



Monitoramento e Gerenciamento de Redes

- Firewall e Access-Control List-

- Continuação – arquivo com mesmo conteúdo da Aula 06 -

Mauro Cesar Bernardes

São Paulo, 2023

Plano de Aula

- **Objetivo**

- Revisar conceitos de segurança da Informação
- Compreender a utilização de Listas de Controle de Acesso como um mecanismo de Firewall

- **Conteúdo**

- Revisão sobre Segurança da Informação
- Revisão sobre Firewall
- Configurando roteador para utilização de ACLs padrão (*access control lists*)

- **Metodologia**

- Aula expositiva sobre os conceitos de Segurança da Informação Firewall e desenvolvimento de atividade prática com configuração em simulador (*Packet Tracer*) de ACLs (*access control lists*) em roteador.

Agenda do Primeiro semestre - 2023

Janeiro 2023							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
52							1
1	2	3	4	5	6	7	8
2	9	10	11	12	13	14	15
3	16	17	18	19	20	21	22
4	23	24	25	26	27	28	29
5	30	31					

Fevereiro 2023							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
5			1	2	3	4	5
6	6	7	8	9	10	11	12
7	13	14	15	16	17	18	19
8	20	21	22	23	24	25	26
9	27	28					

Março 2023							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
9			1	2	3	4	5
10	6	7	8	9	10	11	12
11	13	14	15	16	17	18	19
12	20	21	22	23	24	25	26
13	27	28	29	30	31		

1º Checkpoint da disciplina

Aula 7 Segurança: Firewall + ACL

Abril 2023							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
13						1	2
14	3	4	5	6	7	8	9
15	10	11	12	13	14	15	16
16	17	18	19	20	21	22	23
17	24	25	26	27	28	29	30

Maio 2023							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
18	1	2	3	4	5	6	7
19	8	9	10	11	12	13	14
20	15	16	17	18	19	20	21
21	22	23	24	25	26	27	28
22	29	30	31				

Junho 2023							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
22				1	2	3	4
23	5	6	7	8	9	10	11
24	12	13	14	15	16	17	18
25	19	20	21	22	23	24	25
26	26	27	28	29	30		

○ Início das aulas

○ 2º Checkpoint da disciplina ○ 3º Checkpoint da disciplina

1º Ponto importante:

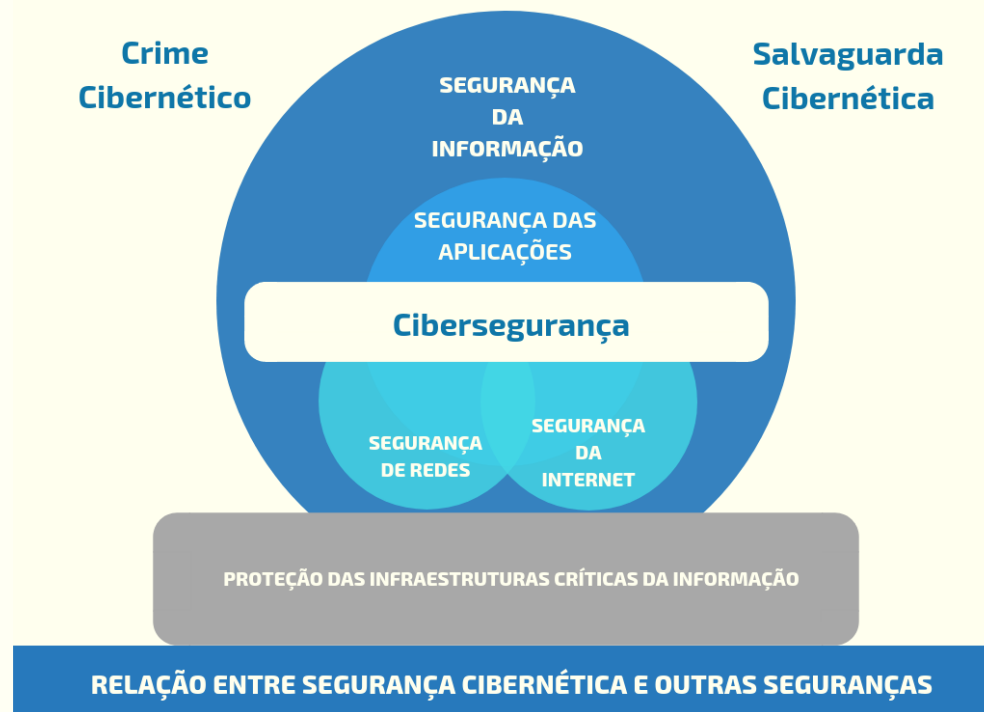
Fique atento ao horário de início das aulas
Atrasos refletem descaso!

Segurança da Informação e Firewall

(revisão)

Segurança da Informação

- O termo Segurança;
- A demanda por segurança;
- Soluções em segurança;



<https://medium.com/@ferrorresfs/voc%C3%AA-sabe-a-diferen%C3%A7a-entre-ciberseguran%C3%A7a-e-seguran%C3%A7a-da-informa%C3%A7%C3%A3o-19bada8d047f>

Considerações sobre segurança

- **“Segurança não é uma questão técnica, mas uma questão gerencial e humana.**
- **Não adianta adquirir uma série de dispositivos de hardware e software sem treinar e conscientizar o nível gerencial da empresa e todos os seus funcionários”**

Christopher Klaus
CTO – Chief Technology Officer
ISS – Internet Security System

“Segurança é um Processo”

Pode-se aplicar o processo seguidamente à rede e à empresa que a mantém e, dessa maneira, melhorar a segurança dos sistemas.

Se não iniciar ou interromper a aplicação do processo, sua segurança será cada vez pior, à medida que surgirem novas ameaças técnicas.



Definições de Segurança

O que é pior que não termos segurança alguma em nossos sistemas?

uma **falsa** sensação de segurança

Garantindo a segurança

- **Segurança da Informação:**

- Confidencialidade;
- Integridade;
- Disponibilidade.

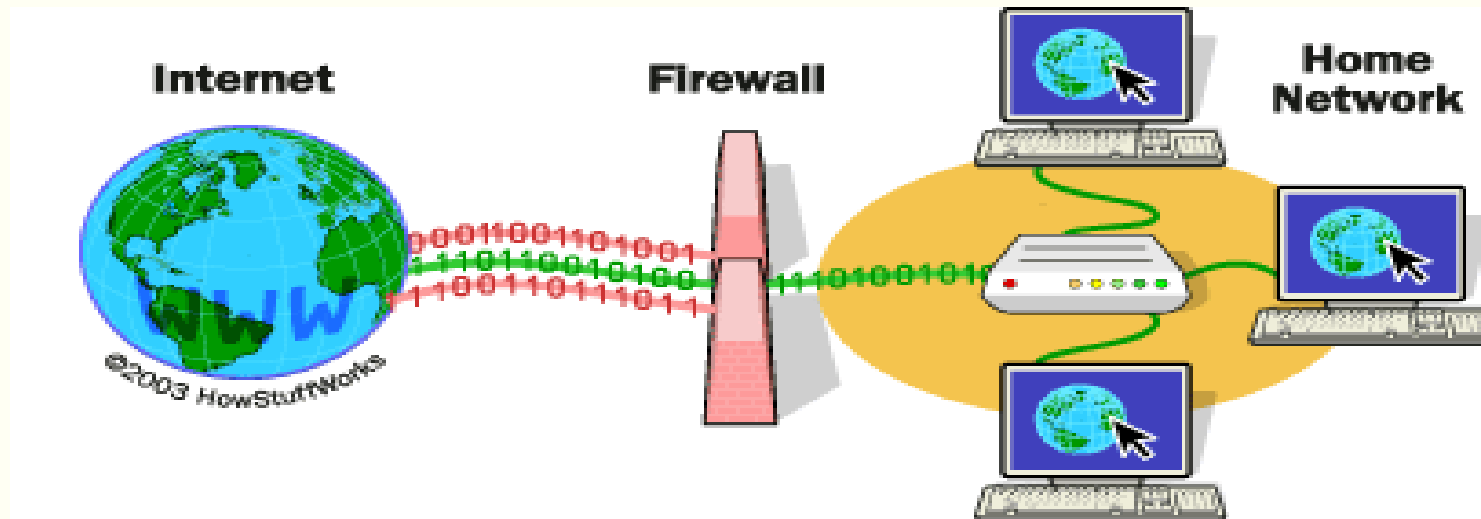
- **Acesso à Informação:**

- Autenticação;
- Autorização;
- Não-Repúdio.



Firewall

Equipamento ou conjunto de equipamentos que garantem o controle da conexão entre duas ou mais redes.



Firewall

Abordagens clássicas de configuração:

O que **não** é expressamente proibido é permitido;

O que **não** é expressamente permitido é proibido;



**Segurança com listas de
controle de acesso**
(Access Control Lists)

Agenda

Listas de controle de acesso (ACLs)

Tarefas da configuração ACL

ACLs padrão

Introdução

- Os administradores de rede devem configurar equipamentos de rede para **negar o acesso não desejado à rede**, enquanto devem **permitir o acesso apropriado**.
- Apesar de ferramentas de segurança como senhas e dispositivos físicos de segurança serem úteis, eles não possuem a flexibilidade da filtragem básica de tráfego e os controles específicos que a maioria dos administradores preferem.
- Por exemplo, um administrador de rede talvez deseje permitir que os usuários acessem a Internet, mas não que os usuários externos tenham acesso a um servidor na LAN da empresa.
- Isso é possível ser configurado **em firewalls e em roteadores**;
- Os roteadores fornecem recursos de filtragem básica, como bloqueio de tráfego da Internet, com as **Access Control Lists (ACLs)**.

Listas de controle de acesso (ACLs)

- As ACLs são listas de instruções que o administrador **aplica à interface do roteador**.
- Essas listas **informam o roteador** sobre que tipos de pacotes deve aceitar e que tipos de pacotes deve recusar.
- A **aceitação e a recusa de pacotes** podem ser baseadas em certas especificações, como o endereço IP de origem.
- As ACLs permitem que se gerencie o tráfego e que se examine pacotes específicos ao aplicar a ACL à interface de um roteador.
- Qualquer tráfego que passe pela interface de um roteador é testado com relação a determinadas condições que fazem parte da ACL configurada **naquela interface**.

Roteador em uma Rede Doméstica

The screenshot shows a web browser window with the Vivo router's configuration page. The browser's address bar shows 'Vivo' and a warning 'Não seguro' (Not secure). The page has a purple sidebar on the left with a menu. The main content area is titled 'AUTENTICAÇÃO' (Authentication) and displays a login form. The form includes fields for 'Usuário:' (Username) and 'Senha:' (Password), and a green 'ENTRAR' (Enter) button. A message at the top of the form states 'Você não está Autenticado' (You are not authenticated) and 'Para acessar as configurações você precisa estar autenticado.' (To access the settings you need to be authenticated).

Vivo

Não seguro

Apps Cotações: Câmbio,... BPMN usp unis orientações Converter PDF em... CA Service Desk Ma... Outros favoritos Lista de leitura

English | Português

vivo

> Status

✓ Configurações

Internet

Rede Local

Wi-fi 2.4 GHz

Wi-fi 5 GHz

Jogos & Aplicativos

Firewall

Modo da WAN

> Gerenciamento

> Sobre o dispositivo

AUTENTICAÇÃO

Você não está Autenticado

Para acessar as configurações você precisa estar autenticado.

Usuário:

Senha:

ENTRAR

Roteador em uma Rede Doméstica

Vivo

Não seguro | 192.168.15.1/cgi-bin/sophia_index.cgi

Apps Cotações: Câmbio, BPMN usp unis orientações Converter PDF em... CA Service Desk Ma... QUT | Fundamental... Outros favoritos Lista de leitura

English | Português | Sair

vivo

▼ 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: TCP

Porta Local: Porta Remota:

IP Local: IP Remoto:

Ação: Local ☒ Remoto

Rejeita Local

Rejeita Remoto

Rejeita Ambos

Aceita Local

Aceita Remoto

Aceita Ambos

ADICIONAR APAGAR

Rules List

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

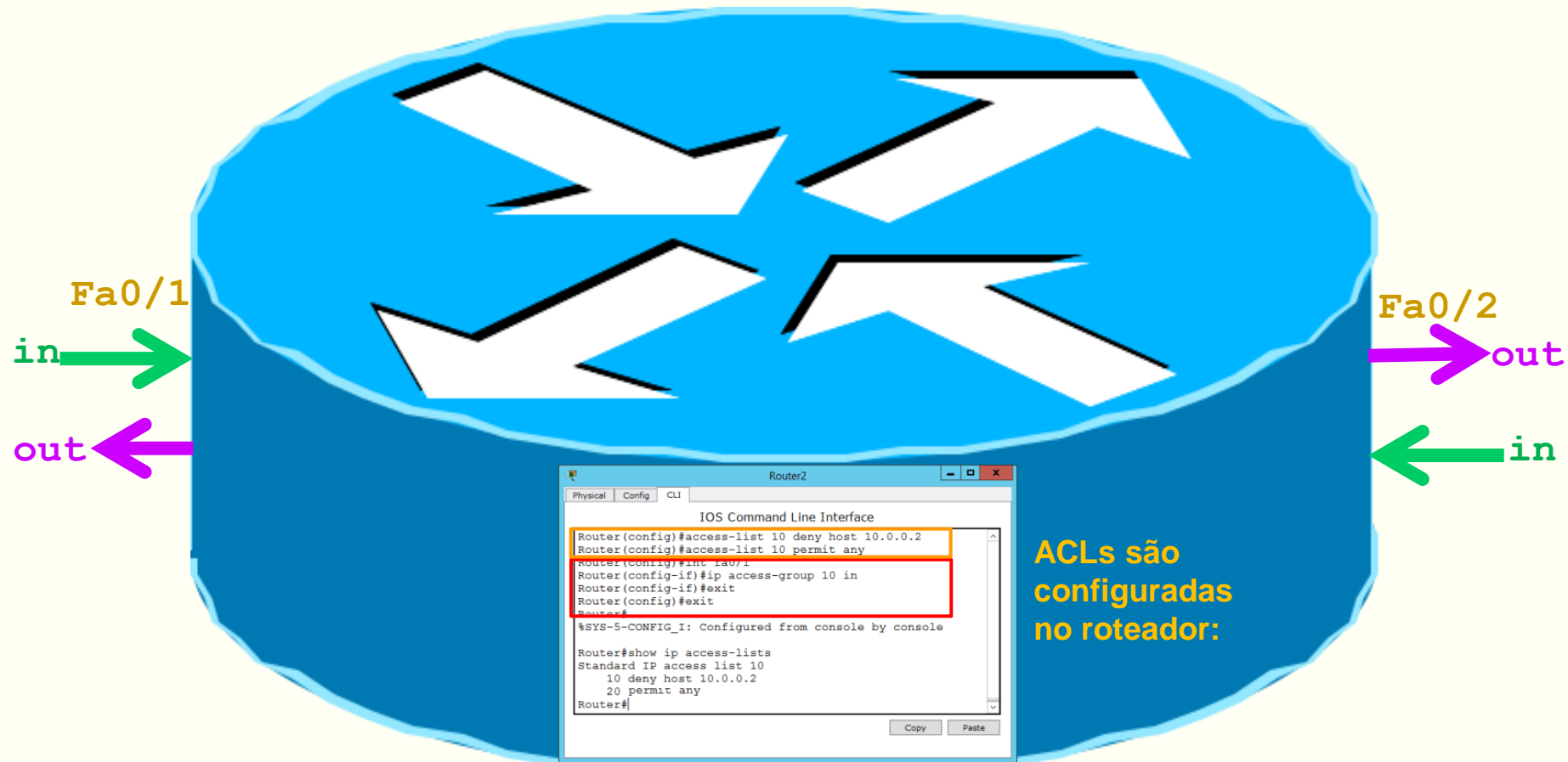
Listas de Controle de Acesso

ACLs podem ser configurados para serem aplicados ao tráfego de entrada e/ou de saída de um roteador, como mostrado na figura.



- **ACLs de entrada** - os pacotes de entrada são processados antes de serem roteados para a interface de saída. Uma ACL de entrada é eficiente porque salva a sobrecarga de pesquisas de roteamento se o pacote é descartado. Se o pacote for permitido pela ACL, ele será processado para roteamento. As ACLs de entrada são mais usadas para filtrar pacotes quando a rede conectada a uma interface de entrada é a única origem dos pacotes que precisa ser examinada.
- **ACLs de saída** - os pacotes de entrada são encaminhados para a interface de saída e processados em seguida por meio da ACL de saída. As ACLs de saída são mais usadas quando o mesmo filtro é aplicado aos pacotes que vêm de várias interfaces de entrada antes de saírem da mesma interface de saída.

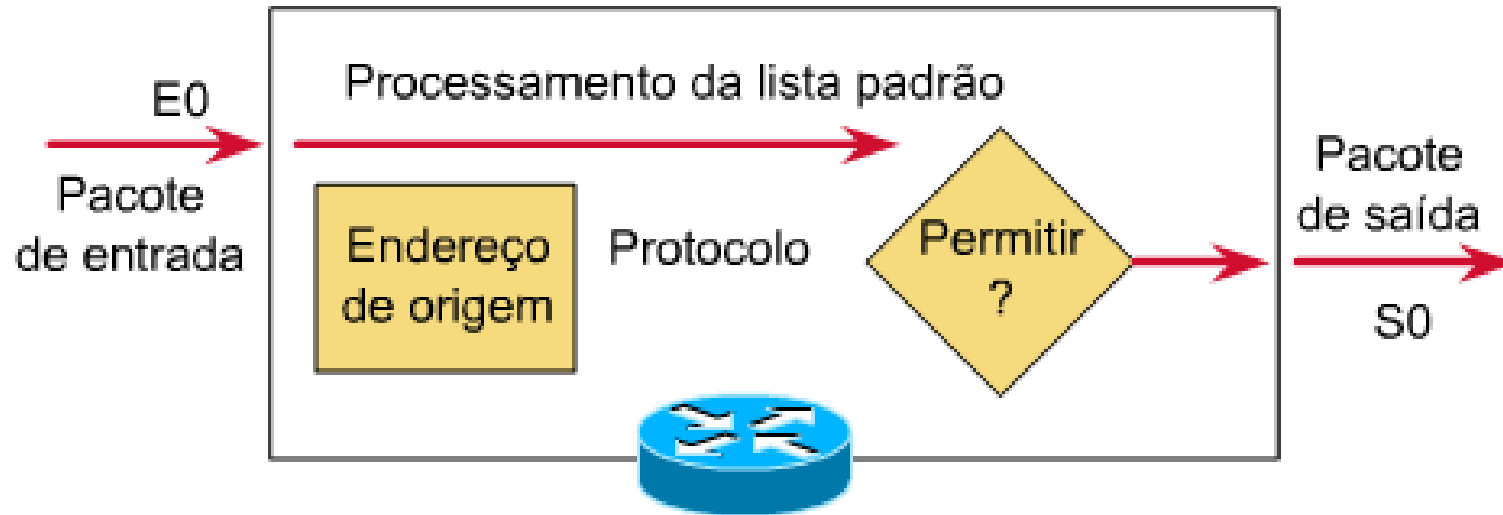
Listas de Controle de Acesso: Recordando



Para seu funcionamento ACLs precisam ser associadas a uma interface configurada 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 List padrão



Access-List Padrão:

A regra é construída para **permitir** (**permit**) ou **negar** (**deny**) pacotes a partir do endereço IP de origem.


Exemplo:

```
#access-list 1 deny host 10.0.0.1 // bloqueia (nega) pacotes com origem no host 10.0.0.1
#access-list 1 permit host 10.0.0.2 // permite pacotes com origem no host 10.0.0.1
#access-list 1 permit any // permite pacotes com qualquer outra origem
```

Protocolos com ACLs

especificados por números

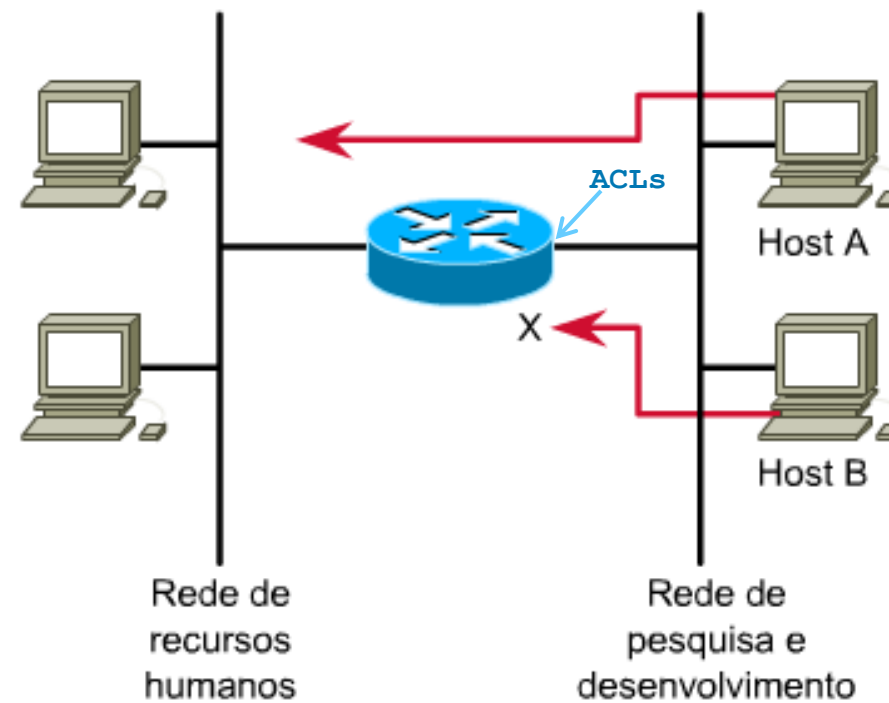
Protocolo	Intervalo
IP	1-99
IP estendido	100-199
AppleTalk	600-699
IPX	800-899
IPX estendido	900-999
Protocolo de anúncio de serviços IPX	1000-1099



Razões para criar ACLs

- Limitar tráfego na rede e aumentar o desempenho da rede;
- Fornecer controle de fluxo de tráfego;
- Fornecer um nível básico de segurança para acesso à rede;
- Escolha que tipos de tráfego serão encaminhados ou bloqueados nas interfaces do roteador.

Limitando o tráfego com ACL



Testando os pacotes com ACLs

- A ordem em que se cria as regras da ACL é importante.
- Por exemplo, quando um roteador CISCO está decidindo se deve encaminhar ou bloquear um pacote, o software Cisco *Internetwork Operating System* (IOS) testa o pacote em relação a cada instrução de condição, na ordem em que as instruções foram criadas

Exemplo:

```
#access-list 1 deny    host 10.0.0.1 // regra 1
#access-list 1 permit host 10.0.0.2 // regra 2
#access-list 1 permit any           // regra 3
```

Na regra 1: pacotes de dados com origem no endereço IP 10.0.0.1 serão bloqueados na interface do roteador onde a regra for aplicada.

Na regra 3: pacotes de dados com origem em qualquer endereço (any) serão permitidos na interface do roteador onde a regra for aplicada.

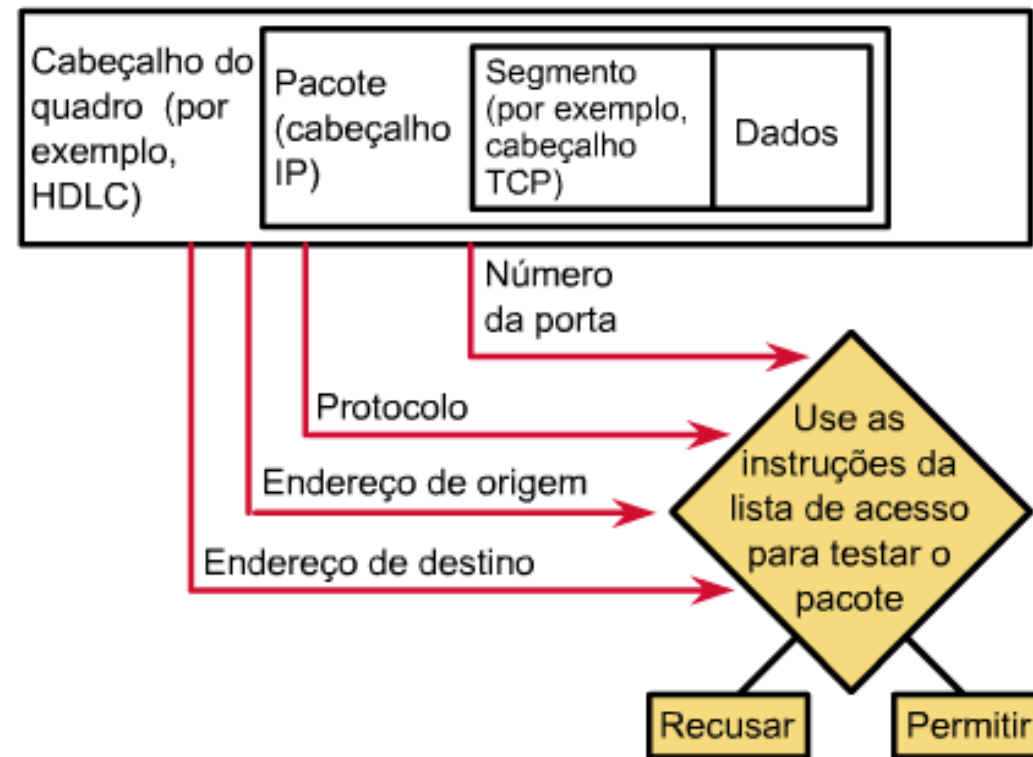
A regra número 1 terá prioridade sobre a regra número 3. Ou seja, apesar a regra número 3 permitir pacotes de qualquer origem, o pacotes com origem em 10.0.0.1 serão bloqueados pela regra 1. (a regra 1 tem prioridade maior que a regra 3, uma vez que está apresentada primeiro.

Testando os pacotes com ACLs

- Se você criar uma instrução de condição que permita todo tráfego (**any**), nenhuma instrução adicionada posteriormente será verificada.
- Se precisar de instruções adicionais, em uma ACL padrão ou estendida, você deve excluir e recriar a ACL com as novas instruções de condição.
- **Por isso, é uma boa ideia editar a configuração de um roteador em um PC usando um editor de texto, e depois enviá-la ao roteador usando o protocolo TFTP.**

Comportamento das ACLs

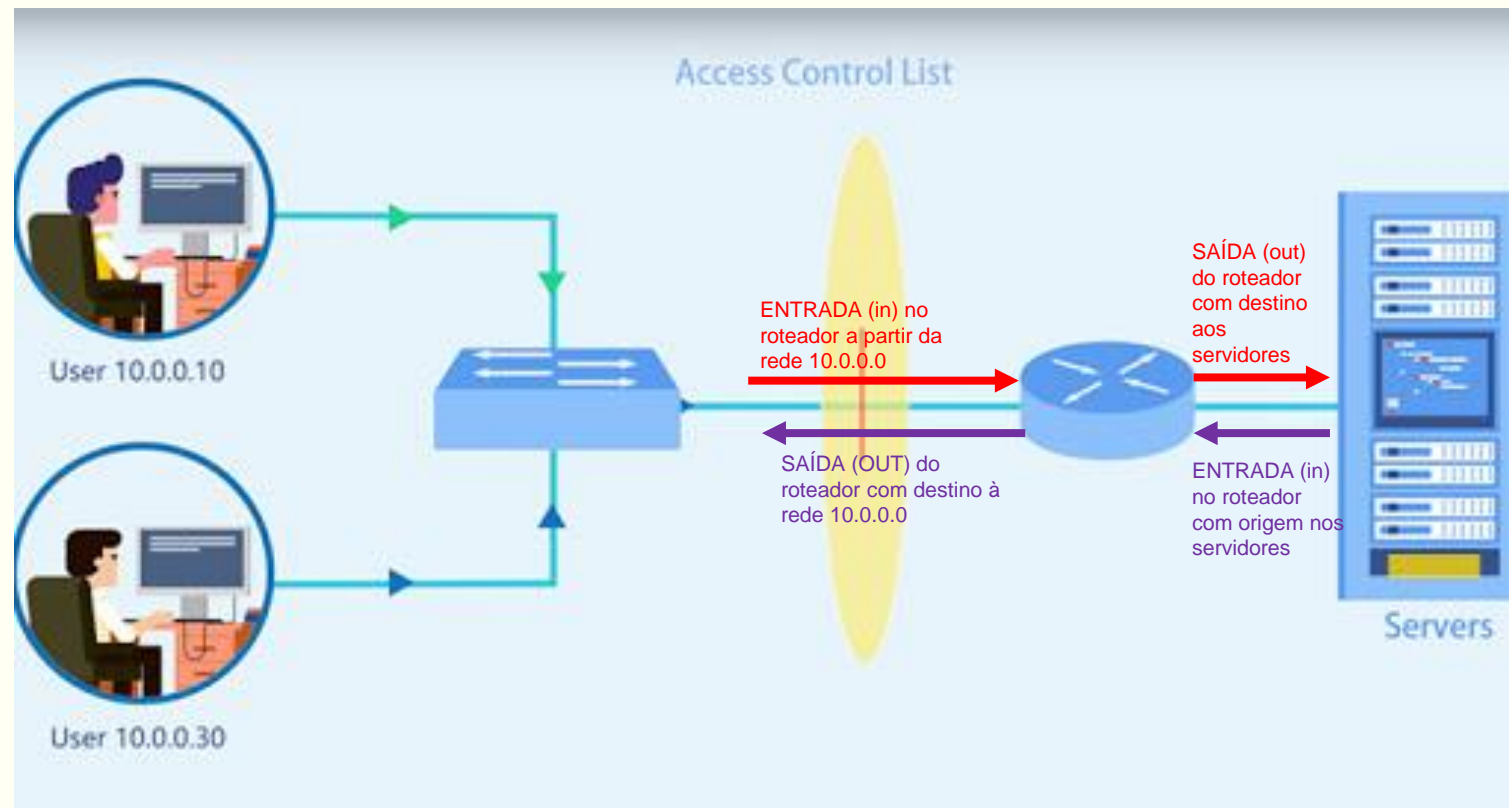
As ACLs do Cisco IOS verificam os cabeçalhos do pacote e os das camadas superiores



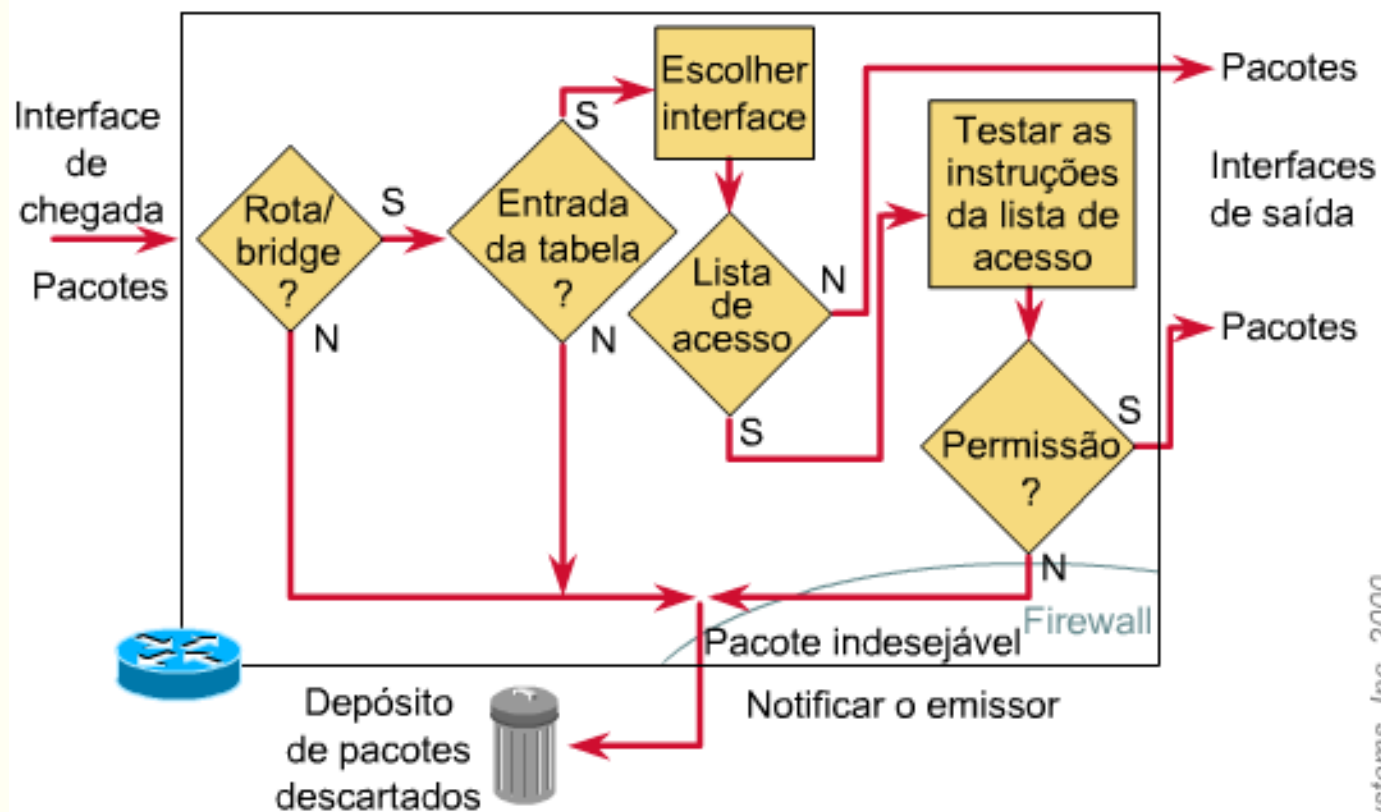
Como as ACLs funcionam

Uma ACL é um grupo de instruções que definem como os pacotes:

- Entram nas interfaces de entrada do roteador
- São retransmitidos através do roteador
- Saem das interfaces de saída do roteador



Como as ACLs funcionam



Como as ACLs funcionam

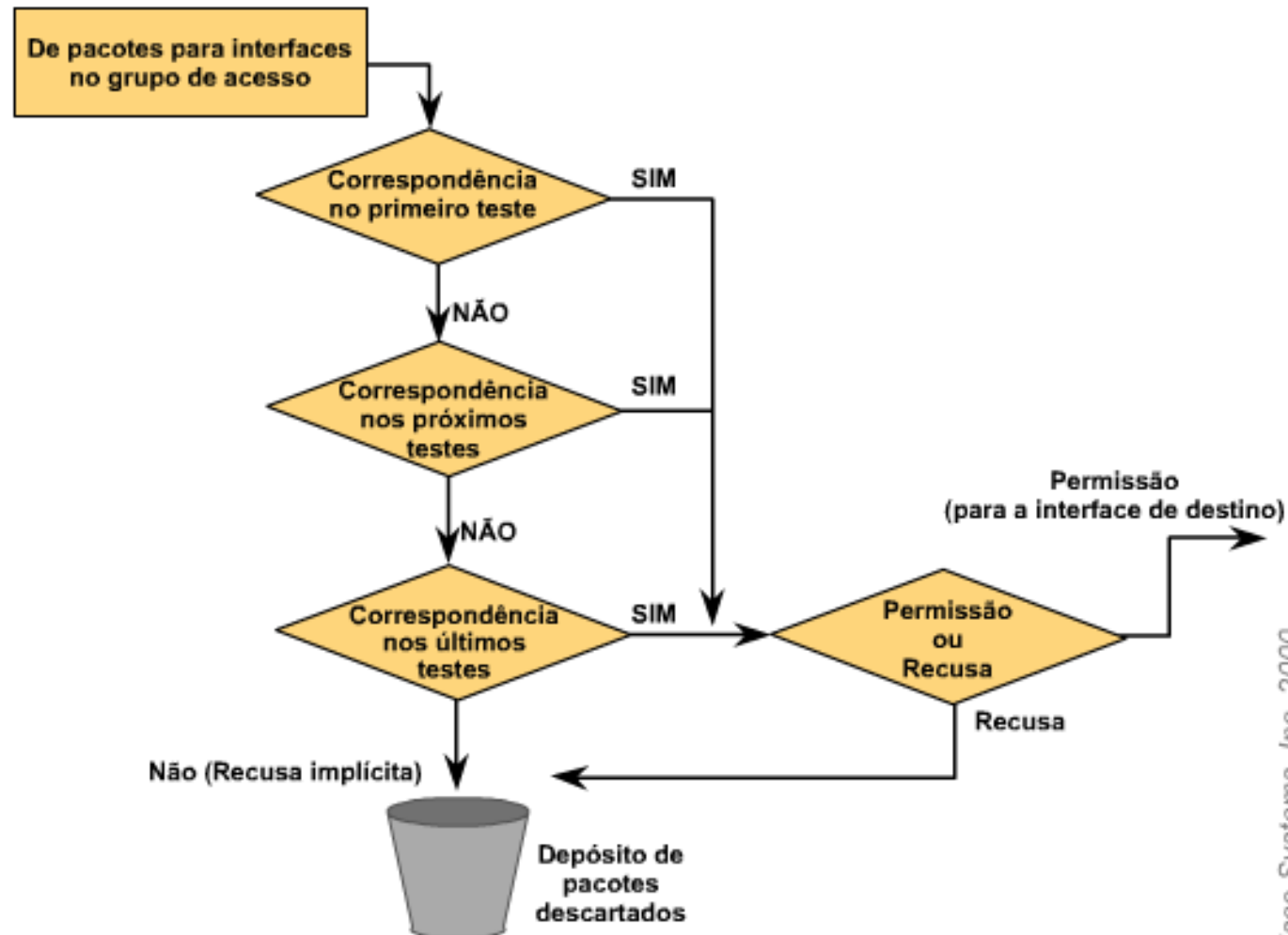
- O início do processo de comunicação é o mesmo, estejam as ACLs sendo usadas ou não.
- À medida que um pacote entra em uma interface (**in**), o roteador verifica se o pacote é *roteável*.
- Em seguida, o roteador verifica se a interface de entrada (**in**) tem uma ACL.
- Se tiver, o pacote é testado em relação às condições da lista de entrada (**in**).
- Se o pacote for permitido, ele será testado em relação às entradas da tabela de roteamento para determinar a interface de saída do roteador (**out**).
- Na interface de saída do roteador (**out**) o roteador verifica se há alguma ACL.
- Caso afirmativo o roteador irá testar o pacote de dados em relação às regras existentes.

Como as ACLs funcionam

- As instruções da ACL operam em ordem sequencial e lógica.
- Se a correspondência com a condição for verdadeira, o pacote será permitido (**permit**) ou negado (**deny**) e as instruções da ACL restantes não serão verificadas.
- Se não houver correspondência em nenhuma das instruções da ACL, uma instrução "**deny any**" implícita será imposta.
- Isso significa que mesmo que você não veja "**deny any**" como a última linha de uma ACL, um roteador funcionará como se **ela está lá**.

Fluxograma do processo de correspondência do teste de ACL

Como as ACLs funcionam



Para configurar uma ACL IP padrão:

- Criar ACLs usando o modo de configuração global.

```
Router>  
Router>  
Router>enable  
Router#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#  
Router(config)#access-list 1 permit host 10.0.0.1|
```

- Especificar um número de ACL de 1 a 99 instrui o roteador a aceitar as instruções de ACL padrão.
- Selecionar cuidadosamente a ACL e colocá-la em ordem lógica.

Tarefa de Configuração da ACL

Etapa 1

Definir a ACL usando o seguinte comando:

```
Router(config)# número da lista de acesso  
          {permit | deny} (condições de teste)
```

Uma instrução global identifica a ACL. Especificamente, o intervalo 1-99 é reservado para o padrão IP. Esse número se refere ao tipo do ACL. No Cisco IOS Versão 11.2 ou mais recente, as ACLs podem também usar um nome ACL, como `education_group`, em vez de usar um número.

O termo `permit` ou `deny` na instrução ACL global indica como os pacotes que satisfazem às condições de teste são tratados pelo software Cisco IOS . O termo `permit` geralmente significa que o pacote poderá usar uma ou mais interfaces que você especificará mais adiante. O(s) termo(s) `final(is)` especifica(m) as condições de teste usadas pela instrução ACL.

Tarefa de Configuração da ACL

Etapa 2

Depois, você precisa aplicar as ACLs em uma interface usando o comando `access-group`, como mostrado neste exemplo:

```
Router(config-if)# {protocol} access-group número da lista de acesso
```

Todas as instruções ACL identificadas pelo número da lista de acesso estão associadas a uma ou mais interfaces. Todos os pacotes que passarem nas condições do teste ACL podem usar qualquer interface no grupo de acesso das interfaces.

Atribuir um número exclusivo a cada ACL

- Quando configurar ACLs em um roteador, você deverá identificar cada ACL com exclusividade, atribuindo um número à ACL do protocolo.
- Quando você usar um número para identificar uma ACL, o número deverá estar dentro de um intervalo específico que seja válido para o protocolo.
- Você pode especificar ACLs pelos números dos protocolos listados na tabela.
- A tabela também lista o intervalo de números de ACL válidos para cada protocolo.
- Depois de criar uma ACL numerada, você deve atribuí-la a uma interface para que seja usada.
- Se você deseja alterar uma ACL que contenha instruções numeradas, precisa excluir todas as instruções da ACL numerada usando o comando **no access-list** número da lista

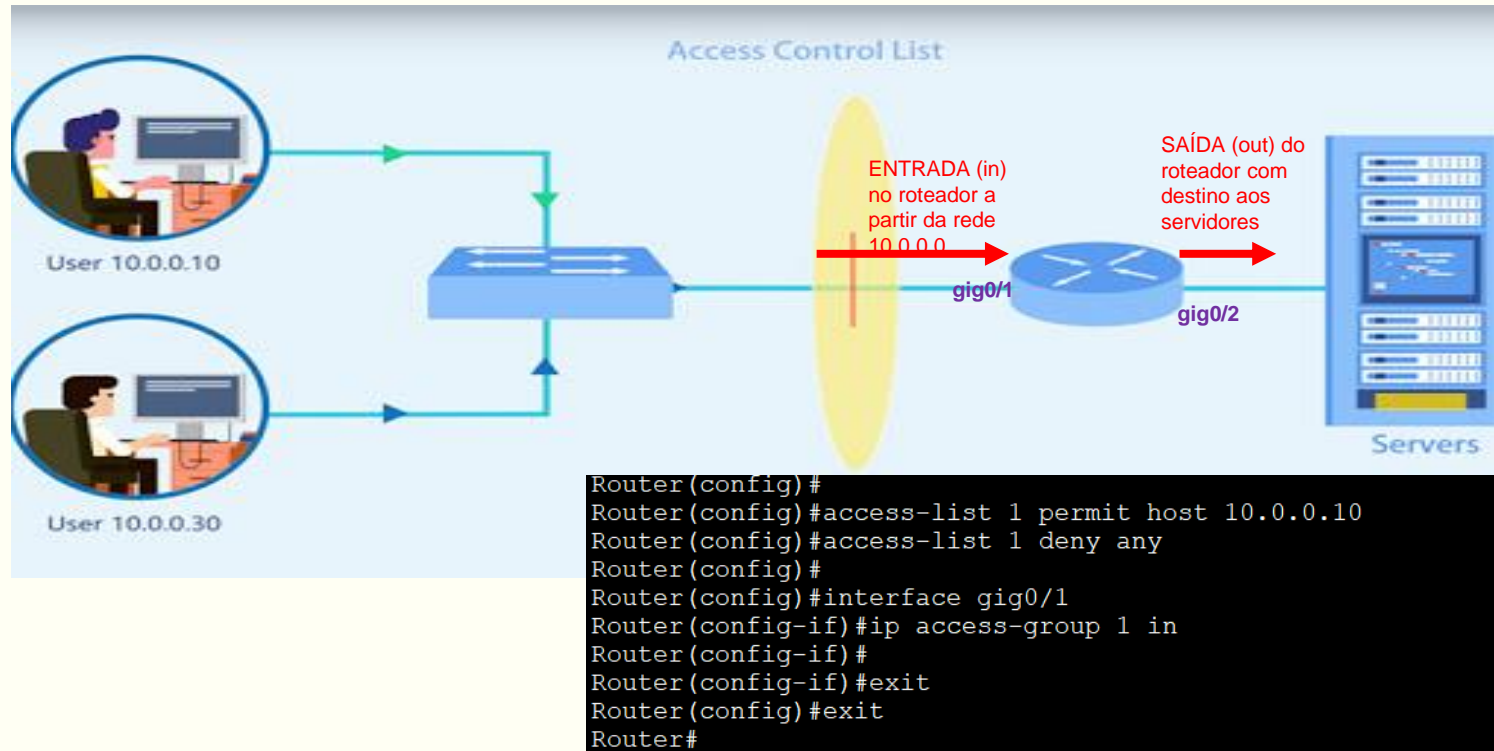
ACLs padrão

- Você usa as ACLs padrão quando deseja bloquear todo tráfego de uma rede, permitir todo tráfego de uma rede específica ou negar conjuntos de protocolos.
- As ACLs padrão verificam o **endereço de origem** dos pacotes que devem ser roteados.
- O resultado permite ou nega a saída de um conjunto inteiro de protocolos, baseado nos endereços de host, sub-rede e rede.



```
Router(config)#
Router(config)#access-list 1 permit host 10.0.0.10
Router(config)#access-list 1 deny any
Router(config)#
Router(config)#interface gig0/1
Router(config-if)#ip access-group 1 in
Router(config-if)#
Router(config-if)#exit
Router(config)#exit
Router#
```

ACLs padrão



- No exemplo (imagem) anterior, será feita a verificação do protocolo e do endereço de origem nos pacotes que chegam à interface (**in**) **gig0/1**.
- Em seguida serão aplicadas as regras ACL de entrada na interface **gig0/1**. Se obtiverem permissão, os pacotes de dados sairão pela **gig0/2**.
- Se não obtiverem permissão, os pacotes de dados serão descartados.

Sintaxe do comando ACL padrão

Parâmetro	Descrição
<i>número da lista de acesso</i>	Número de uma ACL. Esse é um número decimal de 1 a 99 (para uma ACL IP padrão).
deny	Recusa o acesso se as condições forem correspondentes.
permit	Permite o acesso se as condições forem correspondentes.
<i>origem</i>	Número da rede ou do host de onde o pacote está sendo enviado. Existem duas formas de especificar a origem: <ul style="list-style-type: none">· Use uma quantidade de 32-bits, em um formato decimal com ponto em quatro partes.· Use a palavra-chave any como uma abreviatura para uma origem e um <i>curinga da origem</i> de 0.0.0.0 255.255.255.55.
<i>curinga de origem</i>	(Opcional) Bits curingas a serem aplicados à origem. Existem duas formas de especificar o <i>curinga de origem</i> : <ul style="list-style-type: none">· Use uma quantidade de 32 bits, em um formato decimal com ponto em quatro partes. Posicione os uns nas posições do bit que você deseja ignorar.· Use a palavra-chave any como a abreviatura para uma origem e um <i>curinga da origem</i> de 0.0.0.0 255.255.255.255. (Opcional) Produz uma mensagem de registro de informações sobre o pacote que corresponde à entrada a ser enviada ao console. (O nível das mensagens que efetuam logon no console é controlado pelo comando logging do console.)
log	A mensagem inclui o número da ACL, independentemente do pacote ter sido permitido ou recusado, o endereço de origem e o número de pacotes. A mensagem é gerada para o primeiro pacote que corresponde e depois em intervalos de cinco minutos, incluindo o número de pacotes permitidos ou recusados no intervalo de cinco minutos anterior.

ACLs padrão

- Usa-se a versão padrão do comando de configuração global `access-list` para definir uma ACL padrão numerada.
- Esse comando é usado no modo de comando da configuração global.
- A sintaxe completa do comando é
`Router(config)# access-list número-da-lista-de-acesso {deny | permit} rede-origem [máscara-curinga-origem] [log]`
- Use a forma no desse comando para retirar uma ACL padrão.
- Esta é a sintaxe:
`Router(config)# no access-list número da lista de acesso`
- A tabela anterior mostra as descrições dos parâmetros usados nessa sintaxe.

Exemplos de ACL padrão

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

Como Verificar Listas de Acesso

- Use o comando EXEC **show access-lists** para exibir o conteúdo de todas as ACLs.
- Além disso, use o comando EXEC **show access-lists** seguido do nome ou número de uma ACL para exibir o conteúdo de uma ACL.

```
Router(config)#  
Router(config)#access-list 1 permit host 10.0.0.10  
Router(config)#access-list 1 deny any  
Router(config)#  
Router(config)#interface gig0/1  
Router(config-if)#ip access-group 1 in  
Router(config-if)#  
Router(config-if)#exit  
Router(config)#exit  
Router#  
%SYS-5-CONFIG_I: Configured from console by console  
  
Router#show access-list 1  
Standard IP access list 1  
    permit host 10.0.0.10  
    deny any  
  
Router#
```



Exemplos de Access List

O exemplo a seguir de uma ACL padrão permite que os pacotes oriundos de hosts de três redes especificadas sejam transmitidos:

```
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
```

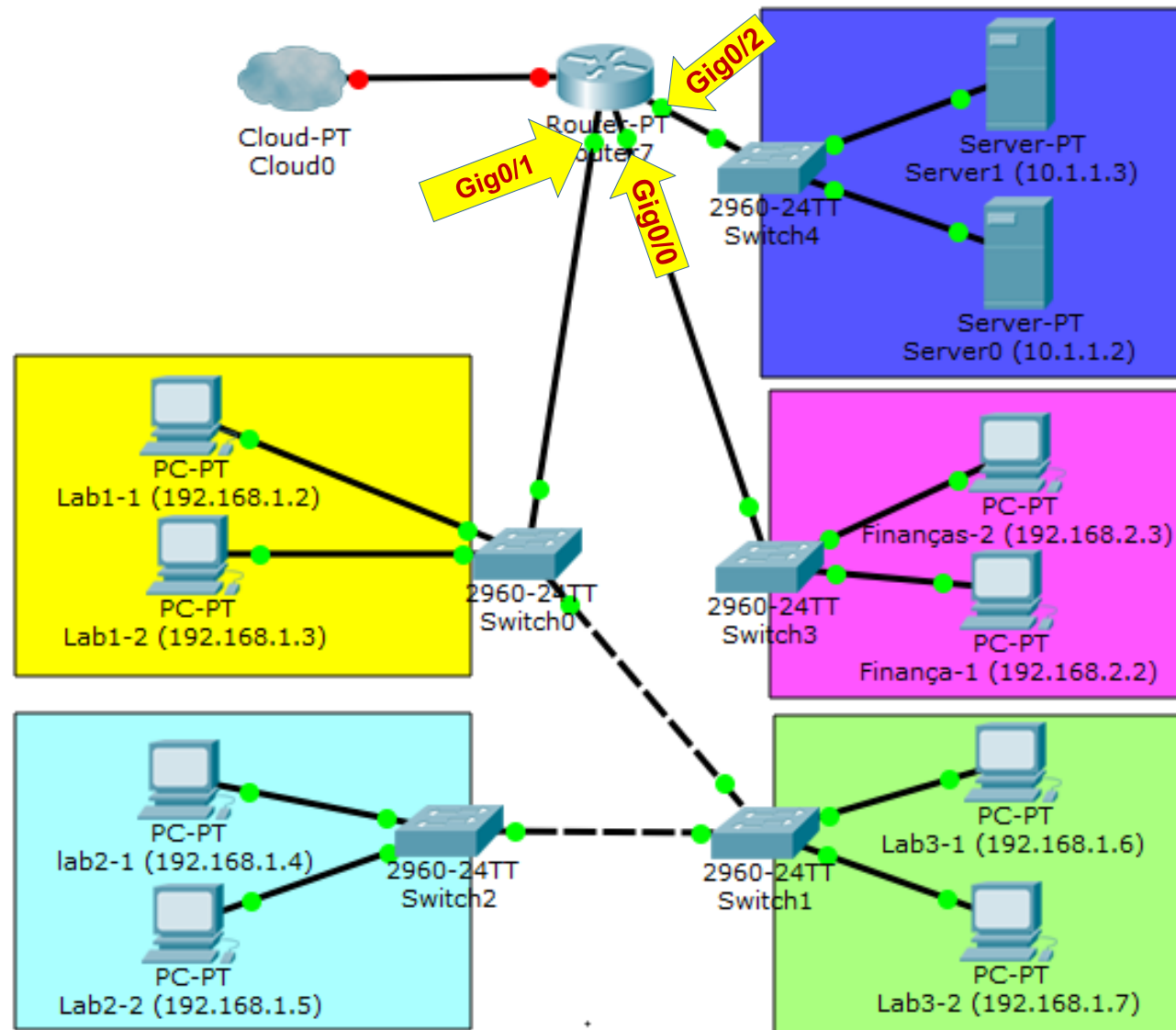
Observação: qualquer outro acesso implicitamente negado

Exemplos de Access List

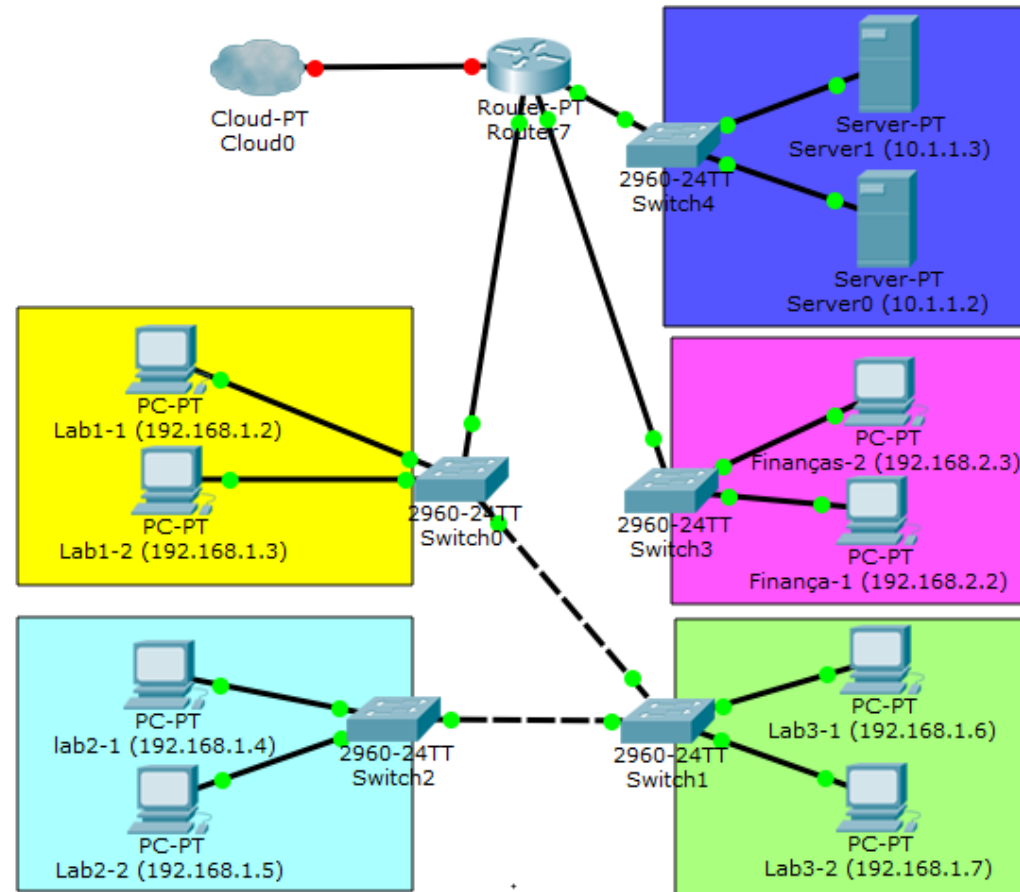
- O comando **ip access-group** agrupa uma ACL existente a uma interface.
- Lembre-se de que somente uma ACL por porta por protocolo por direção é permitida.
- O formato do comando é:

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

Atividade Prática: Aula 06 2023.pkt



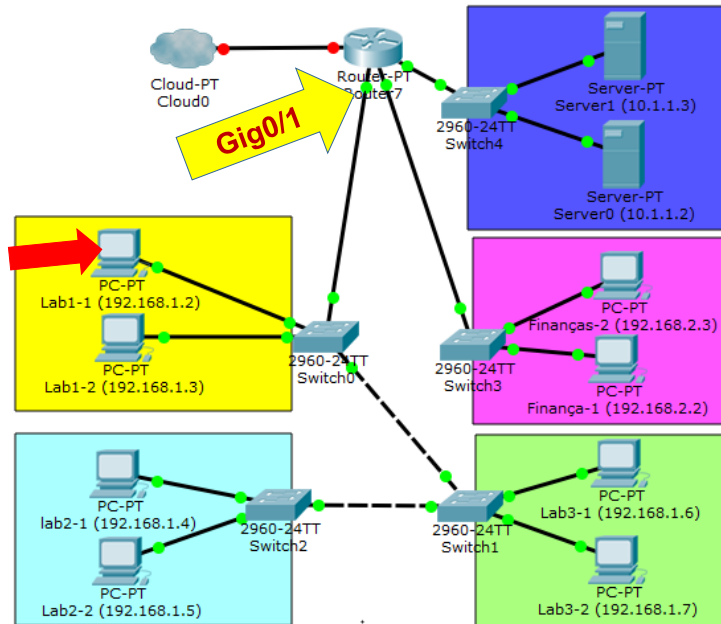
Atividade Prática:



Configurar ACLs para:

1. Não permitir a saída de pacotes do host 192.168.1.2 da rede 192.168.1.0
2. Não permitir que pacotes do host 192.168.1.3 alcancem a rede 192.168.2.0
3. Não permitir que os pacotes da rede 192.168.1.0 alcancem a rede 10.1.1.0
4. Tudo o que não estiver explícito nas regras acima deve estar **liberado**

Atividade Prática:



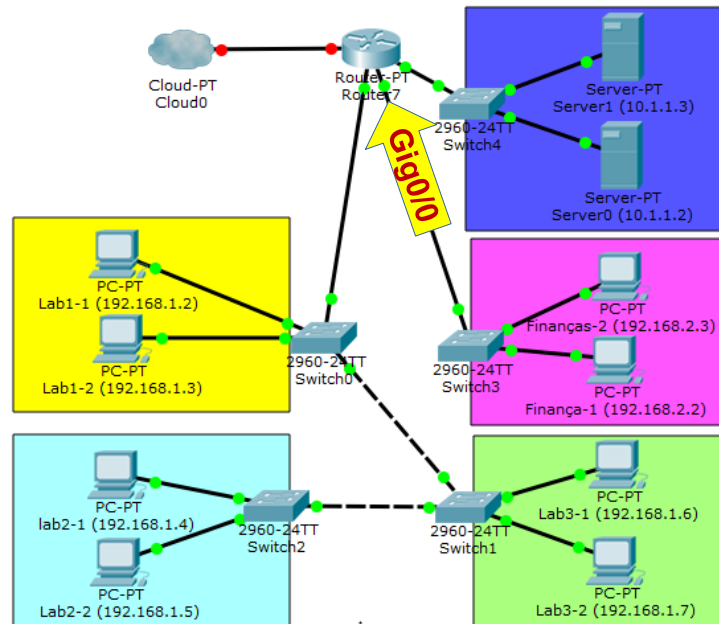
Configurar ACLs para:

1. Não permitir a saída de pacotes do host
192.168.1.2 da rede 192.168.1.0

Configurar ACLs no roteador Router7:

```
Router>
Router>enable
Router#configure terminal
Router(config)#access-list 1 deny host 192.168.1.2
Router(config)#access-list 1 permit any
Router(config)#
Router(config)#interface gig0/1
Router(config-if)#ip access-group 1 in
Router(config-if)#
```

Atividade Prática:



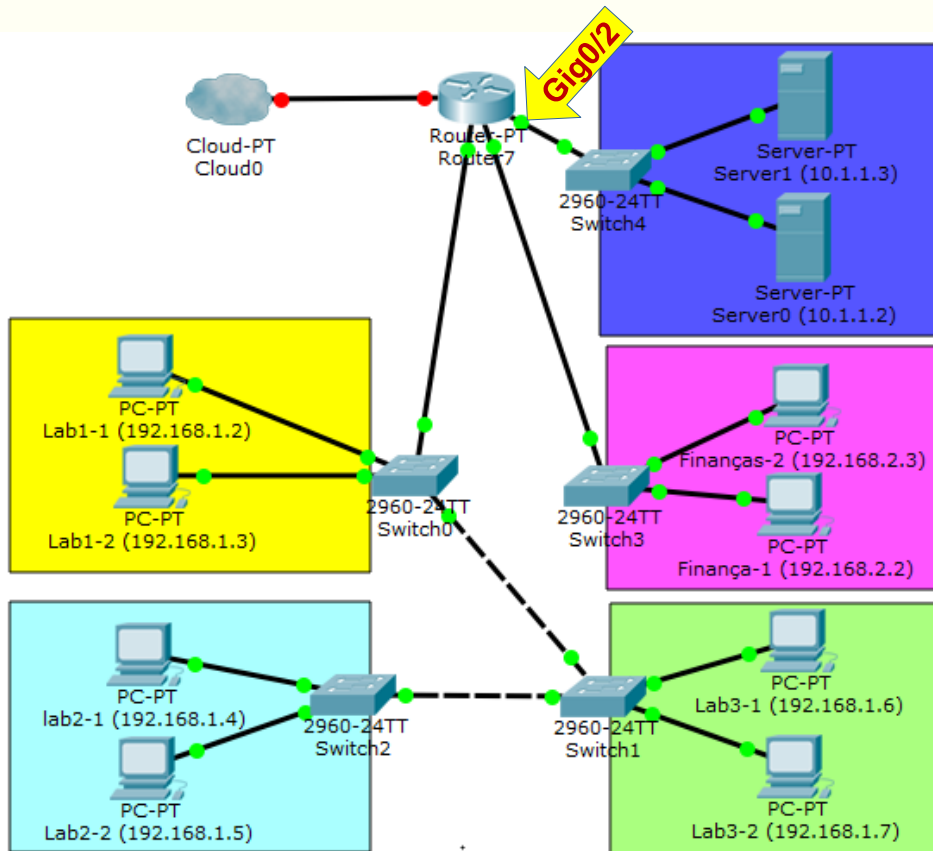
Configurar ACLs para:

2. Não permitir que pacotes do host **192.168.1.3** alcancem a rede **192.168.2.0**

Configurar ACLs no roteador Router7:

```
Router>
Router>enable
Router#configure terminal
Router(config)#access-list 1 deny host 192.168.1.3
Router(config)#access-list 1 permit any
Router(config)#
Router(config)#interface gig0/0
Router(config-if)#ip access-group 1 out
Router(config-if)#
```


Atividade Prática:



Configurar ACLs no roteador **Router7**:

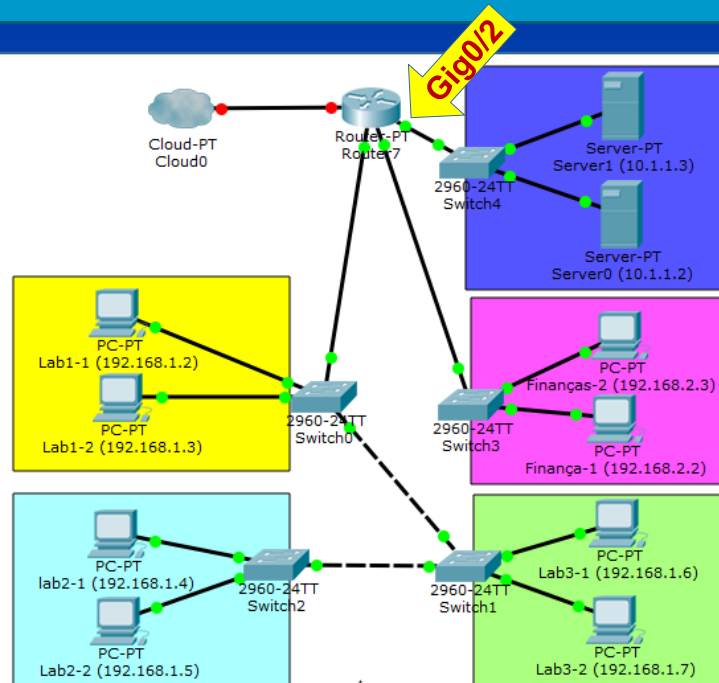
Configurar ACLs para:

3. Não permitir que os pacotes da rede

192.168.1.0 alcancem a rede 10.1.1.0

```
Router>
Router>enable
Router#configure terminal
Router(config)#access-list 1 deny host 192.168.1.2
Router(config)#access-list 1 deny host 192.168.1.3
Router(config)#access-list 1 deny host 192.168.1.4
Router(config)#access-list 1 deny host 192.168.1.5
Router(config)#access-list 1 deny host 192.168.1.6
Router(config)#access-list 1 deny host 192.168.1.7
Router(config)#access-list 1 permit any
Router(config)#
Router(config)#interface gig0/2
Router(config-if)#ip access-group 1 out
Router(config-if)#
```

Atividade Prática:



Configurar ACLs para:

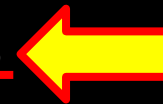
3. Não permitir que os pacotes da rede

192.168.1.0 alcancem a rede 10.1.1.0

Configurar ACLs no roteador Router7

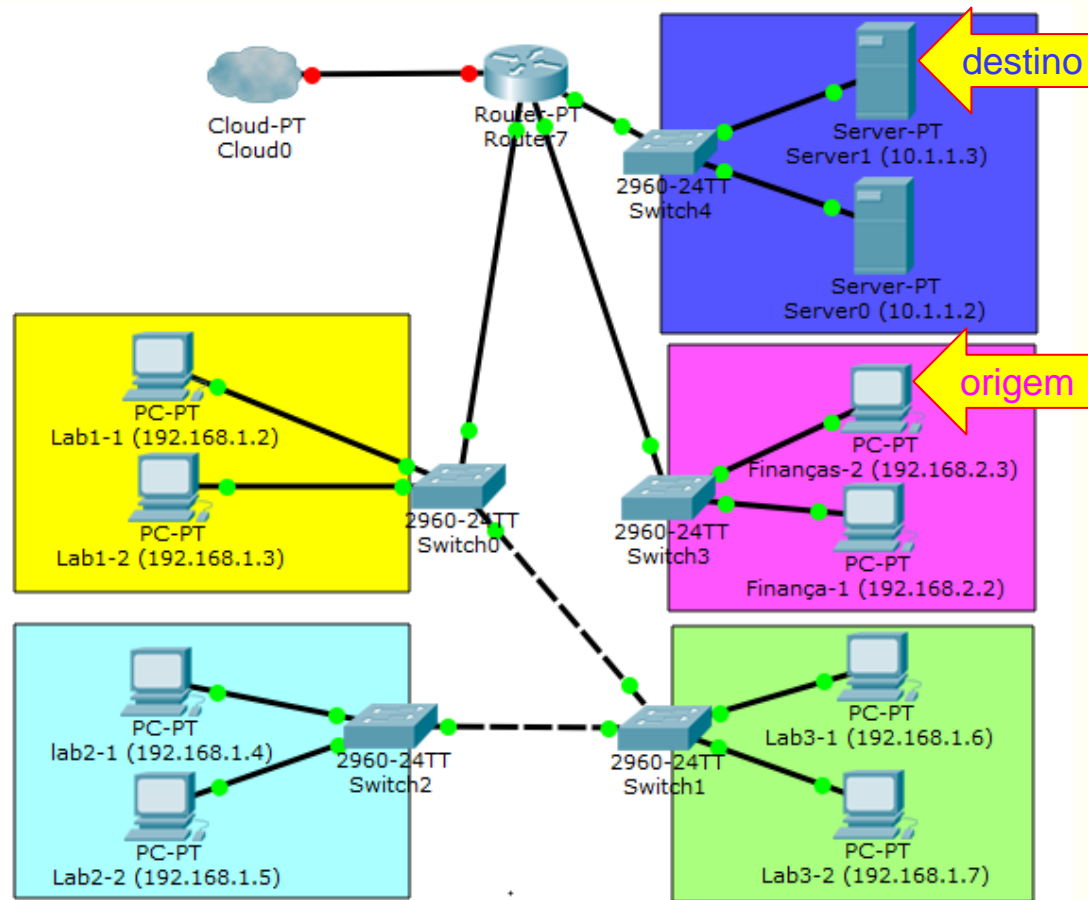
(outra solução, com uso de máscara curinga):

```
Router>
Router>enable
Router#configure terminal
Router(config)#access-list 1 deny 192.168.1.2 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#
Router(config)#interface gig0/2
Router(config-if)#ip access-group 1 out
Router(config-if)#
```



**Até o momento foram criadas regras
(ACL) que analisam apenas o
endereço de ORIGEM
dos pacotes de dados
(*access-control-list* padrão)**

Exemplo



Configurar ACLs para:

1. Não permitir que pacotes com origem no host com IPv4 **192.168.2.3** alcancem o host (servidor) com IPv4 **10.1.1.3**
 - origem: **192.168.2.3**
 - destino: **10.1.1.3**
2. Tudo o que não estiver explícito nas regras criadas até o momento deve estar **liberado**

**Configuração de regras para analisar o
endereço IPv4 de ORIGEM dos pacotes
e o
endereço IPv4 de DESTINO dos pacotes
(*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.

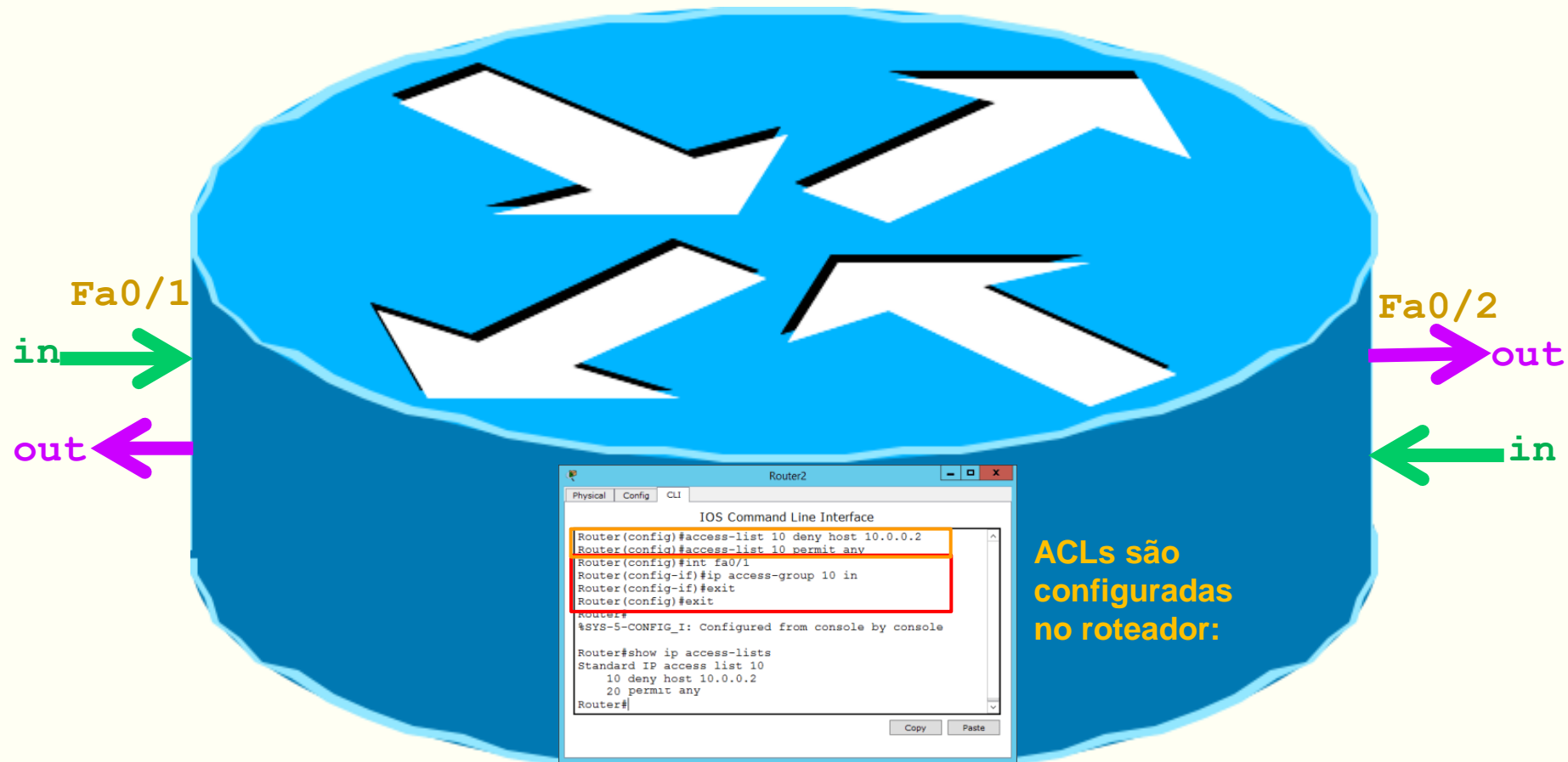
Access-List Estendidas: recordando

ACLs podem ser configurados para serem aplicados ao tráfego de entrada e/ou de saída de um roteador, como mostrado na figura.



- **ACLs de entrada** - os pacotes de entrada são processados antes de serem roteados para a interface de saída. Uma ACL de entrada é eficiente porque salva a sobrecarga de pesquisas de roteamento se o pacote é descartado. Se o pacote for permitido pela ACL, ele será processado para roteamento. As ACLs de entrada são mais usadas para filtrar pacotes quando a rede conectada a uma interface de entrada é a única origem dos pacotes que precisa ser examinada.
- **ACLs de saída** - os pacotes de entrada são encaminhados para a interface de saída e processados em seguida por meio da ACL de saída. As ACLs de saída são mais usadas quando o mesmo filtro é aplicado aos pacotes que vêm de várias interfaces de entrada antes de saírem da mesma interface de saída.

Access-List Estendidas: recordando

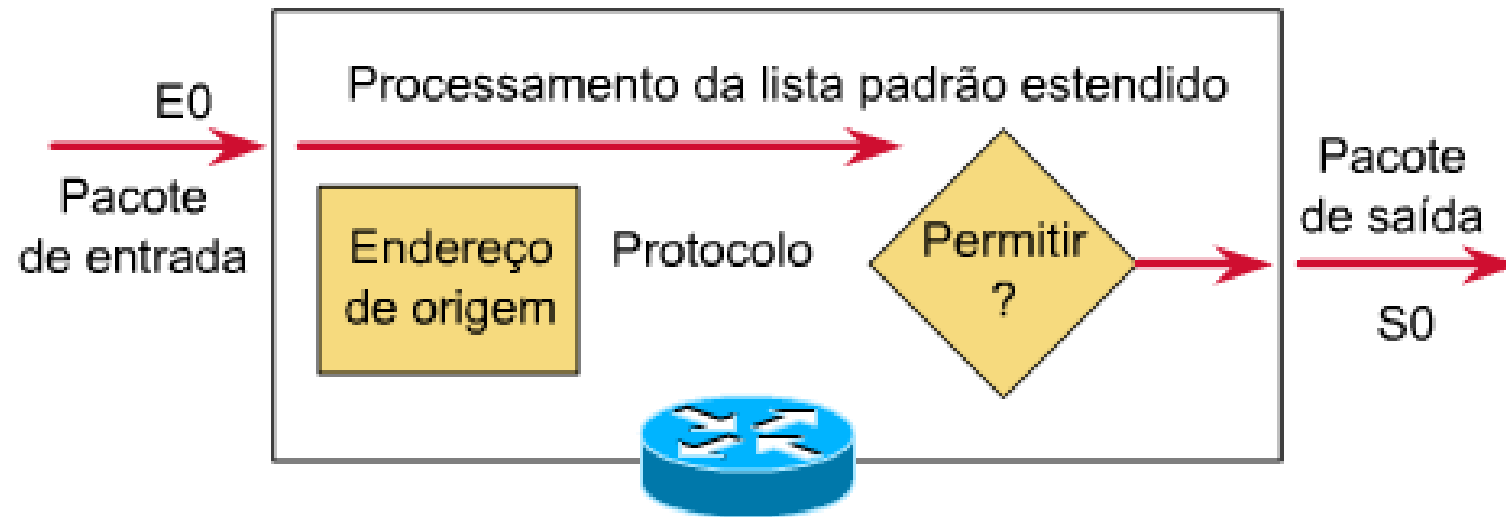


Para seu funcionamento ACLs precisam ser associadas a uma interface configuradas no roteador.

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.

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



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
```



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}
```

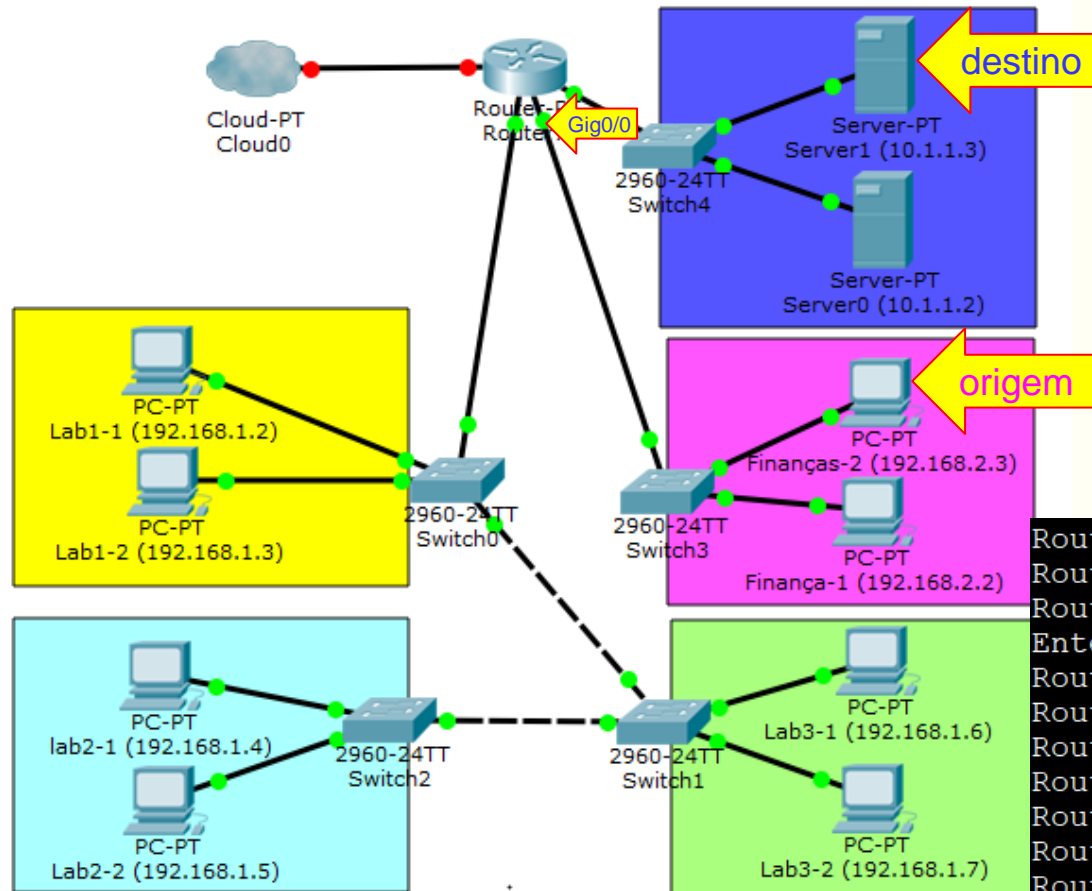
Exemplo:

```
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.

Atividade Prática:



Configurar ACLs para:

1. Não permitir que pacotes com origem no host com IPv4 **192.168.2.3** alcancem o host (servidor) com IPv4 **10.1.1.3**
 - origem: **192.168.2.3**
 - destino: **10.1.1.3**
2. Tudo o que não estiver explícito nas regras criadas até o momento deve estar **liberado**

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#access-list 100 deny ip host 192.168.2.3 host 10.1.1.3
Router(config)#access-list 100 permit ip any any
Router(config)#
Router(config)#interface gig0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#
```

A forma parcial do comando **access-list** estendida é:

Router(config)# access-list número-da-lista-de-acesso {permit | deny} protocolo origem destino

No exemplo:

router# access-list 100 permit ip host 192.168.2.3 host 10.1.1.3

4ª Atividade Avaliativa (Parte integrante da 1ª NAC)

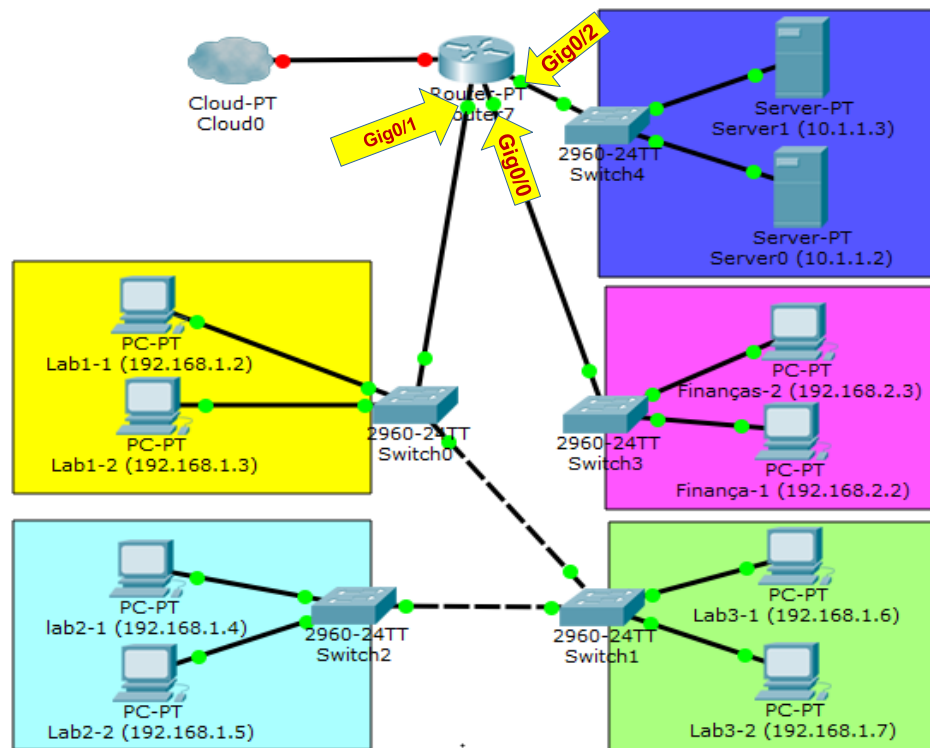
Configurar regras ACLs padrão para:

1. Não permitir a saída de pacotes com origem no host com IPv4 **192.168.1.2** da rede com IPv4 **192.168.1.0**
2. Não permitir que pacotes com origem no host com IPv4 **192.168.1.3** alcancem a rede com IPv4 **192.168.2.0**
3. Não permitir que os pacotes com origem na rede com IPv4 **192.168.1.0** alcancem a rede com IPv4 **10.1.1.0**

Configurar regras ACLs estendida para:

1. Não permitir que pacotes com origem no host com IPv4 **192.168.2.3** alcancem o host (servidor) com IPv4 **10.1.1.3**
2. 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 06 2023 ACL.pkt

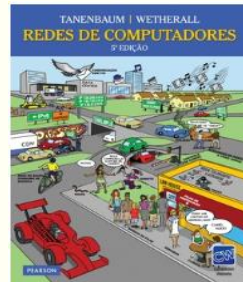
ATENÇÃO:

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