UNIVERSIDADE
EDUARDO
MONDLANE

FACULDADE DE ENGENHARIA
DEPARTAMENTO DE ENGENHARIA ELECTROTÉCNICA
LICENCIATURA EM ENGENHARIA INFORMÁTICA
REDES DE COMPUTADORES II

Access Control Lists (ACLs)

- Engº. Felizardo Munguambe (MsC.)
- Engº. Délcio Chadreca (MsC.)

Tópicos da Aula

- Introdução a IPv4 Access Control Lists (ACLs);
- Tipos de IP ACLs;
- Standard Numered and Named IP ACL;
- Troubleshooting;
- Extended Numered and Named IP ACL;
- Troubleshooting; e
- Exercícios/Laboratórios.

Introdução à Access Control Lists (ACLs)

Uma **ACL** é uma lista de regras configuradas num dispositvo de rede, e normalmente é utilizada para filtrar tráfego que passa por esse dispositivo.

Uma ACL permite ao Engenheiro de Redes, uma maneira de identificar diferentes tipos de pacotes.

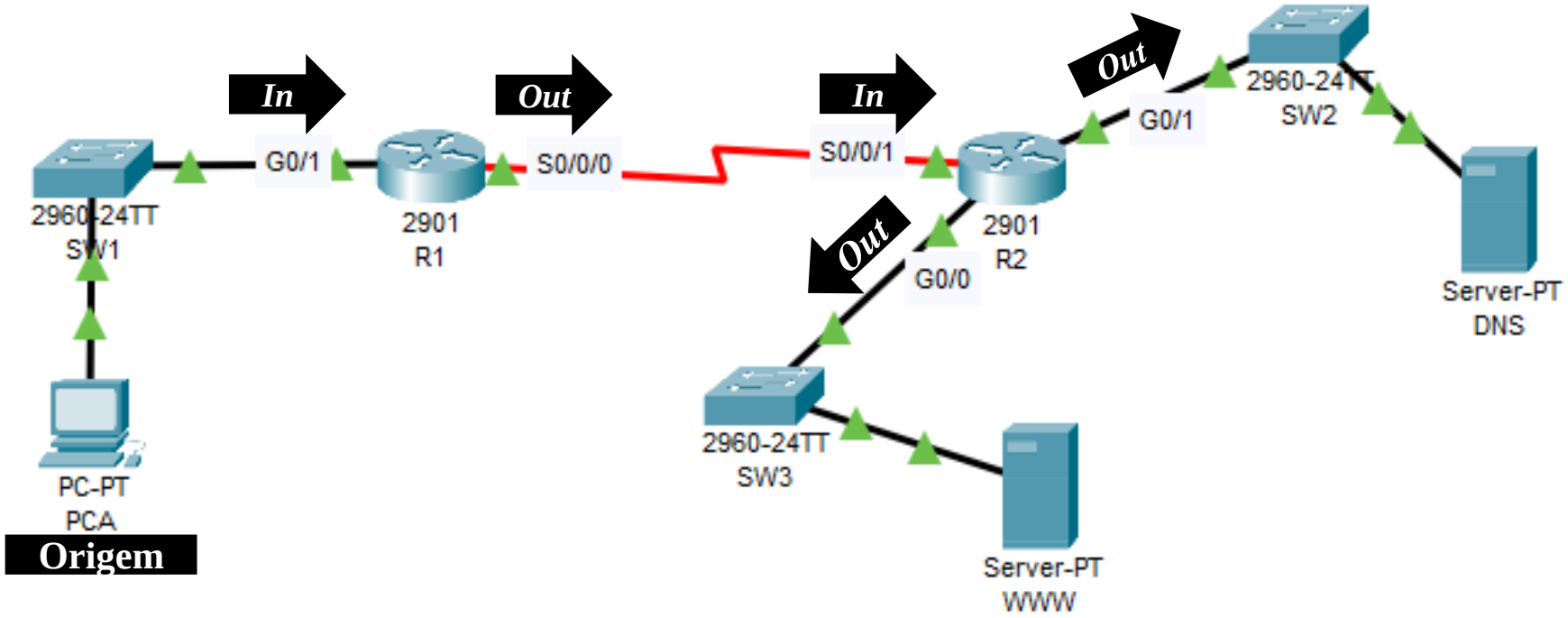
Para que isso aconteça a configuração da lista nos permite informar qual ou quais características desejamos identificar, como por exemplos: IP de Origem ou Destino, Protocolos, Porta de Origem ou Destino.

As ACLs nos dispositivos da Cisco podem desempenhar diferentes papéis, o mais comum deles é como filtro de pacotes, mas ela também pode ser utilizada em configurações NAT e políticas QoS (Qualidade de serviço) por exemplo.

Nesta aula, iremos nos focar no uso e configuração de ACL para filtragem de tráfego.

Access Control Lists (ACLs) – Location and Direction

A ACL pode ser aplicada *inbound*, antes que o roteador tome sua decisão de roteamento (encaminhamento), ou *outbound*, após o roteador tomar sua decisão de encaminhamento e determinar a interface de saída a ser usada.



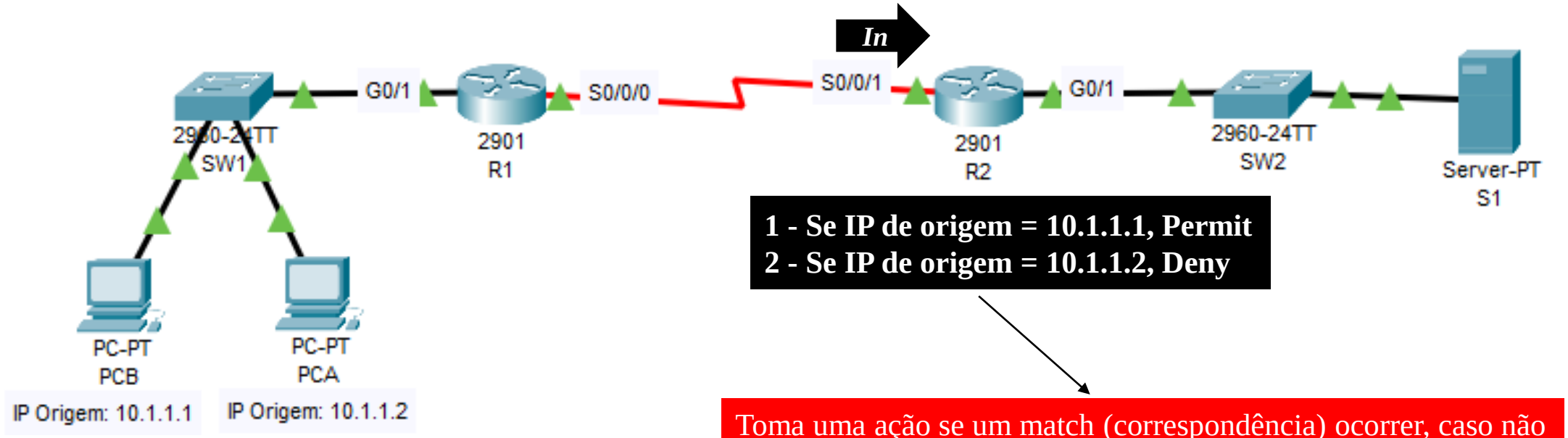
Tipos de IP Access Control Lists (ACLs)

Standard **Numbered** **(1-99) ou (1300-1999)**	**Standard** **Named**	**Standard – Matching:** = IP de Origem
Extended **Numbered** **(100-199) ou (2000-2699)**	**Extended** **Named**	**Extended – Matching:** = Protocolo = IP de Origem & Destino = Porta de Origem e Destino

Numbered: = ID with Number = Global Commands	**Named**: = ID with Name = Subcommands

Matching “Correspondência” de Pacotes

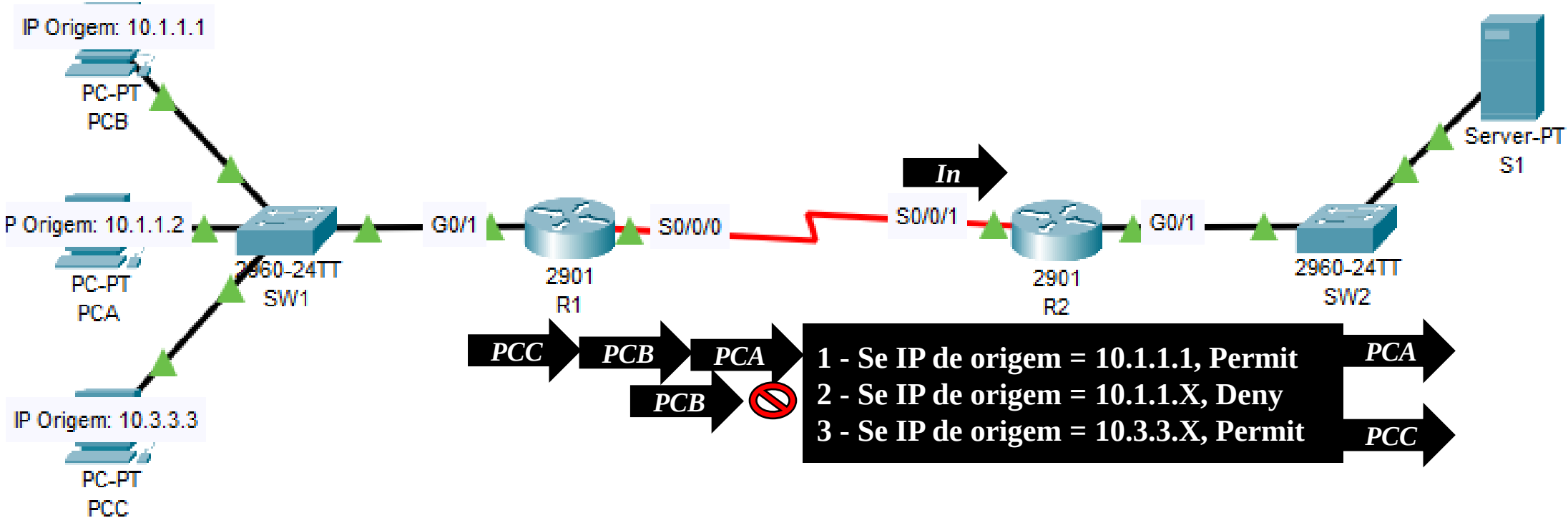
Cada ACL consiste em um ou mais comandos de configuração, com cada comando listando detalhes sobre os valores a serem procurados nos cabeçalhos de um pacote. Geralmente, um comando ACL usa uma lógica como "*procure esses valores no cabeçalho do pacote e, se encontrado, descarte (**deny**) o pacote*". A ação poderia ser permitir (***permit***) o pacote, ao invés de descartá-lo.



Toma uma ação se um match (correspondência) ocorrer, caso não ocorra o match a ACL passa a próxima linha.

Lógica *First-Match*

ACLs usam lógica de primeira correspondência (*first-match logic*). Uma vez que um pacote corresponda a uma linha na ACL, o roteador executa a ação listada nessa linha da ACL e para de procurar mais na ACL.



Nota: Se um pacote não corresponder a nenhum dos itens na ACL, o pacote será descartado. O motivo é que cada IP ACL tem uma instrução deny all/any implícita no final da ACL.

Standard Numbered IP ACL – Syntax

Standard Numbered IP ACLs (Comando de Configuração Global)

access-list {1-99 | 1300-1999} {permit | deny} **IP_Origem**

Matching Host (Endereço IP específico/exacto de Computador)

access-list 1 permit 10.1.1.1 (ACL Standard verifica IP de origem)

access-list 1 permit host 10.1.1.1 (IOS mais antigos)

Matching Subnet (Todos Endereços IP de uma Sub-rede)

access-list 1 deny 192.168.10.0 **0.0.0.255**

Wildcard/Máscara Curinga da Subnet 192.168.10.0/24

Matching Any/all IP Addresses (Qualquer Host/Sub-rede)

access-list 1 deny any

access-list 1 permit any

Máscara Curinga (*Wildcard*)

Em muitos casos, uma ACL precisa corresponder a todos os hosts em uma determinada sub-rede. Para combinar uma sub-rede com uma ACL, basta seguirmos os passos abaixo:

1 – Use o Endereço de Rede da sub-rede como o valor de origem no comando access-list.
2 – Use uma máscara curinga encontrada subtraindo a máscara da sub-rede por 255.255.255.255.

Exemplo: Criar uma ACL corresponda a subnet 172.16.8.0 255.255.252.0 ou Criar uma ACL cujos pacotes dos hosts tem 172.16.8 como os três primeiros octetos.

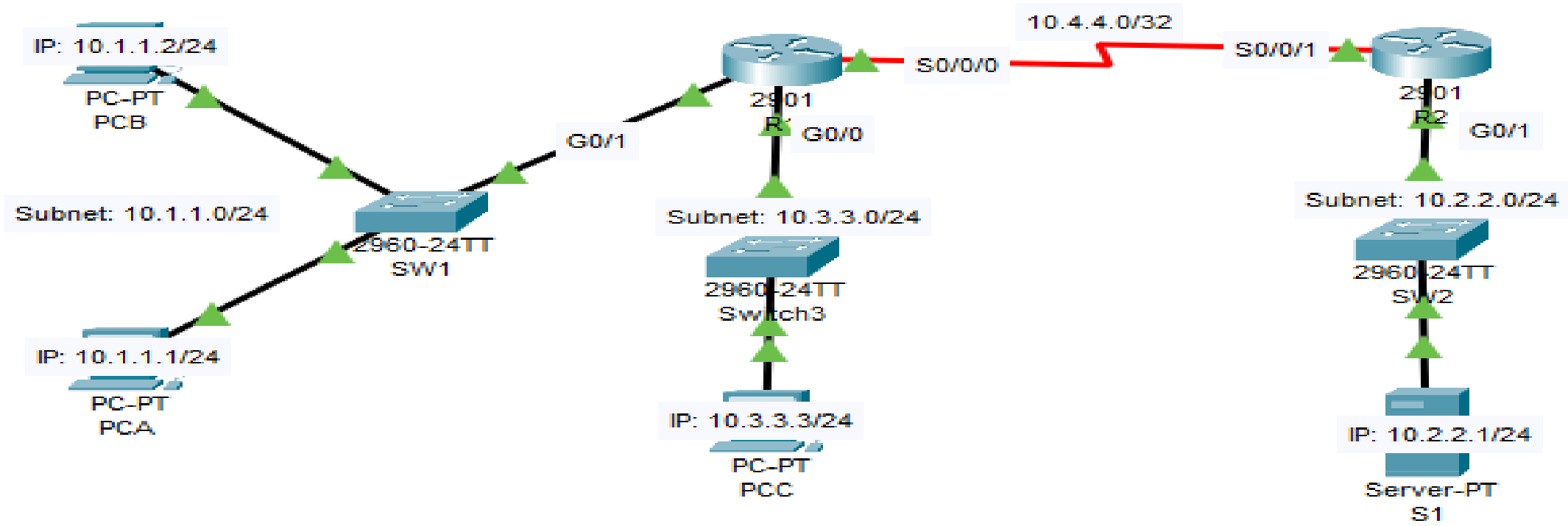
access-list 1 permit 172.16.8.0 Wildcard (???)

	255	**255**	**255**	**255**
-	**255**	**255**	**252**	**0**
=	0	0	3	255

access-list 1 permit 172.16.8.0 0.0.3.255

Sempre que quisermos descobrir a Wildcard correspondente a alguma máscara, basta subtrair a máscara por 255.255.255.255.255.

Standard IP ACL – Exemplo



Rules:

1. Permit packets from Host A going to Server 1 Subnet;
2. Deny all packets from Host A's Subnet going to Server 1 Subnet;
3. Permit all packets from Host C's Subnet going to Server 1 Subnet.

Standard Numbered IP ACL – Configs

```
R2# configure terminal
R2(config)# access-list 1 permit 10.1.1.1
R2(config)# access-list 1 deny 10.1.1.0 0.0.0.255
R2(config)# access-list 1 permit 10.3.3.0 0.0.0.255
R2(config)# interface S0/0/1
R2(config-if)# ip access-group 1 in
```

```
R2# show running-config
access-list 1 permit 10.1.1.1
access-list 1 deny 10.1.1.0 0.0.0.255
access-list 1 permit 10.3.3.0 0.0.0.255
```

```
R2# show ip access-lists
Standard IP access list 1
    10 permit 10.1.1.1 (7 matches)
    20 deny 10.1.1.0, wildcard bits 0.0.0.255 (4 matches)
    30 permit 10.3.3.0, wildcard bits 0.0.0.255 (10 matches)
    ...
```

```
R2# show access-lists
Standard IP access list 1
    10 permit 10.1.1.1 (7 matches)
    20 deny 10.1.1.0, wildcard bits 0.0.0.255 (4 matches)
    30 permit 10.3.3.0, wildcard bits 0.0.0.255 (10 matches)
```

Standard Numbered IP ACL – Configs

```
R2# show ip interface s0/0/1
Serial0/0/1 is up, line protocol is up Internet address is
   10.1.2.2/24  Broadcast address is 255.255.255.255
   [...]
   Outgoing access list is not set
   Inbound access list is 1
```

Standard Named IP ACL – Syntax & Configs

```
R1# configure terminal
R2(config)#ip access-list standard Nome_ACL
```

```
R2(config-std-nacl)#permit 10.1.1.1
R2(config-std-nacl)#deny 10.1.1.0 0.0.0.255
R2(config-std-nacl)#permit 10.3.3.0 0.0.0.255
R2(config-std-nacl)#exit
R2(config)# interface S0/0/1
R2(config-if)# ip access-group Nome_ACL in
```

```
R2# show access-lists
Standard IP access list Nome_ACL
    10 permit 10.1.1.1 (7 matches)
    20 deny 10.1.1.0, wildcard bits 0.0.0.255 (4 matches)
    30 permit 10.3.3.0, wildcard bits 0.0.0.255 (10 matches)
    ...
```

```
R2(config)#ip access-list standard Nome_ACL
R2(config-std-nacl)#5 deny 10.3.3.15
R2(config-std-nacl)#no 20
```

```
R2# show access-lists
Standard IP access list Nome_ACL
    5  deny 10.3.3.15
    10 permit 10.1.1.1 (7 matches)
    30 permit 10.3.3.0, wildcard bits 0.0.0.255 (10 matches)
    ...
```

⚠ Considerações Importantes – Standard IP ACL

- Colocar instruções mais específicas no início da ACL;
- Várias ACLs podem ser criadas num Router, mas essas listas não irão filtrar nenhum tráfego até que sejam aplicadas nalguma Interface desse Router;
- Só podemos aplicar uma ACL em cada direcção (*In* ou *Out*) de uma Interface;
- Desabilitar a ACL na interface onde tiver sido aplicada antes de realizar alguma alteração na ACL.
- Coloque a **ACL Standard** o mais próximo possível do destino do pacote. Essa medida evita o erro de descarte involuntário de pacotes que não precisam ser descartados;
- Por defeito, sempre que se adiciona uma nova regra na ACL ela vai para o final da lista a não ser que ela sofra alguma influência (em casos como Standard Named);
- Quando aplicada uma ACL para filtrar pacotes na direção *Out*, ela não filtra os pacotes que o próprio Router cria.

Dúvidas?

Exercícios

Problema	Crie uma Standard Numbered ACL para cada problema e filtre (deny ou permit) o tráfego a sua escolha
1	Packets from 172.16.5.4
Resposta	
2	Packets from hosts with 192.168.6 as the first three octets
Resposta	
3	Packets from hosts with 192.168 as the first two octets
Resposta	
4	Packets from any host
Resposta	
5	Packets from subnet 10.1.200.0/21
Resposta	
6	Packets from subnet 10.1.200.0/27
Resposta	
7	Packets from subnet 172.20.112.0/23
Resposta	
8	Packets from subnet 172.20.112.0/26
Resposta	
9	Packets from subnet 192.168.9.64/28
Resposta	
10	Packets from subnet 192.168.9.64/30
Resposta	

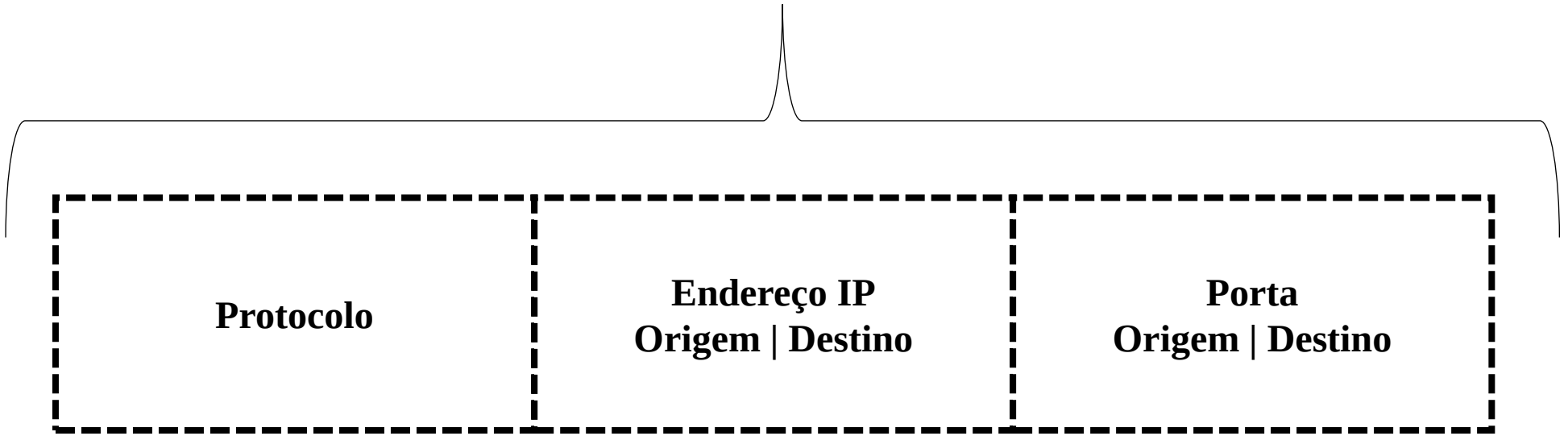
Problema	Crie uma Standard Numbered ACL para cada problema e filtre (deny ou permit) o tráfego a sua escolha
1	Packets from 172.16.5.4
Resposta	access-list 1 deny 172.16.5.4
2	Packets from hosts with 192.168.6 as the first three octets
Resposta	access-list 2 permit 192.168.6.0 0.0.0.255
3	Packets from hosts with 192.168 as the first two octets
Resposta	access-list 3 deny 192.168.0.0 0.0.255.255
4	Packets from any host
Resposta	access-list 4 permit any
5	Packets from subnet 10.1.200.0/21
Resposta	access-list 5 permit 10.1.200.0 0.0.7.255
6	Packets from subnet 10.1.200.0/27
Resposta	access-list 6 deny 10.1.200.0 0.0.0.31
7	Packets from subnet 172.20.112.0/23
Resposta	access-list 7 permit 172.20.112.0 0.0.1.255
8	Packets from subnet 172.20.112.0/26
Resposta	access-list 8 deny 172.20.112.0 0.0.0.63
9	Packets from subnet 192.168.9.64/28
Resposta	access-list 9 deny 192.168.9.64 0.0.0.15
10	Packets from subnet 192.168.9.64/30
Resposta	access-list 10 permit 192.168.9.64 0.0.0.3

Problema	Descubra em cada ACL o range (intervalo) dos Endereços IPs de Origem
1	access-list 1 permit 10.7.6.5
Resposta	
2	access-list 2 deny 192.168.4.0 0.0.0.127
Resposta	
3	access-list 3 permit 192.168.6.0 0.0.0.31
Resposta	
4	access-list 4 permit 172.30.96.0 0.0.3.255
Resposta	
5	access-list 5 permit 172.30.96.0 0.0.0.63
Resposta	
6	access-list 6 deny 10.1.192.0 0.0.0.31
Resposta	
7	access-list 7 permit 10.1.192.0 0.0.1.255
Resposta	
8	access-list 8 deny 10.1.192.0 0.0.63.255
Resposta	
9	access-list 9 permit 0.0.0.0 255.255.255.255
Resposta	
10	access-list 10 deny 192.168.10.1 0.0.0.0
Resposta	

Problema	Descubra em cada ACL o range (intervalo) dos Endereços IPs de Origem
1	access-list 1 permit 10.7.6.5
Resposta	One address: 10.7.6.5
2	access-list 2 deny 192.168.4.0 0.0.0.127
Resposta	192.168.4.0 – 192.168.4.127
3	access-list 3 permit 192.168.6.0 0.0.0.31
Resposta	192.168.6.0 – 192.168.6.31
4	access-list 4 permit 172.30.96.0 0.0.3.255
Resposta	172.30.96.1 – 172.30.99.255
5	access-list 5 permit 172.30.96.0 0.0.0.63
Resposta	172.30.96.0 – 172.30.96.63
6	access-list 6 deny 10.1.192.0 0.0.0.31
Resposta	10.1.192.0 – 10.1.192.31
7	access-list 7 permit 10.1.192.0 0.0.1.255
Resposta	10.1.192.0 – 10.1.193.255
8	access-list 8 deny 10.1.192.0 0.0.63.255
Resposta	10.1.192.0 – 10.1.255.255
9	access-list 9 permit 0.0.0.0 255.255.255.255 = access-list 9 permit any
Resposta	Qualquer Host/Subnet
10	access-list 10 deny 192.168.10.1 0.0.0.0 = access-list 10 deny 192.168.10.1
Resposta	One address: 192.168.10.1

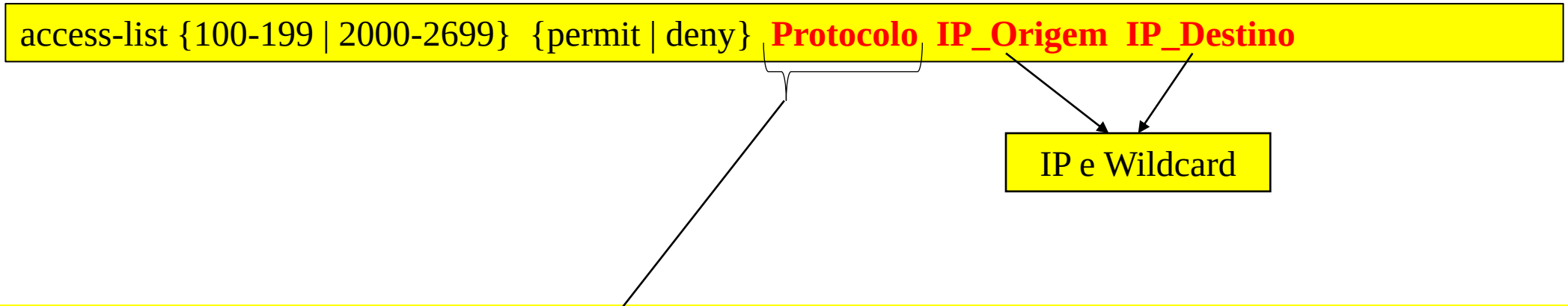
Extended IP ACL – Syntax

As Extended ACLs diferem das Standard ACLs principalmente por causa da grande variedade de campos de cabeçalho de pacote que podem ser usados para combinar um pacote.



Extended Numbered IP ACL – Syntax

As Extended ACLs diferem das Standard ACLs principalmente por causa da grande variedade de campos de cabeçalho de pacote que podem ser usados para combinar um pacote.




```
Router#configure terminal
Router(config)#access-list 100 deny ?
  ahp    Authentication Header Protocol
  eigrp  Cisco's EIGRP routing protocol
  esp    Encapsulation Security Payload
  gre    Cisco's GRE tunneling
  icmp   Internet Control Message Protocol
  ip     Any Internet Protocol
  ospf   OSPF routing protocol
  tcp    Transmission Control Protocol
  udp    User Datagram Protocol
```

Extended Numbered IP ACL – Syntax

As Extended ACLs diferem das Standard ACLs principalmente por causa da grande variedade de campos de cabeçalho de pacote que podem ser usados para combinar um pacote.

access-list {ID_Number} {permit | deny} **Protocolo IP_Origem Porta_Origem IP_Destino Porta_Destino**

{100-199 | 2000-2699}

```
Router#configure terminal
Router(config)#access-list 100 deny ?
  ahp    Authentication Header Protocol
  eigrp  Cisco's EIGRP routing protocol
  esp    Encapsulation Security Payload
  gre    Cisco's GRE tunneling
  icmp   Internet Control Message Protocol
  ip     Any Internet Protocol
  ospf   OSPF routing protocol
  tcp    Transmission Control Protocol
  udp    User Datagram Protocol
```

Extended Numbered IP ACL – Syntax

access-list {ID_Number} {permit | deny} Protocolo **IP_Origem** **Porta_Origem** **IP_Destino** **Porta_Destino**

```
Router#configure terminal
Router(config)#access-list 100 deny tcp 192.168.10.0 0.0.0.255 ?
A.B.C.D Destination address
any Any destination host
eq Match only packets on a given port number
gt Match only packets with a greater port number
host A single destination host
lt Match only packets with a lower port number
neq Match only packets not on a given port number
range Match only packets in the range of port numbers
```

```
Router#configure terminal
Router(config)#access-list 100 deny tcp 192.168.10.0 0.0.0.255 eq ?
  <0-65535>  Port number
  ftp        File Transfer Protocol (21)
  pop3       Post Office Protocol v3 (110)
  smtp       Simple Mail Transport Protocol (25)
  telnet     Telnet (23)
  www        World Wide Web (HTTP, 80)
```

Extended Numbered IP ACL – Syntax

```
Router#configure terminal
Router(config)#access-list 100 deny udp 192.168.10.0 0.0.0.255 eq ?
  <0-65535>      Port number
  bootpc         Bootstrap Protocol (BOOTP) client (68)
  bootps         Bootstrap Protocol (BOOTP) server (67)
  domain         Domain Name Service (DNS, 53)
  isakmp         Internet Security Association and Key Management Protocol (500)
  non500-isakmp  Internet Security Association and Key Management Protocol
                 (4500)
  snmp           Simple Network Management Protocol (161)
  tftp           Trivial File Transfer Protocol (69)
```

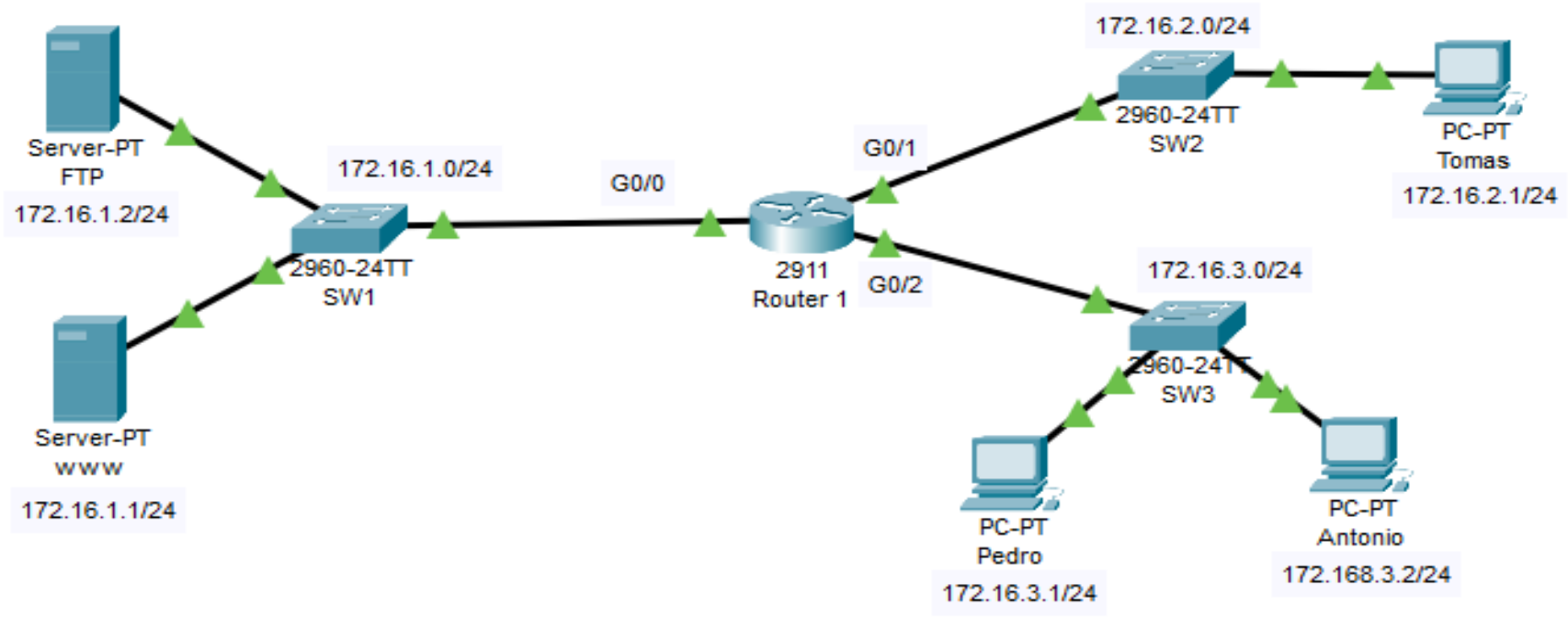
Extended Numbered IP ACL – Interpretando

Extented IP ACL	Significado
access-list 101 deny tcp any any	Bloquea qualquer pacote IP que tenha um cabeçalho TCP
access-list 101 deny udp any any	Bloquea qualquer pacote IP que tenha um cabeçalho UDP
access-list 101 deny icmp any any	Bloquea qualquer pacote IP que tenha um cabeçalho ICMP
access-list 101 deny ip host 1.1.1.1 host 2.2.2.2	Independentemente do protocolo, todos os pacotes IP do host 1.1.1.1 indo para o host 2.2.2.2 serão bloqueados.
access-list 101 deny udp 1.1.1.0 0.0.0.255 any	Bloquea todos os pacotes IP que têm um cabeçalho UDP com origem na sub-rede 1.1.1.0/24 e indo para qualquer destino

Extended Numbered IP ACL – Interpretando

Extented IP ACL	Significado
access-list 101 deny tcp any gt 49151 host 10.1.1.1 eq 23	Bloquea pacotes com um cabeçalho TCP, qualquer endereço IP de origem, com uma porta de origem maior que (gt) 49151, um endereço IP de destino 10.1.1.1 e uma porta de destino igual a (eq) 23.
access-list 101 deny tcp any host 10.1.1.1 eq 23	O mesmo que o exemplo anterior, mas agora com qualquer porta de origem. Parâmetro (porta_origem) é omitido neste caso.
access-list 101 deny tcp any host 10.1.1.1 eq telnet	O mesmo que no exemplo anterior. A palavra-chave telnet é usada ao invés da porta 23.
access-list 101 deny udp 1.0.0.0 0.255.255.255 lt 1023 any	Bloquea todos pacotes com origem na rede 1.0.0.0/8, usando cabeçalho UDP com porta de origem menor que (lt) 1023, com qualquer endereço IP de destino

Extended Numbered IP ACL – Exemplo



Rules:

1. Deny all packets from Antonio's Host going to FTP Server;
2. Deny all packets from WWW replying to Tomas's Host requests;
3. All other communications are allowed.

Extended Numbered IP ACL – Exemplo 1 Configs

```
R1# configure terminal
R1(config)# access-list 101 deny tcp host 172.16.3.1 host 172.16.1.2 eq ftp
R1(config)# access-list 101 permit ip any any
R1(config)# access-list 102 deny tcp host 172.16.1.1 eq www host 172.16.2.1
R1(config)# access-list 102 permit ip any any
```

```
R2(config)# interface gig0/0
R2(config-if)# ip access-group 102 in

R2(config)# interface gig0/2
R2(config-if)# ip access-group 101 in
```

Extended Named IP ACL – Exemplo Configs

```
Router# configure terminal
Router(config)# ip access-list extended Name_ACL
Router(config-ext-nacl)# permit tcp host 10.1.1.2 eq www any
Router(config-ext-nacl)# deny udp host 10.1.1.1 10.1.2.0 0.0.0.255
Router(config-ext-nacl)# deny ip 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255
Router(config-ext-nacl)# deny ip 10.1.2.0 0.0.0.255 10.2.3.0 0.0.0.255
Router(config-ext-nacl)# permit ip any any
Router(config-ext-nacl)# interface serial1
Router(config-if)# ip access-group Name_ACL out
```

```
Router# show running-config
interface serial 1
ip access-group Name_ACL out
!
ip access-list extended Name_ACL
permit tcp host 10.1.1.2 eq www any
deny udp host 10.1.1.1 10.1.2.0 0.0.0.255
deny ip 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255
deny ip 10.1.2.0 0.0.0.255 10.2.3.0 0.0.0.255
permit ip any any
```

Extended Named IP ACL – Exemplo Configs

```
Router# configure terminal
Router(config)# ip access-list extended Name_ACL
Router(config-ext-nacl)# no deny ip 10.1.2.0 0.0.0.255 10.2.3.0 0.0.0.255
```

```
Router# show access-list
Extended IP access list Name_ACL
10 permit tcp host 10.1.1.2 eq www any
20 deny udp host 10.1.1.1 10.1.2.0 0.0.0.255
30 deny ip 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255
50 permit ip any any
```

⚠ Considerações Importantes – Extended IP ACL

- Sugestão: Coloque a ACL Extended o mais próximo possível da origem dos pacotes que serão filtrados;
- Por defeito, sempre que se adiciona uma nova regra na ACL ela vai para o final da lista a não ser que ela sofra alguma influência (em casos como Extended Named);

Dúvidas?

Exercícios

Problema	Crie uma Extended Numbered ACL para cada problema e filtre (deny ou permit) o tráfego a sua escolha
1	From web client 10.1.1.1, sent to a web server in subnet 10.1.2.0/24.
Resposta	
2	From Telnet client 172.16.4.3/25, sent to a Telnet server in subnet 172.16.3.0/25. Match all hosts in the client's subnet as well.
Resposta	
3	ICMP messages from the subnet in which 192.168.7.200/26 resides to all hosts in the subnet where 192.168.7.14/29 resides
Resposta	
4	From web server 10.2.3.4/23's subnet to clients in the same subnet as host 10.4.5.6/22.
Resposta	
5	From Telnet server 172.20.1.0/24's subnet, sent to any host in the same subnet as host 172.20.44.1/23.
Resposta	
6	From web client 192.168.99.99/28, sent to a web server in subnet 192.168.176.0/28. Match all hosts in the client's subnet as well.
Resposta	
7	ICMP messages from the subnet in which 10.55.66.77/25 resides to all hosts in the subnet where 10.66.55.44/26 resides.
Resposta	
8	Any and every IPv4 packet .
Resposta	

Problema	Crie uma Extended Numbered ACL para cada problema e filtre (deny ou permit) o tráfego a sua escolha
1	From web client 10.1.1.1, sent to a web server in subnet 10.1.2.0/24.
Resposta	access-list 101 deny tcp host 10.1.1.1 10.1.2.0 0.0.0.255 eq www
2	From Telnet client 172.16.4.3/25, sent to a Telnet server in subnet 172.16.3.0/25. Match all hosts in the client's subnet as well.
Resposta	access-list 102 permit tcp 172.16.4.0 0.0.0.127 172.16.3.0 0.0.0.127 eq telnet
3	ICMP messages from the subnet in which 192.168.7.200/26 resides to all hosts in the subnet where 192.168.7.14/29 resides
Resposta	access-list 103 deny icmp 192.168.7.192 0.0.0.63 192.168.7.8 0.0.0.7
4	From web server 10.2.3.4/23's subnet to clients in the same subnet as host 10.4.5.6/22.
Resposta	access-list 104 permit tcp 10.2.2.0 0.0.1.255 eq www 10.4.4.0 0.0.3.255
5	From Telnet server 172.20.1.0/24's subnet, sent to any host in the same subnet as host 172.20.44.1/23.
Resposta	access-list 105 deny tcp 172.20.1.0 0.0.0.255 eq 23 172.20.44.0 0.0.1.255
6	From web client 192.168.99.99/28, sent to a web server in subnet 192.168.176.0/28. Match all hosts in the client's subnet as well.
Resposta	access-list 106 permit tcp 192.168.99.96 0.0.0.15 192.168.176.0 0.0.0.15 eq www
7	ICMP messages from the subnet in which 10.55.66.77/25 resides to all hosts in the subnet where 10.66.55.44/26 resides.
Resposta	access-list 107 deny icmp 10.55.66.0 0.0.0.127 10.66.55.0 0.0.0.63
8	Any and every IPv4 packet .
Resposta	access-list 108 deny ip any any

Laboratórios

OBRIGADO !!!