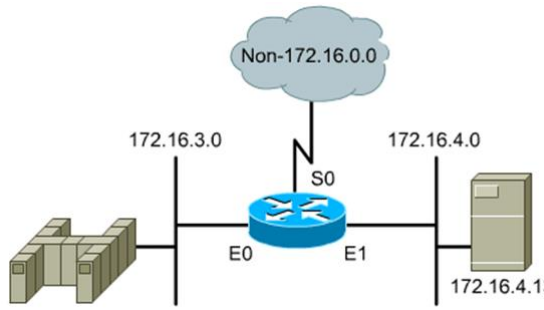
Exemplo 2 Negação do *host 172.16.4.13*



Command Output

```
access-list 1 deny 172.16.4.13  0.0.0.0
access-list 1 permit 0.0.0.0  255.255.255.255
(implicit deny any)
(access-list 1 deny 0.0.0.0  255.255.255.255)

interface ethernet 0
ip access-group 1 out
```

Exemplo 3 Negação sub-rede 172.16.4.0/24



Command Output

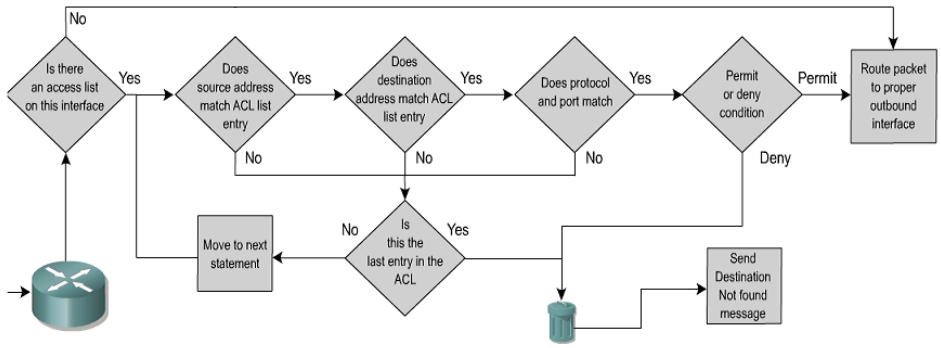
```
access-list 1 deny 172.16.4.0  0.0.0.255
access-list 1 permit any
(implicit deny any)
access-list 1 deny any

interface ethernet 0
ip access-group 1 out
```


ACLs Estendidas (*Extended* ACLs)

- **Permitem maior controlo que as *standard***
- **Permitem negar ou permitir aplicações que usem protocolos específicos (FTP, telnet)**
- **Verificam tanto endereço origem como destino**
- **Na negação certos *routers* avisam para trás: *unreachable***

  - **ACL *extended: entre* 100 e 199**

ACLs Estendidas (*Extended* ACLs)




```
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
```

- Access list number range of 100-199
- Source destination IP address
- Layer 4 protocol number
- Applied to port closest to source host

Sintaxe duma ACL estendida

- Router(config)#**access-list** nº {**permit|deny**} protocol **source** [source-mask **destination** destination-mask operator operand] [established]

Parameter	Description
access-list-number	Identifies the list using a number in the range 100 to 199.
permit | deny	Indicates whether this entry allows or blocks the specified address.
protocol	The protocol, such as IP, TCP, UDP, ICMP, GRE, or IGRP.
source and destination	Identifies source and destination addresses.
source-mask and destination-mask	Wildcard mask; zeros indicate positions that must match, ones indicate don't-care positions.
operator operand	lt, gt, eq, neq (less than, greater than, equal, not equal), and a port number.
established	Allows TCP traffic to pass if the packet uses an established connection (for example, has ACK bits set).

Nota:
Só é permitida uma ACL:
- **por porto,**
- **por protocolo,**
- **por direção**

{in|out}
Aplica a ACL ao tráfego de entrada ou de saída.
Se nada especificado:
- aplica-se ao de saída

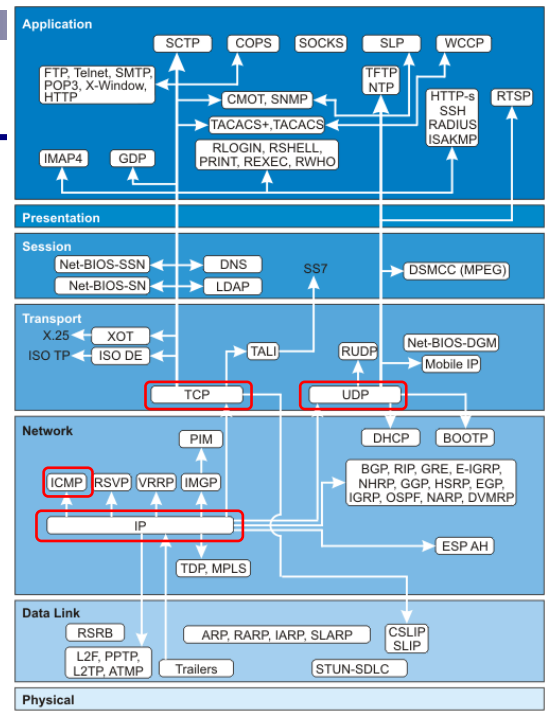
Não esquecer este 2º passo!

- **Router(config-if)#ip access-group access-list-number {in | ou**

Nºs. dos Portos TCP e UDP

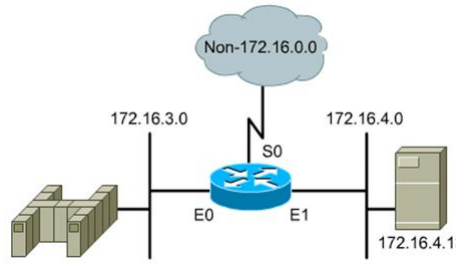
Decimal	Keyword	Description	Protocol
0		Reserved	
1-4		Unassigned	
20	FTP-DATA	FTP (data)	TCP
21	FTP	FTP	TCP
23	TELNET	Terminal connection	TCP
25	SMTP	SMTP	TCP
42	NAMESERVER	Host name server	UDP
53	DOMAIN	DNS	TCP/UDP
69	TFTP	TFTP	UDP
70		Gopher	TCP/IP
80	HTTP	WWW	TCP
133-159		Unassigned	
160-223		Reserved	
162		FNP	UDP
224-241		Unassigned	
242-251		Unassigned	

Modelo OSI VS Protocolos



Origem da figura: http://www.protocols.com /pbook/tcpip1.htm

Exemplo 1 (negação do serviço FTP em E0) (1)

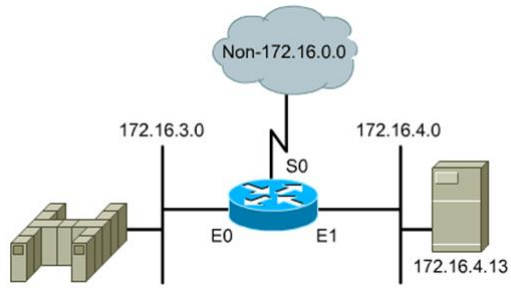


Command Output

```
access-list 101 deny tcp 172.16.4.0
    0.0.0.255 172.16.3.0  0.0.0.255  eq 21
access-list 101 permit ip 172.16.4.0
    0.0.0.255 0.0.0.0 255.255.255.255
(implicit deny any)
(access-list 101 deny ip 0.0.0.0
    255.255.255.255  0.0.0.0  255.255.255.255)

interface ethernet 0
ip access-group 101
```

Field	Description
101	ACL number; indicates extended ACL.
deny	Traffic that matches selected parameters will be blocked.
tcp	Transport-layer protocol.
172.16.4.0 and 0.0.0.255	Source address and mask; the first three octets must match, but the last octet does not matter.
172.16.3.0 and 0.0.0.255	Destination address and mask; the first three octets must match, but the last octet does not matter.
eq 21	Specifies the well-known port number for FTP.
eq 20	Specifies the well-known port number for FTP data.

Exemplo 2
(Negação do Telnet e permissão do restante tráfego)



Command Output

```
access-list 101 deny tcp 172.16.4.0  0.0.0.255 any eq 23
access-list 101 permit ip any any
(implicit deny any)
(access-list 101 deny ip 0.0.0.0  255.255.255.255
    0.0.0.0  255.255.255.255)

interface ethernet 0
ip access-group 101 out
```

ACLs com nome (*Named* ACLs)

- **Identificação por um nome *(standard* ou *extended)***
- **Permite apagar uma entrada só, duma ACL, sem ter de reconfigurar**
- **Usam-se quando:**
  - **queremos identificação intuitiva**
  - **Temos:**
    99 standard ou 100 extended (por protocolo)

- **Para nomear uma ACL:**
  Router(config)# ip access-list {standard | extended} <nome>

- **No modo de configuração ACL, especificar as condições:**
  Router(config {std- |ext-}nacl)# deny {source [source-wildcard] |any}
  ou Router(config {std- |ext-}nacl)# permit {source [source-wildcard] |any}

O comando **deny**

- **Sintaxe:**
  deny {source [source-wildcard]|any}

Output

```
ip access-list standard Internetfilter
deny 192.5.34.0.0.0.0.255
permit 128.88.0.0.0.0.255.255
permit 36.0.0.0.0.255.255.255
! (Note: all other access implicity denied)
```

- **Aplica a condição deny à ACL de nome *Internetfilter***

O comando **permit**

- **Sintaxe:**
  Router(config{std- | ext-}nac)# permit {source [sour-ce-wildcard] | any } log

Usa-se no modo de configuração, após o comando ip access-list

Output

```
ip access-list extended come-on
permit tcp any 171.69.0.0.0.255.255.255 eq telnet

deny tcp any any
deny udp any 171.69.0.0.0.255.255.255 lt 1024

deny ip any any
interface ethernet0/5
ip address 2.0.5.1 255.255.255.0
ip access-group over_out out
ip access-group come_on in
ip access-list standard over_and
permits 1.2.3.4

deny any
```


ACLs com nome (*Named* ACLs)

- **Criação duma ACL:**
  - **standard**
  - **nome:** **Interfilter**
- **E duma ACL:**
  - **estendida**
  - **nome:** **marketing_group**

Output

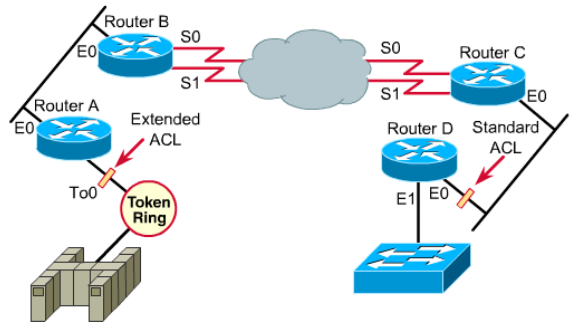
```
ip interface ethernet0/5
ip address 2.0.5.1.255.255.255.0
ip access-group Internetfilter out
ip access-group marketinggroup in
...
ip access-list standard Internetfilter
permit 1.2.3.4

deny any
ip access-list extended marketing_group
permit tcp any 171.69.0.0.0.255.255.255 eq telnet

deny tcp any any
deny udp any 171.69.0.0.0.255.255.255 lt 1024

deny ip any log
```

Adicionar uma linha a uma ACL com nome

```
R1# show access-lists
Standard IP access list WEBSERVER
    10 permit 192.168.10.10
    20 deny   192.168.10.0, wildcard bits 0.0.0.255
    30 deny   192.168.11.0, wildcard bits 0.0.0.255

R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip access-list standard WEBSERVER
R1(config-std-nacl)# 15 permit host 192.168.11.10
R1(config-std-nacl)# end
R1#
*Nov  1 19:20:57.591: %SYS-5-CONFIG_I: Configured from console by console

R1# sho access-lists
Standard IP access list WEBSERVER
    10 permit 192.168.10.10
    15 permit 192.168.11.10
    20 deny   192.168.10.0, wildcard bits 0.0.0.255
    30 deny   192.168.11.0, wildcard bits 0.0.0.255
R1#
```


Colocação das ACLs

- A redução do tráfego depende do local onde se colocam as ACLs
- **Regra:**
  - Colocar ACLs extendidas o mais próximo possível da fonte de tráfego a negar (já nem chega a percorrer desnecessariamente a rede)
  - ACLs standard não especificam endereço destino: pô-las o mais próximo possível do destino



Verificação de ACLs

- Router> show ip interface
- Router> show access-lists

Output

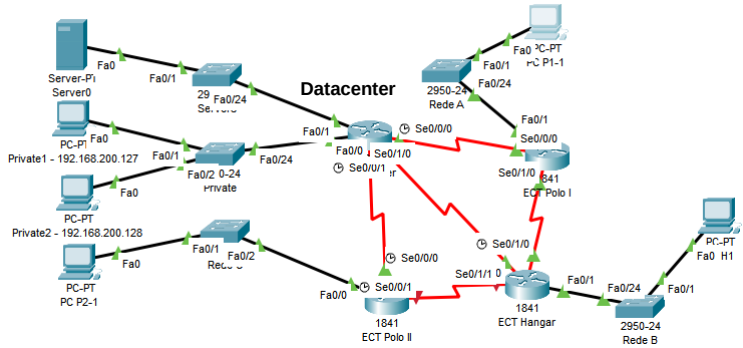
```
Ethernet0 is up, line protocol is up
  Internet address is 192.54.22.2, subnet mask is 255.255.255.0
  Broadcast address is 255.255.255.255
  Address determined by nonvolatile memory
  MTU is 1500 bytes
  Helper address is 192.52.71.4
  Secondary address 131.192.115.2, subnet mask 255.255.255.0
  Outgoing ACL 10 is set
  Inbound ACL is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is anabled
  ICMP redirects are always sent
  ICMP unreachables are never sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  Gateway Discovery is disabled
  IP accounting is disabled
  TCP/IP header compression is disabled
  Probe proxy name replies are disabled
Router>
```


Baseado em:
https://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula9.pdf

Exercícios ACLs (1)

- Qual é a limitação colocada por esta ACL?

```
ECT Hangar(config)#access-list 1 deny 12.0.0.0 0.255.255.255
ECT Hangar(config)#access-list 1 permit any
ECT Hangar(config)#interface Fa0/1
ECT Hangar(config-if)#ip access-group 1 out
```



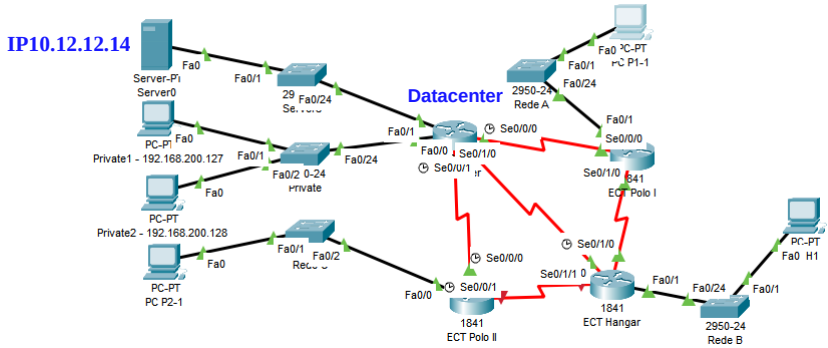
Considere que toda a rede está bem

Baseado em:
https://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula9.pdf

Exercícios ACLs (2)

- Qual é a limitação colocada por esta ACL?

```
Datacenter(config)#access-list 2 permit 10.12.12.16
Datacenter(config)#interface Fa0/1
Datacenter(config-if)#ip access-group 2 in
```



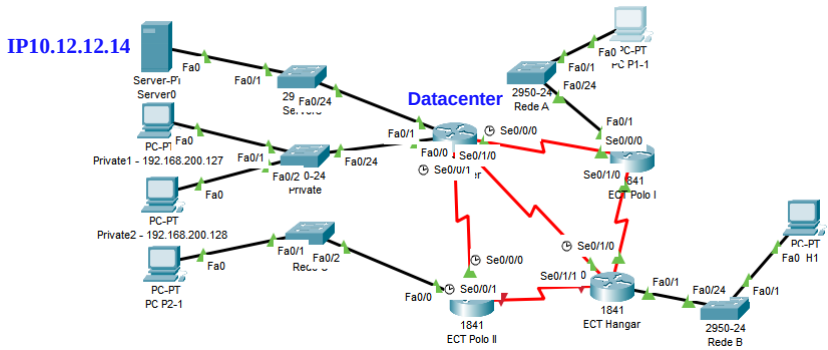
Considere que toda a rede está bem

Baseado em:
https://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula9.pdf

Exercícios ACLs (3)

- Qual é a limitação colocada por esta ACL?

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



Considere que toda a rede está bem

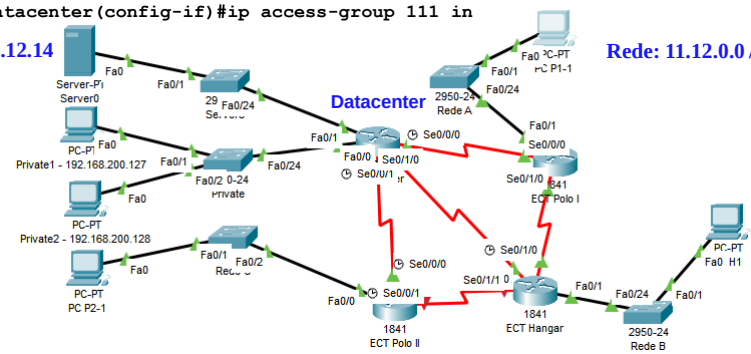
https://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula9.pdf

Exercícios ACLs (4)

- Qual é a limitação colocada por esta ACL?

```
Datacenter(config)#access-list 111 deny tcp 10.0.0.0 0.255.255.255
11.12.0.0 0.0.255.255
Datacenter(config)#access-list 111 permit ip any any
Datacenter(config)#int Fa0/1
Datacenter(config-if)#ip access-group 111 in
```

IP10.12.12.14



Rede: 11.12.0.0 / 16

Redes de Computadores

Considere que toda a rede está bem

78

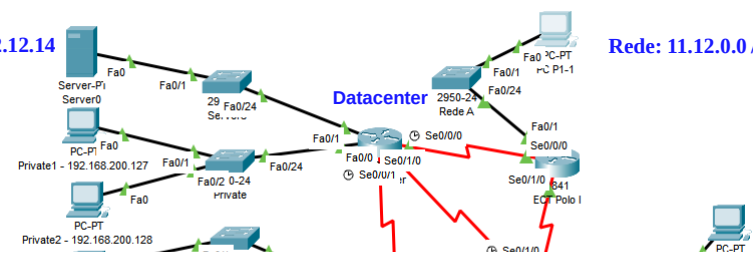
Baseado em:
https://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula9.pdf

Exercícios ACLs (5)

- Qual é a limitação colocada por esta ACL?

```
ECTPoloI(config)#access-list 111 deny tcp 10.0.0.0 0.255.255.255
11.12.0.0 0.0.255.255
ECTPoloI(config)#access-list 111 permit ip any any
ECTPoloI(config)#int Se0/0/0
ECTPoloI(config-if)#ip access-group 111 in
ECTPoloI(config)#int Se0/1/0
ECTPoloI(config-if)#ip access-group 111 in
```

IP10.12.12.14



Rede: 11.12.0.0 / 16

Redes

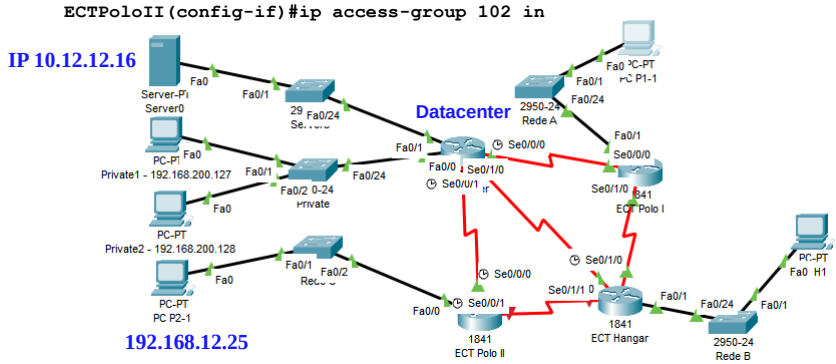
79

Baseado em:
https://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula9.pdf

Exercícios ACLs (6)

- Qual é a limitação colocada por esta ACL?

```
ECTPoloII(config)# access-list 102 deny tcp host 192.168.12.25 any eq 23
ECTPoloII(config)# access-list 102 permit tcp any any
ECTPoloII(config)#int Fa0/0
ECTPoloII(config-if)#ip access-group 102 in
```



Considere que toda a rede está bem

Baseado em:
https://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula9.pdf

Exercícios ACLs (7)

- O quê que faz esta ACL?

```
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
```

Baseado em:
https://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula9.pdf

Exercícios ACLs (8)

- O quê que faz esta ACL?

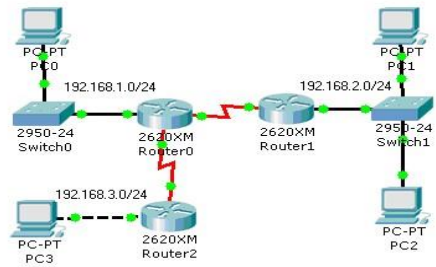
```
Router(config)# ip access-list extended Restringe
Router(config-ext-acl)# permit tcp any 172.16.0.0 0.0.255.255
Router(config-ext-acl)# permit udp any host 172.16.1.1 eq dns log
Router(config-ext-acl)# permit tcp 172.17.0.0 0.0.255.255 host
     176.16.1.2 eq telnet log
Router(config-ext-acl)# permit icmp any 176.16.0.0 0.0.255.255
Router(config-ext-acl)# deny ip any any log
Router(config)# interface Ethernet0
Router(config-if)# ip access-group Restringe
```


Baseado em:
https://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula9.pdf

Exercícios ACLs (9)

- Considere a o cenário de rede seguinte figura:

  Implemente- o no Packet



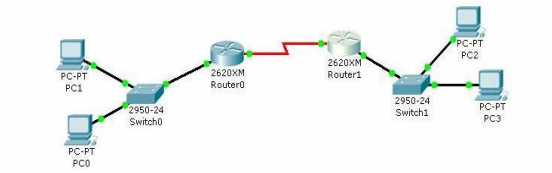
  - Verifique as configurações e teste a conectividade entre todos os pcs.
  - Através da utilização de ACLs, configure a rede de modo a que o PC1 não consiga aceder a todas as máquinas da rede 192.168.1.0/24. Aplique a lista construída à interface mais adequada.
  - Teste a conectividade de modo a confirmar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

Baseado em:
https://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula9.pdf

Exercícios ACLs (10)

- Considere a o cenário de rede seguinte figura:

  Implemente- o no Packet



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):

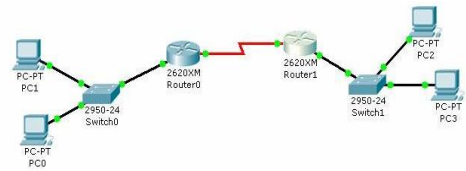
PC0 172.16.10.5/24
PC1 172.16.10.6/24
PC2 172.30.10.20/24
PC3 172.30.10.21/24

Baseado em:
https://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula9.pdf

Exercícios ACLs (10)

- Considere a o cenário de rede seguinte figura:

  Implemente- o no Packet Tracer



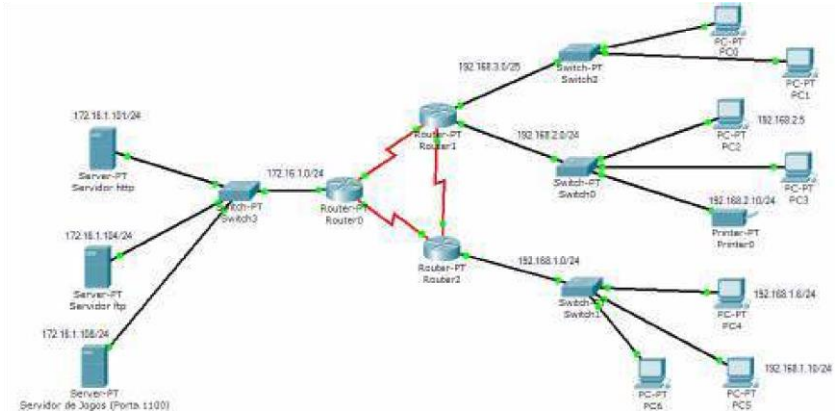
C) Configure RIP V2 de modo a que exista conectividade entre todas as redes e teste a conectividade de/para todas as máquinas.

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.

Baseado em:
https://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula9.pdf

Exercícios ACLs (10)

- Considere a seguinte figura da página seguinte.



Baseado em:
https://www.dei.isep.ipp.pt/~npereira/aulas/asist/07/misc/aula9.pdf

Exercícios ACLs (10)

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