



Monitoramento e Gerenciamento de Redes

- Segurança da Informação e Access-Control-List: parte III -

Mauro Cesar Bernardes

São Paulo, 2024

Plano de Aula

- **Objetivo**

- Revisar os conceitos de ACL estendida
- Compreender a utilização de *Máscara Curinga*

- **Conteúdo**

- Configurando roteador para utilização de Listas de Controle de Acesso Estendidas com Máscara Curinga

- **Metodologia**

- Aula expositiva sobre os conceitos e desenvolvimento de atividade prática com configuração em simulador (*Packet Tracer*) de Listas de Controle de Acesso Estendidas em roteador.

Agenda do Primeiro semestre

Janeiro 2024							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
1	1	2	3	4	5	6	7
2	8	9	10	11	12	13	14
3	15	16	17	18	19	20	21
4	22	23	24	25	26	27	28
5	29	30	31				

Calendário de Fevereiro 2024

Nº	Se	Te	Qu	Qu	Se	Sá	Do
5				1	2	3	4
6	5	6	7	8	9	10	11
7	12	13	14	15	16	17	18
8	19	20	21	22	23	24	25
9	26	27	28	29			


Início das aulas

 Março 2024							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
9					1	2	3
10	4	5	6	7	8	9	10
11	11	12	13	14	15	16	17
12	18	19	20	21	22	23	24
13	25	26	27	28	29	30	31

1º Checkpoint da disciplina

A calendar for April 2024. The days of the week are listed at the top: Se, Te, Qu, Qu, Se, Sá, Do. The dates are arranged in rows. The date 21 is circled in red.

Nº	Se	Te	Qu	Qu	Se	Sá	Do
14	1	2	3	4	5	6	7
15	8	9	10	11	12	13	14
16	15	16	17	18	19	20	21
17	22	23	24	25	26	27	28
18	29	30					

 Maio 2024							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
18			<u>1</u>	2	3	4	5
19	6	7	8	9	10	11	12
20	<u>13</u>	<u>14</u>	<u>15</u>	<u>16</u>	<u>17</u>	<u>18</u>	19
21	20	21	22	23	24	25	26
22	27	28	29	<u>30</u>	31		

3º Checkpoint da disciplina

Junho 2024							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
22						1	2
23	3	4	5	6	7	8	9
24	10	11	12	13	14	15	16
25	17	18	19	20	21	22	23
26	24	25	26	27	28	29	30

Roteador em uma Rede Doméstica

The image shows a web browser window displaying the Vivo router's configuration page. The browser's address bar shows "Vivo" and "Não seguro". The page features the Vivo logo and a language selector for "English | Português".

On the left, a dark purple sidebar menu contains the following items:

- > Status
- ∨ Configurações
 - Internet
 - Rede Local
 - Wi-fi 2.4 GHz
 - Wi-fi 5 GHz
 - Jogos & Aplicativos
 - Firewall** (highlighted with a red and yellow arrow)
 - Modo da WAN
- > Gerenciamento
- > Sobre o dispositivo

The main content area is titled "AUTENTICAÇÃO" and displays a login form. It includes the following text and fields:

- Header: "Você não está Autenticado"
- Message: "Para acessar as configurações você precisa estar autenticado."
- Fields: "Usuário:" and "Senha:" with corresponding input boxes.
- Button: "ENTRAR" (green)

Roteador em uma Rede Doméstica

The screenshot shows the Vivo router's web interface. A sidebar on the left contains a menu with the following items: Status, Configurações, Gerenciamento, and Sobre o dispositivo. A red arrow points from the 'Configurações' item to the 'FIREWALL' section in the main content area. The 'FIREWALL' section is titled 'POLITICA PADRÃO' and contains two sections: 'Estado:' and 'Ping Interface WAN'. Both sections have radio buttons for 'Aceita' and 'Rejeita', with 'Rejeita' being selected. Below these is the 'ADICIONAR' section, which includes a form for adding a rule. The form has fields for 'Nome da Regra:', 'Protocolo:' (set to 'TCP'), 'Porta Local:', 'Porta Remota:', 'IP Local:', and 'IP Remoto:'. The 'Ação' dropdown menu is open, showing options: 'Rejeita Local', 'Rejeita Remoto', 'Rejeita Ambos', 'Aceita Local', 'Aceita Remoto', and 'Aceita Ambos'. The 'Rejeita Local' option is selected. Below the form is a 'Rules List' table with columns: Rule Name, Local, Action, Remote, and Modify. The table is currently empty.

Vivo

English | Português | Sair

▼ Status

> Configurações

> Gerenciamento

> Sobre o dispositivo

FIREWALL

POLITICA PADRÃO

Estado: ☐ Aceita ☒ Rejeita

Ping Interface WAN

Estado: ☐ Aceita ☒ Rejeita

ADICIONAR

Restrinja ou permita tráfegos com origem ou destino a sua rede.

Nome da Regra: Protocolo:

Porta Local: Porta Remota:

IP Local: IP Remoto:

Ação:

Local ☒ Remoto

ADICIONAR APAGAR

Rules List

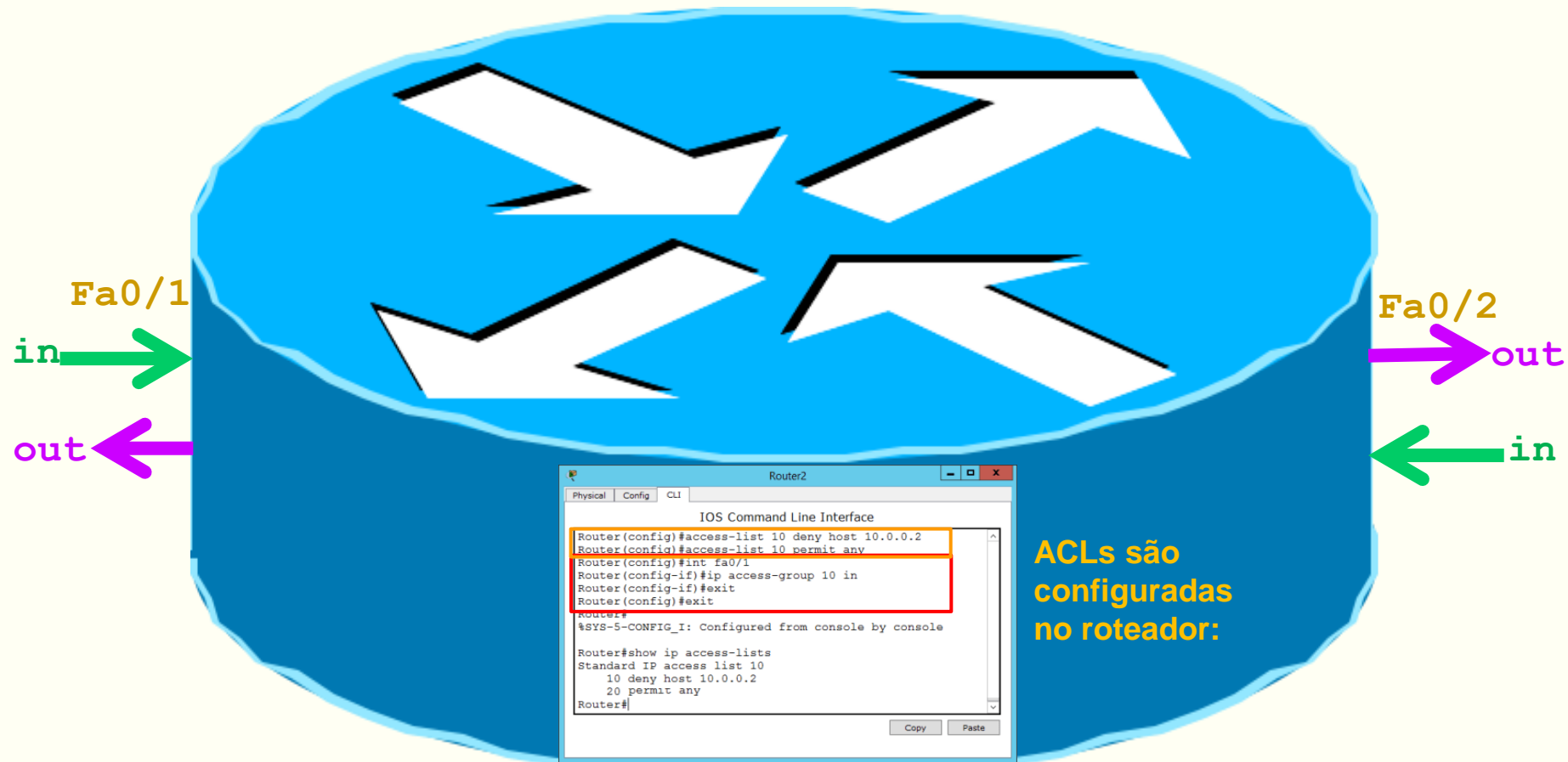
Rule Name:	Local	Action	Remote	Modify
Name	Protocol:	Port	IP	Policy

**Segurança com listas de
controle de acesso**
(*access-control-list* estendidas)

Extended Access Control List

- As ACLs estendidas são usadas mais frequentemente para testar condições por proporcionarem um intervalo maior de controle que as ACLs padrão.
- As ACLs estendidas verificam os endereços de origem e endereços de destino dos pacotes.
- ACLs estendidas também podem verificar protocolos específicos (IP, TCP, UDP) números de portas e outros parâmetros.
- Isso torna mais flexível o processo de descrever que tipo de verificação a ACL fará.
- O tráfego de pacotes pode ser permitido (**permi t**) ou recusado (**deny**) baseada em onde o pacote foi originado e/ou no seu destino.

Access-List Estendidas: recordando

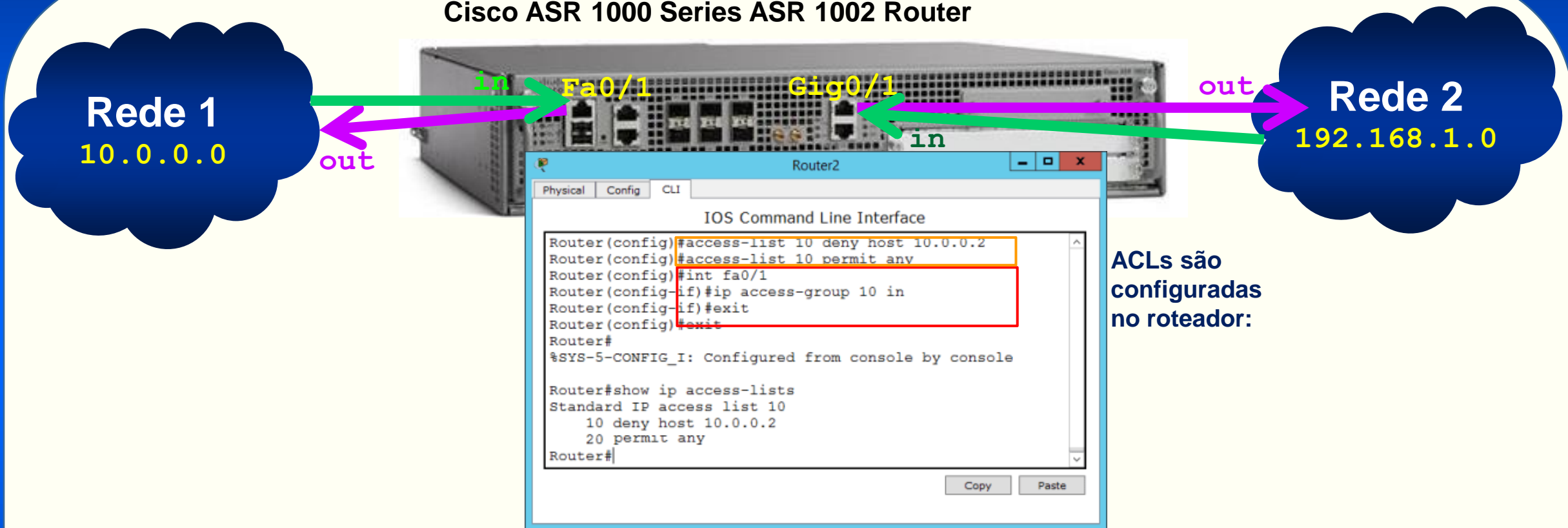


Para seu funcionamento ACLs precisam ser associadas a uma interface configuradas no roteador.
Na entrada do roteador (in) ou na saída do Roteador (out).

No exemplo: pacotes com origem no host 10.0.0.2 serão negados (deny) na entrada da interface fa0/1 e os pacotes em qualquer outra origem (any) serão permitidos (permit) pela interface.

Access Control Lists (ACL): recordando

Cisco ASR 1000 Series ASR 1002 Router



ACLs são configuradas no roteador:

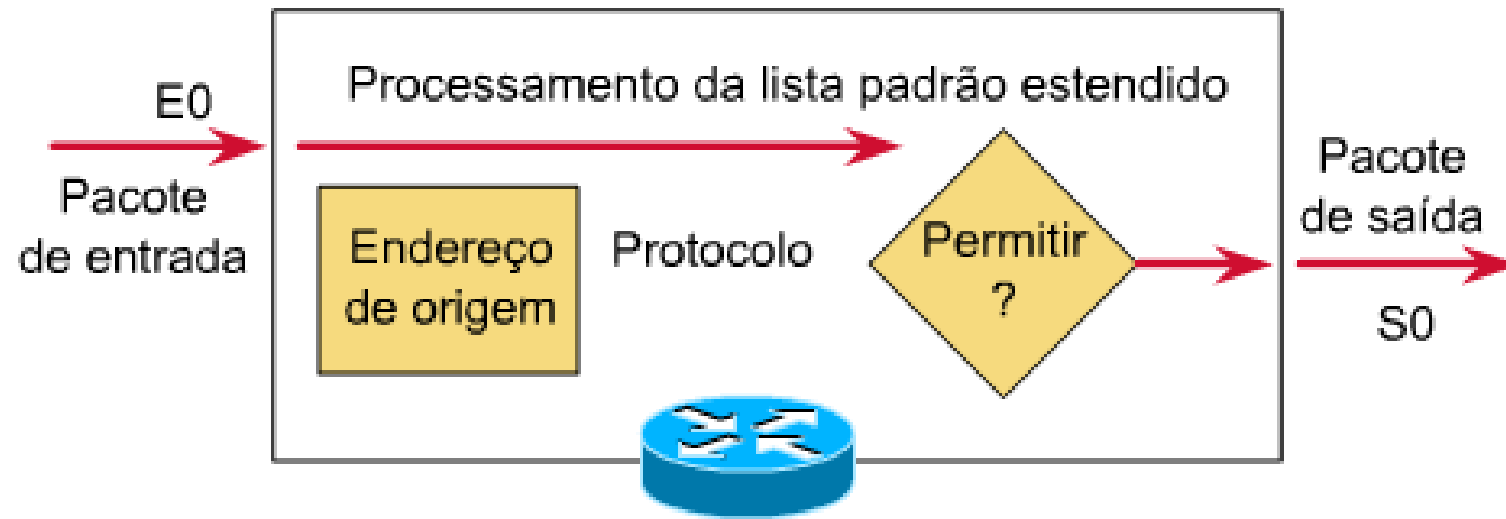
Para seu funcionamento ACLs precisam ser associadas a uma interface configuradas no roteador.

Na entrada do roteador (in) ou na saída do Roteador (out).

No exemplo:

pacotes com origem no host 10.0.0.2 serão negados (deny) na entrada da interface fa0/1 e os pacotes em qualquer outra origem (any) serão permitidos (permit) pela interface.

Extended Access Control List



Padrão

- ◆ Especificações de endereço mais simples
- ◆ Geralmente permite ou recusa todo o conjunto de protocolos


Estendida

- ◆ Especificações de endereço mais complexas

Protocolos com ACLs

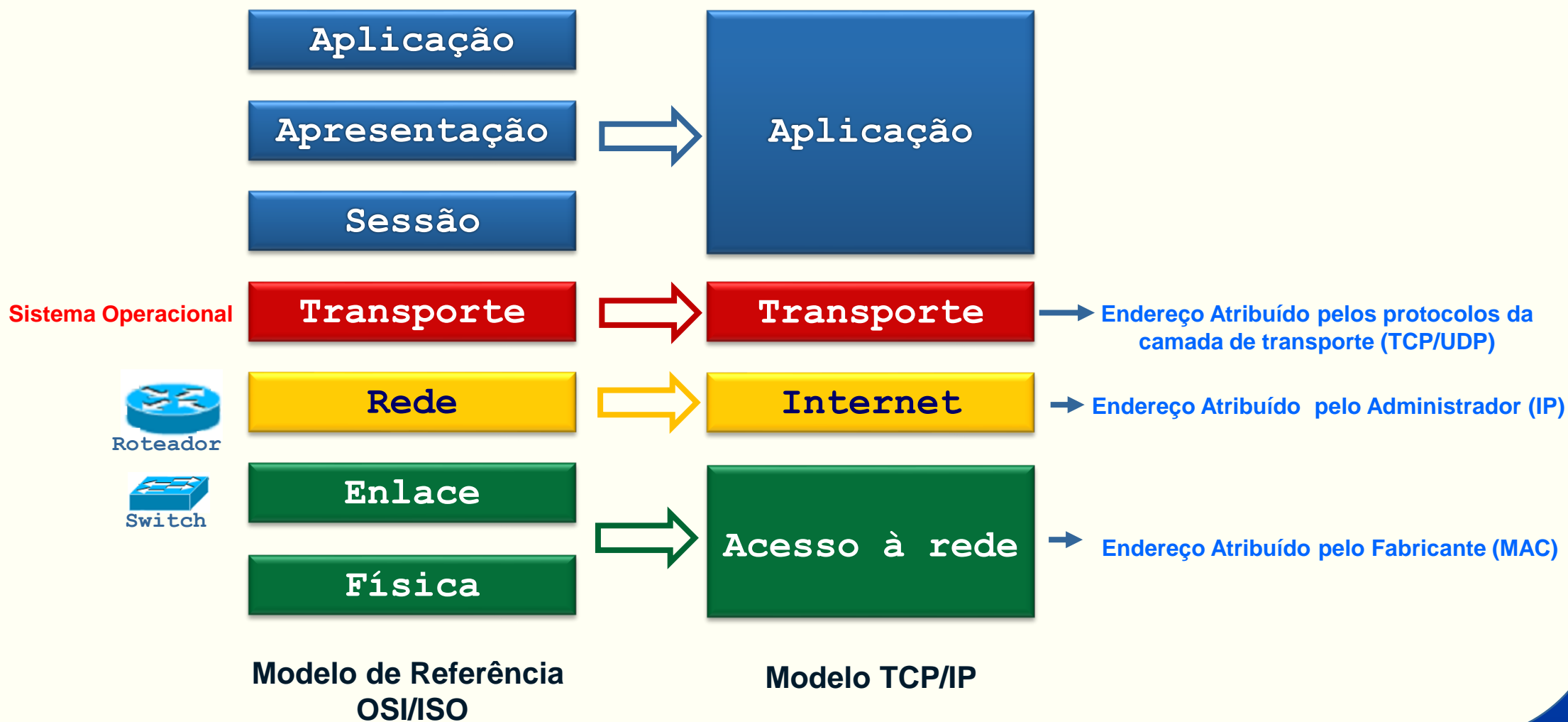
especificados por números

Protocolo	Intervalo
IP	1-99
IP estendido	100-199
AppleTalk	600-699
IPX	800-899
IPX estendido	900-999
Protocolo de anúncio de serviços IPX	1000-1099

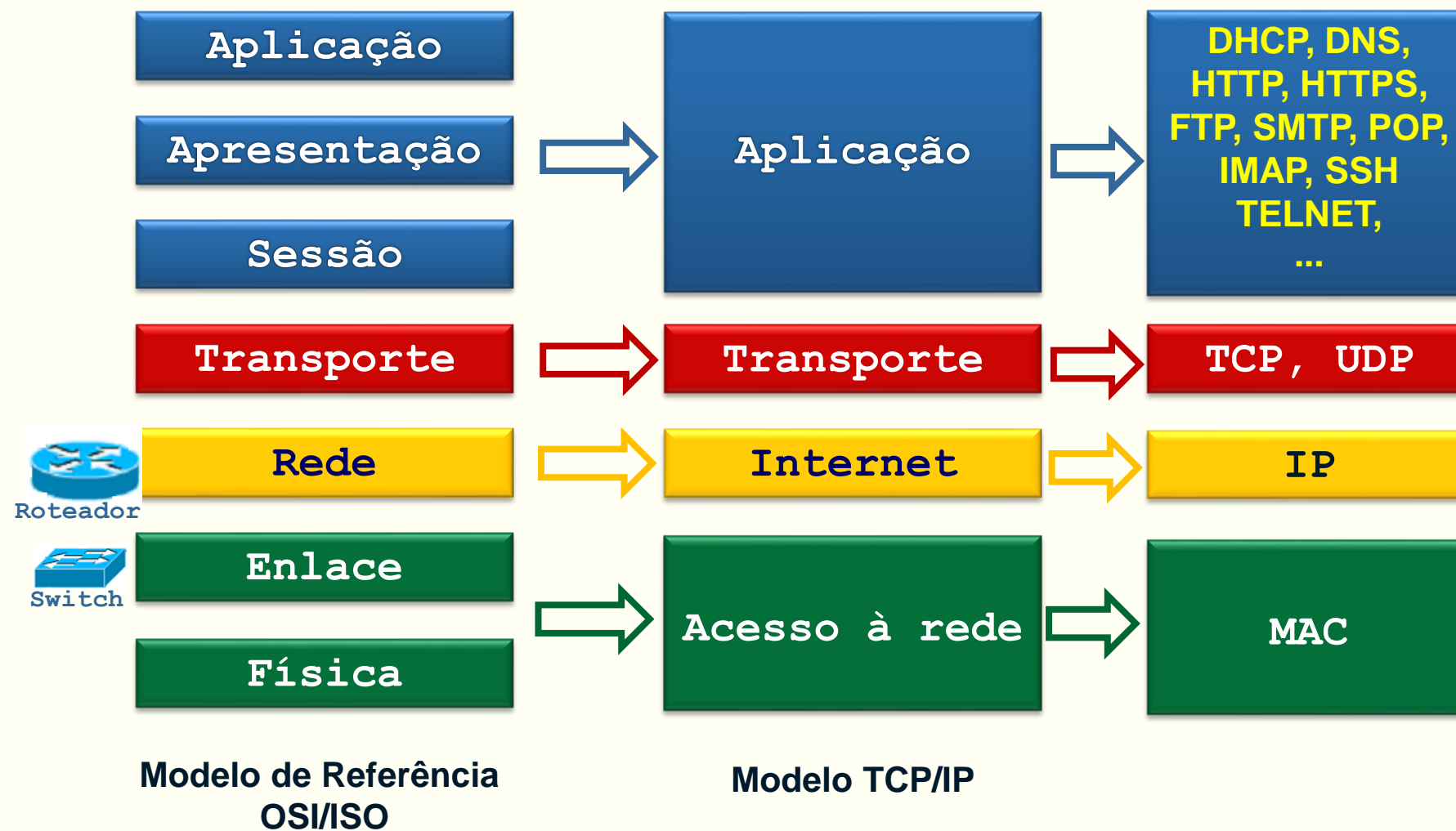


**Segurança com listas de
controle de acesso**
(*access-control-list* estendidas)
(Portas TCP/UDP)

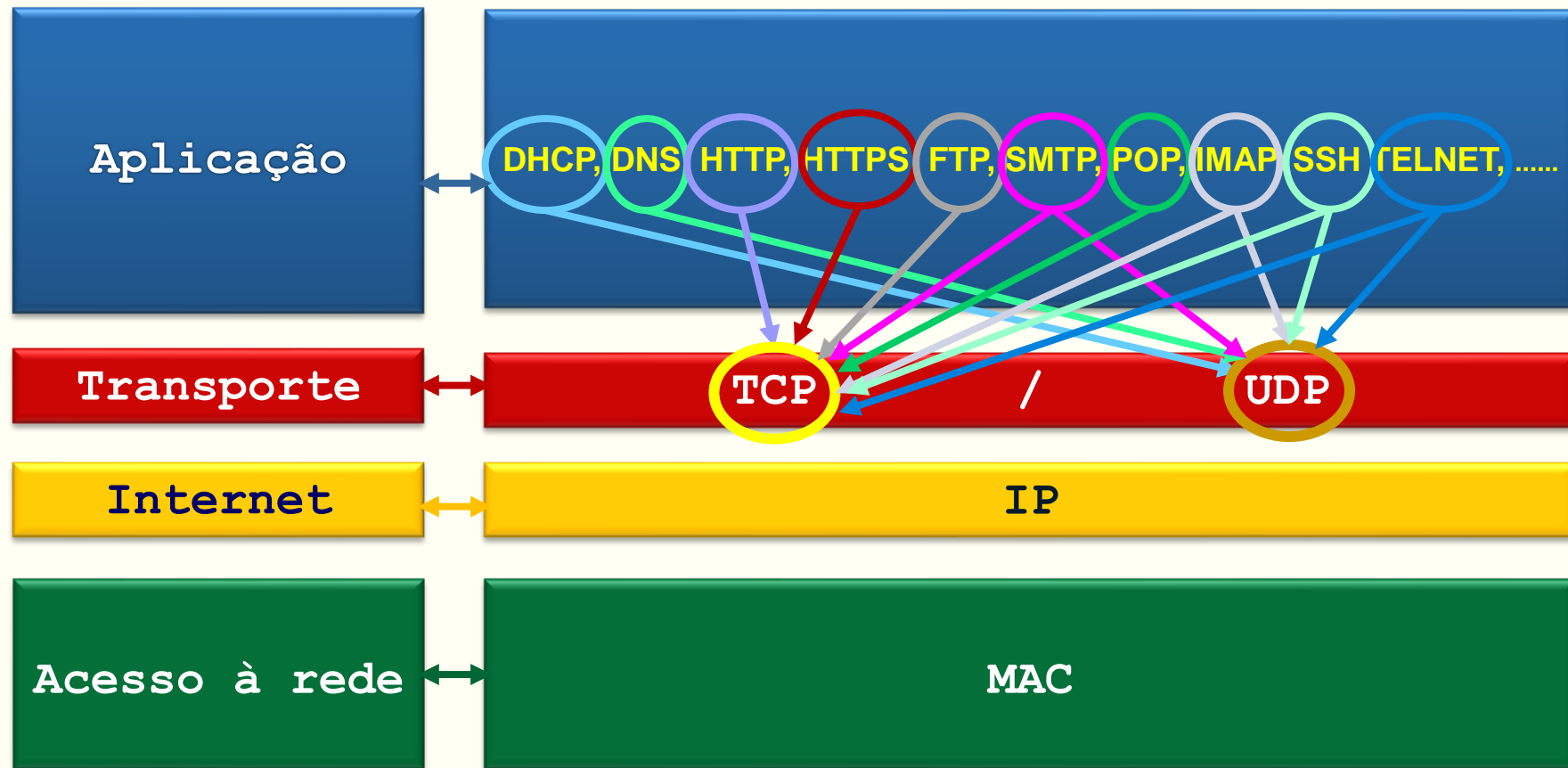
Revisão: OSI x TCP/IP



Revisão: OSI x TCP/IP

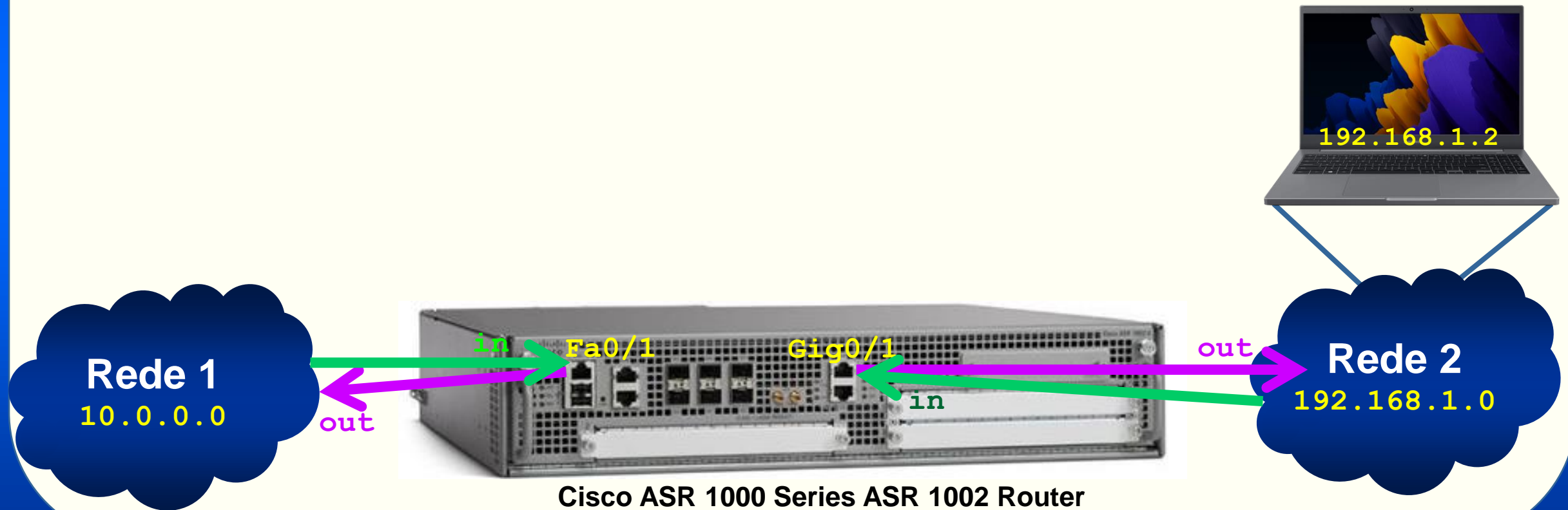


Revisão: TCP/IP

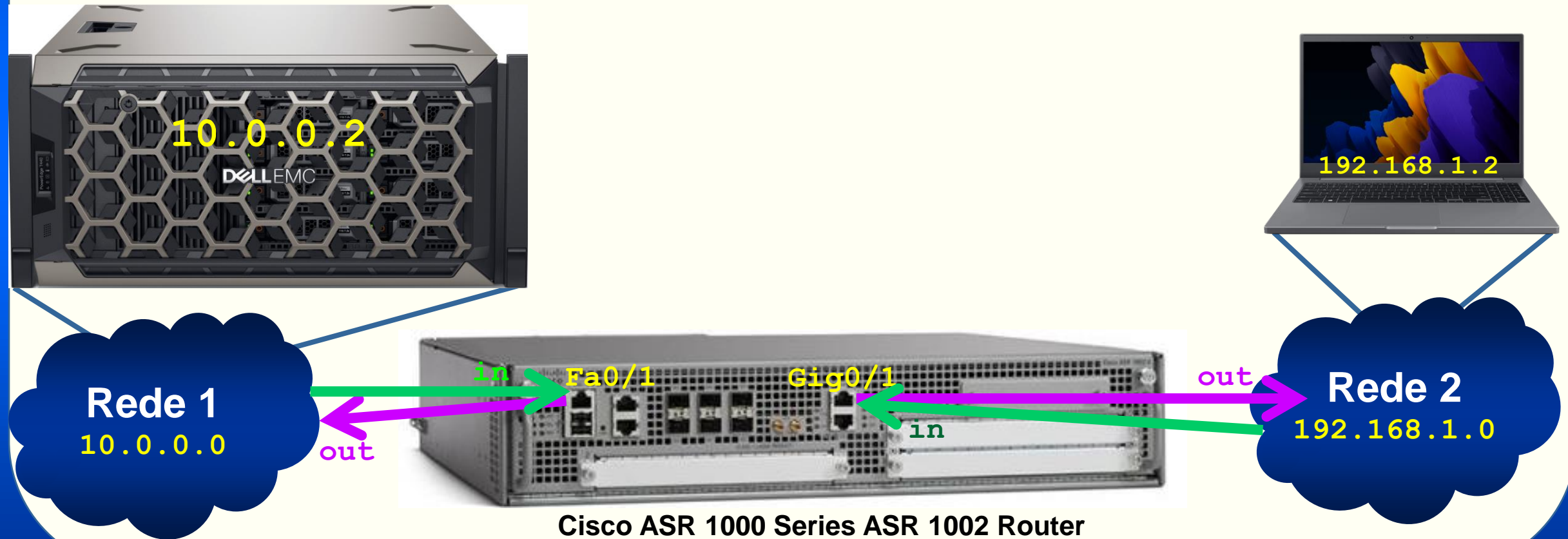


Modelo TCP/IP

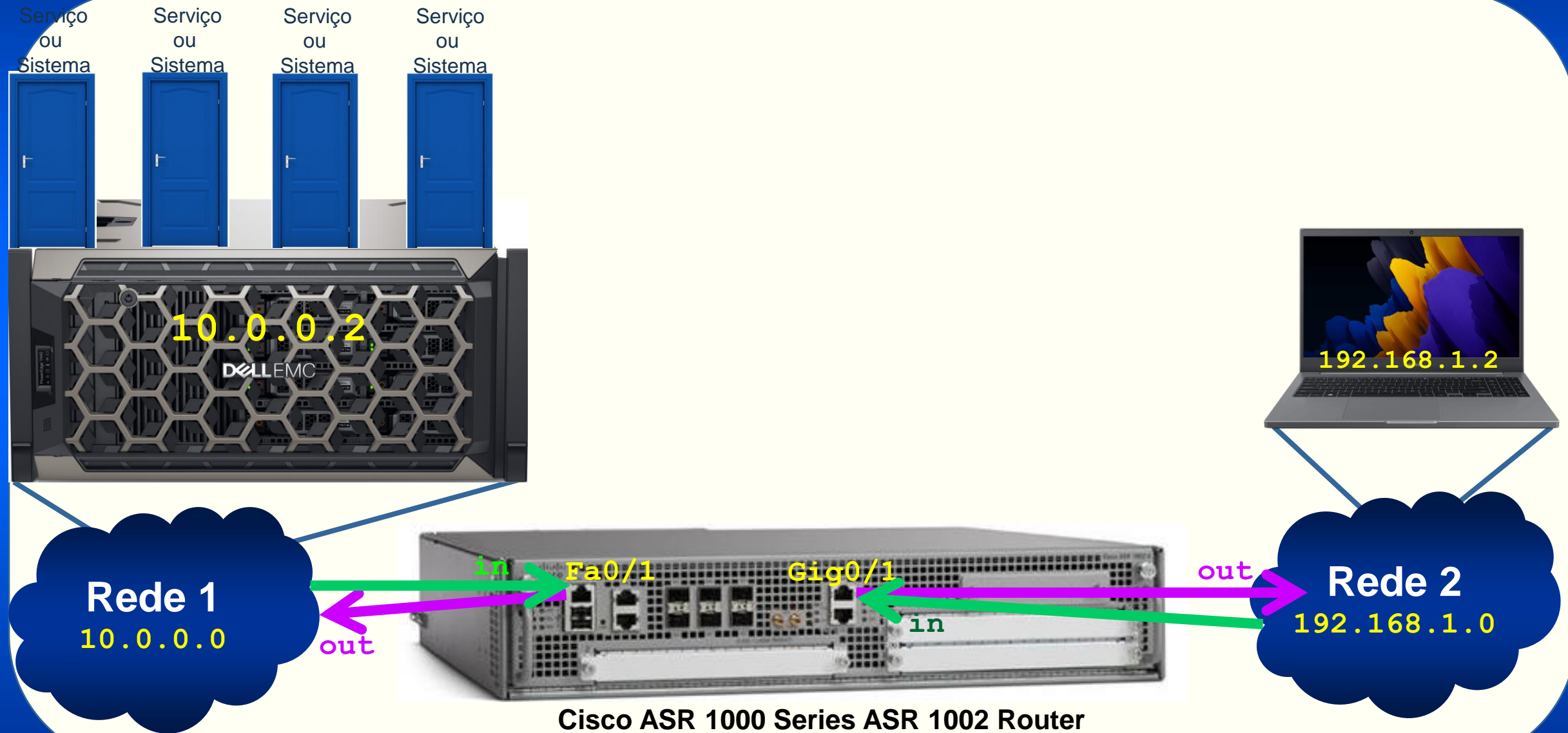
Access Control List: recordando



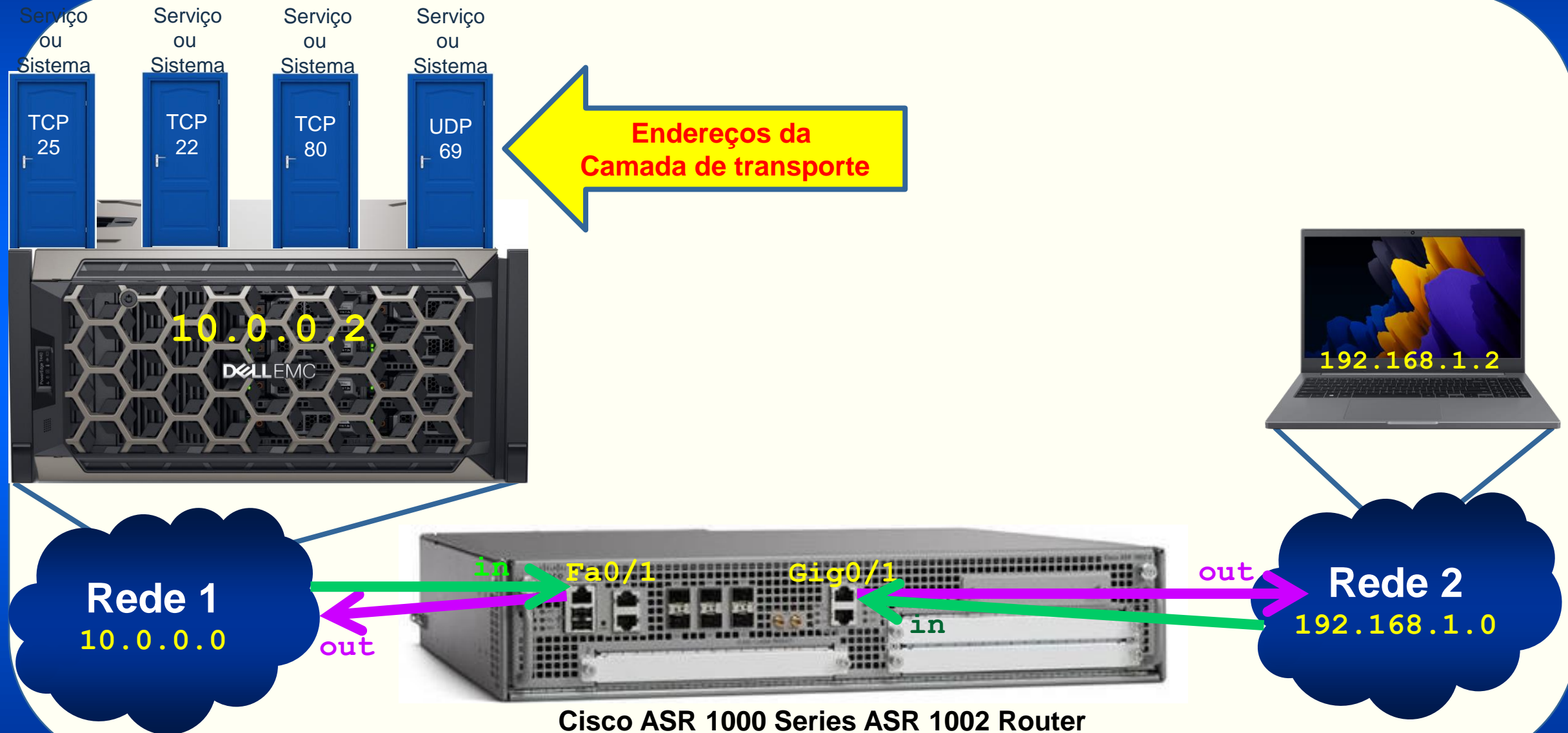
Access Control List: recordando



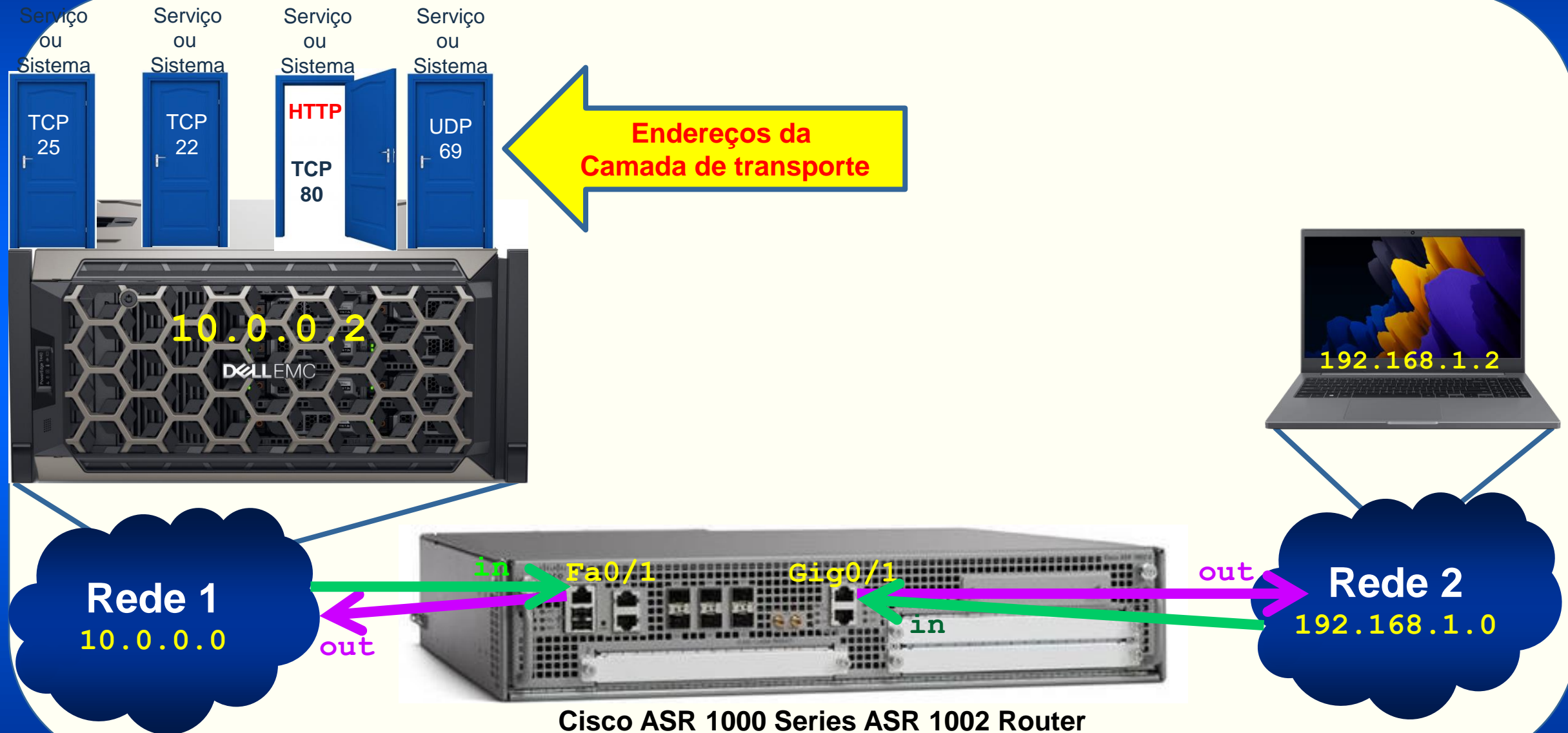
Access Control List: recordando



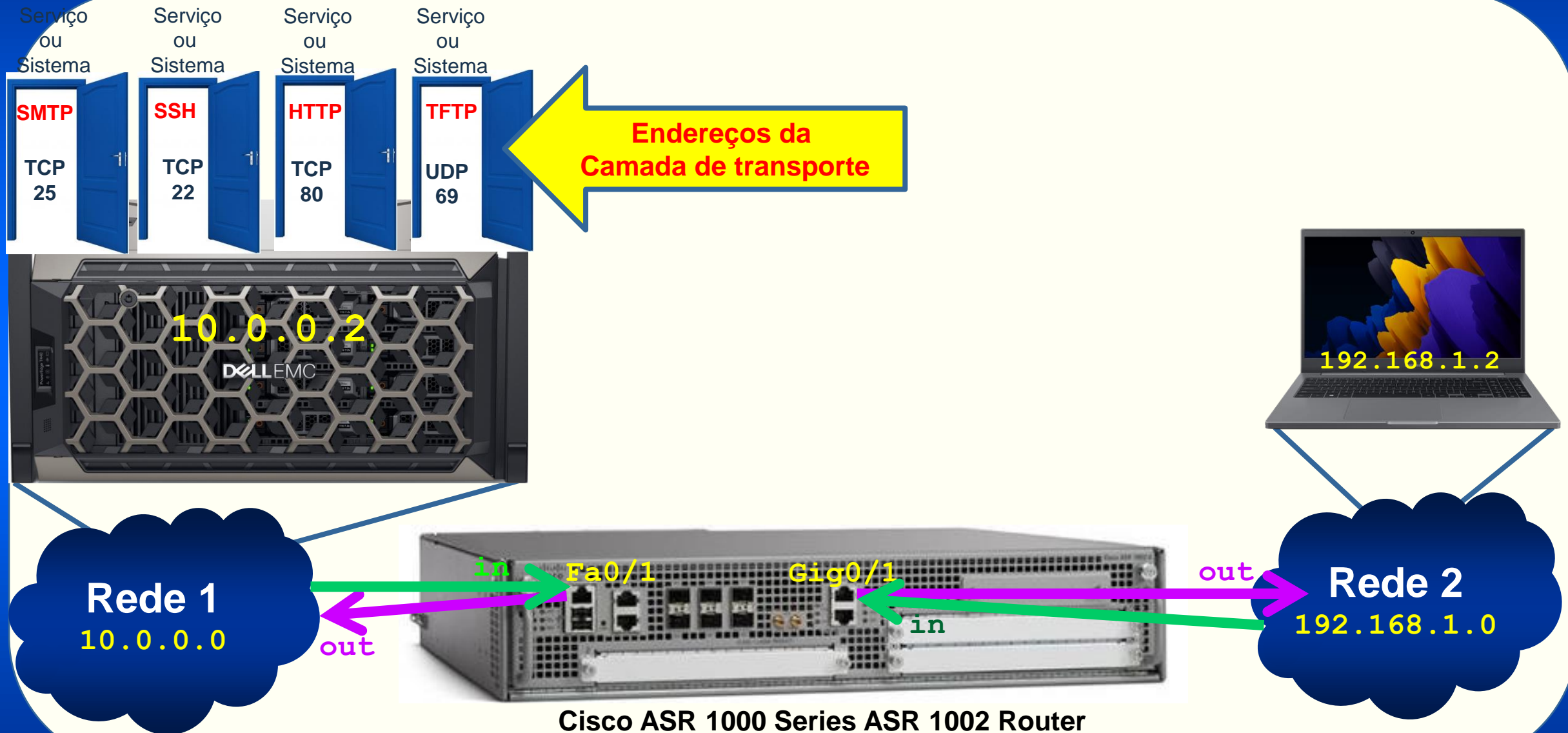
Access Control List: recordando



Access Control List: recordando

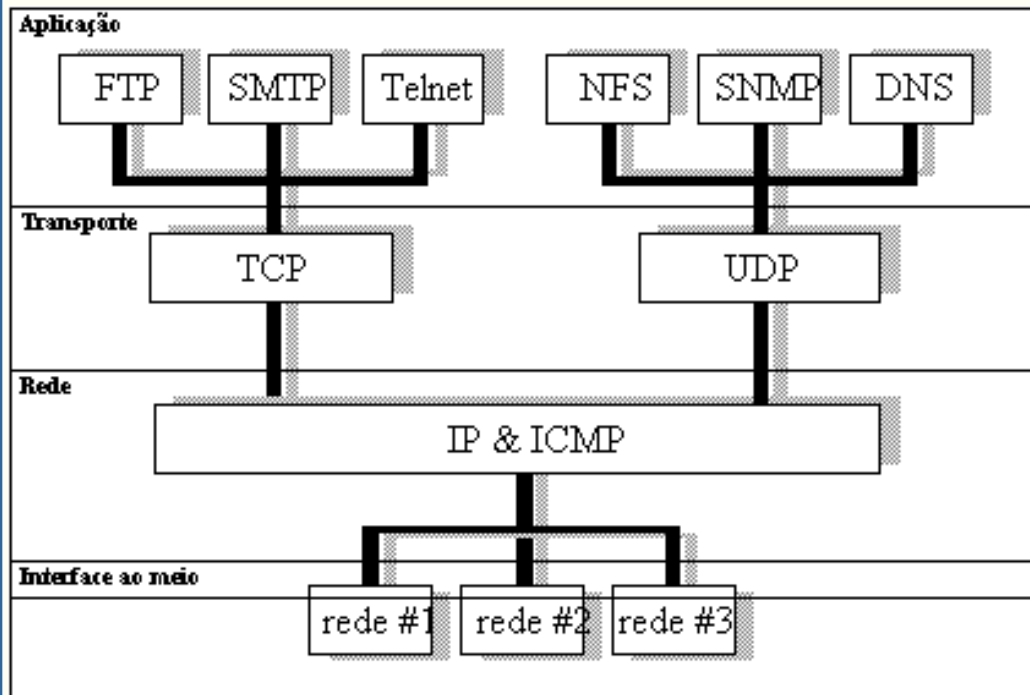


Access Control List: recordando



Portas TCP e Portas UDP

- https://pt.wikipedia.org/wiki/Lista_de_portas_dos_protocolos_TCP_e_UDP



PORT NUMBER	TRANSPORT PROTOCOL	SERVICE NAME	RFC
20, 21	TCP	File Transfer Protocol (FTP)	RFC 959
22	TCP and UDP	Secure Shell (SSH)	RFC 4250-4256
23	TCP	Telnet	RFC 854
25	TCP	Simple Mail Transfer Protocol (SMTP)	RFC 5321
53	TCP and UDP	Domain Name Server (DNS)	RFC 1034-1035
67, 68	UDP	Dynamic Host Configuration Protocol (DHCP)	RFC 2131
69	UDP	Trivial File Transfer Protocol (TFTP)	RFC 1350
80	TCP	HyperText Transfer Protocol (HTTP)	RFC 2616
110	TCP	Post Office Protocol (POP3)	RFC 1939
119	TCP	Network News Transport Protocol (NNTP)	RFC 8977
123	UDP	Network Time Protocol (NTP)	RFC 5905
135-139	TCP and UDP	NetBIOS	RFC 1001-1002
143	TCP and UDP	Internet Message Access Protocol (IMAP4)	RFC 3501
161, 162	TCP and UDP	Simple Network Management Protocol (SNMP)	RFC 1901-1908, 3411-3418
179	TCP	Border Gateway Protocol (BGP)	RFC 4271
389	TCP and UDP	Lightweight Directory Access Protocol	RFC 4510
443	TCP and UDP	HTTP with Secure Sockets Layer (SSL)	RFC 2818
500	UDP	Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)	RFC 2408 - 2409
636	TCP and UDP	Lightweight Directory Access Protocol over TLS/SSL (LDAPS)	RFC 4513
989/990	TCP	FTP over TLS/SSL	RFC 4217

<https://ipwithease.com>

Exemplos de Número de Portas

Portas 0 a 995 [[editar](#) | [editar código-fonte](#)]

Porta	Descrição
0/TCP,UDP	Reservada.
1/TCP,UDP	TCPMUX (Serviço de porta TCP multiplexador)
5/TCP,UDP	RJE (Remote Job Entry - Entrada de trabalho remoto)
7/TCP,UDP	ECHO protocol
9/TCP,UDP	DISCARD protocol
11/TCP,UDP	SYSTAT protocol
13/TCP,UDP	DAYTIME protocol
17/TCP,UDP	QOTD (Quote of the Day) protocol
18/TCP,UDP	Message Send Protocol (Protocolo de envio de mensagem)
19/TCP,UDP	CHARGEN protocol (Character Generator Protocol - Protocolo de geração de caracter)
20/TCP	FTP (File Transfer protocol - Protocolo de transferência de arquivo) - data port
21/TCP	FTP (File Transfer protocol - Protocolo de transferência de arquivo) - control (command) port
22/TCP,UDP	SSH (Secure Shell - Shell seguro) - Usada para logins seguros, transferência de arquivos e redirecionamento de porta
23/TCP,UDP	Telnet protocol - Comunicação de texto sem encriptação
25/TCP,UDP	SMTP (Simple Mail Transfer Protocol - Protocolo simples de envio de e-mail) - usada para roteamento de e-mail entre servidores (Atualmente é utilizada a porta 587, conforme Comitê Gestor da Internet no Brasil CGI.br)
26/TCP,UDP	RSFTP - protocolo similar ao FTP
35/TCP,UDP	QMS Magicolor 2 printer
37/TCP,UDP	TIME protocol (Protocolo de Tempo)
38/TCP,UDP	Route Access Protocol (Protocolo de Acesso ao roteador)
39/TCP,UDP	Resource Location Protocol (Protocolo de localização de recursos)
41/TCP,UDP	Graphics (gráficos)
42/TCP,UDP	Host Name Server (Servidor do Nome do Host)
42/TCP,UDP	WINS [3]
43/TCP	WHOIS (protocolo de consulta de informações de contato e DNSprotocol)
49/TCP,UDP	TACACS Login Host protocol(Protocolo de Login no Host)
53/TCP,UDP	DNS (Domain Name System - Sistema de nome de domínio)
57/TCP	MTP, Mail Transfer Protocol (Protocolo de transferência de e-mail)
67/UDP	BOOTP (BootStrap Protocol) server; também utilizada por DHCP (Protocolo de configuração dinâmica do Host)
68/UDP	BOOTP client; também utilizada por DHCP
69/UDP	TFTP (Trivial File Transfer Protocol) (Protocolo de transferência de arquivo trivial)

Exemplos de Número de Portas

Portas 0 a 995 [[editar](#) | [editar código-fonte](#)]

Porta	Descrição
69/UDP	TFTP (Trivial File Transfer Protocol) (Protocolo de transferência de arquivo trivial)
70/TCP	Gopher (Protocolo para indexar repositórios)
79/TCP	Finger protocol
80/TCP	HTTP (HyperText Transfer Protocol - Procolo de transferência de HiperTexto) - usada para transferir páginas WWW
80/TCP	HTTP Alternate (HyperText Transfer Protocol - Protocolo de transferência de HiperTexto)
81/TCP	Skype protocol
81/TCP	Torpark - Onion routing ORport
82/UDP	Torpark - Control Port
88/TCP	Kerberos (Protocolo de comunicações individuais seguras e identificadas) - authenticating agent
101/TCP	HOSTNAME
102/TCP	ISO-TSAP protocol
107/TCP	Remote Telnet Service (Serviço remoto Telnet)
109/TCP	POP (Post Office Protocol): Protocolo de Correio Eletrônico, versão 2
110/TCP	POP3 (Post Office Protocol version 3): Protocolo de Correio Eletrônico, versão 3 - usada para recebimento de e-mail
111/TCP,UDP	sun protocol (Protocolo da sun)
113/TCP	ident - antigo identificador de servidores, ainda usada em servidores IRC para identificar seus usuários
115/TCP	SFTP, (Simple File Transfer Protocol) (Protocolo de simples transferência de arquivo)
117/TCP	UUCP-PATH
118/TCP,UDP	SQL Services
119/TCP	NNTP (Network News Transfer Protocol) (Protocolo de transferência de notícias na rede) - usada para recebimento de mensagens de newsgroups
123/UDP	NTP (Network Time Protocol) (Protocolo de tempo na rede) - usada para sincronização de horário
135/TCP,UDP	EPMAP (End Point Mapper) / Microsoft RPC Locator Service (Microsoft RPC Serviço de localização)
137/TCP,UDP	NetBIOS NetBIOS Name Service
138/TCP,UDP	NetBIOS NetBIOS Datagram Service (Serviço de datagrama NetBios)
139/TCP,UDP	NetBIOS NetBIOS Session Service (Serviço de sessão NetBios)
143/TCP,UDP	IMAP4 (Internet Message Access Protocol 4) (Protocolo de Acesso a mensagens na Internet) - usada para recebimento de e-mail
152/TCP,UDP	BFTP, Background File Transfer Program (Protocolo de transferência de arquivo em Background(fundo))
153/TCP,UDP	SGMP, Simple Gateway Monitoring Protocol (Protocolo de simples monitoramento do gateway)
156/TCP,UDP	SQL Service (Serviço SQL)
158/TCP,UDP	DMSP, Distributed Mail Service Protocol (Protocolo de serviço de e-mail distribuído)
161/TCP,UDP	SNMP (Simple Network Management Protocol) (Protocolo simples de gerenciamento de rede)
162/TCP,UDP	SNMPTRAP

Extended Access Control List

A forma completa do comando *access-list* é:

```
Router(config)# access-list  
                número da lista de acesso  
                {permit | deny}  
                IP, TCP, UDP ... protocolo  
                origem  
                [máscara da origem]  
                destino  
                [máscara do destino]  
                eq, gt, lt, neq, ... operador  
                Número da porta [operando]  
                [established]
```

Exemplo:

```
router# access-list 103 permit tcp host 10.0.0.3 host 192.168.10.4 eq 80
```

Parâmetros estendidos da ACL

Parâmetro	Descrição
access-list-number	Identifica a lista usando um número no intervalo de 100 a 199.
permit deny	Indica se essa entrada permite ou bloqueia o endereço especificado.
protocol	O protocolo, como, por exemplo, IP, TCP, UDP, ICMP, GRE ou IGRP.
source and destination	Identifica os endereços de origem e de destino.
source-mask and destination-mask	Máscara curinga; os zeros indicam as posições que devem corresponder, os uns indicam as posições que não importam.
operator operand	lt, gt, eq, neq (menor que, maior que, igual, diferente) e um número de porta.
established	Permite que o tráfego TCP passe se o pacote usar uma conexão estabelecida (por exemplo, se tiver bits ACK definidos).

Extended Access Control List

- O comando **ip access-group** vincula uma ACL estendida a uma interface.
- Lembre-se de que somente uma ACL por interface, por direção, por protocolo é permitida.
- O formato do comando é:
router (config-if) # ip
access-group
número-da-lista-de-acesso
{in | out}

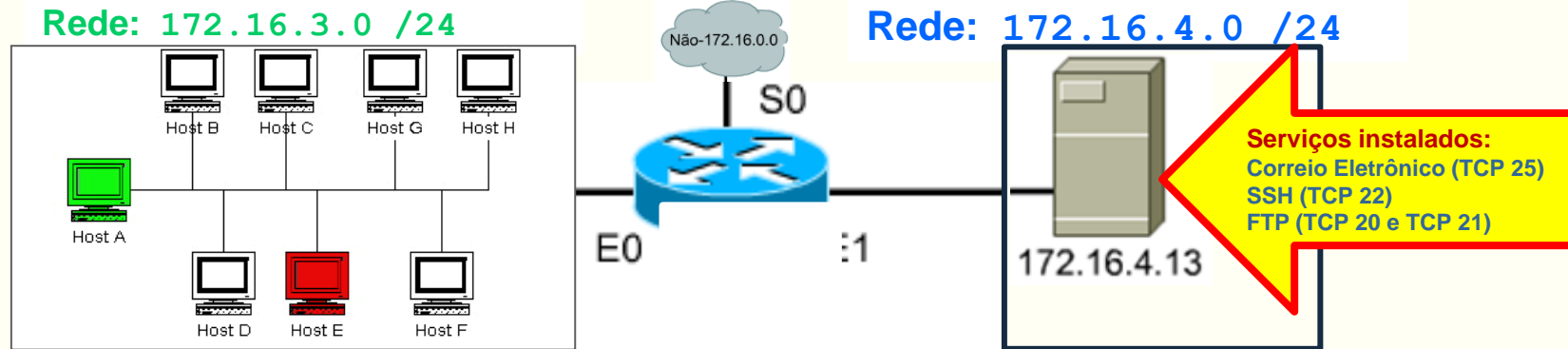
Exemplo:

```
router# ip access-group 103 in
```

Parâmetros estendidos da ACL

Parâmetro	Descrição
access-list-number	Indica o número da ACL a ser vinculada a essa interface.
in out	Seleciona se a ACL é aplicada ao pacote de chegada ou ao pacote de saída na interface. Se in ou out não estiver especificado, out será o padrão.

Extended Access Control List



Exemplo: Considerando o tráfego com origem na rede 172.16.3.0/24 conectada à porta **E0** do roteador e com destino ao servidor 172.16.4.13, conectado à porta **E1** do roteador, é possível criar regras ACL estendida para:

- permitir tráfego ao serviço correio eletrônico (porta tcp 25) de qualquer endereço de origem:

```
router# access-list 101 permit tcp any host 172.16.4.13 eq 25
```

- negar logins remotos via ssh (porta tcp 22)

```
router# access-list 101 deny tcp any host 172.16.4.13 eq 22
```

- negar transferências de arquivos via FTP (porta tcp 20 e 21).

```
router# access-list 101 deny tcp any host 172.16.4.13 eq 20
router# access-list 101 deny tcp any host 172.16.4.13 eq 21
```

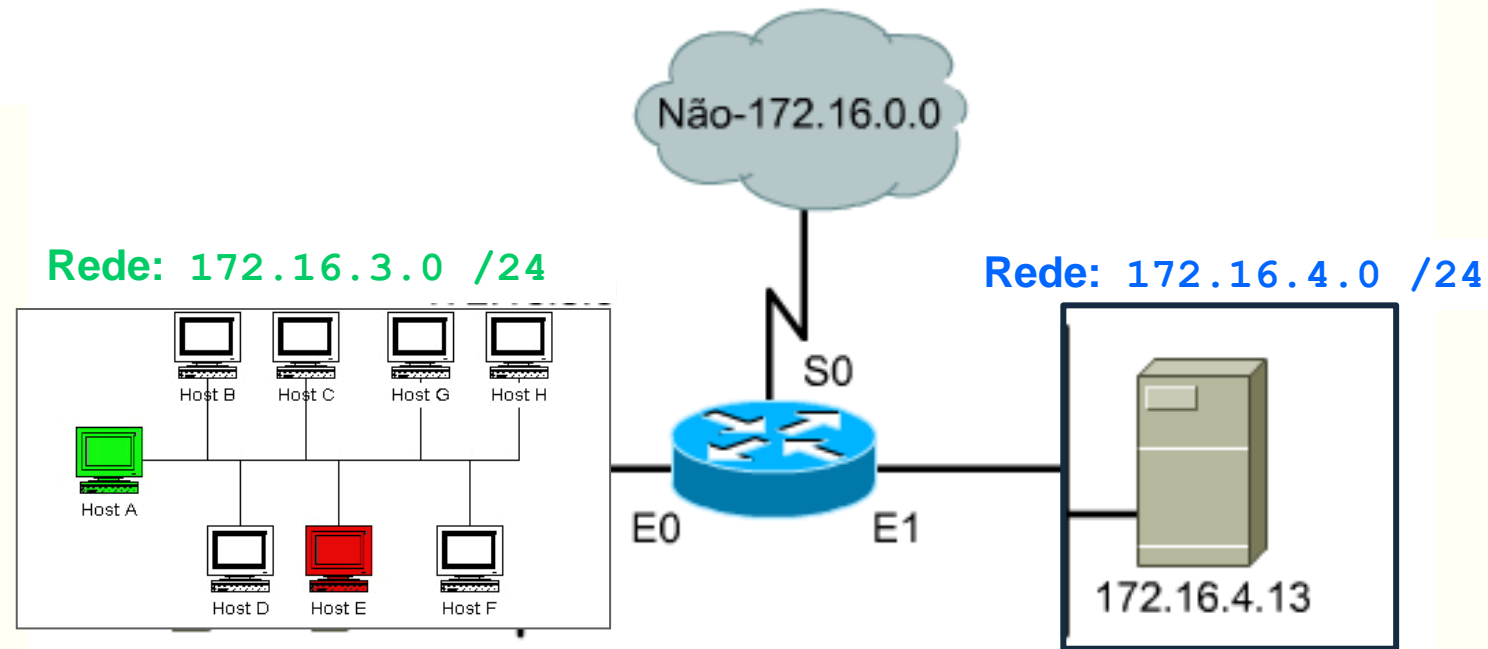
- Permitir qualquer outro tráfego:

```
router# access-list 101 permit ip any any
```

- Aplicar as regras na entrada (in) da interface **E0** do roteador:

```
router# interface e0
router# ip access-group 101 in
```

Exemplo 1: Lista de acesso estendida

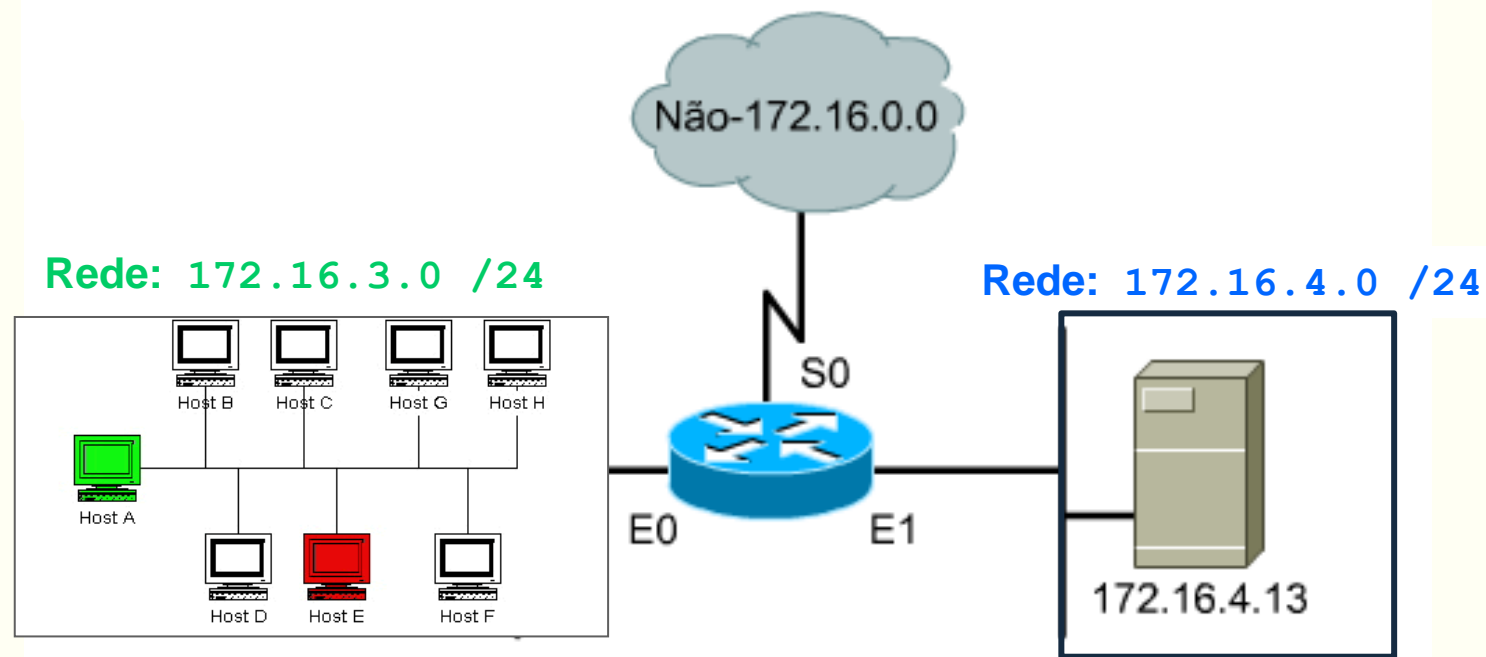


Exemplos: Criar regras ACL para:

1. Permitir o acesso do host A (172.16.3.2) a todos os serviços disponíveis na rede 172.16.4.0 e bloquear o tráfego desse host para a Internet (bloqueio total a qualquer serviço na Internet). Todos os demais tráfegos deverão estar liberados.

```
router# access-list 102 permit ip host 172.16.3.2 172.16.4.0 0.0.0.255
router# access-list 102 deny ip host 172.16.3.2 any
router# access-list 102 permit ip any any
router#
router# interface e0
router# ip access-group 102 in
```

Exemplo 2: Lista de acesso estendida



Exemplos: Criar regras ACL para:

1. Bloquear o acesso do host A (172.16.3.2) ao serviço SSH (porta TCP 23) no servidor 172.16.4.13
2. Bloquear o acesso do host E (172.16.3.5) ao serviço HTTP (porta TCP 80) no servidor 172.16.4.13
3. Liberar o acesso de qualquer equipamento da rede 172.16.3.0 a qualquer serviço na rede 172.16.4.0
4. Liberar qualquer outro tráfego com origem na rede 172.16.3.0 para qualquer destino.


```
router# access-list 101 deny tcp host 172.16.3.2 host 172.16.4.13 eq 23
router# access-list 101 deny tcp host 172.16.3.5 host 172.16.4.13 eq 80
router# access-list 101 permit ip 172.16.3.0 0.0.0.255 172.16.4.0 0.0.0.255
router# access-list 101 permit ip 172.16.3.0 0.0.0.255 any
router#
router# interface e0
router# ip access-group 101 in
```

**Segurança com listas de
controle de acesso**
(*access-control-list* estendidas)
Máscara Curinga

Extended Access Control List

A forma completa do comando *access-list* é:

```
Router(config)# access-list  
                número da lista de acesso  
                {permit | deny}  
                protocolo  
                origem  
                [máscara da origem]  
                destino  
                [máscara do destino]  
                operador  
                [operando]  
                [established]
```



Exemplo:

```
router# access-list 103 permit tcp host 10.0.0.3 host 192.168.10.4 eq 80
```

Parâmetros estendidos da ACL

Parâmetro	Descrição
access-list-number	Identifica a lista usando um número no intervalo de 100 a 199.
permit deny	Indica se essa entrada permite ou bloqueia o endereço especificado.
protocol	O protocolo, como, por exemplo, IP, TCP, UDP, ICMP, GRE ou IGRP.
source and destination	Identifica os endereços de origem e de destino.
source-mask and destination-mask	Máscara curinga; os zeros indicam as posições que devem corresponder, os uns indicam as posições que não importam.
operator operand	lt, gt, eq, neq (menor que, maior que, igual, diferente) e um número de porta.
established	Permite que o tráfego TCP passe se o pacote usar uma conexão estabelecida (por exemplo, se tiver bits ACK definidos).

Extended Access Control List

- O comando **ip access-group** vincula uma ACL estendida a uma interface.
- Lembre-se de que somente uma ACL por interface, por direção, por protocolo é permitida.
- O formato do comando é:

```
Router(config-if) # ip  
                    access-group  
                    número-da-lista-de-acesso  
                    {in | out}
```

Exemplo:

```
router# ip access-group 103 in
```

Parâmetros estendidos da ACL

Parâmetro	Descrição
access-list-number	Indica o número da ACL a ser vinculada a essa interface.
in out	Seleciona se a ACL é aplicada ao pacote de chegada ou ao pacote de saída na interface. Se in ou out não estiver especificado, out será o padrão.

O objetivo e a função dos bits da máscara-curinga

- Uma máscara-curinga é composta de 32 bits divididos em quatro octetos, cada octeto com 8 bits.
- Um bit de máscara-curinga 0 significa "**verificar o valor do bit correspondente**" e um bit de máscara-curinga 1 significa "**não verificar (ignorar) esse valor do bit correspondente**".

O objetivo e a função dos bits da máscara-curinga

Bits de máscara curinga

128	64	32	16	8	4	2	1	
↓	↓	↓	↓	↓	↓	↓	↓	
<hr/>								
0	0	0	0	0	0	0	0	=
0	0	1	1	1	1	1	1	=
0	0	0	0	1	1	1	1	=
1	1	1	1	1	1	0	0	=
1	1	1	1	1	1	1	1	=

Posição de bit do octeto e valor do endereço do bit

Exemplos

Verificar todos os bits do endereço (corresponda todos)

Ignore os 6 últimos bits do endereço

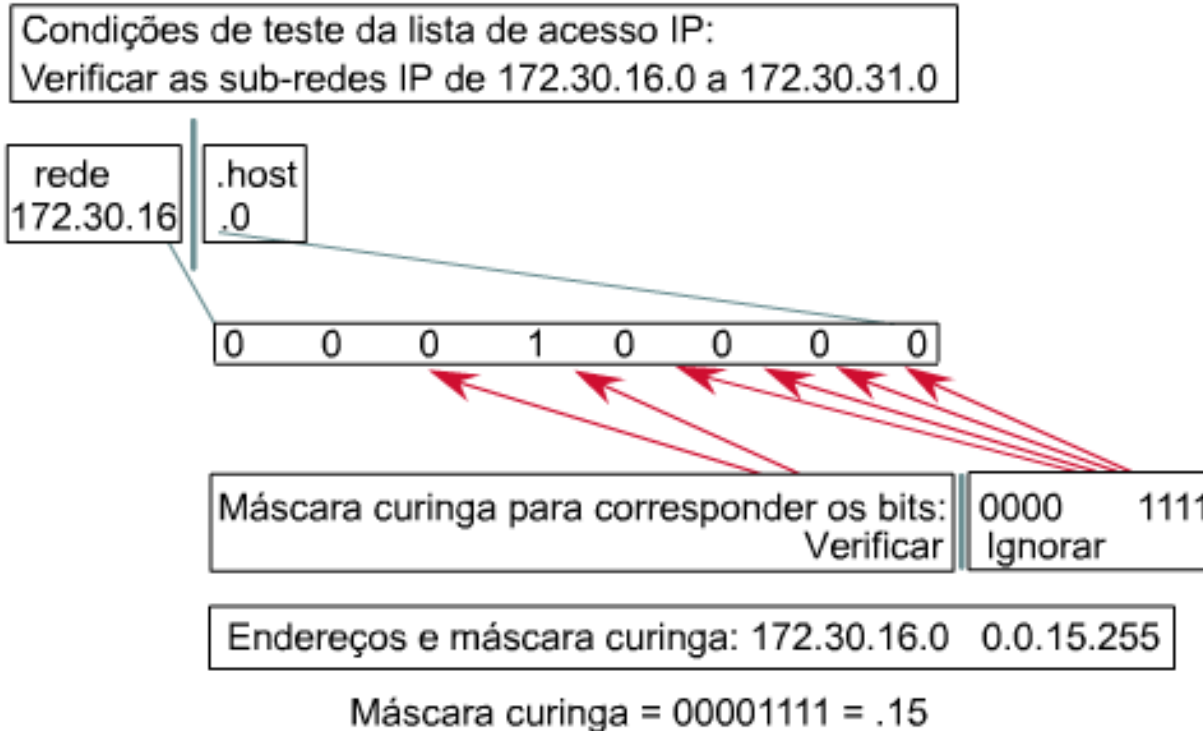
Ignore os 4 últimos bits do endereço

Verifique os 2 últimos bits do endereço

Não verifique o endereço (ignore os bits no octeto)

O objetivo e a função dos bits da máscara-curinga

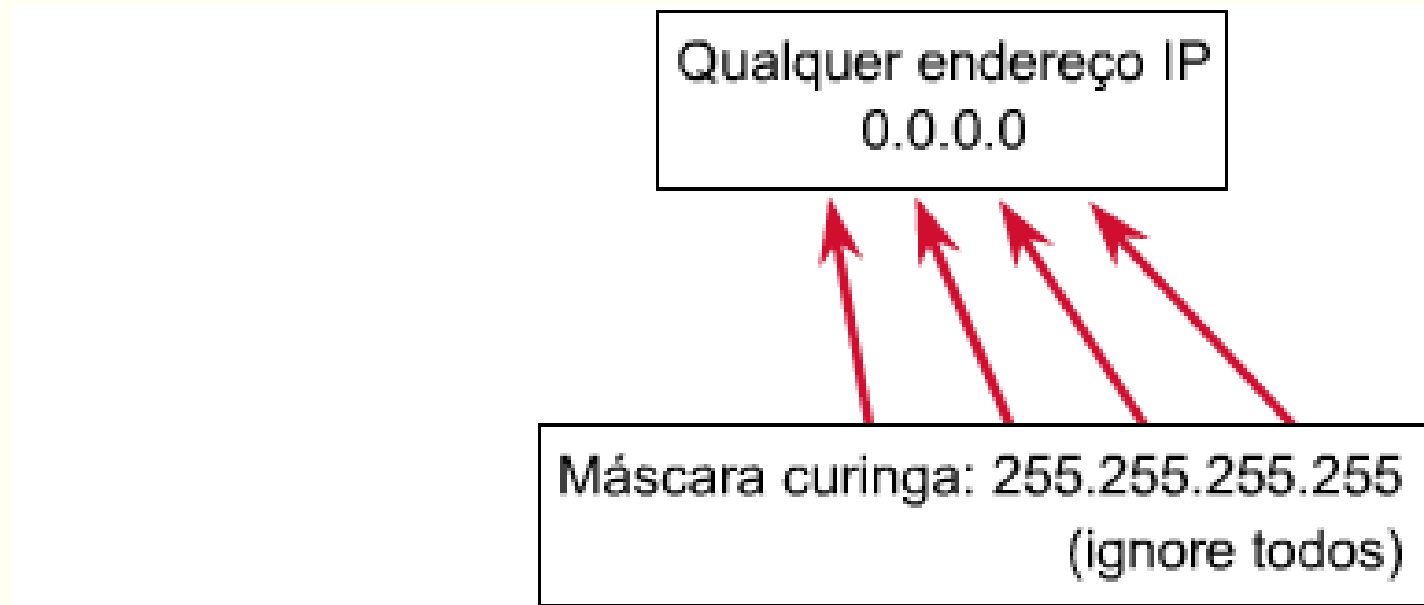
Bits de máscara curinga



Máscara-Curinga

- Uma máscara-curinga é emparelhada com um endereço IP.
- Os números um e zero são usados para identificar como lidar com os bits do endereço IP correspondentes.
- As ACLs usam as máscaras-curinga para identificar um único endereço ou vários endereços para testes de permitir ou negar.
- O termo *utilização de máscaras-curinga* é um apelido para o processo de correspondência de bit de máscara da ACL e provém de uma analogia de um curinga que corresponde a qualquer outra carta em um jogo de pôquer.

Qualquer host



- Ao invés de utilizar:

```
Router(config) # access-list 1 permit 0.0.0.0 255.255.255.255
```

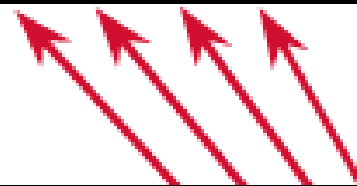
- Pode-se utilizar:

```
Router(config) # access-list 1 permit any
```

Host Curinga

Um endereço de host IP, por exemplo:
172.30.16.29

Máscara curinga: 0.0.0.0
(verifique todos os bits)



- ◆ O exemplo 172.30.16.29 0.0.0.0 verifica todos os bits do endereço.
- ◆ Abrevie o curinga usando a palavra-chave host, seguida do endereço IP.
Ex: host 172.30.16.29

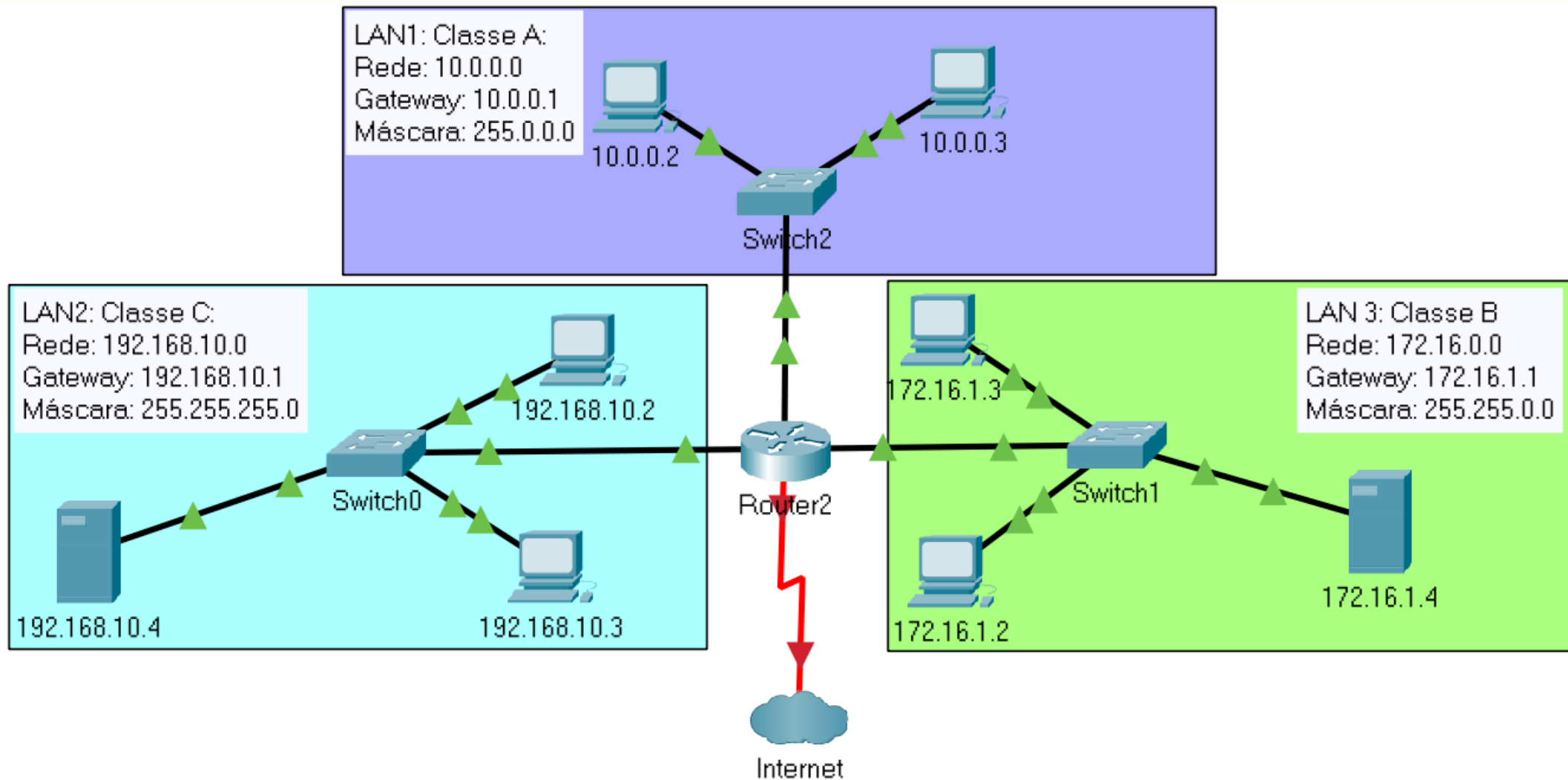
Ao invés de usar:

```
Router(config)# access-list 1 permit 172.30.16.29 0.0.0.0
```

Pode-se utilizar:

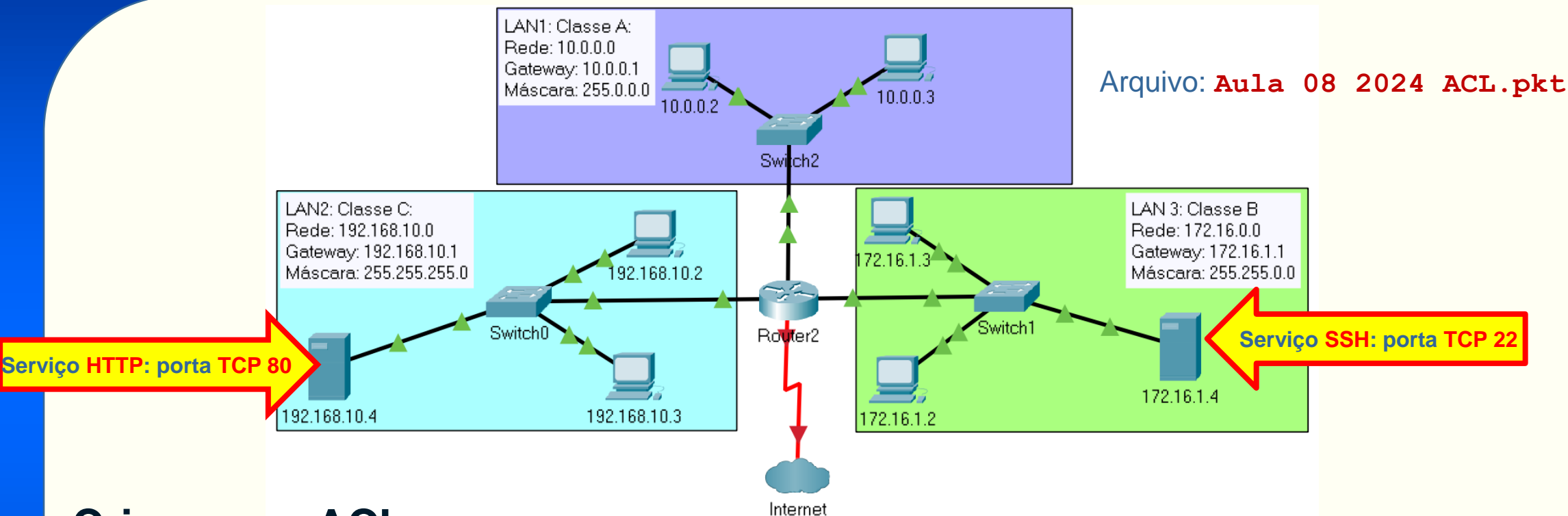
```
Router(config)# access-list 1 permit host 172.30.16.29
```

Exercícios: Analise a topologia



Arquivo: Aula 08 2024 ACL.pkt

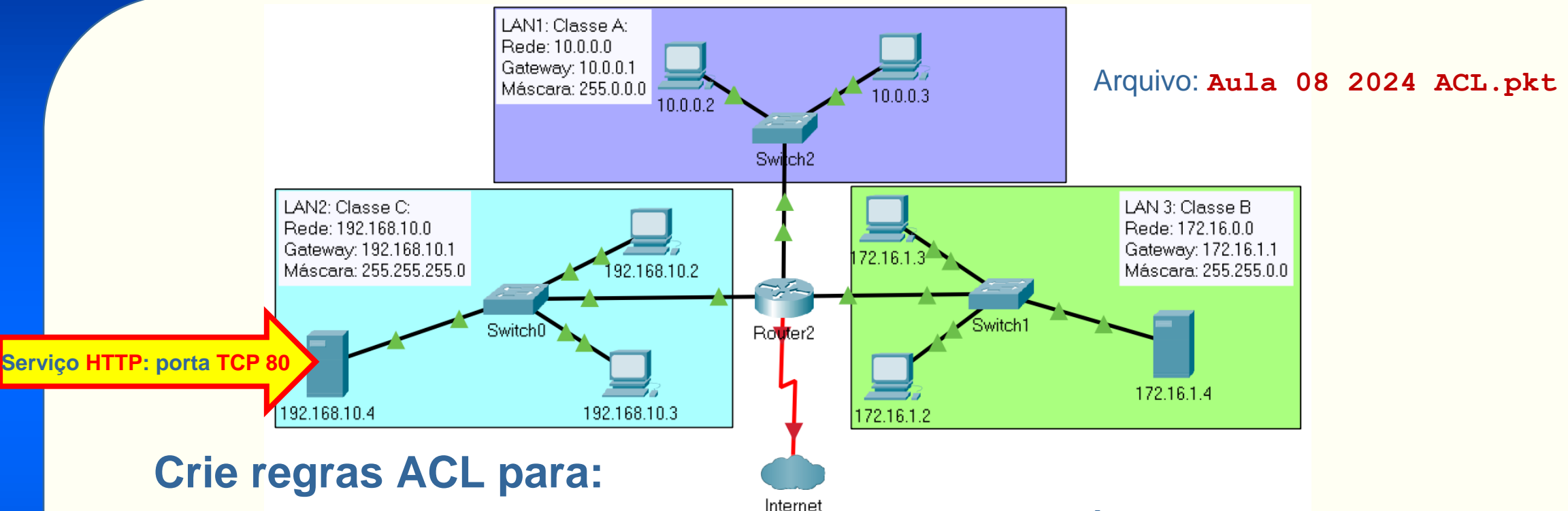
Exercícios: Analise a topologia



Crie regras ACL para:

1. Bloquear acesso do ip **10.0.0.2** ao serviço **http** disponível no servidor **192.168.10.4**
2. Bloquear acesso do ip **10.0.0.3** ao serviço **ssh** disponível no servidor **172.16.1.4**
3. Permitir acesso do ip **10.0.0.3** apenas ao serviço **http** disponível no servidor **192.168.10.4**.
4. O acesso aos demais endereços/serviços disponíveis na rede **192.168.1.0** deverão estar proibidos para o ip **10.0.0.3**

Exercícios: Analise a topologia



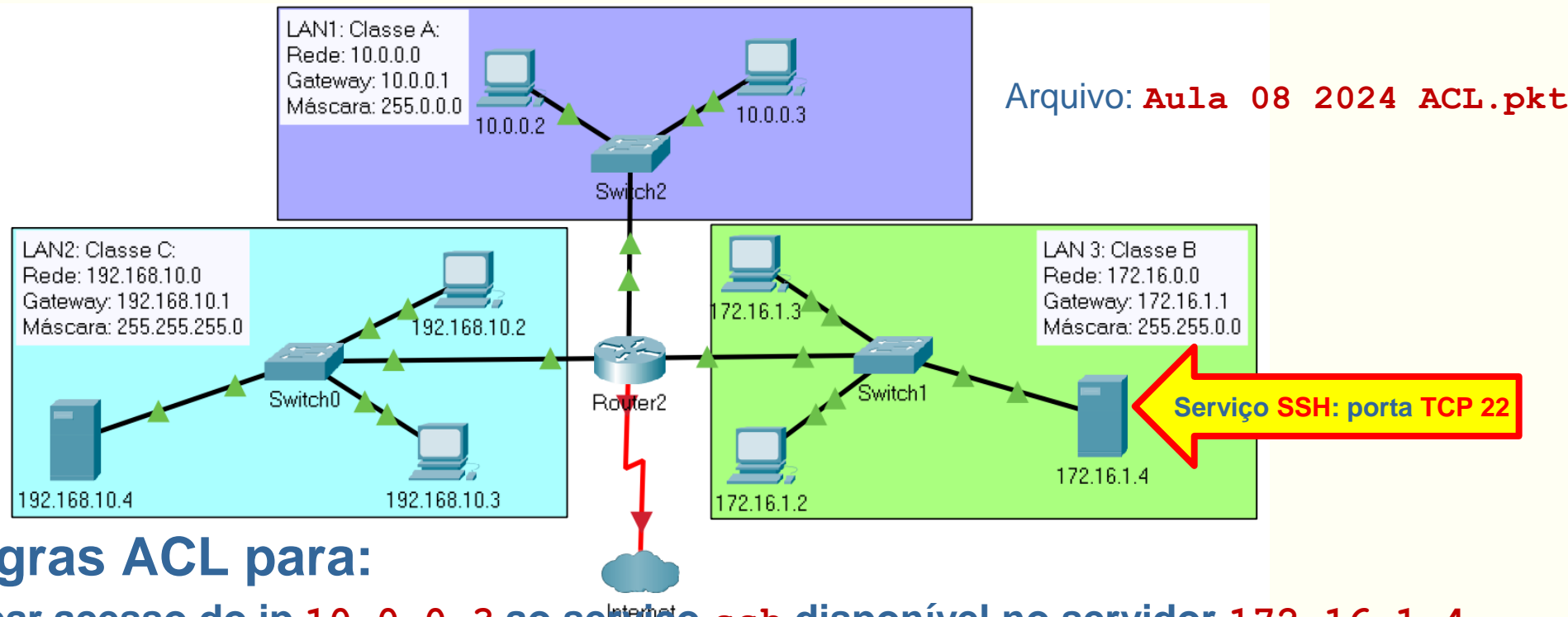
Crie regras ACL para:

1. Bloquear acesso do ip 10.0.0.2 ao serviço **http** disponível no servidor 192.168.10.4

protocolo origem destino porta tcp

```
router# access-list 101 deny tcp host 10.0.0.2 host 192.168.10.4 eq 80
router# access-list 101 permit ip any any
router#
router# interface gig0/1
router# ip access-group 101 in
```

Exercícios: Analise a topologia



Crie regras ACL para:

2. Bloquear acesso do ip 10.0.0.3 ao serviço **ssh** disponível no servidor 172.16.1.4

router# access-list 102 deny tcp host 10.0.0.3 host 172.16.1.4 eq 22

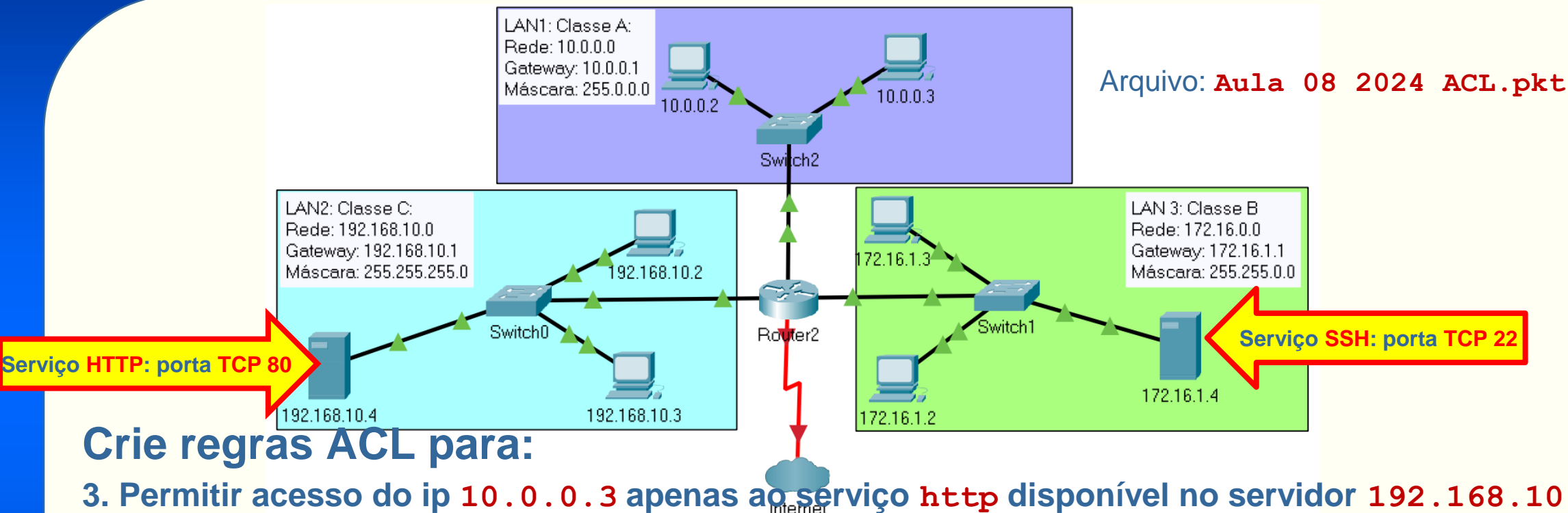
router# access-list 102 permit ip any any

router#

router# interface gig0/1

router# ip access-group 102 in

Exercícios: Analise a topologia



Crie regras ACL para:

3. Permitir acesso do ip **10.0.0.3** apenas ao serviço **http** disponível no servidor **192.168.10.4**. O acesso aos demais endereços/serviços disponíveis na rede **192.168.1.0** deverão estar proibidos para o ip **10.0.0.3**

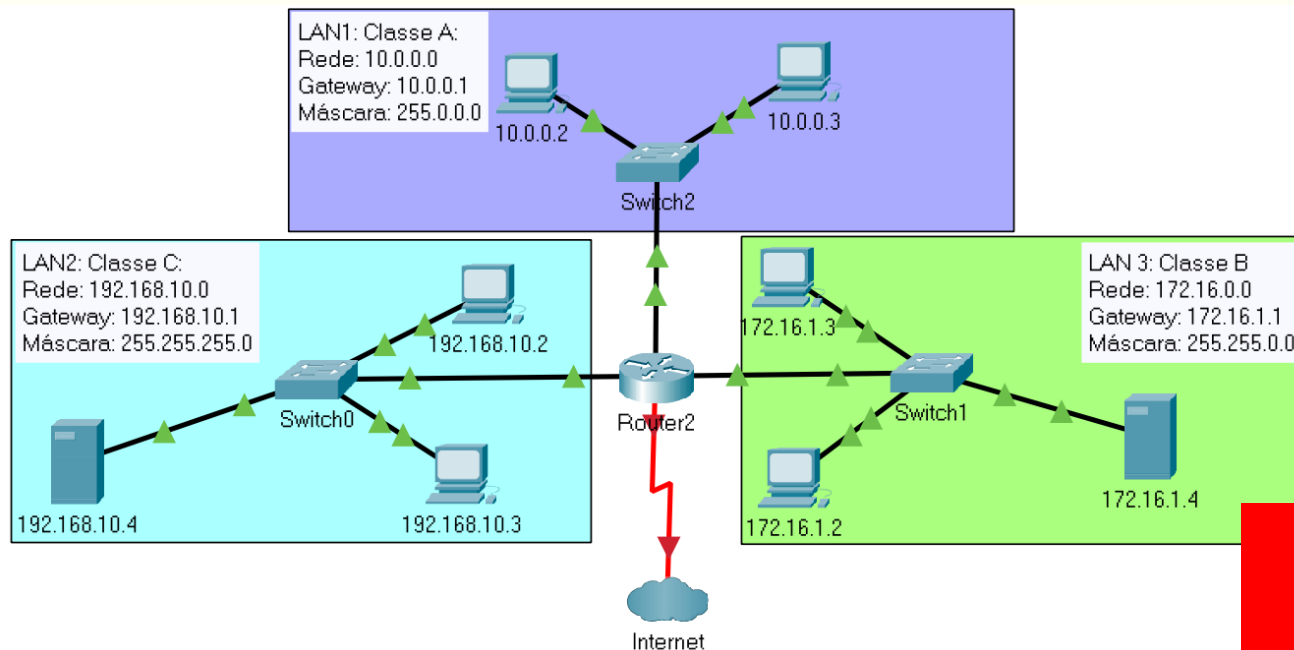
```
router# access-list 103 permit tcp host 10.0.0.3 host 192.168.10.4 eq 80
router# access-list 103 deny ip host 10.0.0.3 192.168.10.0 0.0.0.255
router# access-list 103 permit ip any any
router#
router# interface gig0/1
router# ip access-group 103 in
```

Preparação para Atividade Avaliativa (Parte checkpoint)

Configurar regras ACLs estendida para:

1. Bloquear acesso do ip 10.0.0.2 ao serviço **http** disponível no servidor 192.168.10.4
2. Bloquear acesso do ip 10.0.0.3 ao serviço **ssh** disponível no servidor 172.16.1.4
3. Permitir acesso do ip 10.0.0.3 apenas ao serviço **http** disponível no servidor 192.168.10.4.
4. Implementar uma situação proposta por você (você deve propor e configurar 1 (uma) regra diferente das anteriores).

Tudo o que não estiver explícito nas regras acima deve estar **liberado**



Utilize o Arquivo:
Aula 08 2024 ACL.pkt

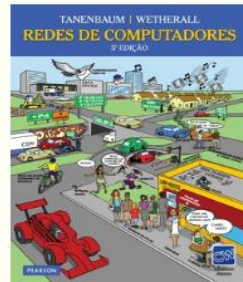
ATENÇÃO:

Além de ser uma atitude antiética, o plágio em trabalhos acadêmicos pode ser considerado crime e poderá comprometer sua carreira acadêmica e profissional.

Referências Bibliográficas



Kurose, James F. Redes de computadores e a Internet: uma abordagem top-down/James F. Kurose e Keith W. Ross; 6ª edição, São Paulo: Addison Wesley, 2013. ISBN 978-85-8143-677-7.



Tanenbaum, Andrew S; Wetherall, David. Redes de Computadores. São Paulo: Pearson Prentice Hall, 2011. 5ª edição americana. ISBN 978-85-7605-924-0.



BIRKNER, Mathew H. Projeto de Interconexão de Redes. São Paulo: Pearson Education do Brasil, 2003. ISBN 85.346.1499-7.

Referências Bibliográficas

- Tanenbaum, A.; Wetherall, D. Redes de Computadores. 5ª ed. Pearson, 2011.
- Wikipedia. IEEE 802.1Q. Disponível em http://en.wikipedia.org/wiki/IEEE_802.1Q
- IEEE. 802.1Q-2011 - IEEE Standard for Local and metropolitan area networks--Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks. Disponível em <http://standards.ieee.org/findstds/standard/802.1Q-2011.html>
- ODOM, W. CCNA ICND2 – Guia Oficial de Certificação do Exame. 2ª ed. Alta Books, 2008.

Referência Complementar

- Comer, Douglas E., Interligação de Redes Com Tcp/ip