



***TIC***

***AULA 13 - 14***

***PROF. ROBERTO***

# ***O QUE VAMOS VER NESSA AULA***

## ■ Switches:

- Layer 3;
- Roteamento inter-VLAN;
- Segurança:
  - Port Security;
  - BPDU Guard;
  - Root Guard;
  - DHCP Snooping;
- EtherChanel;
- HSRP;
- ACLs:
  - Controle de Tráfego;
- Redes Sem fio.



The background features a complex network diagram with nodes and connecting lines in shades of blue and purple. Overlaid on this are several geometric shapes: a large black trapezoid on the left, a yellow and orange diagonal band across the middle, and various triangular and polygonal shapes in orange, yellow, and black at the corners. The overall aesthetic is modern and technological.

1.

# *SWITCH*

Layer 3

# LAYER 3



- Um switch **Layer 3** combina funções de switches de camada 2 e roteadores de camada 3.
- **Funcionalidade principal:** Ele é capaz de rotear pacotes entre diferentes VLANs, além de realizar switching dentro de uma VLAN.
- **Benefícios:**
  - Menor latência comparado ao uso de um roteador externo para o roteamento entre VLANs.
  - Simplicidade ao integrar roteamento e switching em um único dispositivo.

# LAYER 3 - DIFERENÇAS



- **Layer 2:** Switches tradicionais que funcionam na camada de enlace e usam MAC addresses para encaminhar tráfego.
- **Layer 3:** Além do switching, também realiza roteamento baseado em IP addresses, assim como um roteador.
- Quando usar cada um?
  - Use Layer 2 para segmentação simples dentro de uma VLAN.
  - Use Layer 3 para rotear entre VLANs (inter-VLAN routing).



# *SWITCH L3 E MODULO NEXAN*



# SWITCH L3 E MODULO NEXAN



TECNOLOGIA

TIC



INFORMAÇÃO



COMUNICAÇÃO

Característica	Switch Layer 2 (L2)	Switch Layer 3 (L3)
Função Principal	Faz comutação de pacotes dentro de um VLAN	Realiza comutação e roteamento entre VLANs
Endereçamento	Usa endereços MAC para encaminhar pacotes	Usa endereços MAC e endereços IP
Roteamento	Não suporta roteamento IP	Suporta roteamento entre VLANs (Inter-VLAN Routing)
Tabela de Encaminhamento	Mantém apenas a Tabela de Endereços MAC	Mantém Tabela de Endereços MAC e Tabela de Roteamento
Gateway	Não pode atuar como gateway de rede	Pode atuar como gateway de rede para diferentes sub-redes
Protocolos de Roteamento	Não suporta protocolos de roteamento IP	Suporta protocolos como OSPF, RIP, EIGRP, etc.

# LAYER 3 INTER-VLAN



- Quando temos várias VLANs (exemplo: uma VLAN para o departamento de TI e outra para RH), as VLANs não podem se comunicar diretamente.
- Um switch Layer 3 pode rotear o tráfego entre as VLANs, permitindo a comunicação entre elas.
- Exemplo de Configuração:
  - **Switch(config)# interface vlan 10**
  - **Switch(config-if)# ip address 192.168.10.1 255.255.255.0**
  - **Switch(config-if)# no shutdown**

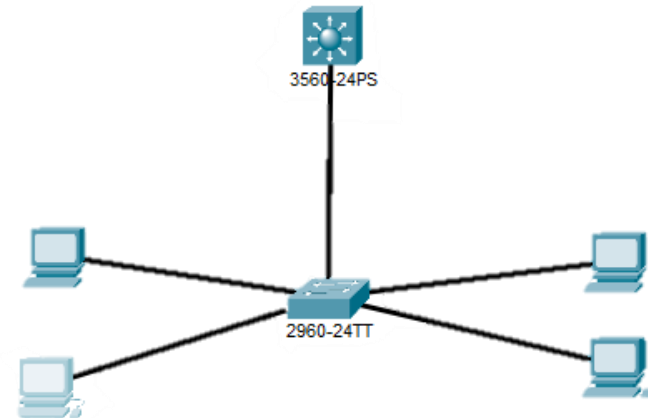


# LAYER 3 INTER-VLAN



## Equipamentos:

- SW L3 - 3560;
- SW L2 - 2960;
- SW L2 G1 → SW L3 Fast 1
- 2 PC VLAN ADM - Portas 1 e 2
- 2 PC VLAN TI - Portas 10 e 11



# LAYER 3 INTER-VLAN



TECNOLOGIA

TIC



INFORMAÇÃO



COMUNICAÇÃO

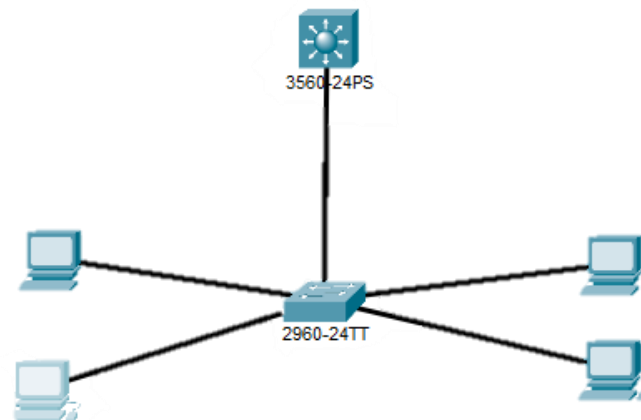
## Configuração dos PCs:

### PC0 e PC1 (VLAN 10):

- ▶ IP: 192.168.10.2 (PC0)
- ▶ IP: 192.168.10.3 (PC1)
- ▶ Gateway: 192.168.10.1

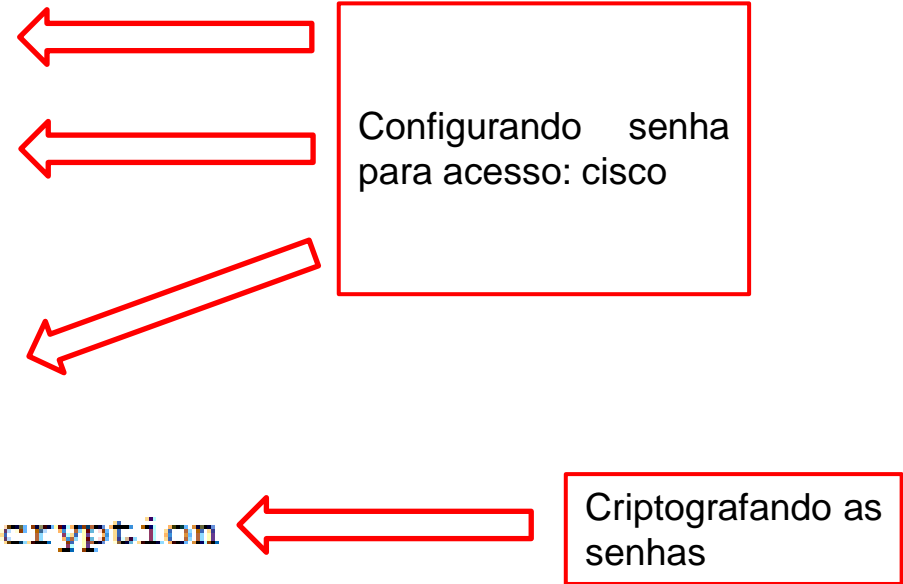
### PC2 e PC3 (VLAN 20):

- ▶ IP: 192.168.20.2 (PC2)
- ▶ IP: 192.168.20.3 (PC3)
- ▶ Gateway: 192.168.20.1



# CONFIG SW-CORE

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname CORE
CORE(config)#enable secret cisco
CORE(config)#line con 0
CORE(config-line)#password cisco
CORE(config-line)#login
CORE(config-line)#exit
CORE(config)#line vty 0 4
CORE(config-line)#password cisco
CORE(config-line)#login
CORE(config-line)#exit
CORE(config)#service password-encryption
```



Configurando senha para acesso: cisco

Criptografando as senhas

# CONFIG SW-CORE

```
CORE(config)#vlan 10
CORE(config-vlan)#name VLAN_10
CORE(config-vlan)#exit
CORE(config)#vlan 20
CORE(config-vlan)#name VLAN_20
CORE(config-vlan)#exit
CORE(config)#interface vlan 10
CORE(config-if)#ip address 192.168.10.1 255.255.255.0
CORE(config-if)#no shutdown
CORE(config-if)#exit
CORE(config)#interface vlan 20
CORE(config-if)#ip address 192.168.20.1 255.255.255.0
CORE(config-if)#no shutdown
CORE(config-if)#exit
CORE(config)#ip routing
```

Configurando as  
Vlans

Definindo IP das  
VLANs

Habilitando  
Roteamento para as  
VLANs

```
SW-1(config)#interface fastethernet0/1
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 10
SW-1(config-if)#exit
SW-1(config)#interface fastethernet0/2
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 10
SW-1(config-if)#exit
SW-1(config)#interface fastethernet0/10
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 20
SW-1(config-if)#exit
SW-1(config)#interface fastethernet0/11
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 20
SW-1(config-if)#exit
```

Configuração portas  
switch SW-1

```
SW-1(config)#interface gi0/1
SW-1(config-if)#switchport mode trunk

SW-1(config-if)#switchport trunk allowed vlan all
SW-1(config-if)#no shutdown
SW-1(config-if)#exit
```

Configurando porta  
conectada ao CORE  
para modo TRUNK

## ■ Configurando portas TRUNK.

```
S0#  
S0#en  
S0#enable  
S0#conf t  
Enter configuration commands, one per line.  End with CNTL/Z.  
S0(config)#interface range giga  
S0(config)#interface range gigabitEthernet 0/1 - 2  
S0(config-if-range)#sw  
S0(config-if-range)#switchport mod  
S0(config-if-range)#switchport mode tr  
S0(config-if-range)#switchport mode trunk
```

Selecione mais de 1 porta ao mesmo tempo

Configurando portas selecionadas para modo TRUNK



## LAYER 3 - TROUBLESHOOTING



- Em switches Layer 3, é importante verificar as rotas e o status das interfaces para garantir que o roteamento inter-VLAN esteja funcionando corretamente.
- Dois principais comandos:
  - **show ip Route**
  - **show ip interface brief**
  - Esses comandos ajudam a verificar as interfaces de VLAN (SVI) e as rotas no switch.

## LAYER 3 – TROUBLESHOOTING – LISTA DE COMANDOS



- show ip route** - Exibe a tabela de roteamento do switch Layer 3.
- show ip interface brief** - Exibe o status das interfaces e os endereços IP configurados.
- show vlan brief** - Exibe as VLANs configuradas e as portas associadas.
- show ip protocols** - Exibe os protocolos de roteamento dinâmico configurados.
- show interfaces** - Exibe o status detalhado das interfaces e estatísticas de transmissão.
- show running-config** - Exibe a configuração ativa do switch.
- show spanning-tree** - Exibe o status do protocolo Spanning Tree e o estado das portas.
- show ip arp** - Exibe a tabela ARP que mapeia endereços IP para endereços MAC.
- ping** - Testa a conectividade com um dispositivo na rede.
- traceroute** - Exibe o caminho que os pacotes percorrem até um destino.
- show mac address-table** - Exibe a tabela de endereços MAC e suas associações com portas.
- show ip dhcp binding** - Exibe as concessões de DHCP ativas no switch.
- show ip nat translations** - Exibe a tabela de traduções de NAT (se aplicável).
- show ip bgp summary** - Exibe o status das sessões BGP (se aplicável).
- show ip ospf neighbor** - Exibe o status das adjacências OSPF (se aplicável).

The background features a complex network diagram with nodes and connecting lines in shades of blue, purple, and pink. Overlaid on this are several geometric shapes: a large black trapezoid on the left, a yellow and orange diagonal stripe on the top right, and a yellow and orange diagonal stripe on the bottom right. There are also patterns of small triangles in the top left and bottom right corners.

2.

# ***SWITCH***

Layer 3 - Segurança

## SW L3 - SECURITY - PORT SECURITY



- Técnica de segurança para limitar o número de endereços MAC por porta.
- Protege contra ataques como **MAC flooding**, onde um invasor tenta esgotar a tabela CAM do switch.

### ■ Benefícios:

- Prevenção contra dispositivos não autorizados na rede.
- Controle sobre quantos dispositivos podem se conectar por uma porta específica.

# SW L3 - SECURITY - PORT SECURITY



## Tipos de Violação no Port Security:

- **Protect:** Descarta pacotes de endereços MAC desconhecidos, sem enviar alertas.
- **Restrict:** Descarta pacotes e gera logs e alertas.
- **Shutdown:** Desativa a porta quando ocorre uma violação de segurança (padrão).

# SW L3 - SECURITY - PORT SECURITY

```
Switch>
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTRL/Z.
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#switchport port-security mac-address sticky
```

Habilita segurança da porta

Limita a 1 dispositivo por porta

Desativa a porta em caso de violação.

Aprende dinamicamente o MAC e o associa à porta



## *SW L3 - SECURITY - PORT SECURITY*

```
Switch#show port-security interface fa0/1
Port Security           : Enabled
Port Status             : Secure-down
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 0
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

# SW L3 - SECURITY - PORT SECURITY



TECNOLOGIA

TIC



INFORMAÇÃO



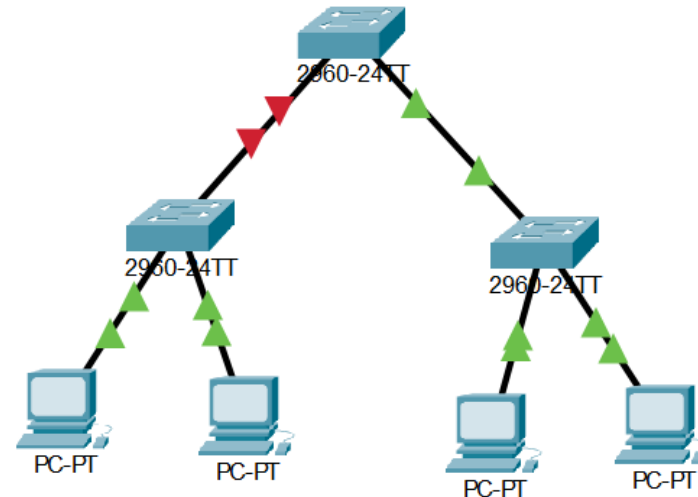
COMUNICAÇÃO

## Equipamentos:

- 3 SW 2960;
- 4 Computadores.

## Conexão:

- SW 1 Fast 1 → SW2
- SW 1 Fast 2 → SW3

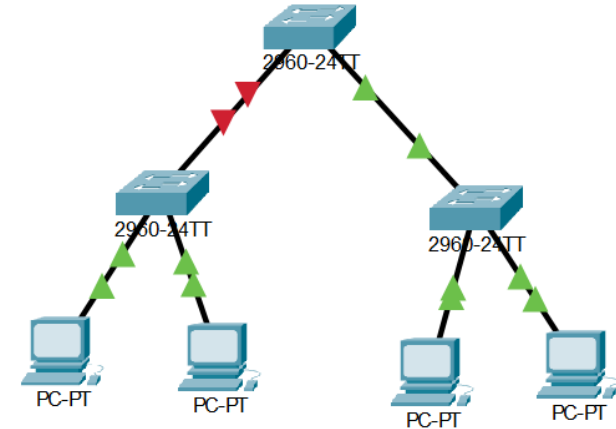


# SW L3 - SECURITY - PORT SECURITY



## Comandos SW1:

- interface fa0/1
- switchport mode access
- switchport port-security
- switchport port-security maximum 1
- switchport port-security violation shutdown
- switchport port-security mac-address sticky



## *SW L3 - SECURITY - PORT SECURITY*

```
show port-security interface fa0/1
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 00E0.F967.7678:1
Security Violation Count : 1
```

# SW L3 - SECURITY - PORT SECURITY - COMPARAÇÃO

## Sem Bloqueio

```
Switch#show port-security interface fa0/1
Port Security           : Enabled
Port Status             : Secure-down
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 0
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

## Com Bloqueio

```
show port-security interface fa0/1
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 00E0.F967.7678:1
Security Violation Count : 1
```

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
```

The background features a complex network diagram with various nodes (clouds, people icons, server racks) connected by lines. The color palette is dominated by blue, purple, and pink, with some orange and yellow accents. A large black polygonal shape is overlaid on the left side, containing the text. There are also some abstract geometric shapes like triangles and lines in orange and yellow at the corners.

2.

# *SWITCH*

Layer 3 - BPDU Guard



# SW L3 – SECURITY - BPDU GUARD E ROOT GUARD



BPDU (Bridge Protocol Data Unit) é um tipo de mensagem usada pelo Spanning Tree Protocol (STP) para prevenir loops na rede.

**Função:** As BPDUs são enviadas entre switches em uma rede para eleger a root bridge e garantir que só haja um caminho ativo entre dois switches.

**Tipos de BPDU:**

- **Configuration BPDU:** Usada para eleger a root bridge e calcular o caminho mais curto.
- **TCN BPDU (Topology Change Notification):** Usada para notificar alterações na topologia de rede, como quando uma porta é ativada ou desativada.

# SW L3 - SECURITY - BPDU GUARD



TECNOLOGIA

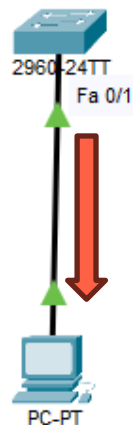
TIC



INFORMAÇÃO



COMUNICAÇÃO



interface Fa0/1  
switchport mode access  
spanning-tree bpduguard enable

Configuração porta específica  
Comando para configuração global:  
spanning-tree portfast bpduguard default

Nesta porta, configuramos o  
BPDU Guard para proteger a  
rede contra pacotes BPDUs  
inesperados

BPDU acontecendo

show interface status err-disabled



Se um dispositivo  
conectado a essa porta  
tentar enviar pacotes  
BPDU, o BPDU Guard  
desativará  
automaticamente a porta,  
colocando-a em estado err-  
disable para proteger a  
topologia da rede.

A porta pode ser reativada  
dando o comando no  
shutdown nela

Não conseguimos simular  
no Packet Tracer

# SW L3 – SECURITY - BPDU GUARD E ROOT GUARD



## Processo de Comunicação:

- **Eleição da Root Bridge:** Todos os switches enviam BPDUs anunciando seu ID (Bridge ID). O switch com o menor Bridge ID é eleito a root bridge.
- **Calcular o Caminho:** Os switches usam as BPDUs para determinar os caminhos mais curtos até a root bridge e desativam qualquer caminho redundante que possa causar loops.

## Frequência:

- As BPDUs são enviadas a cada 2 segundos em portas ativas de um switch para manter a estabilidade da topologia de rede.

# SW L3 - SECURITY - BPDU GUARD E ROOT GUARD



## Prevenção de Loops:

- As BPDUs permitem que o STP detecte loops de rede e desative portas que possam criar loops.
- Em uma rede sem BPDU ou STP, loops podem congestionar o tráfego, causando falhas na rede.

## Segurança com BPDU Guard:

- Em portas de acesso (onde não se espera que switches sejam conectados), o BPDU Guard pode ser ativado para desativar automaticamente a porta se BPDUs forem detectadas, prevenindo loops indesejados.

## *SW L3 - SECURITY - BPDU GUARD E ROOT GUARD*



- Protege a rede contra BPDUs (Bridge Protocol Data Units) em portas onde não deveria haver BPDUs, como portas de acesso.
- Previne loops e falsificação de STP.
- Configuração do **BPDU Guard**:
  - Habilite o BPDU Guard em portas de acesso para impedir que dispositivos enviem BPDUs e causem loops.

# SW L3 - SECURITY - BPDU GUARD E ROOT GUARD



TECNOLOGIA

TIC



INFORMAÇÃO



COMUNICAÇÃO

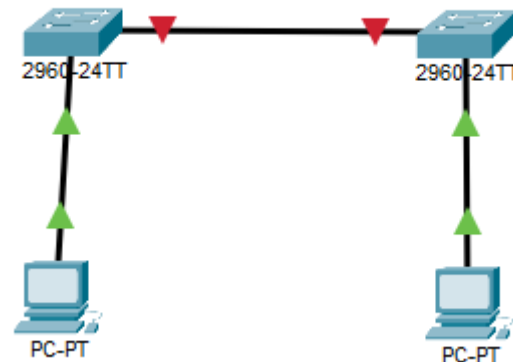
## Equipamentos:

- 2 SW 2960

- SW1 → SW2 (Fa 2/0)

- 2 Pcs

- IPs mesmo range





# SW L3 - SECURITY - BPDU GUARD E ROOT GUARD



TECNOLOGIA

TIC

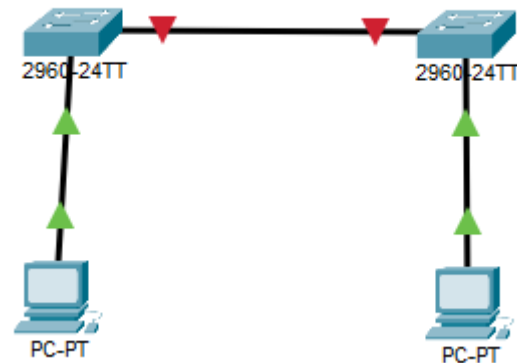


INFORMAÇÃO



COMUNICAÇÃO

- Configurando:
  - interface fa0/2
  - switchport mode access
  - spanning-tree bpduguard enable
  - Exit
- 
- show interfaces fa0/2 status



## Configuração SW1

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#exit
Switch(config)#%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet0/2 with
BPDU Guard enabled. Disabling port.

%PM-4-ERR_DISABLE: bpduguard error detected on 0/2, putting 0/2 in err-disable state

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

Switch#show interfaces fa0/2 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/2		err-disabled	1	auto	auto	10/100BaseTX

## Configuração SW1

```
Switch(config-if)#shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
```

```
Switch(config-if)#no sh
```

```
Switch(config-if)#no shutdown
```

```
Switch(config-if)#
```

```
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```

```
%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet0/2 with BPDU Guard enabled. Disabling port.
```

```
%PM-4-ERR_DISABLE: bpduguard error detected on 0/2, putting 0/2 in err-disable state
```

```
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
```

The background features a complex network diagram with nodes and connecting lines, overlaid on a blurred image of server racks. The nodes are represented by icons of people and clouds, with some nodes highlighted in pink. The overall color scheme is dominated by blue and purple hues, with orange and yellow geometric shapes and patterns (like triangles and stripes) providing contrast and a modern, tech-oriented feel.

2.

# *SWITCH*

Layer 3 - Root Guard

# SW L3 - SECURITY - ROOT GUARD



## Root Guard:

- É uma funcionalidade de segurança do Spanning Tree Protocol (STP) que impede que portas específicas de um switch participem da eleição para root bridge.
- Ele garante que uma determinada porta não permita que outro switch tente se tornar a root bridge, preservando a topologia definida da rede.

## Objetivo do Root Guard:

- **Proteger a Root Bridge:** O Root Guard impede que switches não autorizados ou mal configurados assumam a função de root bridge, o que poderia causar mudanças indesejadas na topologia da rede.

# SW L3 - SECURITY - ROOT GUARD



TECNOLOGIA

TIC



INFORMAÇÃO



COMUNICAÇÃO

Configuração Root Guard:  
interface fa0/1  
switchport mode trunk  
spanning-tree guard root



Root Guard detecta o BPDU do switch de acesso e coloca a porta em **root-inconsistente**  
Porta entra em shutdown temporariamente

**show spanning-tree inconsistentports**

Fa 0/1  
Trunk

Switch de acesso tentando ser Root Bridge

Gi 0/1



O Root Guard é uma funcionalidade de segurança usada no **Spanning Tree Protocol (STP)** para proteger a topologia da rede. Ele impede que dispositivos não autorizados se tornem a **Root Bridge**.

# SW L3 - SECURITY - ROOT GUARD



## Comandos:

- SWITCH(config)# interface fa0/1
- SWITCH(config-if)# spanning-tree guard root

## Verificar a configuração:

- SWITCH# show spanning-tree interface fa0/1 detail
- Switch# show spanning-tree inconsistentports



The background features a complex network diagram with nodes and connecting lines in shades of blue and purple. Overlaid on this are several geometric shapes: a large black trapezoid on the left, and various orange and yellow triangles and polygons on the right and bottom. Some of these shapes have patterns of small triangles or dots.

2.

# *SWITCH*

Layer 3 - DHCP SNOOPING



# SW L3 - SECURITY - DHCP SNOOPING



- **DHCP Snooping** é um mecanismo de segurança utilizado em switches Layer 2 para monitorar e controlar o tráfego DHCP na rede.
- Sua função principal é proteger contra servidores DHCP maliciosos (rogue DHCP) que podem tentar fornecer endereços IP inválidos ou prejudiciais aos dispositivos da rede.
- **Onde é Utilizado:**
  - DHCP Snooping é implementado em switches Layer 2, que são responsáveis por filtrar o tráfego entre dispositivos na rede e garantir que apenas os servidores DHCP confiáveis possam responder aos pedidos de DHCP.

# SW L3 - SECURITY - DHCP SNOOPING



TECNOLOGIA

TIC

INFORMAÇÃO



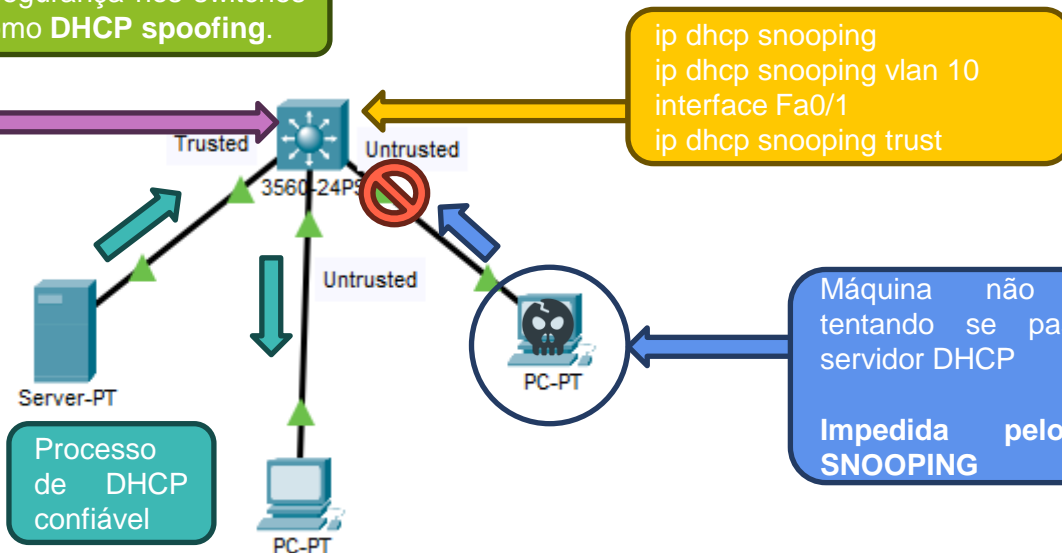
COMUNICAÇÃO

O **DHCP Snooping** é uma funcionalidade de segurança nos switches que protege a rede contra ataques de DHCP, como **DHCP spoofing**.

DHCP Snooping Binding Table

IP	MAC	VLAN	Porta
192.x.x.x	Aa:aa:aa:aa:aa:Aa	10	Fa0/1

DHCP Snooping permite apenas pacotes DHCP de resposta nas portas trusted, protegendo a rede contra ataques de spoofing.



## SW L3 - SECURITY - DHCP SNOOPING



**Portas confiáveis (trusted):** As portas conectadas a servidores DHCP legítimos são configuradas como confiáveis. O switch permite que respostas DHCP dessas portas alcancem os dispositivos da rede.

**Portas não confiáveis (untrusted):** Portas que não estão conectadas a servidores DHCP legítimos são configuradas como não confiáveis. Nessas portas, o switch bloqueia respostas DHCP para proteger a rede de servidores maliciosos.

# SW L3 - SECURITY - DHCP SNOOPING



TECNOLOGIA

TIC



INFORMAÇÃO



COMUNICAÇÃO

## Configuração no SW1:

- SW1(config)# ip dhcp snooping
- SW1(config)# ip dhcp snooping vlan 1
- SW1(config)# interface fa0/1
- SW1(config-if)# ip dhcp snooping trust
- SW1(config-if)# exit

## Comandos de Verificação:

- SW1# show ip dhcp snooping
  - ▶ Verifica o funcionamento
- SW1# show ip dhcp snooping binding
  - ▶ Verifica os dispositivos que receberam IP

# SW L3 - SECURITY - DHCP SNOOPING



## Quando usar?

- **Redes Corporativas e Data Centers:** Em grandes redes, o DHCP Snooping é essencial para garantir que os endereços IP sejam distribuídos apenas por servidores confiáveis.
- **Ambientes com Múltiplos Dispositivos:** Em redes com muitos dispositivos móveis ou de acesso público, o DHCP Snooping previne que servidores maliciosos ofereçam endereços IP incorretos.
- **Prevenção de Ataques MitM:** Evita que dispositivos recebam endereços IP de servidores maliciosos, protegendo contra ataques que comprometem a integridade dos dados.

The background features a complex network diagram with nodes and connecting lines in shades of blue and purple. Overlaid on this are several geometric shapes: a large black trapezoid on the left, and various orange and yellow angular shapes and patterns (like a triangle pattern) scattered around the edges.

2.

# *SWITCH*

Redundância

# STP - REVISÃO



**STP** é um protocolo de rede usado para evitar loops em topologias de switches.

## Eleição da Root Bridge:

- A root bridge é o switch com o menor Bridge ID.
- Os switches determinam o caminho mais curto para a root bridge e desativam portas redundantes para evitar loops.

## Desvantagem do STP:

- Convergência lenta: O STP pode levar entre 30 a 50 segundos para estabilizar a rede após uma mudança na topologia.

# STP - REVISÃO



■ Configurando:

□ spanning-tree mode pvst



# ***RSTP (RAPID SPANNING TREE PROTOCOL)***



**RSTP (Rapid Spanning Tree Protocol)**, definido pelo IEEE 802.1w, é uma evolução do STP e fornece convergência mais rápida.

## **Diferenças Chave entre STP e RSTP:**

- ☐ **Convergência rápida:** O RSTP reduz o tempo de convergência para menos de 10 segundos.

## **Novos Estados de Porta:**

- ☐ **Edge Ports:** Portas que não participam da topologia STP e conectam dispositivos finais.
- ☐ **Alternate/Backup Ports:** Portas que fornecem caminhos redundantes para rápida recuperação.

## **Comando:**

- ☐ `spanning-tree mode rapid-pvst`

**EtherChannel** é uma tecnologia que permite agrupar múltiplas interfaces físicas em uma única interface lógica para aumentar a largura de banda e fornecer redundância.

## Benefícios:

- Aumenta a largura de banda agregando vários links.
- Proporciona redundância; se um link falhar, o tráfego é distribuído pelos links restantes no grupo.

## Modos de EtherChannel:

- Static: Configurado manualmente em ambos os lados.
- LACP (Link Aggregation Control Protocol): Protocolo dinâmico que negocia automaticamente a formação de EtherChannels.

# ETHERCHANNEL



TECNOLOGIA

TIC



INFORMAÇÃO



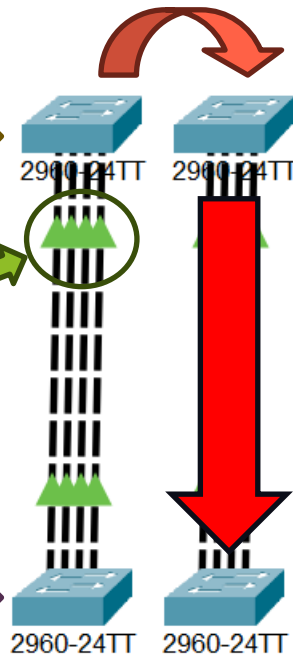
COMUNICAÇÃO

interface range fa x/x-x  
channel-group 1 mode active  
interface Port-channel 1  
switchport mode trunk  
switchport trunk allowed vlan all

**LACP:** Utiliza os modos **active** e **passive**.  
**PAgP:** Utiliza os modos **desirable** e **auto**.

Agregamos o link  
para aumentar a  
velocidade de  
comunicação.

O que muda no outro switch é apenas  
channel-group 1 mode passive



**LACP** (Link Aggregation Control Protocol) é um protocolo padrão aberto definido pelo IEEE 802.3ad. Ele permite a agregação de links entre dispositivos de diferentes fornecedores.

**PAgP** (Port Aggregation Protocol) é um protocolo proprietário da Cisco para agregação de links, usado apenas entre dispositivos Cisco.

# ETHERCHANNEL

## Configuração:

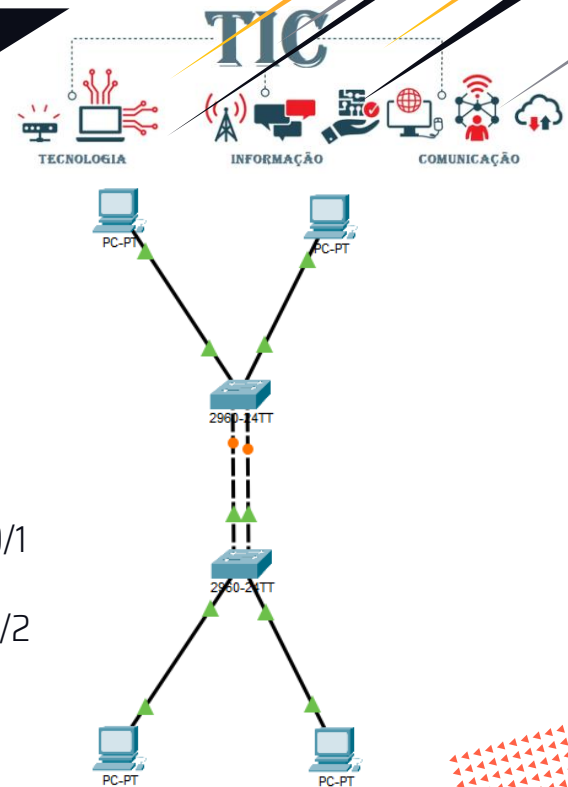
- 2 Switches (Modelo 2960 ou 3560).
- 2 PCs.

## Conexões:

### Conecte o SW1 ao SW2:

- ▶ Conecte um cabo Ethernet da porta Fa0/1 do SW1 para a porta Fa0/1 SW2.
- ▶ Conecte outro cabo Ethernet da porta Fa0/2 do SW1 para a porta Fa0/2 SW2.

### Conecte PCs.



## Configuração SW1 e SW2

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fa0/1 - 2
Switch(config-if-range)#channel-group 1 mode on
Switch(config-if-range)#exit
Creating a port-channel interface Port-channel 1
```

```
%LINK-5-CHANGED: Interface Port-channel1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
```

**Channel-group 1** → as interfaces serão agregadas ao Port-Channel 1

**Mode on** → EtherChannel será configurado no modo estático

## Configuração SW1 e SW2

```
Switch#show etherchannel summary
```

```
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```

```
Number of channel-groups in use: 1
```

```
Number of aggregators: 1
```

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	-	Fa0/1 (P) Fa0/2 (P)

Portas agregadas com  
sucesso

## Configuração SW1 e SW2

```
Switch(config)#interface range fastEthernet 0/1-2
Switch(config-if-range)#no channel-group 1
Switch(config-if-range)#
%LINK-3-UPDOWN: Interface Port-channell, changed state to down
```

Remover o channel-group 1  
para configurar o LACP

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channell, changed state to down
```

```
Switch(config)#interface range fa0/1 - 2
Switch(config-if-range)#channel-group 1 mode active
Switch(config-if-range)#exit
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```

LACP Ativo → SW inicia  
a procura.

## Configuração SW1 e SW2

```
Switch(config)#interface range fa0/1 - 2
Switch(config-if-range)#channel-group 1 mode passive
Switch(config-if-range)#exit
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```

LCAP Passivo → SW  
aguarda ser procurado.

### Regras de Operação entre LACP Ativo e Passivo:

**Ativo + Ativo:** Ambos os lados do link vão iniciar a negociação, e o EtherChannel será formado.

**Ativo + Passivo:** O lado ativo inicia a negociação, e o lado passivo responde, formando o EtherChannel.

**Passivo + Passivo:** Nenhum dos lados vai iniciar a negociação, então o EtherChannel não será formado.



## *HSRP (HOT STANDBY ROUTER PROTOCOL) – GATEWAYS REDUNDANTES*



- **HSRP (Hot Standby Router Protocol)** é um protocolo de alta disponibilidade e redundância usado em redes para garantir que haja um gateway redundante sempre disponível para os dispositivos da rede.
- O principal objetivo do HSRP é fornecer um gateway virtual que permanece acessível mesmo se o roteador ou switch principal falhar, evitando perda de conectividade.

# HSRP (HOT STANDBY ROUTER PROTOCOL) - GATEWAYS REDUNDANTES



```
interface GigabitEthernet0/0/0
ip address 192.168.1.2 255.255.255.0
standby 1 ip 192.168.1.1
standby 1 priority 110
standby 1 preempt
```

A prioridade mais alta (110) garante que o Router1 seja o ativo, enquanto o Router2, com prioridade 90, atuará como standby.

Verificar status com os comandos:  
**show standby brief**  
**show standby**

Computadores configurados com o IP da rede e Gateway 192.168.1.1

Gateway virtual:  
192.168.1.1



```
interface GigabitEthernet0/0/0
ip address 192.168.1.3 255.255.255.0
standby 1 ip 192.168.1.1
standby 1 priority 90
standby 1 preempt
```

Caso o gateway primário falhe o secundário assumirá automaticamente (preempt)

## *HSRP (HOT STANDBY ROUTER PROTOCOL) – GATEWAYS REDUNDANTES*



### **Como o HSRP Funciona:**

- Em uma rede, dispositivos (como PCs) precisam de um gateway para se comunicar fora de sua rede local (LAN).
- Sem HSRP, se o roteador ou switch que fornece esse gateway falhar, a conectividade é interrompida até que o equipamento seja restaurado.
- HSRP cria um endereço IP virtual que é compartilhado entre dois ou mais roteadores ou switches Layer 3. Se o roteador ou switch principal (ativo) falhar, o secundário (em espera ou standby) assume automaticamente o controle, minimizando o tempo de inatividade.

# HSRP (HOT STANDBY ROUTER PROTOCOL) – GATEWAYS REDUNDANTES



## Papéis no HSRP:

### □ Roteador Ativo (Active Router):

- ▶ É o roteador que atualmente encaminha o tráfego dos dispositivos na rede.
- ▶ É quem responde aos pacotes ARP para o gateway virtual.

### □ Roteador Standby (Standby Router):

- ▶ Fica em espera, pronto para assumir o papel de roteador ativo se o roteador ativo falhar.
- ▶ Monitora o status do roteador ativo através de mensagens HSRP.

### □ Gateway Virtual:

- ▶ O endereço IP virtual que é compartilhado pelos roteadores ativos e standby.
- ▶ Esse é o endereço IP que os dispositivos na rede configuram como seu gateway padrão.

## *HSRP (HOT STANDBY ROUTER PROTOCOL) – GATEWAYS REDUNDANTES*



### ■ Processo de Falha e Recuperação:

- Se o roteador ativo falhar (devido a uma falha de hardware ou software), o roteador standby detecta a falha e assume o papel de roteador ativo. O HSRP garante que esse processo de failover seja rápido e automático.
- Quando o roteador original volta a funcionar e é configurado com uma prioridade mais alta, ele pode preemptar o roteador standby e reassumir o papel de ativo.

# HSRP (HOT STANDBY ROUTER PROTOCOL) – GATEWAYS REDUNDANTES

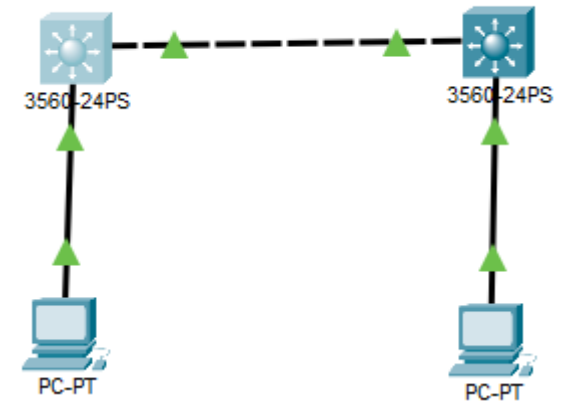


## Dispositivos:

- 2 Switches Layer 3 (modelo: 3560).
- 2 PCs para simular dispositivos na rede.

## Configuração Física:

- Conecte os PCs aos Switches:
  - Conecte o PC1 à porta Fa0/1 do SW1.
  - Conecte o PC2 à porta Fa0/1 do SW2.
- Conecte os Switches:
  - Conecte o SW1 ao SW2 através de um link na porta Fa0/2 de ambos os switches.



# HSRP (HOT STANDBY ROUTER PROTOCOL) - GATEWAYS REDUNDANTES

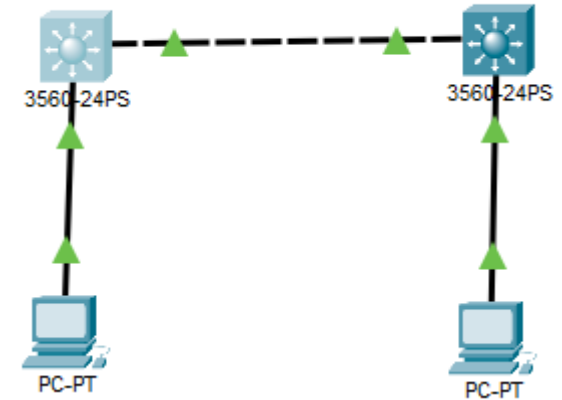


## Configuração de IP em PC1:

- Endereço IP: 192.168.10.10
- Máscara de Sub-rede: 255.255.255.0
- Gateway: 192.168.10.1

## Configuração de IP em PC2:

- Endereço IP: 192.168.10.20
- Máscara de Sub-rede: 255.255.255.0
- Gateway: 192.168.10.1



## Configuração SW1

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.10.2 255.255.255.0
Switch(config-if)#standby 1 ip 192.168.10.1
Switch(config-if)#standby 1 priority 110
Switch(config-if)#standby 1 preempt
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fa0/2
Switch(config-if)#no shutdown
Switch(config-if)#exit
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
%HSRP-6-STATECHANGE: Vlan10 Grp 1 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan10 Grp 1 state Standby -> Active
```

**standby 1 ip 192.168.10.1:**  
Define o gateway virtual para o grupo HSRP 1.

**standby 1 priority 110:**  
Define a prioridade do SW1 (o padrão é 100, valores mais altos ganham).


**standby 1 preempt:** Permite que o SW1 reassuma o controle quando voltar online.



## Configuração SW1

```
Switch(config)#do sh int fa0/2 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/2		connected	1	auto	auto	10/100BaseTX




Verifique se a vlan está na VLAN 10 Caso não esteja coloque a porta na Vlan 10

```
Switch(config-if)#switchport access vlan 10
```

```
Switch(config-if)#do sh int fa0/2 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/2		connected	10	auto	auto	10/100BaseTX



Só funcionará se os 2 SW estiverem configurados corretos.

## Configuração SW1

```
Switch(config-if)#do sh standby
Vlan10 - Group 1
  State is Active
    6 state changes, last state change 00:05:13
  Virtual IP address is 192.168.10.1
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.372 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  Group name is hsrp-V11-1 (default)
```

## Configuração SW2

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.10.3 255.255.255.0
Switch(config-if)#standby 1 ip 192.168.10.1
Switch(config-if)#standby 1 priority 100
Switch(config-if)#standby 1 preempt
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface fa0/2
Switch(config-if)#no shutdown
Switch(config-if)#exit
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

Switch(config-if)#
%HSRP-6-STATECHANGE: Vlan10 Grp 1 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan10 Grp 1 state Standby -> Active
```

**standby 1 ip 192.168.10.1:** Define o gateway virtual para o grupo HSRP 1.


**standby 1 priority 100:** o padrão é 100, valores mais altos ganham.

**standby 1 preempt:** Permite que o SW2 assuma caso tenha alguma falha.

## Configuração SW1

```
Switch(config)#do sh int fa0/2 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/2		connected	1	auto	auto	10/100BaseTX




Verifique se a vlan está na VLAN 10 Caso não esteja coloque a porta na Vlan 10

```
Switch(config-if)#switchport access vlan 10
```

```
Switch(config-if)#do sh int fa0/2 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/2		connected	10	auto	auto	10/100BaseTX



Só funcionará se os 2 SW estiverem configurados corretos.

## Configuração SW2

```
do sh standby
Vlan10 - Group 1
  State is Standby
    7 state changes, last state change 00:16:15
  Virtual IP address is 192.168.10.1
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.128 secs
  Preemption enabled
  Active router is 192.168.10.2
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Vll-1 (default)
```

## Comparando SW1 e SW2

```
Switch(config-if)#do sh standby
```

```
Vlan10 - Group 1
```

```
State is Active
```

```
6 state changes, last state change 00:05:13
```

```
Virtual IP address is 192.168.10.1
```

```
Active virtual MAC address is 0000.0C07.AC01
```

```
Local virtual MAC address is 0000.0C07.AC01 (vl default)
```

```
Hello time 3 sec, hold time 10 sec
```

```
Next hello sent in 0.372 secs
```

```
Preemption enabled
```

```
Active router is local
```

```
Standby router is unknown
```

```
Priority 110 (configured 110)
```

```
Group name is hsrp-Vll-1 (default)
```

← SW1

```
Switch(config-if)#do sh standby
```

```
Vlan10 - Group 1
```

```
State is Standby
```

```
7 state changes, last state change 00:16:15
```

```
Virtual IP address is 192.168.10.1
```

```
Active virtual MAC address is 0000.0C07.AC01
```

```
Local virtual MAC address is 0000.0C07.AC01 (vl default)
```

```
Hello time 3 sec, hold time 10 sec
```

```
Next hello sent in 0.155 secs
```

```
Preemption enabled
```

```
Active router is 192.168.10.2
```

```
Standby router is local
```

```
Priority 100 (default 100)
```

```
Group name is hsrp-Vll-1 (default)
```

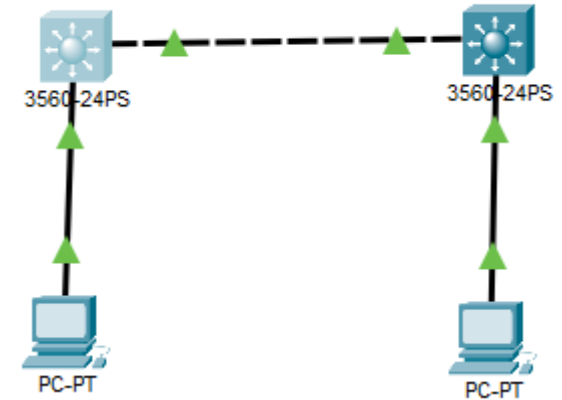
SW2 →

# HSRP (HOT STANDBY ROUTER PROTOCOL) - GATEWAYS REDUNDANTES



## Teste de Failover:

1. Desligue o SW1.
  1. Podemos resetar a configuração com o comando **reload**.
2. Acesse a interface do SW1 e de o comando **shutdown** nela
3. Com isso o SW2 assumirá como principal.





2.

# *SWITCH*

Lista de comandos



## COMANDOS PARA TROUBLESHOOTING E MONITORAMENTO GERAL:



- **show running-config** - Exibe a configuração atual do dispositivo.
- **show ip route** - Mostra a tabela de roteamento do dispositivo, incluindo rotas estáticas e dinâmicas.
- **show vlan brief** - Lista as VLANs configuradas no switch e suas interfaces associadas.
- **show ip interface brief** - Exibe o status das interfaces, incluindo endereços IP e estados das interfaces (up/down).
- **show interfaces** - Exibe estatísticas detalhadas sobre as interfaces, incluindo erros e taxas de pacotes.

## *COMANDOS PARA MONITORAMENTO DE INTERFACES:*



- **show interfaces status** - Exibe o estado atual de todas as interfaces (up/down, speed, duplex).
- **show interfaces counters erros** - Mostra a contagem de erros nas interfaces, ajudando a identificar problemas físicos.
- **show spanning-tree** - Exibe o status do Spanning Tree Protocol (STP), incluindo quais interfaces estão bloqueadas ou ativas.

## COMANDOS PARA MONITORAMENTO DE ROTEAMENTO:



### **show ip protocols**

-  Exibe as informações sobre os protocolos de roteamento configurados (OSPF, EIGRP, etc.).

### **show ip Route**

-  Exibe a tabela de roteamento do dispositivo, mostrando as rotas conhecidas.

## *COMANDOS PARA DIAGNÓSTICO E VERIFICAÇÃO:*



- **ping [ip]** - Testa a conectividade com outro dispositivo na rede.
- **tracert [ip]** - Exibe o caminho que os pacotes percorrem até um destino.
- **show standby** - Exibe o status do HSRP (Hot Standby Router Protocol), útil em cenários de redundância.

## *COMANDOS PARA SIMULAÇÃO DE FALHAS E RESOLUÇÃO:*



### **■ shutdown / no shutdown**

- Desativa e ativa interfaces físicas, útil para simular falhas de conectividade.

### **■ clear ip route \***

- Remove todas as rotas da tabela de roteamento, forçando a convergência de rotas dinâmicas.



3.

# *ACLS*

Trabalhando com controle

- **ACLs (Access Control Lists)** são listas de regras usadas em roteadores e switches para controlar o tráfego de entrada ou saída em uma interface.
- Essas listas dizem ao dispositivo o que ele pode permitir ou bloquear com base em critérios como:
  - Endereços IP de origem e destino (De onde vêm e para onde vão os pacotes).
  - Protocolos (TCP, UDP, ICMP).
  - Portas (HTTP, SSH, FTP, etc.).



- **Segurança:** ACLs ajudam a filtrar o tráfego indesejado, bloqueando acessos não autorizados.
- **Controle de Rede:** Elas permitem o gerenciamento do tráfego entre diferentes partes da rede, por exemplo, restringindo o acesso entre diferentes departamentos (VLANs).





Existem dois tipos principais de ACLs no Cisco:

### □ ACL Standard (Simples):

- ▶ Filtros baseados apenas no endereço IP de origem.
- ▶ Usada para bloquear ou permitir tráfego de um determinado grupo de dispositivos sem muita complexidade.

### □ ACL Extended (Avançada):

- ▶ Filtros baseados no endereço IP de origem e destino, além de poder filtrar por protocolo (TCP, UDP, ICMP) e número de porta.
- ▶ Usada para um controle mais refinado e detalhado do tráfego.



**Aplicação:** As ACLs podem ser aplicadas em:

- Entrada (Inbound): O tráfego é filtrado antes de entrar na interface.
- Saída (Outbound): O tráfego é filtrado antes de sair da interface.

**Ordem:** As ACLs são lidas de cima para baixo. Assim que uma regra é correspondida, as próximas são ignoradas.

**Regra Padrão Implícita:**

- **Negação Implícita:** Se o tráfego não corresponder a nenhuma regra da ACL, ele será automaticamente bloqueado. Isso significa que, por padrão, o tráfego que não for permitido será negado.

## ACLs - EXEMPLO



■ Você quer permitir que o tráfego HTTP (porta 80) da rede 192.168.1.0/24 seja enviado para um servidor na rede 10.1.1.0/24, mas quer bloquear todo o tráfego SSH (porta 22) entre essas redes.

```
SW1(config)# access-list 100 permit tcp 192.168.1.0 0.0.0.255 10.1.1.0 0.0.0.255 eq 80
SW1(config)# access-list 100 deny tcp 192.168.1.0 0.0.0.255 10.1.1.0 0.0.0.255 eq 22
SW1(config)# access-list 100 permit ip any any
```

■ Precisamos vincular a ACL em alguma porta:

```
SW1(config)# interface fastethernet 0/2
SW1(config-if)# ip access-group 100 in
```

## ACLs - EXEMPLO



Explicando:

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 10.1.1.0 0.0.0.255 eq 80
```

Define o número da ACL padrão extendend 100 - 199

Permite o tráfego ou Nega o tráfego

HTTP  
SSH  
FTP

IP  
Origem

Masc.  
Coringa  
Origem

IP  
Destino

Masc.  
Coringa  
Destino

**eq** especifica que esta regra se aplica apenas ao tráfego TCP que está usando a porta 80

Permite tráfego HTTP (porta 80) de **192.168.1.0/24** para **10.1.1.0/24**.

## ACLs - EXEMPLO



Explicando:

```
access-list 100 deny tcp 192.168.1.0 0.0.0.255 10.1.1.0 0.0.0.255 eq 22
```

Define o número da ACL padrão extendend 100 - 199

Permite o tráfego ou Nega o tráfego

HTTP  
SSH  
FTP

IP  
Origem

Masc.  
Coringa  
Origem

IP  
Destino

Masc.  
Coringa  
Destino

**eq** especifica que esta regra se aplica apenas ao tráfego TCP que está usando a porta 22

Bloqueia tráfego SSH (porta 22) de **192.168.1.0/24** para **10.1.1.0/24**.

## ACLs - EXEMPLO



Explicando:

```
access-list 100 permit ip any any
```

Permite todo o restante do tráfego que não foi capturado pelas duas regras anteriores.

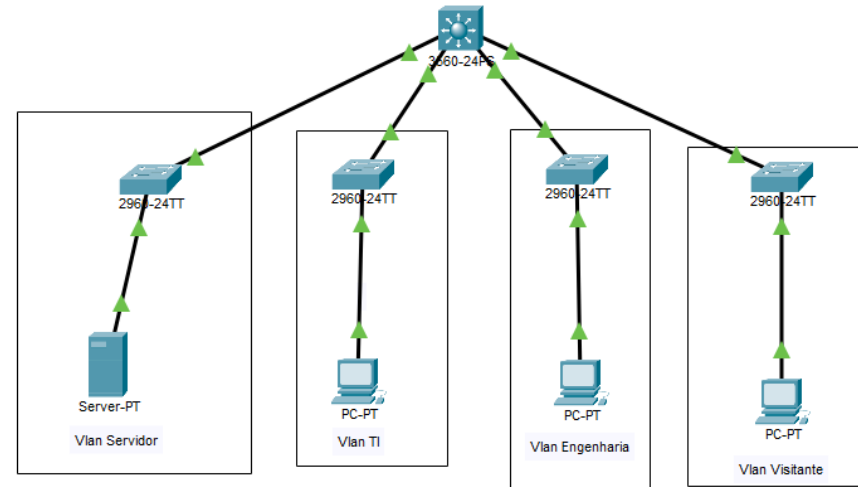
## ACLs - CONFIGURANDO



- Configurar a rede para que a VLAN 30 (Convidados) possa acessar o servidor HTTP na VLAN 40 (Servidores).

- Configurar uma acl para bloquear a comunicação das demais vlans com a vlan 30.

- Também configure a rede para que a VLAN 50 (TI) e a VLAN 60 (Engenharia) possam se comunicar livremente em mão dupla.

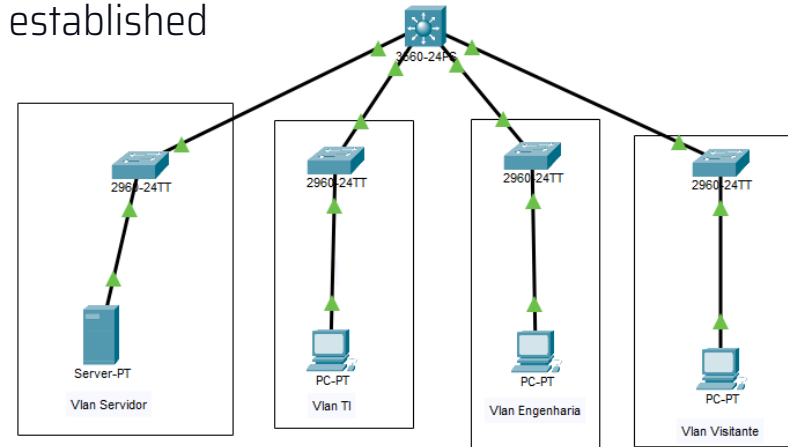


## ACLs - CONFIGURANDO



- access-list 110 deny icmp 192.168.30.0 0.0.0.255 any
- access-list 110 permit tcp 192.168.30.0 0.0.0.255 any eq 80
- access-list 110 permit tcp 192.168.30.0 0.0.0.255 any eq 443
- access-list 110 permit tcp any 192.168.30.0 0.0.0.255 established
- access-list 110 deny ip any any

- int vlan 30
- ip access-group 110 out







■ VLANs de servidores são redes virtuais criadas especificamente para servidores dentro de uma infraestrutura de TI.

■ A criação de uma VLAN dedicada para servidores permite isolar o tráfego de servidores do restante da rede, proporcionando segurança adicional e melhorando o desempenho.

# ACLS - VLAN SERVIDORES



Vantagens de usar ACL para vlan servidores:

## Segurança:

- ▶ A separação do tráfego dos servidores em uma VLAN específica impede que dispositivos de outras VLANs acessem os servidores sem permissão. Isso limita o alcance de possíveis ataques e protege dados sensíveis.

## Controle de Acesso:

- ▶ Com a VLAN de servidores isolada, é possível aplicar ACLs (Access Control Lists) para definir quais VLANs têm permissão para acessar os servidores e em que condições (exemplo: apenas tráfego HTTP ou HTTPS permitido).

## Desempenho:

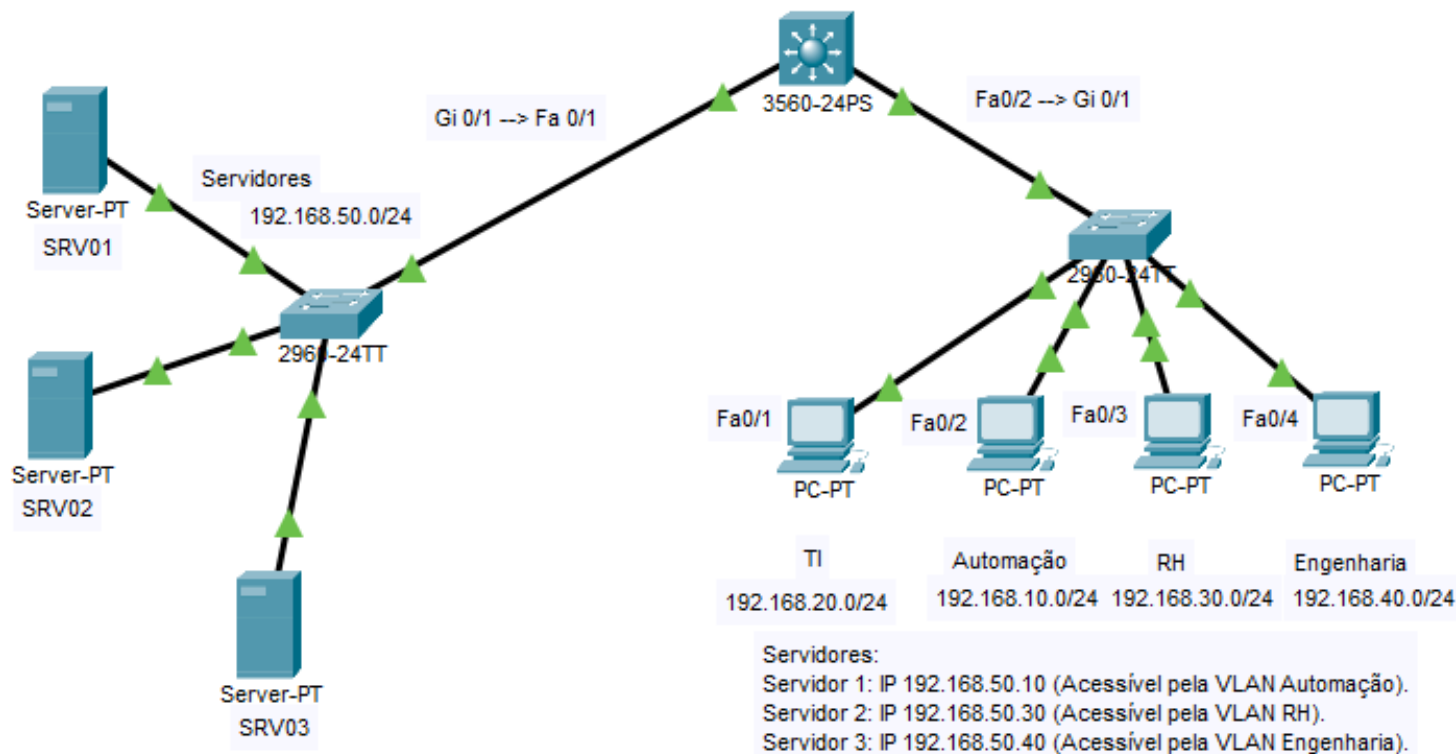
- ▶ O tráfego da VLAN de servidores fica restrito, o que pode reduzir a congestão na rede e melhorar a eficiência do roteamento.

## ACLS - SERVIDORES CONFIGURANDO



TIC

INFORMAÇÃO



## ACLs - VLAN SERVIDORES - TERMINAR ACLS



```
SW-Core(config)#! ACL VLAN 10 - AUTOMACAO
SW-Core(config)#access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.50.10 0.0.0.0
SW-Core(config)#access-list 110 deny ip any any
SW-Core(config)#
SW-Core(config)#! ACL VLAN 30 - RH
SW-Core(config)#access-list 130 permit ip 192.168.30.0 0.0.0.255 192.168.50.30 0.0.0.0
SW-Core(config)#access-list 130 deny ip any any
SW-Core(config)#
SW-Core(config)#! ACL VLAN 40 - ENGENHARIA
SW-Core(config)#access-list 140 permit ip 192.168.40.0 0.0.0.255 192.168.50.40 0.0.0.0
SW-Core(config)#access-list 140 deny ip any any
SW-Core(config)#
SW-Core(config)#
SW-Core(config)#! Aplicando as ACLs nas interfaces VLAN
SW-Core(config)#interface vlan 10
SW-Core(config-if)#ip access-group 110 in
SW-Core(config-if)#exit
SW-Core(config)#interface vlan 30
SW-Core(config-if)#ip access-group 130 in
SW-Core(config-if)#exit
SW-Core(config)#interface vlan 40
SW-Core(config-if)#ip access-group 140 in
SW-Core(config-if)#exit
```

ACL para  
permitir  
acesso a  
apenas 1  
servidor

Associando as  
regras às  
portas.

The background features a complex network diagram with nodes and connecting lines in shades of blue, purple, and pink. Overlaid on this are several geometric shapes: a large black trapezoid on the left, and various orange and yellow triangles and polygons on the right and bottom. Some of these shapes have patterns of small triangles or dots.

3.

# *DHCP*

Trabalhando com DHCP em Vlans

Servidor para distribuição dinâmica de Ips.

Funcionamento Básico do DHCP

- ▢ **Descoberta (DHCP Discover):** O cliente (dispositivo) envia uma mensagem em broadcast à rede procurando por um servidor
- ▢ **DHCP.Oferta (DHCP Offer):** O servidor DHCP responde com uma oferta de um endereço IP disponível e outras informações de configuração.
- ▢ **Solicitação (DHCP Request):** O cliente escolhe uma oferta e envia uma solicitação para confirmar a atribuição do IP.
- ▢ **Confirmação (DHCP Acknowledgment):** O servidor DHCP confirma a atribuição do IP e outros parâmetros, como gateway e DNS.

## CENÁRIO DHCP - COM SWITCH LAYER 3



TECNOLOGIA

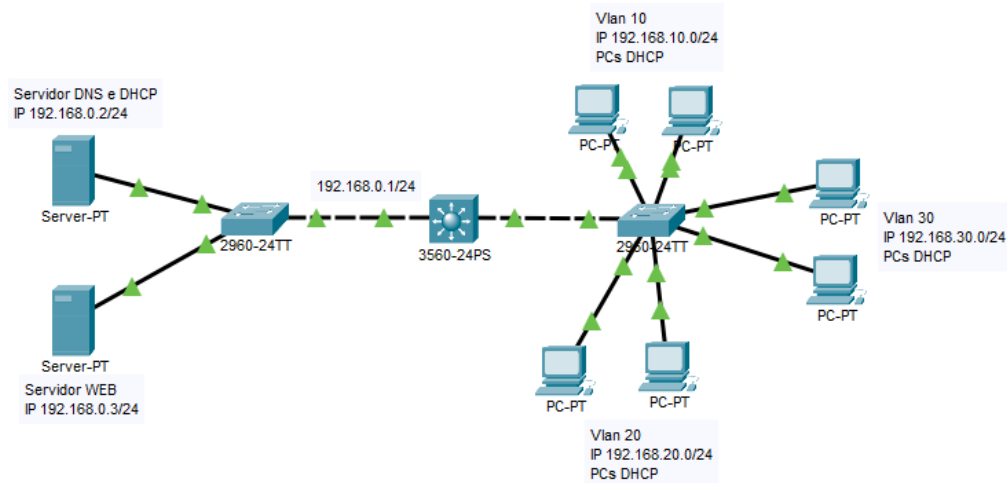
TIC



INFORMAÇÃO



COMUNICAÇÃO



## CENÁRIO DHCP - COM SWITCH LAYER 3



```
Switch(config)#interface vlan 10
Switch(config-if)#ip helper-address 192.168.0.2
Switch(config-if)#exit
Switch(config)#interface vlan 20
Switch(config-if)#ip helper-address 192.168.0.2
Switch(config-if)#exit
Switch(config)#interface vlan 30
Switch(config-if)#ip helper-address 192.168.0.2
Switch(config-if)#end
```

ip helper-address "IP  
Servidor DHCP"  
Comando para utilizar  
em roteadores ou  
switches Layer 3 para  
encaminhar  
solicitações de DHCP





4.

# ***REDES SEM FIO***

Redes sem fio e ACL para  
comunicação.

## CONCEITO BÁSICO DE REDES SEM FIO E INTEGRAÇÃO COM VLANs



Uma rede sem fio (Wi-Fi) permite que dispositivos se conectem à rede sem a necessidade de cabos físicos. O Access Point (AP) atua como o ponto central, transmitindo sinais Wi-Fi que conectam dispositivos como laptops, smartphones e tablets.

Wi-Fi é amplamente utilizado em ambientes corporativos, escolas, residências e em locais públicos, permitindo a conectividade de dispositivos móveis.

### Integração de Wi-Fi com VLANs:

- Em redes corporativas, a integração de redes sem fio (Wi-Fi) com VLANs é fundamental para a segurança, o desempenho e a separação de diferentes tipos de tráfego de rede.

## CONCEITO BÁSICO DE REDES SEM FIO E INTEGRAÇÃO COM VLANs



### Benefícios da integração de Wi-Fi com VLANs:

- ☐ **Segurança:** A integração com VLANs permite segmentar o tráfego de diferentes tipos de usuários. Por exemplo, uma VLAN dedicada a visitantes pode ser configurada separadamente de uma VLAN de funcionários.
- ☐ **Controle de Acesso:** Ao associar uma rede Wi-Fi a uma VLAN específica, você pode controlar o acesso a diferentes recursos da rede.
- ☐ **Desempenho e Prioridade:** A segregação do tráfego Wi-Fi em VLANs permite priorizar o tráfego importante e reduzir a congestão.



### Modos de Autenticação:

- ❑ **WPA2 (Wi-Fi Protected Access 2):** Atualmente, é o padrão mais seguro para redes Wi-Fi. O WPA2 usa criptografia AES (Advanced Encryption Standard), o que dificulta ataques de força bruta ou invasões.
- ❑ **WEP (Wired Equivalent Privacy):** Um protocolo de segurança antigo, considerado obsoleto, devido a várias vulnerabilidades conhecidas. Não é recomendado para uso em redes modernas.
- ❑ **WPA (Wi-Fi Protected Access):** Um intermediário entre o WEP e o WPA2, mas também menos seguro em comparação ao WPA2.



## Criptografia:

- **AES (Advanced Encryption Standard):** Padrão de criptografia usado em redes WPA2. Altamente recomendado devido à sua robustez e nível de segurança.
- **TKIP (Temporal Key Integrity Protocol):** Um método de criptografia mais antigo, usado em WPA, mas considerado menos seguro que o AES.

## Autenticação de Usuários:

- **Autenticação WPA2-PSK (Pre-Shared Key):** Utiliza uma senha predefinida para permitir que os usuários se conectem ao Wi-Fi. Ideal para redes domésticas ou pequenos escritórios.
- **Autenticação WPA2-Enterprise:** Usa um servidor RADIUS para autenticar usuários individualmente. Muito comum em redes empresariais, pois oferece mais controle e segurança.

## SSID (SERVICE SET IDENTIFIER)



O SSID é o nome da rede Wi-Fi que será exibido para os dispositivos que tentam se conectar.

### Visibilidade do SSID:

- Um SSID pode ser público ou oculto. Redes ocultas não mostram o nome da rede aos usuários, mas ainda podem ser descobertas por hackers que saibam o que procurar.

### Redes Segmentadas por SSID:

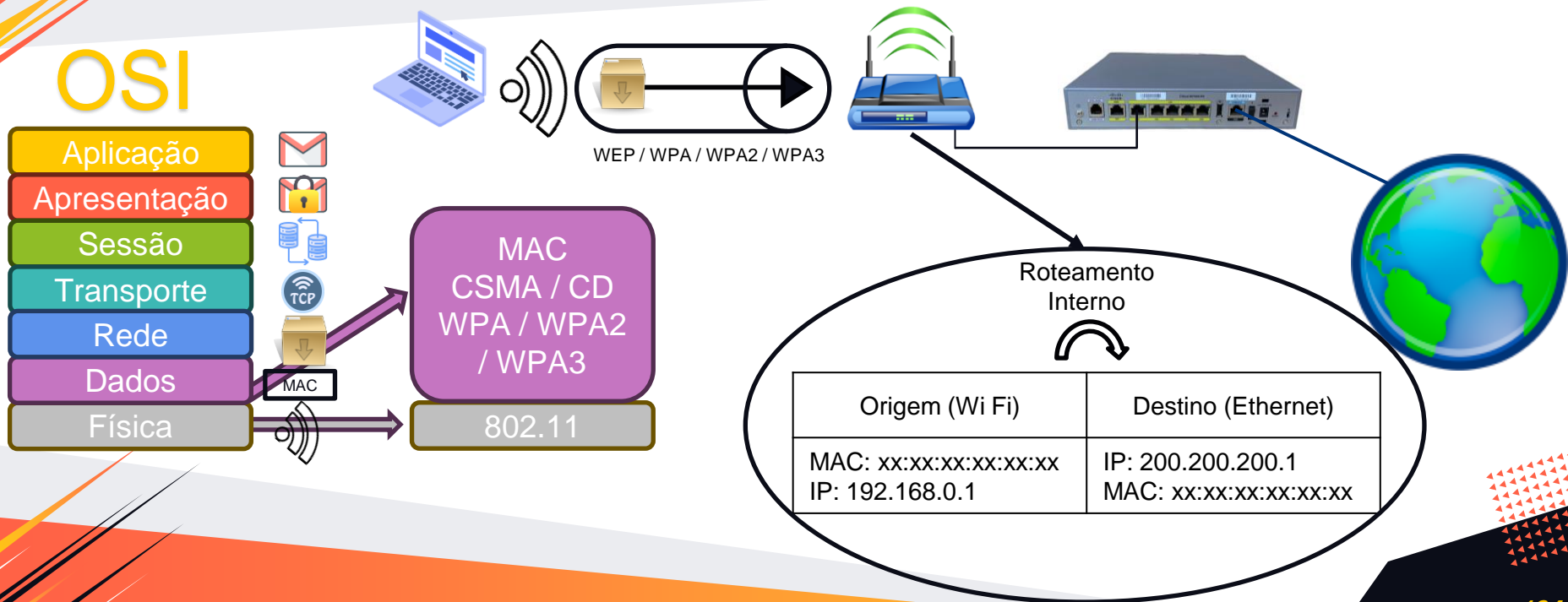
- Redes Corporativas geralmente possuem múltiplos SSIDs. Por exemplo, um SSID para funcionários, outro para visitantes e, em alguns casos, um para dispositivos IoT. Cada SSID pode ser associado a uma VLAN diferente, garantindo que o tráfego de diferentes usuários ou dispositivos seja segmentado.

## PONTOS IMPORTANTES EM REDES SEM FIO



- **Segurança:** A escolha do protocolo de segurança Wi-Fi (WPA2) e a configuração de senhas fortes são cruciais.
- **Cobertura e Interferência:** A configuração de canais Wi-Fi e a escolha da frequência (2.4 GHz vs. 5 GHz) afetam o desempenho da rede sem fio.
- **QoS e Limites de Banda:** Permitem gerenciar o tráfego e garantir que os aplicativos críticos tenham prioridade.
- **Integração com VLANs:** Segmentar redes sem fio com VLANs aumenta a segurança e facilita o controle de acesso.
- **SSID e Segmentação:** Vários SSIDs podem ser associados a diferentes VLANs, permitindo redes separadas para funcionários, visitantes e dispositivos IoT.

# FUNCIONAMENTO DA REDE SEM FIO - MODELO OSI





## CENÁRIO REDE SEM FIO



ECNOLOGIA

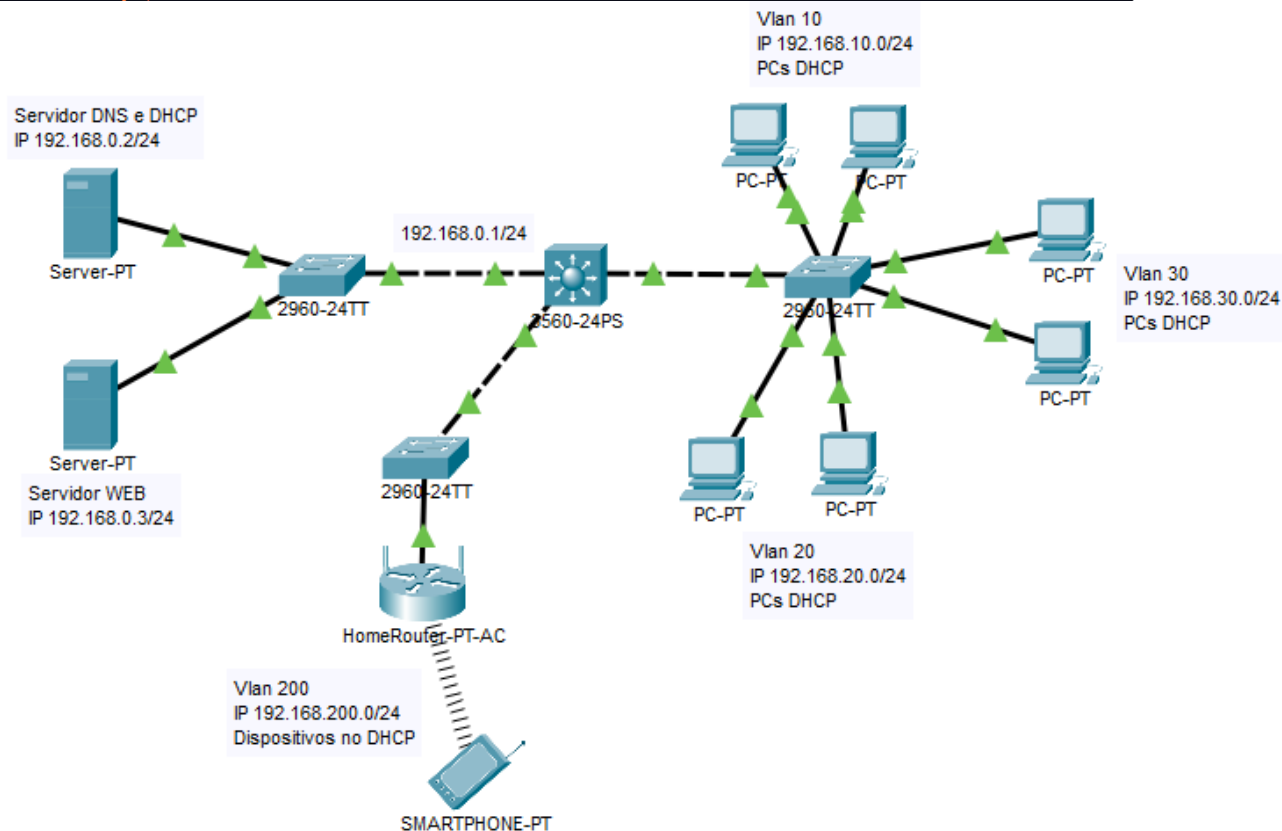
# TIC



INFORMAÇÃO



COMUNICAÇÃO





### ■ EtherChannel:

- show etherchannel summary
- show interfaces port-channel

### ■ HSRP:

- show standby brief
- show standby

### ■ STP:

- show spanning-tree

### ■ ACLs:

- show access-lists
- show ip access-lists

### ■ Trunks e VLANs:

- show interfaces trunk
- show vlan brief

3.

# *EXERCÍCIOS*

Usando packet tracer



***OBRIGADO!***

