Redes de Computadores II

Na aula anterior

- Rotas dinâmicas

Na aula de hoje

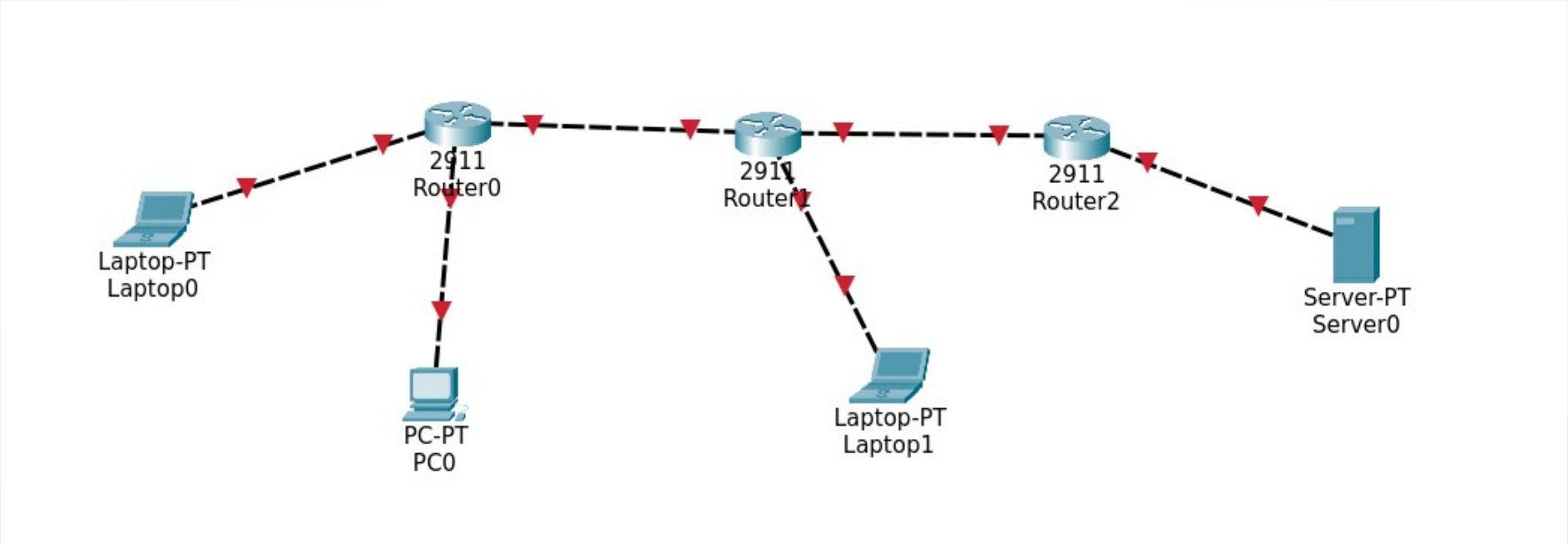
- Access Control List (ACL)

Access Control List (ACL)

- Mecanismo que permite que o equipamentos que usam o Cisco IOS incorpore as funcionalidades de um firewall simples
  - Mais usadas em roteadores pois são os elementos que interligam as redes

Proximidade

- Regras podem estar
  - Próximo da origem: evita tráfego desnecessário dentro da rede
  - Próximo do destino: mais simples de entender as regras em cada roteador



Tipos de regra

- Padrão: são mais simples mas não permitem detalhar portas e protocolos
- Extendidas: um pouco mais complexas mas dão maior controle ao administrador de redes

Regra padrão

- Sintaxe geral
  - Router(config)# access-list NUMERO TIPO ORIGEM [WILDCAST_MASK]

Importante: é essencial sempre adicionar pelo menos uma regra de permissão, pois, por padrão uma access list sempre tem comportamento de bloqueio. Esse tipo de acesso é chamado de acesso por white list, ou seja, todos são barrados, a menos que estejam permitidos explicitamente

Wildcard mask

- A wildcard mask (ou máscara coringa) é um conceito utilizado pelo protocolo OSPF. Calculamos o seu valor diminuindo a máscara de rede de 255.255.255.255
- Ex: Para uma rede /24 (255.255.255.0) a a wildcard mask será
  - 255. 255. 255. 255
- 255. 255. 255. 0
----
0. 0. 0. 255

Regras p/ hosts específicos

Router> enable

Router# configure terminal

Router(config)# access-list 10 permit host 192.168.1.10

Router(config)# access-list 10 deny host 192.168.1.20

Visualizando as regras

Router # show access-list

Comportamento padrão

Router> enable

Router# configure terminal

Router(config)# access-list 20 deny any

- Ou

Router(config)# access-list 20 permit any

Regras p/ múltiplos hosts

Router> enable

Router# configure terminal

Router(config)# access-list 11 permit 192.168.1.0 0.0.0.255

Router(config)# access-list 11 deny 192.168.2.0 0.0.0.255

Regras extendidas

- As regras extendidas permitem
  - adicionar o endereço de destino na regra
  - filtragem por porta
    - Algumas portas mais comuns ftp, pop3, smtp, telnet, www (http) podem ser referenciadas pelo nome
- Regras extendidas tem id entre 100 e 199, enquanto as normais devem usar o id entre 01 e 99.

Regras por portas específicas

Router> enable

Router# configure terminal

Router(config)# access-list 12 permit tcp host 192.168.1.10 host 192.168.2.20 eq 80

- Acessando o protocolo pelo nome:

Router(config)# access-list 12 permit tcp host 192.168.1.10 host 192.168.2.20 eq ftp

Referências

- Configurar e filtrar listas de acesso IP https://www.cisco.com/c/pt_br/support/docs/security/ios-firewall/23602-confaccesslists.html
-