Redes Convergentes

Laboratório de Projetos

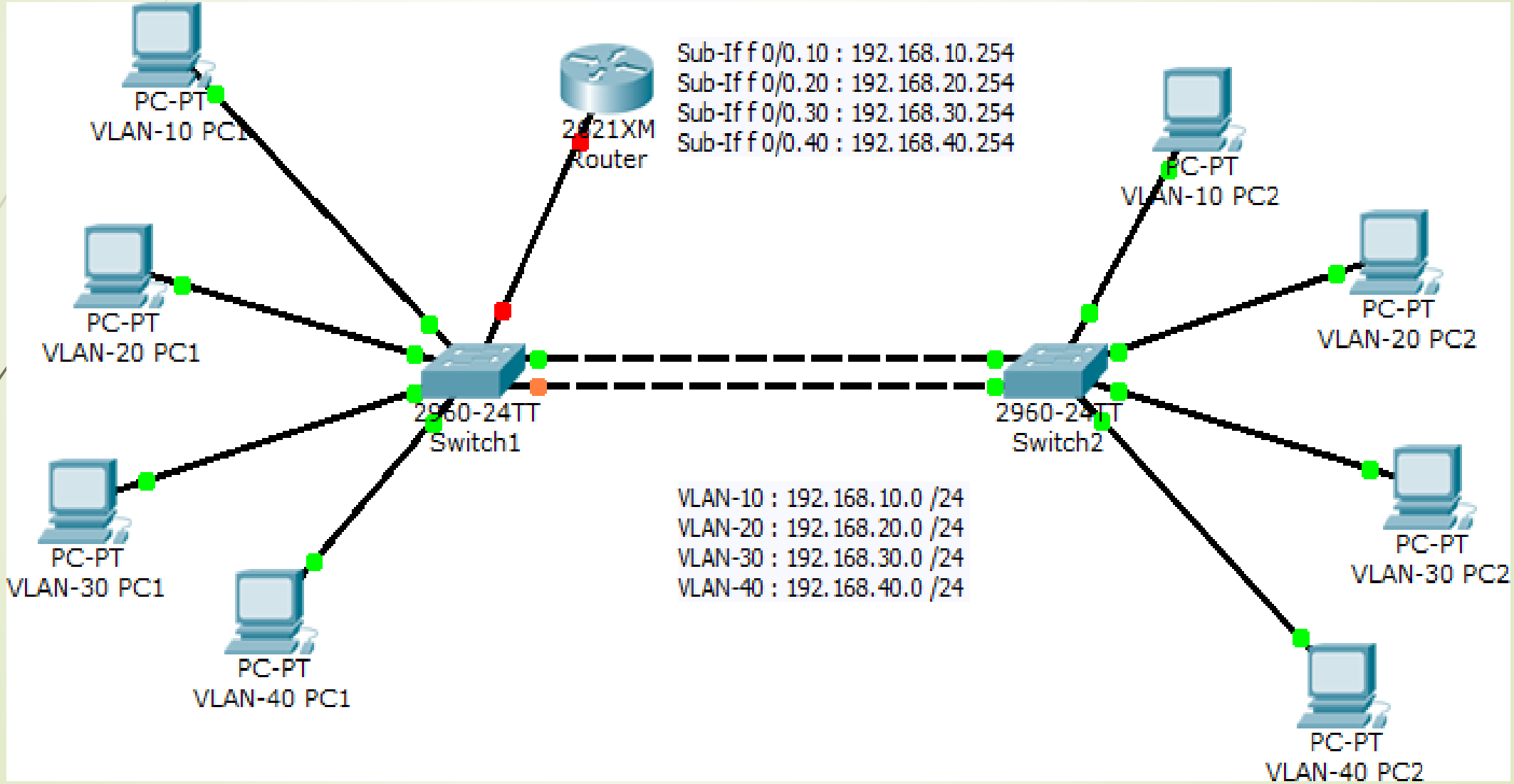
Prof. Wellington Brito

Redes Convergentes

Projetos VLAN

Prof. Wellington Brito

Configuração de switches e VLANs



Configuração de switches e VLANs

Proposta: 2 switches CISCO interligados com redundância (dois cabos) em um cenário que requer a utilização de VLANs (redes virtuais)

- No cenário proposto, serão configurados:

➢VLANs;

➢Roteamento Inter-VLANs (802.1q);

➢VTP (Virtual Trunk Protocolo).

Detalhes

- Existe redundância entre os 2 switches
- Os modelos da CISCO fazem isso automaticamente via STP
- STP = Spanning Tree Protocol
- Esse protocolo bloqueia uma das portas redundantes para evitar a ocorrência de loops

Configuração nos PCs das sub-redes

- O fato das máquinas estarem fisicamente conectadas aos mesmos switches não é suficiente para garantir a comunicação entre os computadores que estejam logicamente configurados em sub-redes distintas;
- Não existe comunicação na camada de REDE, porém o domínio de broadcast na camada de ENLACE ainda é único para todo o switch...

Continua...

Configuração nos PCs das sub-redes

- ... dessa forma, quadros podem ser capturados e o desempenho da rede ficará comprometido
- Para contornar essa limitação, faremos uso de VLANs associadas às sub-redes para quebrar o domínio de broadcast (segurança e desempenho)

VLANs

- Uma instância virtualizada de um switch lógico dentro de um switch físico;
- Por exemplo, se criarmos 4 VLANs num switch físico equivale a 4 switches lógicos.

Plano de IPs por VLAN

HOST	IP	MASK	GW
VLAN10-PC1	192.168.10.1	/24	192.168.10.254
VLAN10-PC2	192.168.10.2	/24	192.168.10.254
VLAN20-PC1	192.168.20.1	/24	192.168.20.254
VLAN20-PC2	192.168.20.2	/24	192.168.20.254
VLAN30-PC1	192.168.30.1	/24	192.168.30.254
VLAN30-PC2	192.168.30.2	/24	192.168.30.254
VLAN40-PC1	192.168.40.1	/24	192.168.40.254
VLAN40-PC1	192.168.40.2	/24	192.168.40.254

Configuração dos switches e VLANs

- Faremos a ativação do **VTP** (Virtual Trunk Protocolo) para que todas as configurações de **VLAN** de um switch operando em modo **SERVIDOR** sejam automaticamente propagadas para todos os demais switches **CLIENTES** da rede
- Teremos um domínio de switches chamado de **REDES**

Modos de um Switch

- SERVIDOR: adicionam, alteram e removem VLANs e propagam as alterações;
- CLIENTE: recebem as configurações do switch servidor;
- TRANSPARENTE: membro do domínio, mas não aplica as configurações de VLANs para ele mesmo, somente no seu contexto local, não propagando para os demais.

Switch SERVIDOR - Parte 1 de 2

```
enable
configure terminal
hostname Switch1
vtp mode server
vtp domain NOME
vlan 10
name VLAN-10
vlan 20
name VLAN-20
vlan 30
name VLAN-30
vlan 40
name VLAN-40
end
```

Switch SERVIDOR - Parte 2 de 2

configure terminal
interface f 0/1
switchport access vlan 10
interface f 0/2
switchport access vlan 20
interface f 0/3
switchport access vlan 30
interface f 0/4
switchport access vlan 40
interface f 0/24
switchport mode trunk
interface range g 1/1 - 2
switchport mode trunk
end

Switch CLIENTE

enable
configure terminal
hostname Switch2
vtp mode client
vtp domain NOME
end
configure terminal
interface f 0/1
switchport access vlan 10
interface f 0/2
switchport access vlan 20
interface f 0/3
switchport access vlan 30
interface f 0/4
switchport access vlan 40
interface range g 1/1 – 2
switchport mode trunk
End

Roteador

- Temos agora 4 redes distintas conectadas em 2 switch fazendo uso de VLANs;
- Essas redes não se comunicam entre si, mas um roteador pode realizar tal procedimento;
- Em tese precisaríamos de 4 interfaces físicas no roteador para ligar cada uma das 4 redes, o que não é interessante ($$$);
- Fazemos uso então do **modo trunk** (com **encapusulamento dot1q**).

Roteador

enable
configure terminal
interface f 0/0
no shutdown
interface f 0/0.10
encapsulation dot1Q 10
ip address 192.168.10.254 255.255.255.0
interface f 0/0.20
encapsulation dot1Q 20
ip address 192.168.20.254 255.255.255.0
interface f 0/0.30
encapsulation dot1Q 30
ip address 192.168.30.254 255.255.255.0
interface f 0/0.40
encapsulation dot1Q 40
ip address 192.168.40.254 255.255.255.0
End

Exercício Lab – Análise das Saídas

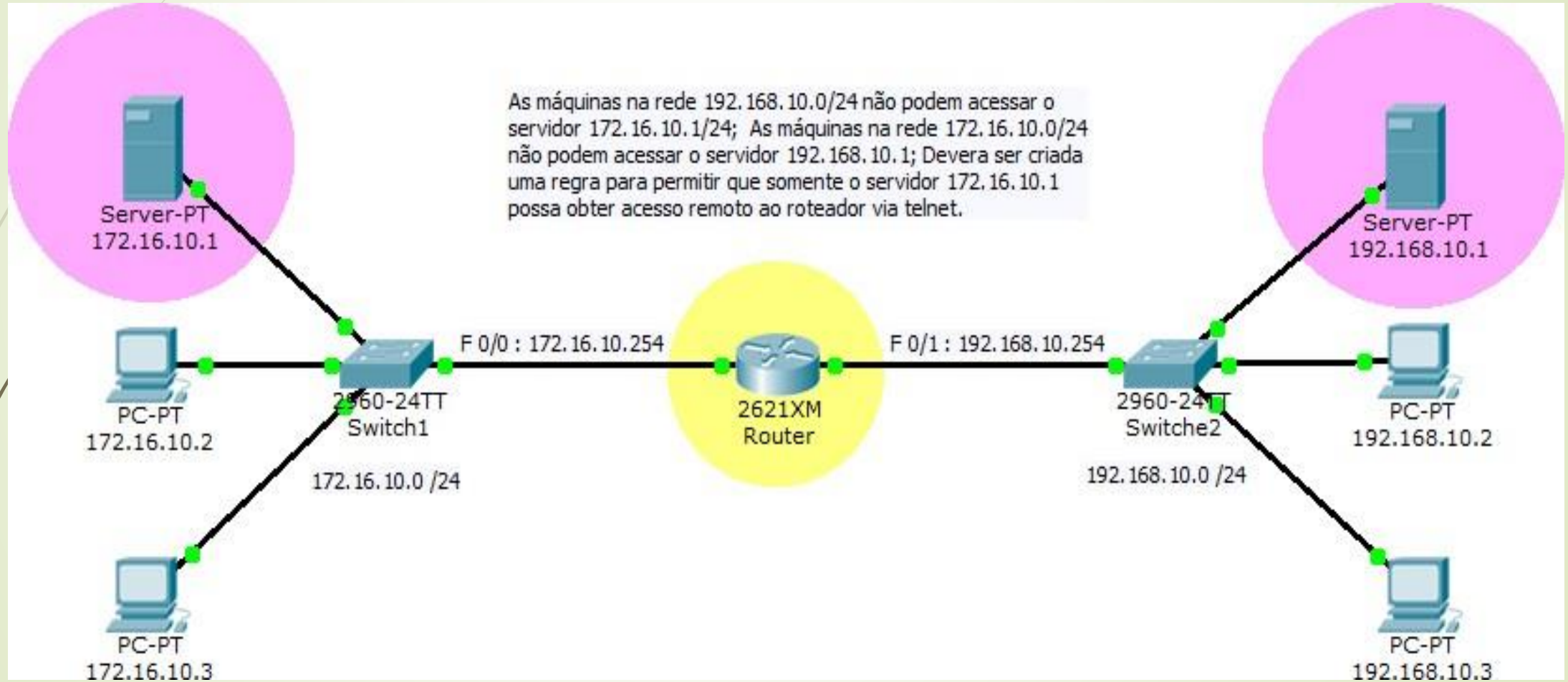
- Digite o comando (nos 2 switches):
  - ✓ *show mac-address-table*
  - ✓ *show vlan*
  - ✓ *show interface trunk*
  - ✓ *show vtp status*
- Produza um relatório sucinto explicando o funcionamento da rede e analisando os dados mostrados pelos comandos acima...

Redes Convergentes

Laboratório de projeto: ACL

Prof. Wellington Brito

Lista de Controle de Acesso - ACL



ACLs

- ACL = Lista de Controle de Acesso
- Pode transformar um roteador em firewall
- Podemos criar regras de acesso específico

Explicação

- Somente a máquina 172.16.10.1 poderá obter acesso remoto ao roteador
- As máquinas da rede 192.168.10.0/24 deverão ser impedidas de acessar o servidor 172.16.10.1/24
- As máquinas da rede 172.16.100.0/24 não podem acessar o servidor 192.168.10.1/24

Entendendo as ACLs – CISCO

- Lembre-se que o roteador não consegue tratar máquinas da mesma rede, isso ocorre no switch ou ainda diretamente no servidor
- Podemos aplicar até 2 listas de acesso por porta de um roteador (in e out)
- Toda lista deve ter ao menos uma linha de permissão (permit), para não ocorrer o bloqueio total na interface (toda lista tem em seu final uma regra implícita que nega tudo que não foi previamente liberado)

Tipos de ACL

- Padrão: somente trabalha com endereços de origem e destino. São aplicadas o mais próximo possível do destino. (NEGATIVO)
- Estendida: trabalha na camada de transporte, portanto consegue identificar o tipo de aplicação, baseado no protocolo de uso. Recomenda-se aplicar as regras o mais próximo da origem possível. (POSITIVO)

Sintaxe - Lista Padrão

access-list <número> [permit/deny]
[IP origem]

Regra 1 - Lista Padrão
enable
configure terminal
access-list 10 permit 172.16.10.1
line vty 0 15
access-class 10 in

Sintaxe – Lista Estendida

- access-list <número> [permit/deny] [protocolo] [IP de origem] [IP de destino] [número da porta ou nome do protocolo]

  Obs: Protocolo de Rede ou Transporte: ip, udp ou tcp

Regras – Lista Estendida

Regra 2 - Lista Estendida
access-list 100 deny ip 192.168.10.0 0.0.0.255 host 172.16.10.1
access-list 100 permit ip any any
interface f 0/1
ip access-group 100 in
Regra 3 - Lista Estendida
access-list 110 deny ip 172.16.10.0 0.0.0.255 host 192.168.10.1
access-list 110 permit ip any any
interface f 0/0
ip access-group 110 in

Exercício Lab - Análise das Saídas

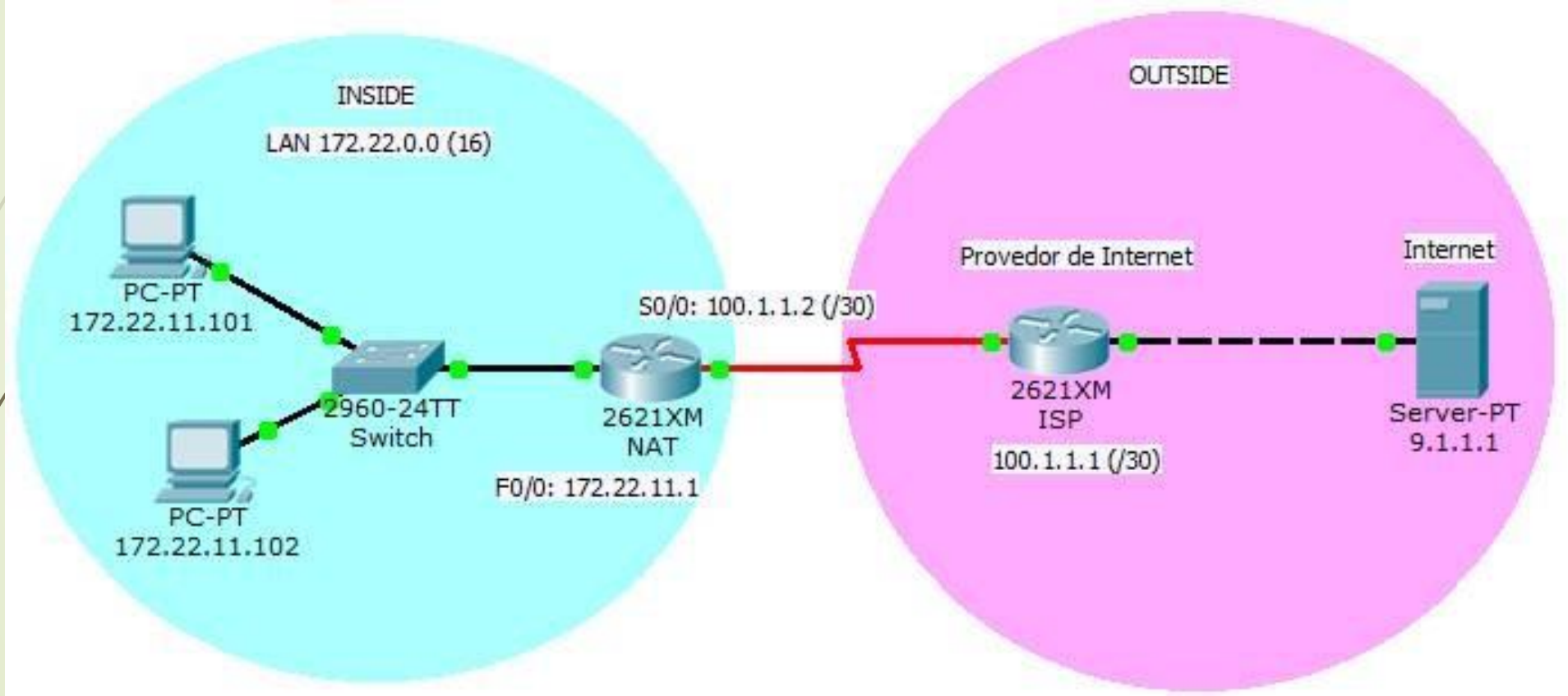
- Digite o comando (no roteador):
  - *show run*
  - *show ip access-list*
  - *show ip interface f 0/0*
  - *show ip interface f 0/1*
- Produza um relatório sucinto explicando o funcionamento da rede e analisando os dados mostrados pelos comandos acima...

Redes Convergentes

Laboratório de projeto: NAT

Prof. Wellington Brito

NAT


INSIDE
LAN 172.22.0.0 (16)
OUTSIDE
PC-PT
172.22.11.101
Provedor de Internet
Internet
S0/0: 100.1.1.2 (/30)
2960-24TT
Switch
2621XM
NAT
F0/0: 172.22.11.1
2621XM
ISP
100.1.1.1 (/30)
Server-PT
9.1.1.1
PC-PT
172.22.11.102

NAT

- Faremos tradução de endereços privados (frios) para um endereço público (quente) fornecido pelo provedor de Internet (ISP)
- Temos a rede local 172.22.0.0/16 que passará por um roteador que irá fazer a tradução dos endereços (NAT)

Config. do Roteador do Provedor

enable
configure terminal
no ip domain lookup
hostname Router-ISP
interface f 0/0
ip address 9.0.0.1 255.0.0.0
no shut
interface s 0/0
ip address 100.1.1.1 255.255.255.252
clock rate 500000
no shut
end

IPs dos PCs e do Servidor

Hostname	Rede	Interface	Gateway
PC-PT1	172.22.11.101	S 0/0	172.22.11.1
PC-PT2	172.22.11.102	F 0/0	172.22.11.1
SERVIDOR	9.1.1.1	F 0/1	9.0.0.1

Roteador da Empresa

- A interface fast-ethernet do roteador receberá um IP para se comunicar com a rede interna;
- A interface serial estará conectada a WAN e receberá um IP fixo do provedor de Internet;
- Teremos também um rota default, cuja saída apontará para a interface serial conectada ao provedor de Internet;
- Toda rede de destino que não for encontrada na tabela de rotas será encaminhada para a interface serial (ex: Internet).

Config. Roteador Empresa

enable
configure terminal
no ip domain lookup
hostname Router-NAT
ip route 0.0.0.0 0.0.0.0 serial 0/0
interface f 0/0
ip address 172.22.11.1 255.255.0.0
no shut
inteface s 0/0
ip address 100.1.1.2 255.255.255.252
no shut
end

Definição das zonas “inside” e “outside”

- Nos roteadores da CISCO precisamos informar ao NAT qual interface representa a rede local (nat inside) e qual interface representa a conexão com a Internet (nat outside)...

Conf. Zonas - Roteador Empresa

enable
configure terminal
interface f 0/0
ip nat inside
interface s 0/0
ip nat outside
end

ACL e NAT

- Antes de ativar o NAT precisamos criar uma ACL informando quais hosts poderão participar do processo de tradução e acesso a Internet
- Depois de criar a ACL, basta aplicá-la em conjunto com o comando que ativa a tradução de endereços...

Conf. NAT – Roteador Empresa

enable
configure terminal
access-list 1 permit 172.22.11.0 0.0.255.255
ip nat inside source list 1 interface s0/0 overload
end

Exercício – Análise das Saídas

- Digite o comando (no roteador da empresa):
  - ✓ show run
  - ✓ show ip nat statistics
  - ✓ show ip nat translations
- Produza um relatório sucinto explicando o funcionamento da rede e analisando os dados mostrados pelos comandos acima...

Bibliografia

- KUROSE, James F. Redes de Computadores e a Internet: uma abordagem top-down – 6 ed. São Paulo. Pearson Education do Brasil. 2013.
- Cisco Networking Academy (www.cisco.com ou https://www.netacad.com/pt-br).