Introdução

Este documento detalha a configuração de um ambiente de laboratório de redes, com ênfase na segmentação de rede por VLANs e na implementação de serviços essenciais para garantir a segurança, desempenho e escalabilidade. O objetivo principal deste projeto foi criar uma infraestrutura de rede que simula um ambiente corporativo, isolando as atividades da Administração, Recursos Humanos e Gerenciamento. Isso permite otimizar o uso de recursos, melhorar a segurança e aumentar o desempenho da rede.

Através da segmentação de rede, foi possível dividir os dispositivos e sistemas de acordo com suas funções e requisitos específicos. O uso de VLANs (Virtual Local Area Networks) garante que as diferentes áreas da organização possam operar de forma isolada, sem interferências entre elas. Para complementar essa configuração, foram implementados recursos de segurança, como a utilização de ACLs (Access Control Lists) para bloquear a comunicação entre as VLANs de forma controlada.

Além disso, o projeto inclui a configuração de um servidor VTP (VLAN Trunking Protocol) para facilitar a propagação das VLANs entre os switches, e a implementação de Port-Channel para aumentar a largura de banda entre os dispositivos e garantir maior redundância. A comunicação entre o switche L3 e o roteador também foi configurada, com o roteador atuando como gateway para as VLANs, permitindo o acesso à rede externa de forma segura.

Com isso, foi possível criar uma rede corporativa funcional, segura e escalável, pronta para suportar um ambiente de trabalho eficiente, isolando tráfego sensível e garantindo a integridade e disponibilidade dos recursos essenciais.

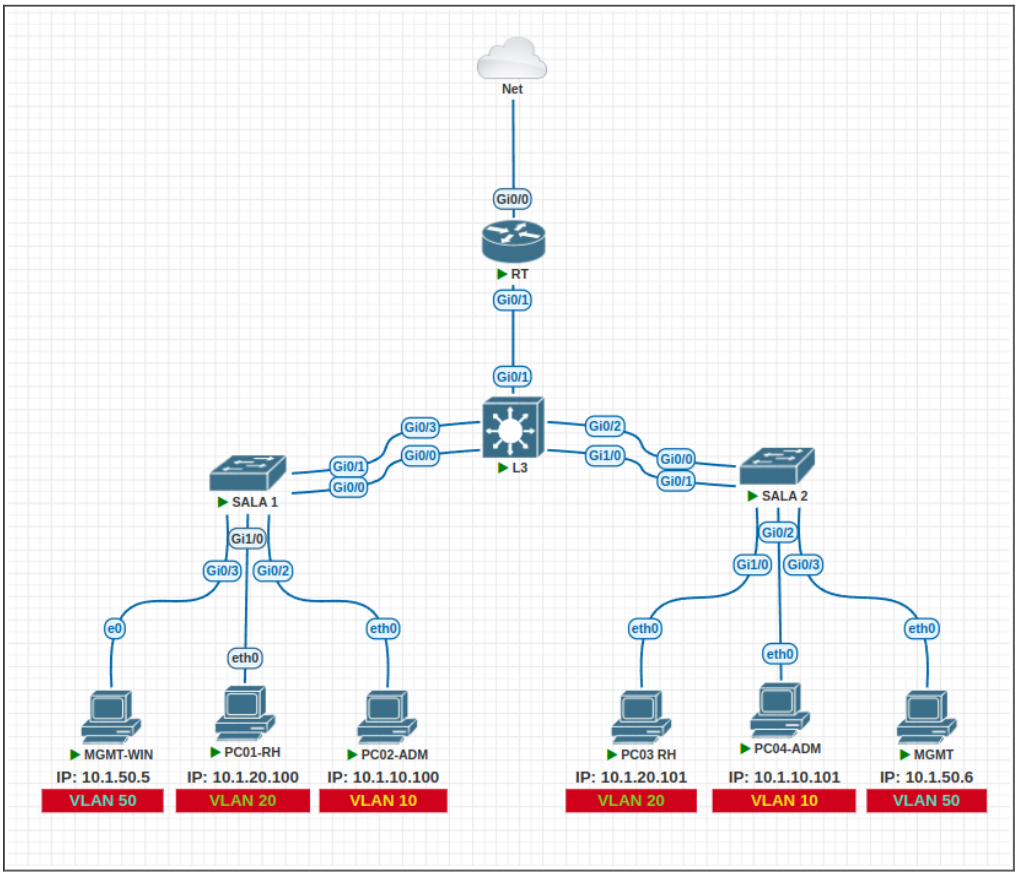


Figura 1 *Autor: https://www.linkedin.com/in/rafaeldsan/*

Objetivos do Projeto

1. **Segmentação de Rede com VLANs:**
   Implementar a segmentação da rede utilizando VLANs para isolar as atividades da Administração, Recursos Humanos e Gerenciamento, garantindo maior controle e segurança.

2. **Configuração de Dispositivos de Rede:**
   Configurar roteadores e switches para permitir comunicação eficiente entre as VLANs e com a Internet, mantendo a integridade de cada segmento de rede.

3. **Uso de NAT (Network Address Translation):**
   Implementar NAT para permitir a tradução de endereços das VLANs de Administração e Recursos Humanos, garantindo acesso seguro à Internet.

4. **Controle de Acesso com ACLs (Access Control Lists):**
   Implementar ACLs para restringir a interação entre as VLANs de Administração e Recursos Humanos, assegurando que essas VLANs não se comuniquem entre si, aumentando a segurança da rede.

5. **Facilitação do Gerenciamento de VLANs com VTP (VLAN Trunking Protocol):**
   Utilizar o VTP para facilitar a propagação e o gerenciamento centralizado das VLANs em toda a rede.

6. **Aumento da Largura de Banda com EtherChannel:**
   Ampliar a redundância e melhorar a qualidade da conexão com a Internet por meio da configuração de EtherChannel, agregando links de forma eficiente entre as salas.

7. **Gerenciamento Remoto Seguro via SSH:**
   Implementar o SSH exclusivamente na VLAN de Gerenciamento, permitindo o acesso remoto seguro aos dispositivos de rede a partir de pelo menos uma porta de switch em cada sala, garantindo a segurança do gerenciamento.

1. Configurando Switch L3

É muito importante visualizar a **figura 1, presente na pagina 1,** para compreender as configurações.

1.1 Criação das VLANs no L3

Na topologia apresentada na Figura 1.0, as VLANs foram configuradas no equipamento **L3**, dentro do modo de configuração global (config#), utilizando os seguintes comandos:

```
vlan 10
 name ADM
vlan 20
 name RH
vlan 50
 name MGMT
vlan 100
 name LIXO
```

Descrição das VLANs Criadas

- **VLAN 10 (ADM):** Segmentação destinada às atividades Administrativas.
- **VLAN 20 (RH):** Segmentação destinada às atividades de Recursos Humanos.
- **VLAN 50 (MGMT):** Segmentação reservada para dispositivos e gerenciamento da rede.
- **VLAN 100 (LIXO):** VLAN reservada para descarte ou configurações não utilizadas.

Este procedimento garante a segmentação lógica da rede, organizando os dispositivos em grupos específicos com base na função ou departamento, melhorando o desempenho e a segurança.

1.1 Configuração do VTP Server

Ainda no equipamento **L3**, dentro do modo de configuração global, foi configurado o **VTP Server** para facilitar o gerenciamento das VLANs entre os switches conectados. A configuração foi feita com os seguintes comandos:

```
vtp mode server
vtp version 2
vtp domain LAB.net
vtp password LAB
```

- **Benefícios do VTP Server**

  O uso do VTP Server simplifica a criação e propagação de VLANs para outros switches na rede, centralizando o gerenciamento e reduzindo o esforço manual em configurações

1.2 Configuração das Interfaces Trunk

Para que o VTP seja propagado para os switches conectados nas diferentes salas, é necessário habilitar o **modo trunk** nas interfaces que interligam os switches. Além disso, foi configurada a interface que liga do L3 para RT e agregação de links utilizando **LACP (Link Aggregation Control Protocol)**, permitindo maior largura de banda e redundância entre os switches

1.2.1 Configuração das Interfaces Físicas

As interfaces físicas foram associadas ao **Port-Channel** com os seguintes comandos:

```
interface gigabitEthernet0/0
 description SALA 1
 channel-group 1 mode active
exit

interface gigabitEthernet0/3
 description SALA 1
 channel-group 1 mode active
exit

interface gigabitEthernet0/2
 description SALA 2
 channel-group 1 mode active
exit

interface gigabitEthernet1/0
 description SALA 2
 channel-group 1 mode active
exit
```

1.2.2 Configuração do Port-Channel

Após a configuração das interfaces físicas, foram criados dois **Port-Channels** (um para cada sala), configurados como **trunks** e permitindo o tráfego das VLANs 10, 20 e 50:

```
interface Port-channel1
 description Trunk - SALA 1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,50
exit

interface Port-channel2
 description Trunk - SALA 2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,50
exit
```

1.2.3 Resumo da Configuração

- As interfaces físicas (**gigabitEthernet0/0 e gigabitEthernet0/0**) foram agrupadas logicamente no **Port-Channel** 1, correspondente a sala 1.
- As interfaces físicas (**gigabitEthernet0/2 e gigabitEthernet1/0**) foram agrupadas logicamente no **Port-Channel** 2, correspondente a sala 2.
- O **Port-Channel** foi configurado como **trunk**, permitindo o tráfego das VLANs configuradas (10, 20 e 50).

- A agregação de links garante maior largura de banda e redundância para as conexões entre o **L3** e os switches das salas.

1.2.4 Configuração da Interface do Switch L3 para o Roteador (RT)

Para estabelecer a comunicação entre o **Switch L3** e o **Roteador (RT)**, foi configurada uma interface no **Switch L3** para atuar como **trunk**. Através dessa interface, as VLANs permitidas e configuradas no **Switch L3** podem ser propagadas para o **Roteador (RT)**. O **Roteador (RT)**, por sua vez, será responsável pelo **roteamento** entre essas VLANs e outras redes externas.

Comandos Utilizados

Dentro do **modo de configuração global** no **Switch L3**, a interface foi configurada com os seguintes comandos para permitir a comunicação trunk entre o **Switch L3** e o **Roteador (RT)**:

```
interface gigabitEthernet0/1
 description Link para RT
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,50
exit
```

1.3 Configuração da Interface VLAN 50 no L3

No **Switch Layer 3 (L3)**, foi configurada a **interface VLAN 50** com o endereço IP **10.1.50.2**, que servirá como um dos dispositivos de gerenciamento da rede. O gateway para a VLAN 50 será configurado posteriormente no **Roteador (RT)** com o endereço **10.1.50.1**.

Comandos Utilizados

Dentro do modo de configuração global no **L3**, a interface VLAN 50 foi configurada com os seguintes comandos:

```
interface vlan 50
 description VLAN de Gerenciamento (L3)
 ip address 10.1.50.2 255.255.255.248
 no shutdown
exit
```

2. Configuração do Switch SALA 1

A configuração do **Switch SALA_1** inclui a criação das VLANs, a configuração das interfaces trunk para interligação com o **Switch L3** e a configuração das interfaces de acesso para conectar os dispositivos das respectivas VLANs. Além disso, foi configurado o **Link Aggregation (LACP)** para garantir maior largura de banda e redundância entre os links.

2.1 Configuração do LACP (Link Aggregation Control Protocol)

As interfaces ativas do sw da SALA 1 conectadas ao **Switch L3** foram configuradas para usar o **LACP**, agregando os links para fornecer maior largura de banda e redundância, portanto, para ativar esse recurso é necessario seguir os seguintes comandos do sw da sala 1.

```
interface GigabitEthernet0/0
 description L3
 channel-group 1 mode passive
 channel-protocol lacp

interface GigabitEthernet0/1
 description L3
 channel-group 1 mode passive
 channel-protocol lacp
```

- **Comando channel-group 1 mode passive:** Configura as interfaces para ingressar no grupo de agregação de links **LACP**.
- **Comando channel-protocol lacp:** Habilita o **LACP** nas interfaces, permitindo a agregação de links e aumentando a largura de banda disponível.

2.2 Configuração do Port-Channel

O **Port-Channel 1** foi configurado para permitir que o tráfego de múltiplas VLANs seja transmitido pela agregação de links entre os switches.

```
interface Port-channel 1
 description L3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,50
```

- **Comando interface Port-channel 1:** Configura o **Port-Channel 1** como uma interface trunk.
- **Comando switchport trunk encapsulation dot1q:** Define o protocolo de encapsulamento como **dot1q**.
- **Comando switchport mode trunk:** Coloca o port-channel em modo trunk, permitindo o tráfego de múltiplas VLANs através dessa interface.
- **Comando switchport trunk allowed vlan 10,20,50:** Permite que as VLANs 10, 20 e 50 trafeguem pelo **Port-Channel 1**.

2.3 Configuração do VTP (VLAN Trunking Protocol)

```
vtp mode client
vtp version 2
vtp domain LAB.net
vtp password LAB
```

2.4 Configuração das Interfaces de Acesso para as VLANs

As interfaces de acesso foram configuradas para associar dispositivos às VLANs específicas de acordo com suas funções ou departamentos. Essas interfaces não são trunk, mas sim configuradas para acesso direto a uma VLAN específica.

```
interface gigabitEthernet0/2
 switchport access vlan 10
 switchport mode access

interface gigabitEthernet0/3
 switchport access vlan 50
 switchport mode access
interface gigabitEthernet1/0
 switchport access vlan 20
 switchport mode access

interface gigabitEthernet1/1
 switchport access vlan 100
 switchport mode access

interface gigabitEthernet1/2
 switchport access vlan 100
 switchport mode access

interface gigabitEthernet1/3
 switchport access vlan 100
 switchport mode access
```

2.5 Configuração da Interface VLAN 50

A **interface VLAN 50** foi configurada no switch para permitir o gerenciamento da rede via IP. Esse endereço IP será usado para a comunicação de gerenciamento dentro da **VLAN MGMT**.

```
interface vlan 50
 ip address 10.1.50.3 255.255.255.248
 no shutdown
```

- **Comando ip address 10.1.50.3 255.255.255.248:** Atribui o endereço IP **10.1.50.3/29** à interface **VLAN 50** para gerenciamento.
- **Comando no shutdown:** Ativa a interface, permitindo a comunicação com o **Switch L3**.

3.0 Configuração do Switch SALA 2

A configuração do **Switch de Sala 2** é praticamente a mesma que a de **Sala 1**, com exceção de duas diferenças principais: o **endereço IP da Interface VLAN 50** e a **configuração do Channel Group**.

3.1 Configuração da interface vlan 50 Switch de Sala 2:

```
! Configuração da Interface VLAN 50
interface vlan 50
 ip address 10.1.50.4 255.255.255.248  ! Endereço IP da VLAN 50 para a Sala 2
 no shutdown
```

3.2 Configuração da interface vlan 50 Switch de Sala 2:

```
interface GigabitEthernet0/0
 description L3
 channel-group 1 mode passive
 channel-protocol lacp

interface GigabitEthernet0/1
 description L3
 channel-group 1 mode passive
 channel-protocol lacp
```

4. Configurando o Roteador

A configuração do **roteador (RT)** envolve a criação de subinterfaces para cada VLAN, o uso de NAT para permitir acesso à Internet e a implementação de listas de controle de acesso (ACLs) para restringir o tráfego entre as VLANs. Abaixo estão os detalhes de todas as configurações feitas:

4.1 Interface GigabitEthernet0/0 (WAN)

Esta interface conecta o roteador à rede externa (Internet). Está configurada para obter o endereço IP via DHCP e marcada como ip nat outside, permitindo a tradução de endereços para o tráfego que sai para a Internet.

```
interface GigabitEthernet0/0
 description WAN
 ip address dhcp
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
 media-type rj45
```

4.2 Interface GigabitEthernet0/1 (LAN)

A interface principal do roteador que conecta as VLANs internas. Está configurada para não ter um IP, mas as subinterfaces associadas a ela estão configuradas com os endereços IPs das VLANs.

```
interface GigabitEthernet0/1
 no ip address
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
 media-type rj45
```

4.3 Subinterface para VLAN 10 (ADM)

Esta subinterface é configurada para a VLAN 10, com o IP 10.1.10.1/24. Além disso, a ACL ONLY-ADM é aplicada para restringir o tráfego da VLAN ADM.

```
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 10.1.10.1 255.255.255.0
 ip access-group ONLY-ADM in
 ip nat inside
 ip virtual-reassembly in
```

4.4 Subinterface para VLAN 20 (RH)

A subinterface para a VLAN 20, com o IP 10.1.20.1/24, é configurada de maneira similar, com a aplicação da ACL ONLY-RH para restringir o tráfego da VLAN RH.

```
interface GigabitEthernet0/1.20
 encapsulation dot1Q 20
 ip address 10.1.20.1 255.255.255.0
 ip access-group ONLY-RH in
 ip nat inside
 ip virtual-reassembly in
```

4.5 Subinterface para VLAN 50 (MGMT)

A subinterface para a VLAN 50, com o IP 10.1.50.1/248, é configurada para gerenciar a comunicação com os dispositivos da VLAN de gerenciamento, com a ACL ONLY-MGMT aplicada.

```
interface GigabitEthernet0/1.50
 encapsulation dot1Q 50
 ip address 10.1.50.1 255.255.255.248
 ip access-group ONLY-MGMT in
```

4.6 Configuração de NAT (Network Address Translation)

O NAT foi configurado para permitir que as VLANs internas acessem a Internet usando o IP da interface externa (WAN). A configuração do NAT foi feita usando a lista de controle de acesso NAT-VLAN, que permite tráfego das VLANs 10 e 20.

```
ip nat inside source list NAT-VLAN interface GigabitEthernet0/0 overload
```

A lista de controle de acesso NAT-VLAN permite que o tráfego da VLAN 10 e 20 seja traduzido para um único IP de saída (overload):

```
ip access-list standard NAT-VLAN
 permit 10.1.10.0 0.0.0.255
 permit 10.1.20.0 0.0.0.255
```

4.7 Configuração das ACLs (Access Control Lists):

As ACLs foram configuradas para restringir o tráfego entre as VLANs de forma controlada:

- **ACL ONLY-ADM (VLAN ADM restrita de interagir com outras VLANs):** A ACL ONLY-ADM bloqueia a comunicação da VLAN 10 (ADM) com a VLAN 20 (RH) e com a VLAN 50 (MGMT), permitindo apenas o tráfego para outras redes.

  ```
  ip access-list extended ONLY-ADM
  ```

```
deny ip 10.1.10.0 0.0.0.255 10.1.50.0 0.0.0.7
deny ip 10.1.10.0 0.0.0.255 10.1.20.0 0.0.0.255
permit ip any any
```

- **ACL ONLY-MGMT (VLAN MGMT restrita de interagir com outras VLANs):** A ACL ONLY-MGMT impede a comunicação da VLAN 50 (MGMT) com a VLAN 10 (ADM) e a VLAN 20 (RH), permitindo apenas o tráfego para outras redes.

```
ip access-list extended ONLY-MGMT
 deny ip 10.1.50.0 0.0.0.7 10.1.10.0 0.0.0.255
 deny ip 10.1.50.0 0.0.0.7 10.1.20.0 0.0.0.255
 permit ip any any
```

- **ACL ONLY-RH (VLAN RH restrita de interagir com outras VLANs):** A ACL ONLY-RH impede a comunicação da VLAN 20 (RH) com a VLAN 10 (ADM) e com a VLAN 50 (MGMT), permitindo apenas o tráfego para outras redes.

```
ip access-list extended ONLY-RH
 deny ip 10.1.20.0 0.0.0.255 10.1.10.0 0.0.0.255
 deny ip 10.1.20.0 0.0.0.255 10.1.50.0 0.0.0.7
 permit ip any any
```

Essa configuração garante que as VLANs 10 (ADM), 20 (RH) e 50 (MGMT) tenham comunicação segregada, com restrições bem definidas entre elas, e também permite que as VLANs internas possam acessar a Internet através do NAT.

5. Recursos de Segurança

A seguir, estão detalhadas as configurações de segurança aplicadas em todos os equipamentos para garantir o controle de acesso e a segurança das redes internas e externas.

5.1 Configuração de Senha do Modo Enable (SHA256):

A senha de acesso ao modo enable foi configurada utilizando o algoritmo de criptografia SHA256 para garantir maior segurança.

```
enable algorithm-type sha256 secret admin
```

5.2 Configuração de Domínio e SSH:

A configuração de um domínio e a geração de chaves RSA para SSH foram realizadas para permitir o acesso remoto seguro ao dispositivo.

```
ip domain-name LAB.net
username admin algorithm-type sha256 secret admin
crypto key generate rsa general-keys modulus 2048
```

5.3 Configuração de Acesso ao Console e VTY:

O acesso ao console e VTY foi configurado para exigir autenticação local, utilizando o usuário e a senha criados anteriormente. Além disso, o tempo de inatividade foi configurado para 30 segundos.

```
line console 0
 login local
 exec-timeout 0 30

line vty 0 4
 transport input ssh
 login local
 exec-timeout 0 30
```

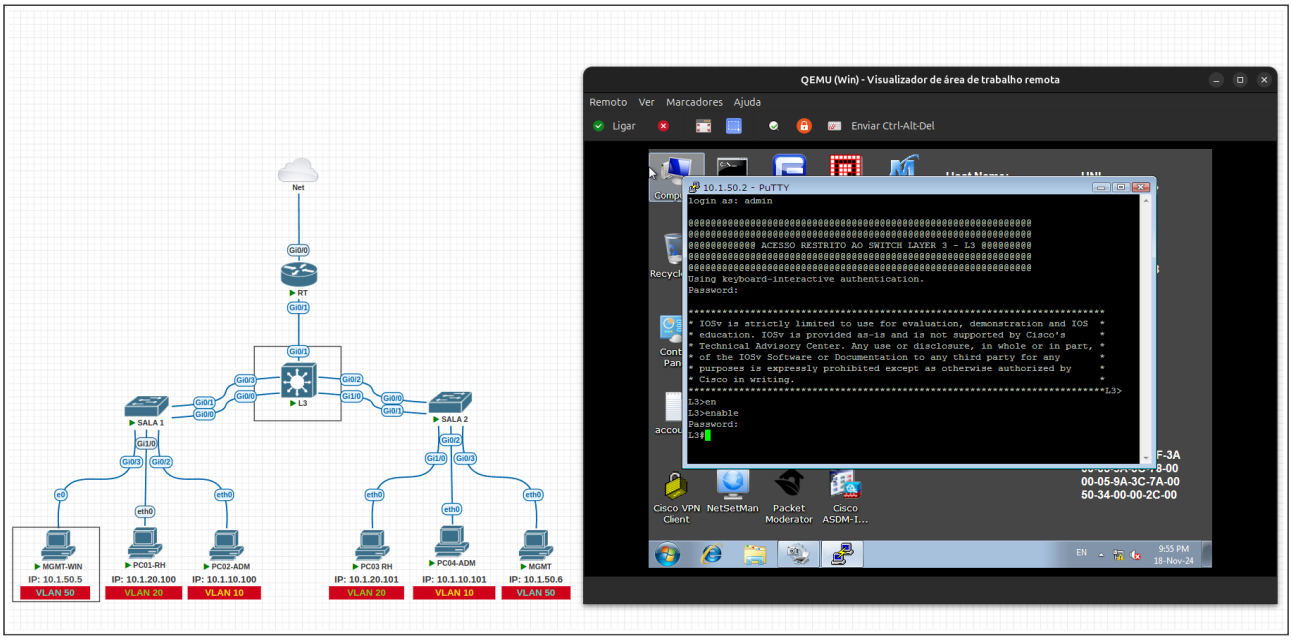
6. Resultados

6.1 Acessando Remotamente via SSH os equipamentos de rede via VLAN 50 (Gerenciamento).

A configuração de acesso remoto via SSH foi realizada com sucesso para os dispositivos da rede, com especial destaque para a utilização da VLAN 50 (destinada ao gerenciamento), que foi isolada e configurada de forma a garantir a segurança e a eficiência do acesso. Abaixo, são apresentados os resultados dos testes realizados para verificar a conectividade e o acesso aos dispositivos da rede.

6.1.1 Teste 1: Acessando Switch Layer 3 (L3)

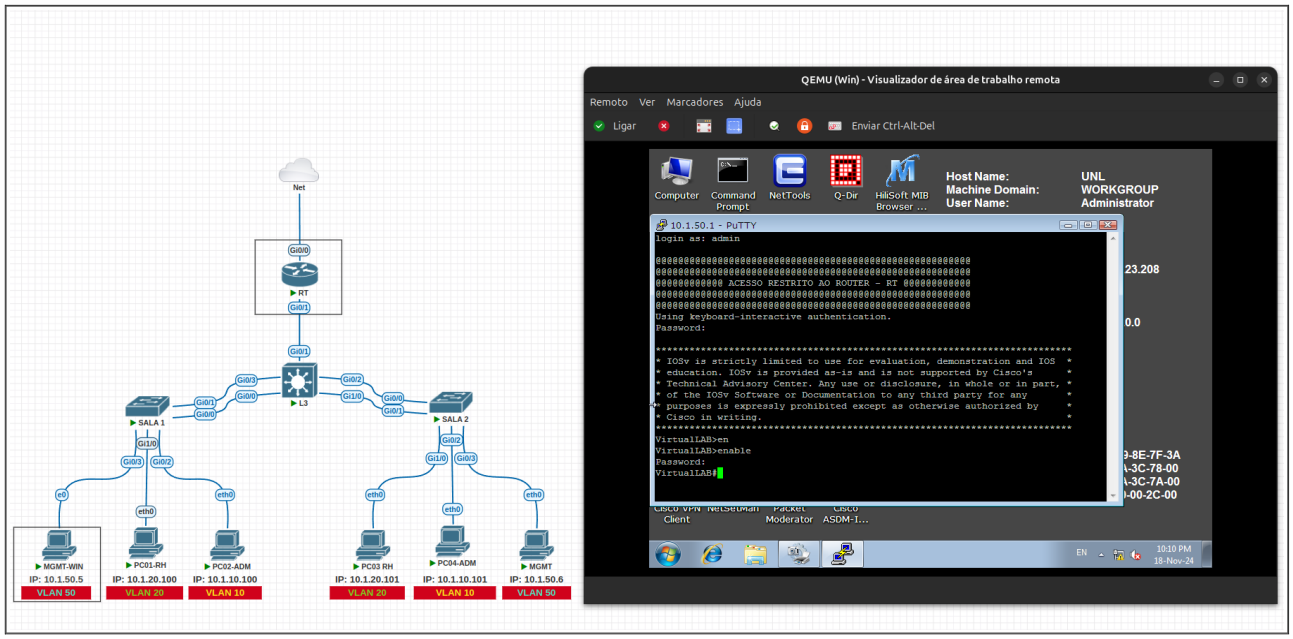
Objetivo: Verificar a conectividade e a capacidade de acessar remotamente o Switch Layer 3 (L3) via SSH, utilizando a VLAN 50 como a rede de gerenciamento



Resultado Obtido: O acesso SSH foi estabelecido com sucesso, confirmando que o Switch L3 pode ser acessado remotamente via VLAN 50 (Gerenciamento), e o ambiente de gerenciamento foi configurado corretamente para garantir a segurança e funcionalidade necessárias.

6.1.2 Teste 2: Acessando Router (RT)

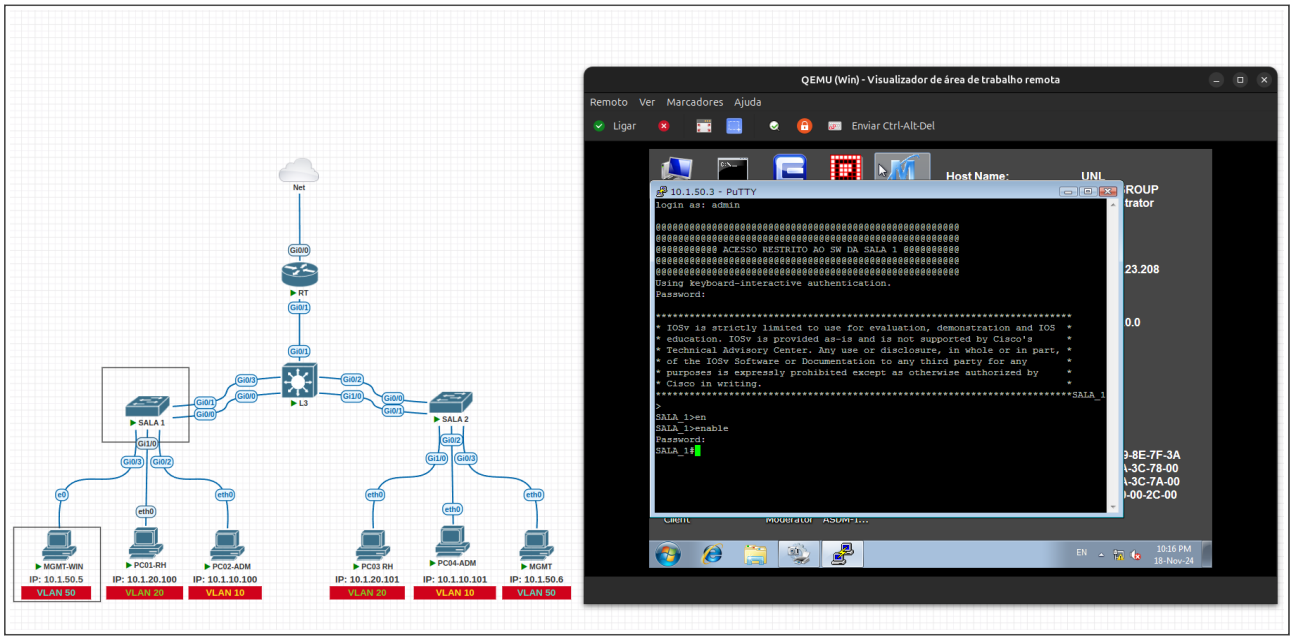
Objetivo: Verificar a conectividade e a capacidade de acessar remotamente o Roteador (RT) via SSH, utilizando a VLAN 50 para o gerenciamento da rede.



Resultado Obtido: O acesso SSH foi estabelecido com sucesso, permitindo o gerenciamento remoto do Roteador (RT) a partir da VLAN 50 (Gerenciamento). Isso confirma que o Roteador está configurado corretamente para acesso remoto seguro e funcional.

6.1.3 Teste 3: Acessando Switch SALA 1

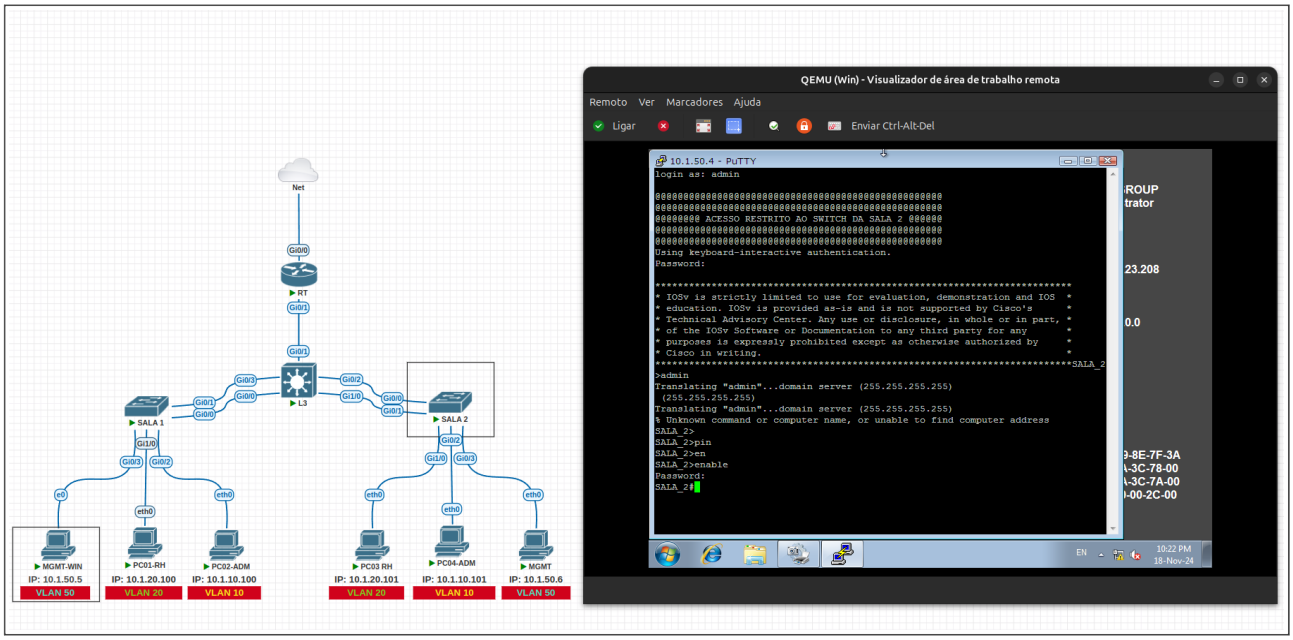
Objetivo: Verificar a conectividade e a capacidade de acessar remotamente o Switch SALA 1 via SSH, utilizando a VLAN 50 para gerenciamento da rede.



Resultado Obtido: O acesso SSH foi estabelecido com sucesso, permitindo o gerenciamento remoto do Switch SALA 1 a partir da VLAN 50 (Gerenciamento).

6.1.4 Teste 4: Acessando Switch SALA 2

Objetivo: Verificar a conectividade e a capacidade de acessar remotamente o Switch SALA 2 via SSH, utilizando a VLAN 50 para gerenciamento da rede, da mesma forma que foi feito para o Switch SALA 1.



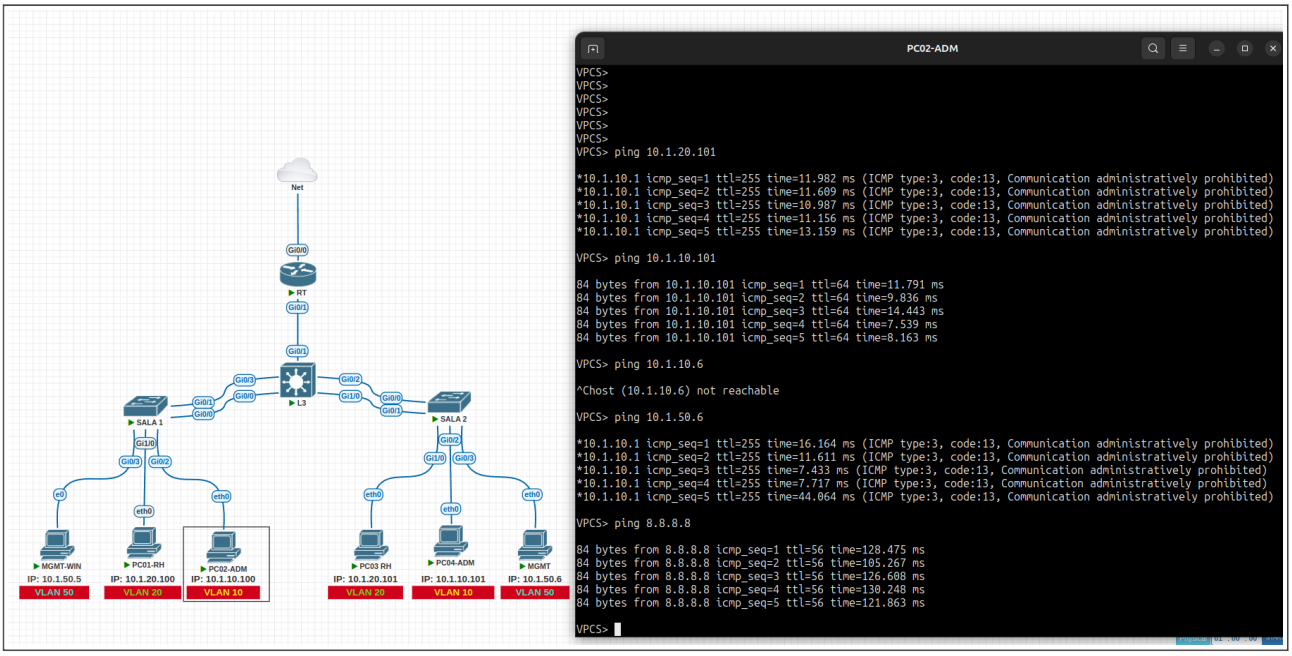
Resultado Obtido: O acesso SSH foi estabelecido com sucesso, permitindo o gerenciamento remoto do Switch SALA 2 a partir da VLAN 50 (Gerenciamento). Isso confirma que o Switch está corretamente configurado para acesso remoto seguro e funcional, assim como o Switch SALA 1.

6.2 Testando conectividade com VLANs

Verificar a conectividade entre a VLAN 10 (Administração) e as demais VLANs (20 - Recursos Humanos, 50 - Gerenciamento) para garantir que as ACLs e a segmentação de rede estejam funcionando conforme esperado, permitindo ou bloqueando o tráfego conforme as configurações definidas.

6.2.1 Teste 1: VLAN 10 (Administração) com as Demais VLANs

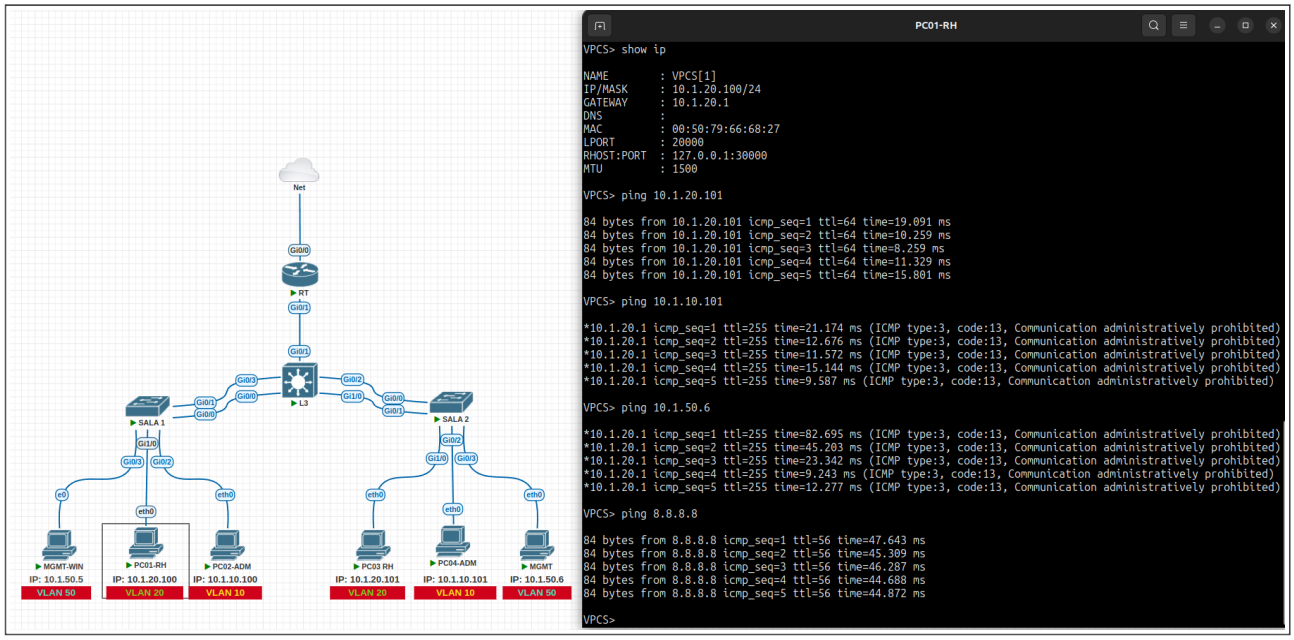
No terminal, foi realizado um teste de ping simultâneo entre a VLAN 10 (Administração) e as VLANs 20 (Recursos Humanos) e 50 (Gerenciamento). O objetivo era validar se as conectividades estavam funcionando **somente entre VLANs equivalentes** e validar o funcionamento das ACLs.



Resultado Obtido: A comunicação entre VLANs diferentes foi corretamente bloqueada conforme esperado pelas ACLs. Ou seja, a configuração de isolamento entre as VLANs, tanto de Administração (VLAN 10), Recursos Humanos (VLAN 20) e Gerenciamento (VLAN 50) foi eficaz.

6.2.2 Teste 2: VLAN 20 (Recursos Humanos) com as Demais VLANs

Verificar a conectividade entre dispositivos na VLAN 20 (Recursos Humanos) e testar a efetividade das ACLs aplicadas, que devem bloquear a comunicação entre VLAN 20 e as demais VLANs, exceto dispositivos da mesma VLAN.



Resultado Obtido: O teste de conectividade entre dispositivos da VLAN 20 e das demais VLANs foi concluído com sucesso, confirmando que a comunicação dentro da mesma VLAN está funcional e que as ACLs configuradas estão corretamente isolando a VLAN 20 das outras VLANs, garantindo segurança e segmentação no ambiente de rede.

6.2.3 Teste 3: VLAN 50 (Gerenciamento) com as Demais VLANs

No terminal, foi realizado um teste de ping simultâneo entre a VLAN 50 (Gerenciamento) e as VLANs 10 (Administração) e 20 (Recursos Humanos). O teste foi efetuado com sucesso.