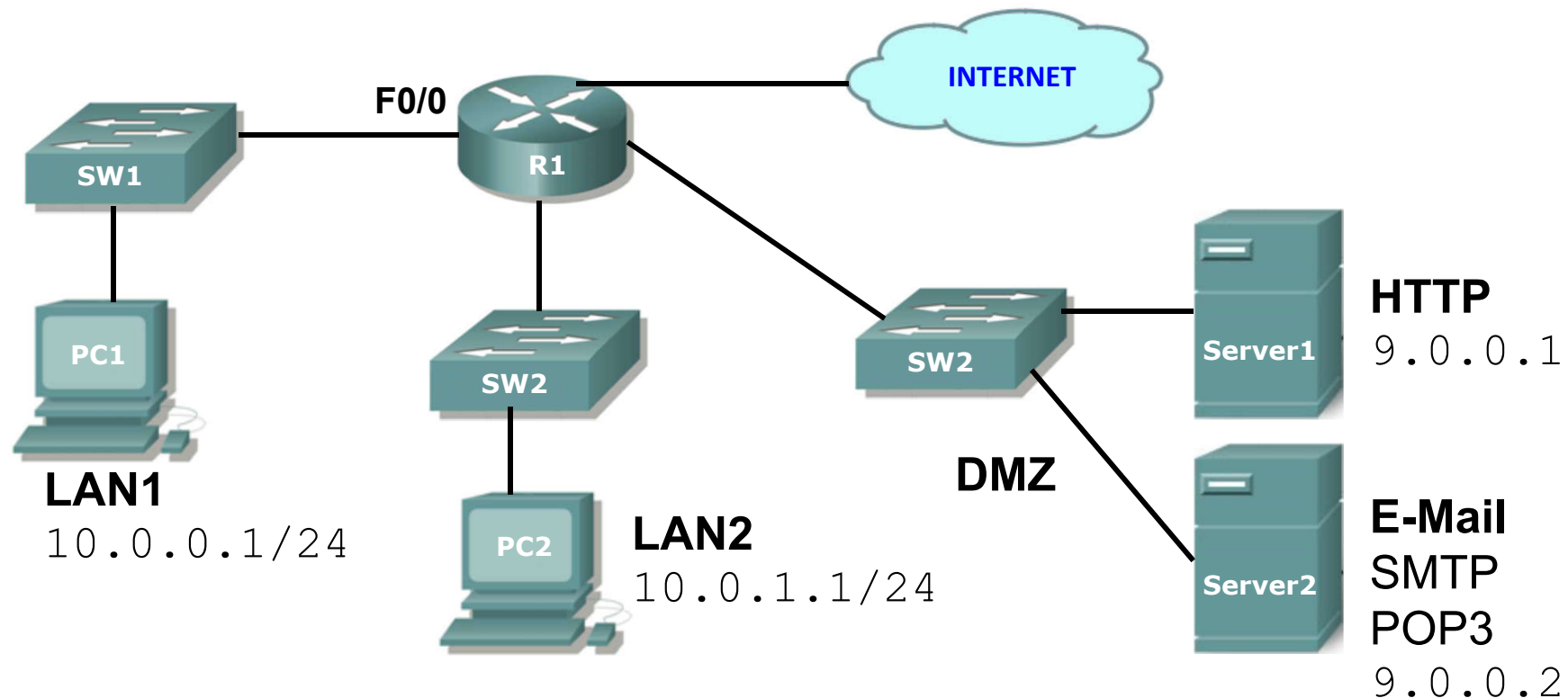


Listas de Controlo de Acesso (ACL's)

Jorge Martins, Manuel Ferreira e Luísa Caeiro

ESTSetúbal (v10)

Motivação para a implementação de ACL's

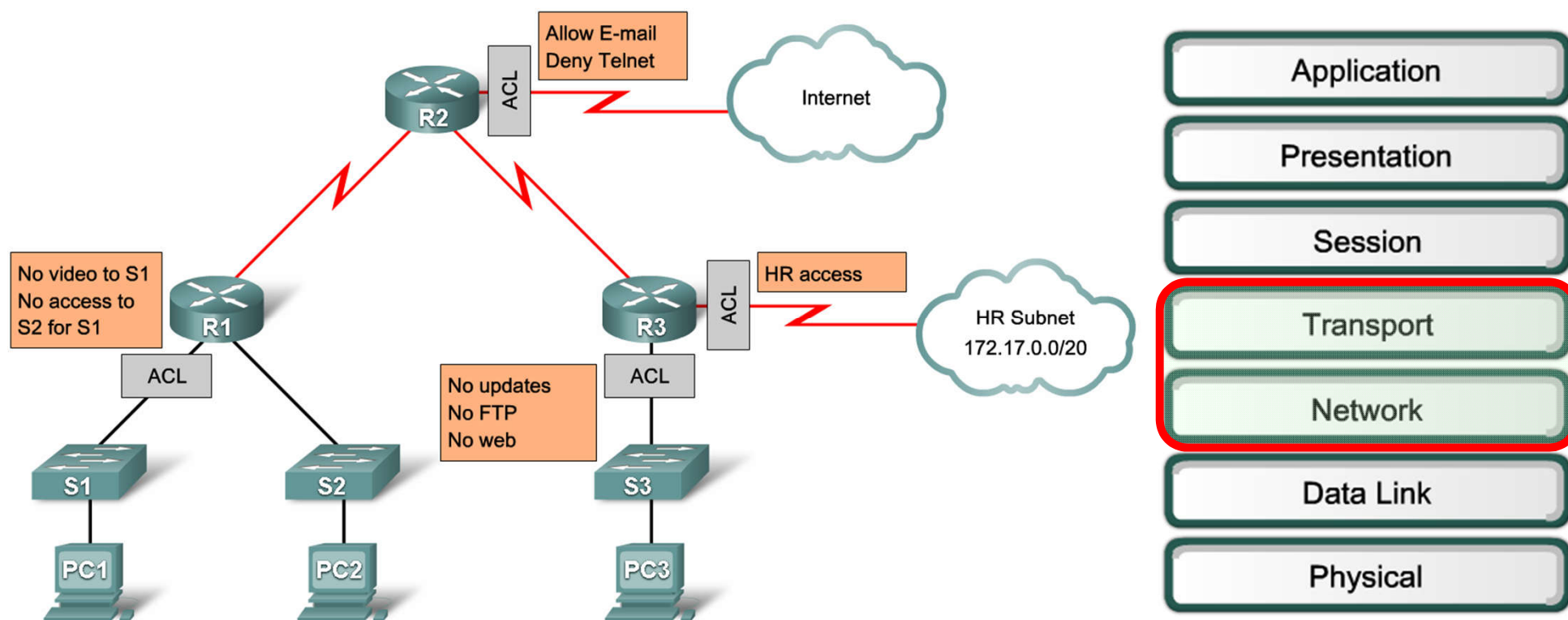


Pretende-se que os Hosts da LAN1

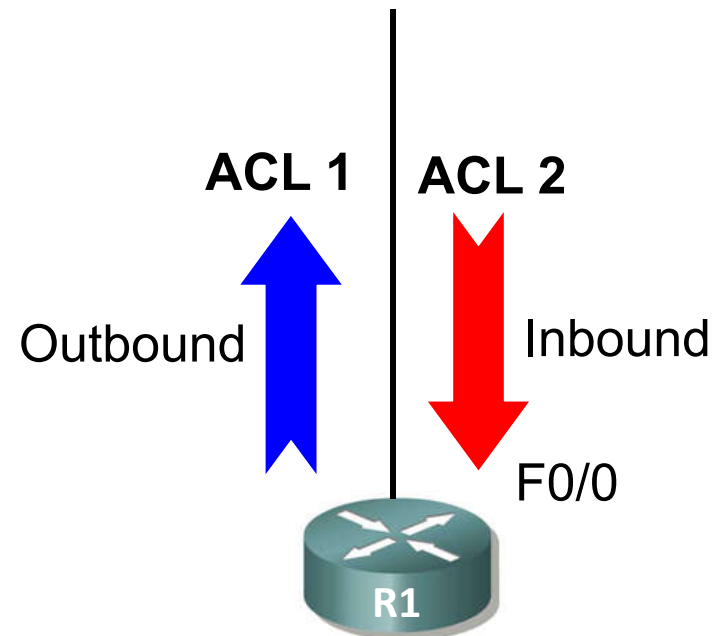
- não consigam aceder à LAN2
- consigam aceder ao servidor de HTTP e E-Mail
- consigam aceder à internet, para os serviços de HTTP e FTP

O que são ACL's?

Listas de Controlo de Acesso (do inglês, *Access Control Lists* – ACL's) são conjuntos de regras de acesso, colocadas nas interfaces de um Router, as quais permitem bloquear ou deixar passar tráfego.

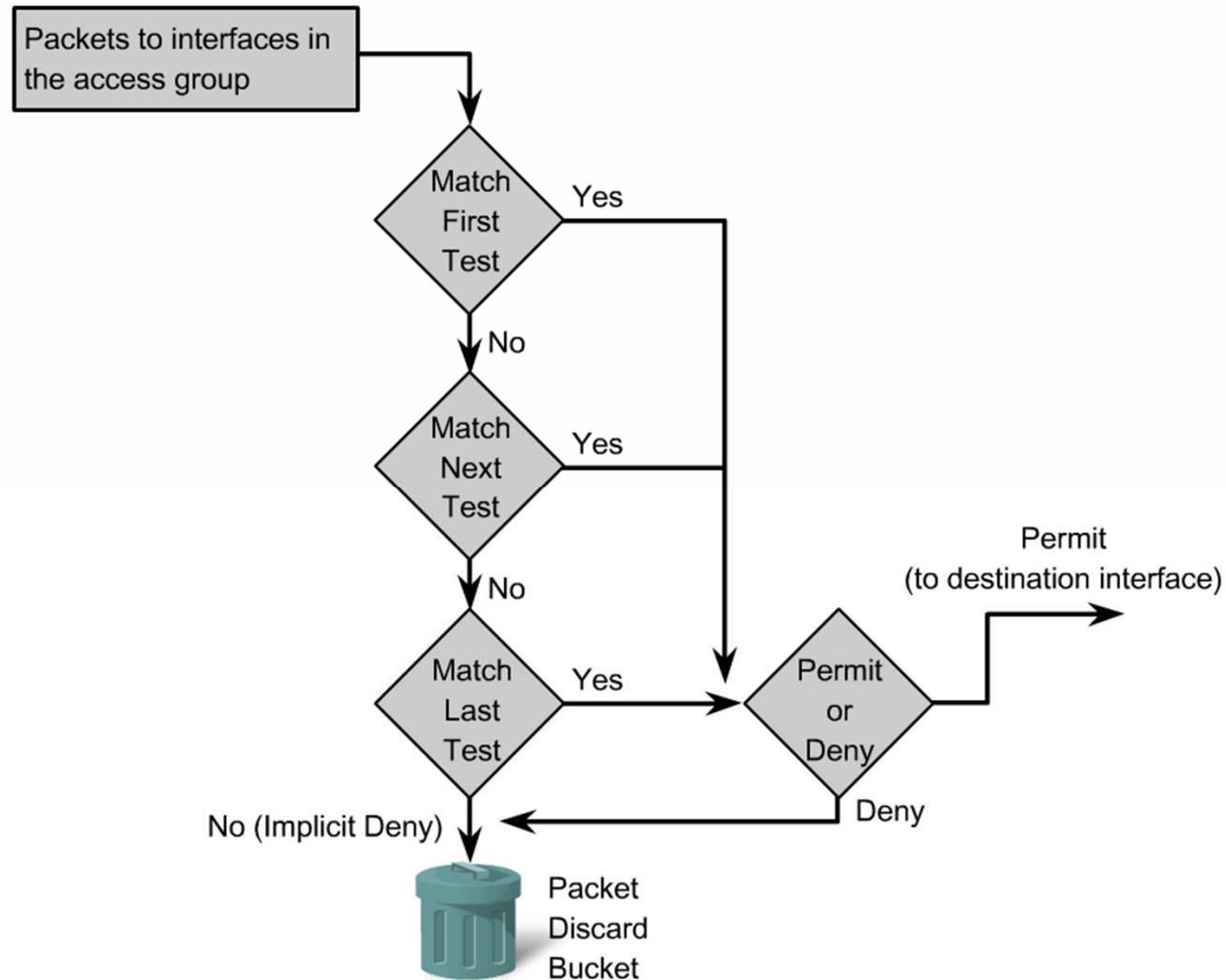


Onde se Aplicam as ACL?



```
R1 (config)# interface F0/0  
R1(config-if)# ip access-group 1 out  
R1(config-if)# ip access-group 2 in
```

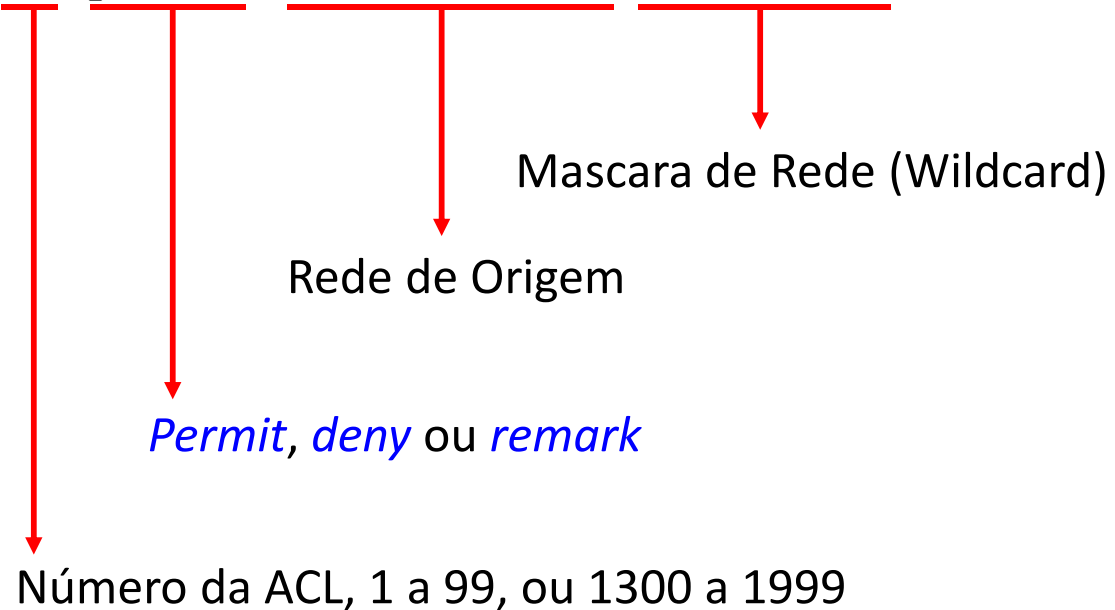
Como Funcionam as ACL's?



ACL's Básicas (Standard ACL's)



```
R1 (config) # access-list 10 permit 192.168.10.0 0.0.0.255
```



ACL's Estendidas (Extended ACL's)



R1 (config) # **access-list 100 permit ip 10.0.0.0 0.0.0.255 11.0.0.0 0.0.0.255**

Annotations for the command:

- 100**: Número da ACL, 100 a 199, ou 2000 a 2699
- permit**: Permit, deny ou remark
- ip**: *ip, icmp, udp* ou *tcp*
- 10.0.0.0**: Rede de Origem
- 0.0.0.255**: Mascara de Rede (Wildcard)
- 11.0.0.0**: Rede de Destino
- 0.0.0.255**: Mascara de Rede (Wildcard)

ACL's Estendidas (Extended ACL's)

```
... access-list 100 permit tcp 10.0.0.0 0.0.0.255 11.0.0.0 0.0.0.255 eq www
```

tcp ou **udp**

Protocolo de nível de transporte

Casos Particulares

Referência a um único endereço IP

```
R1 (config) # access-list 20 permit 192.168.10.10 0.0.0.0
```

Pode ser referido por

```
R1 (config) # access-list 20 permit host 192.168.10.10
```

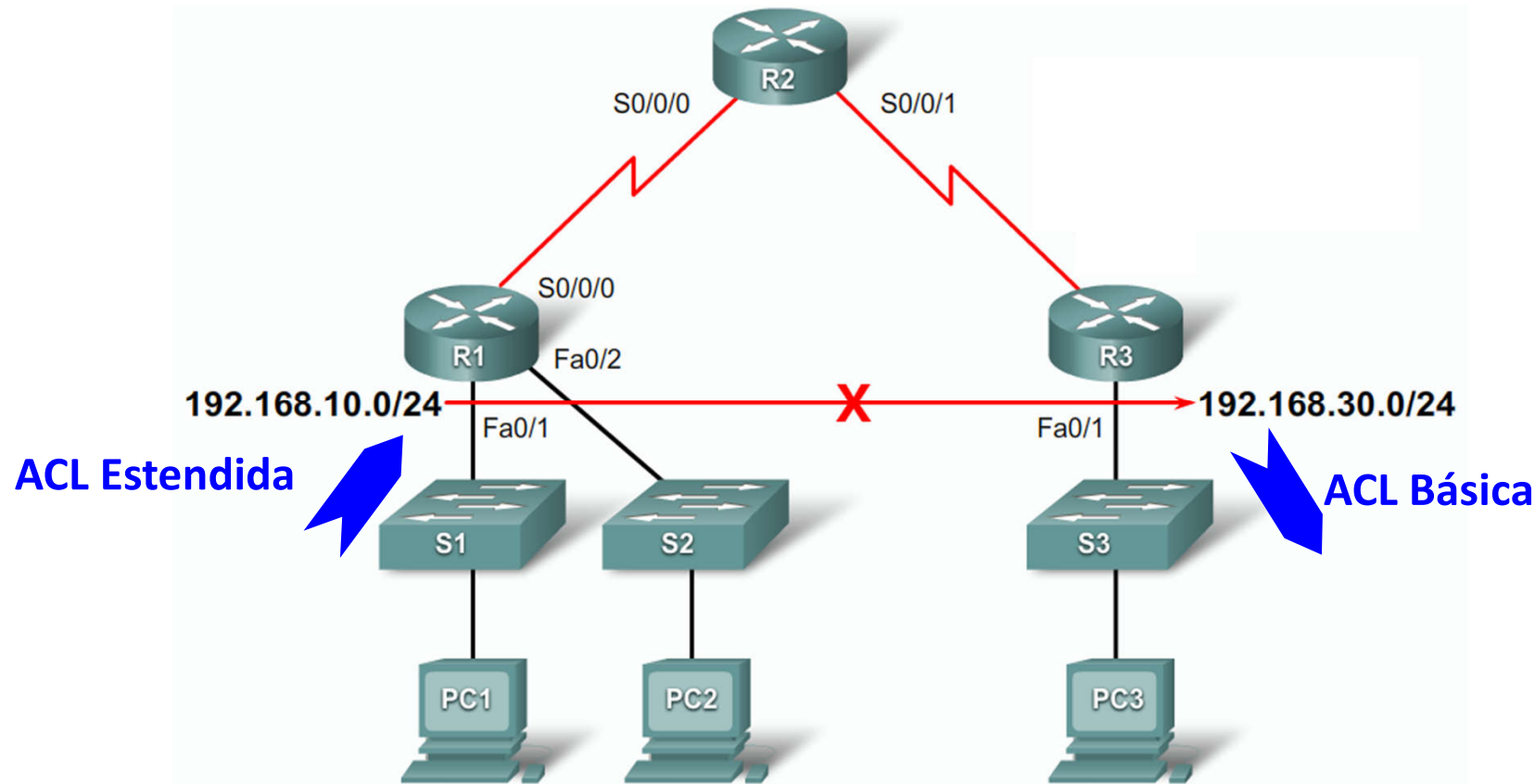
Referência a todos os endereços IP

```
R1 (config) # access-list 30 permit 0.0.0.0 255.255.255.255
```

Pode ser referido por

```
R1 (config) # access-list 30 permit any
```

Onde aplicar ACL's Básicas e Estendidas

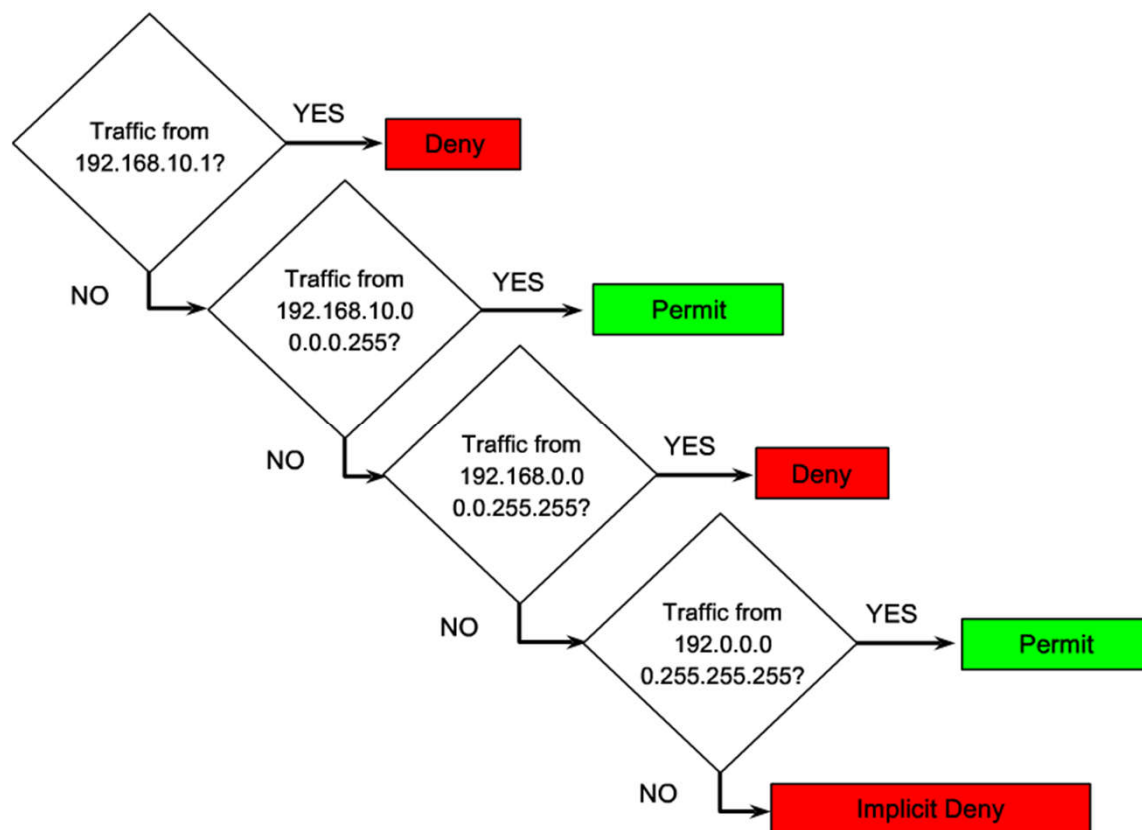


As ACL's estendidas devem ser colocadas junto à rede de origem, as ACL's básicas têm de ser colocadas junto à rede de destino.

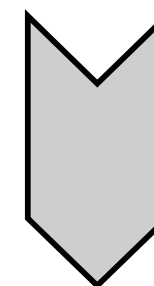
Dado que as ACL's estendidas evitam que o tráfego passe na rede, as mesmas são normalmente as escolhidas.

Ordem das Regras numa ACL

```
R1(config)# access-list 2 deny host 192.168.10.1
R1(config)# access-list 2 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 2 deny 192.168.0.0 0.0.255.255
R1(config)# access-list 2 permit 192.0.0.0 0.255.255.255
```



Particular



Geral

Ver as ACL's Configuradas

```
R1(config)# access-list 2 deny host 192.168.10.1
R1(config)# access-list 2 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 2 deny 192.168.0.0 0.0.255.255
R1(config)# access-list 2 permit 192.0.0.0 0.255.255.255
R1(config)# exit
```

```
R1# show access-lists
```

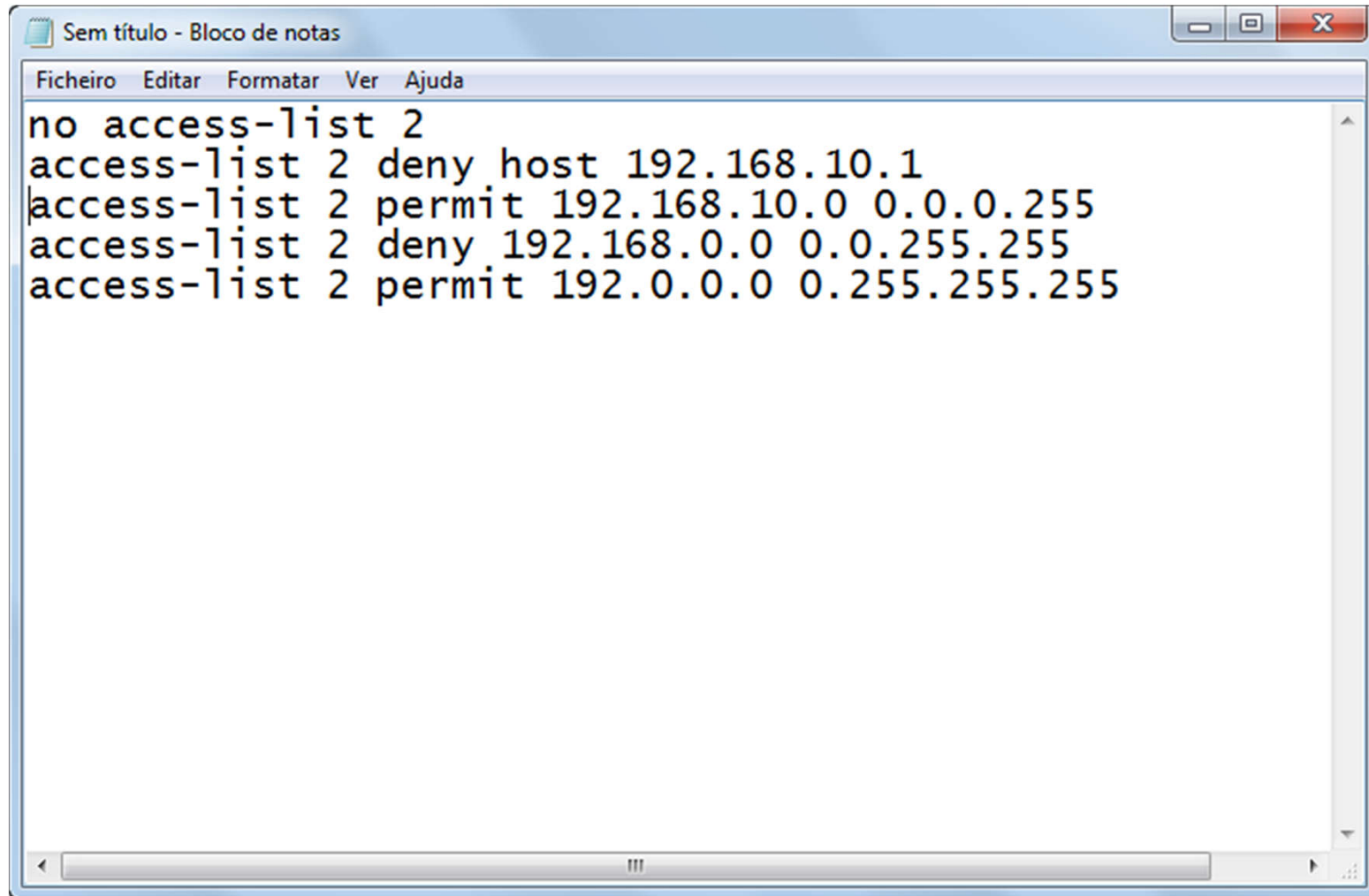
```
Standard IP access list 2
```

```
10 deny 192.168.10.1 (5 match(es))
20 permit 192.168.10.0, wildcard bits 0.0.0.255
30 deny 192.168.0.0, wildcard bits 0.0.255.255
40 permit 192.0.0.0, wildcard bits 0.255.255.255
```

```
R1# conf t
```

```
R1(config)# no access-list 2
```

Edição de ACL's Básicas e Extendidas



```
Sem título - Bloco de notas
Ficheiro  Editar  Formatar  Ver  Ajuda
no access-list 2
access-list 2 deny host 192.168.10.1
access-list 2 permit 192.168.10.0 0.0.0.255
access-list 2 deny 192.168.0.0 0.0.255.255
access-list 2 permit 192.0.0.0 0.255.255.255
```

ACL's com Nome

```
R1# show access-lists
```

```
Standard IP access list WEBSERVER
```

```
10 permit 192.168.10.11
```

```
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 192.168.10.11
```

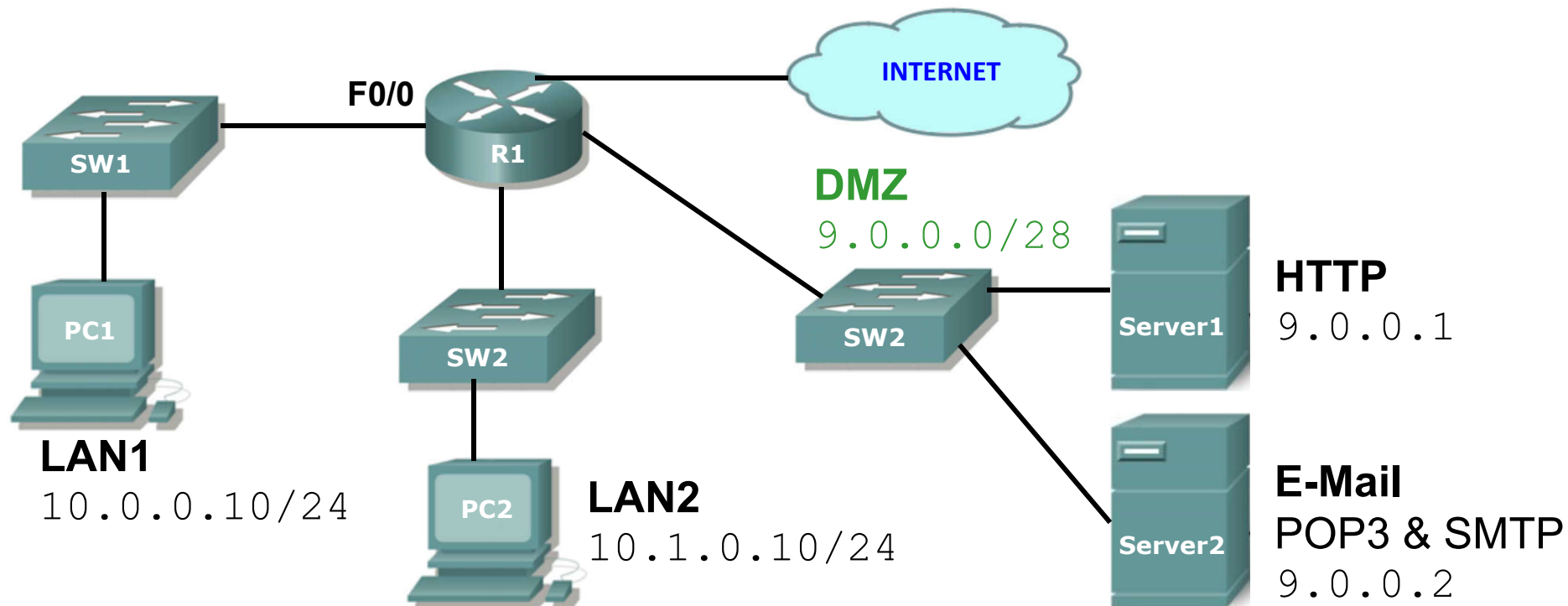
```
15 permit 192.168.11.10
```

```
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#
```

Exemplo da Configuração de uma Rede Local



Escrever uma ACL para que os hosts da LAN1:

- Consigam apenas pingar o host 10.1.0.10 na LAN2
- consigam aceder ao servidor de HTTP e E-Mail
- consigam aceder à internet, para os serviços de HTTP e FTP

Solução

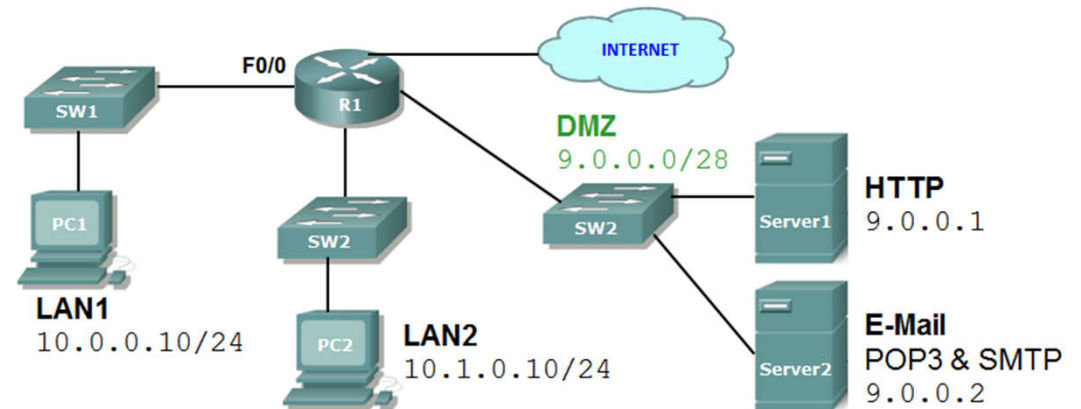
```

R1(config)# access-list 100 permit ip 10.0.0.0 0.0.0.255 host 10.1.0.10
R1(config)# access-list 100 deny ip 10.0.0.0 0.0.0.255 10.0.0.0 0.255.255.255

R1(config)# access-list 100 permit tcp 10.0.0.0 0.0.0.255 host 9.0.0.1 eq www
R1(config)# access-list 100 permit tcp 10.0.0.0 0.0.0.255 host 9.0.0.2 eq pop3
R1(config)# access-list 100 permit tcp 10.0.0.0 0.0.0.255 host 9.0.0.2 eq smtp
R1(config)# access-list 100 deny ip 10.0.0.0 0.0.0.255 9.0.0.0 0.0.0.15

R1(config)# access-list 100 permit tcp 10.0.0.0 0.0.0.255 any eq www
R1(config)# access-list 100 permit tcp 10.0.0.0 0.0.0.255 any eq ftp

R1(config)# int f0/0
R1(config-if)# ip access-group 100 in
R1(config-if)# exit
  
```



Limitar o Acesso Remoto via Telnet

```
R1 (config) # access-list 1 permit host 192.168.10.10
```

```
R1 (config) # line vty 0 15
```

```
R1 (config-line) # password secret
```

```
R1 (config-line) # login
```

```
R1 (config-line) # access-class 1 in
```

```
R1 (config-line) # exit
```

Ip: 192.168.10.10



Exemplo da Inclusão de um Host para Gestão

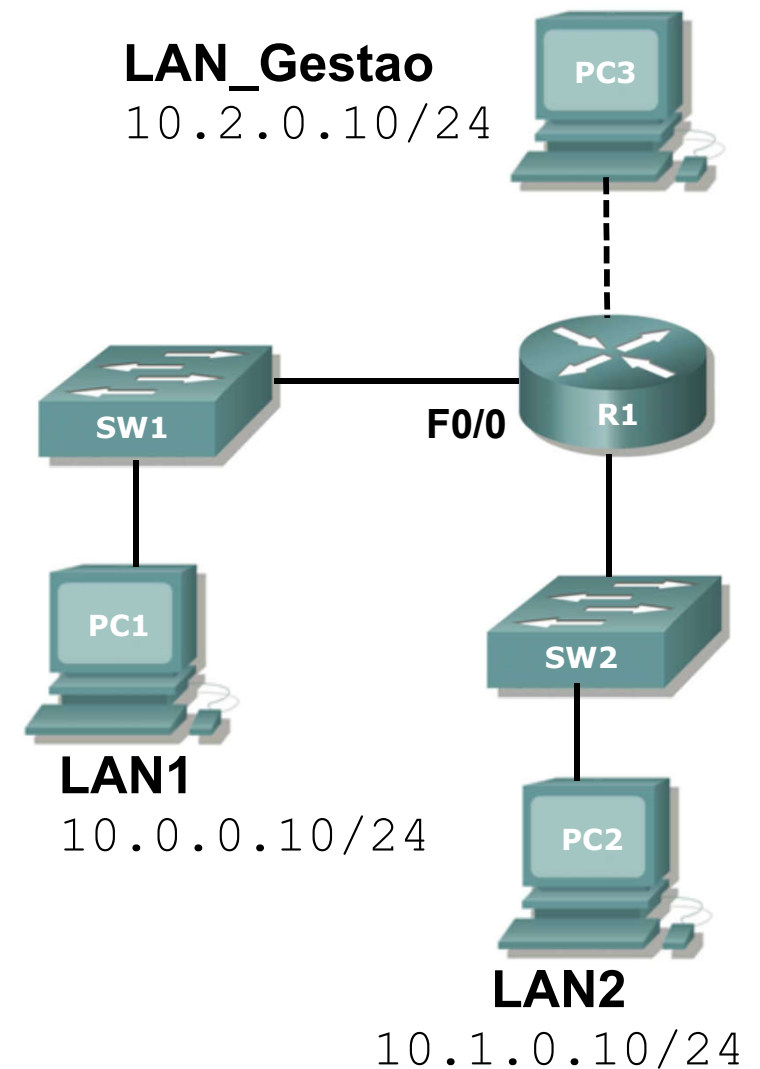
Depois da inclusão de ACL anterior, na interface F0/0, o PC3 consegue chegar ao PC1, mas a resposta é bloqueada.

Uma solução passaria por incluir uma regra para permitir o acesso ao *host* 10.2.0.10 (semelhante ao que se fez para o PC2). No entanto, esta solução permitiria que o PC1 inicia-se ligações para o PC3.

A solução é a inclusão da seguinte regra na ACL 100 (exemplo para a activação do *remote desktop*)

```
R1 (config) # access-list 100 permit tcp  
any host 10.2.0.10 eq 3389 established
```

Esta solução filtra os pacotes IP com a flag SYN=1 e ACK=0 (primeiro pacote do *triple handshake*), e desta forma o PC1 não pode iniciar as secções.



Exemplo da Inclusão de um Host para Gestão

Caso se pretenda que se façam pings a partir do PC3 para o PC1, tem de se acrescentar a regra

```
R1 (config) # access-list 100 permit  
icmp any host 10.2.0.10 echo-reply
```

