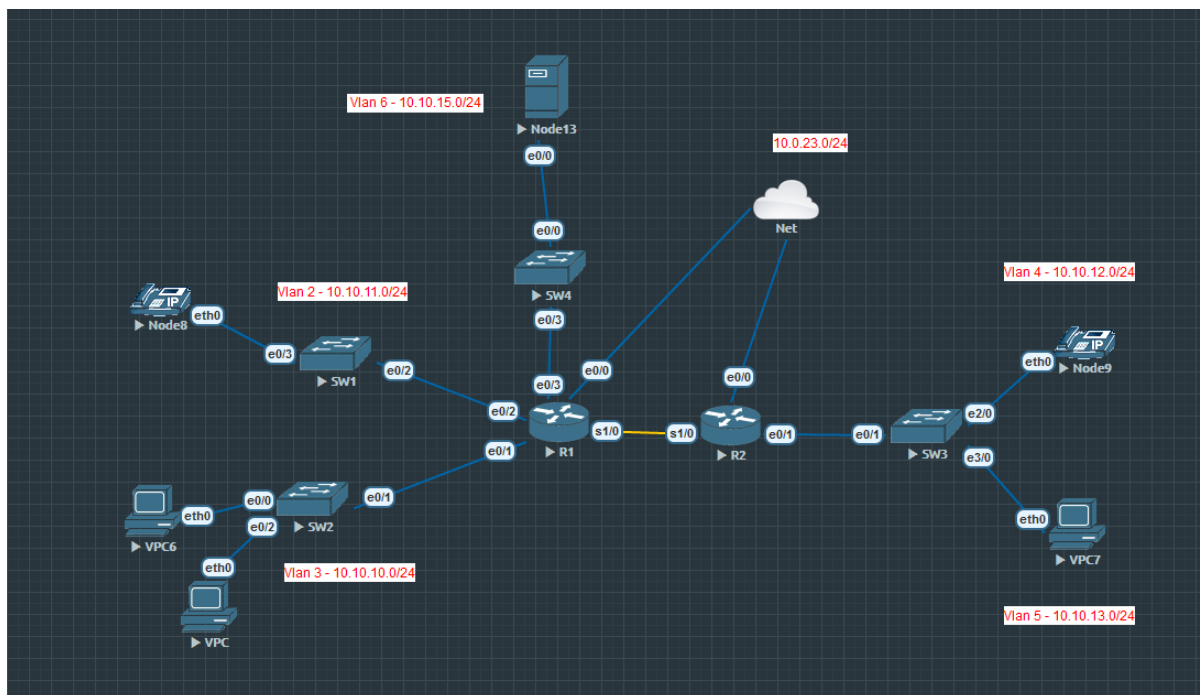


Configurações Desafio



FASE 1 – De cada VLAN conseguir “pingar” todas as outras

Comecei por construir o digrama de rede (imagem acima). Depois para cada uma das VLANS usei apenas um host por motivos de simplificação exceto na VLAN 3.

Configurei os **Hosts** com o IP correspondente a cada uma das VLANs e com default-gateway com o IP do router de saída de cada VLAN.

Cada **Switch** está configurado da seguinte maneira:

- A interface que sai para os **Hosts** está configurada no modo acesso e para aceder a cada VLAN que pertence.
- A interface que sai para o **Router** está configurada no modo trunk e encapsulada por Dotq1.

Cada **Router** está configurado da seguinte maneira:

- A interface que sai para os **Switches** está configurada numa subinterface encapsulada com Dotq1 e endereço IP que corresponde ao default-gateway dos **Hosts**.
- A interface Serial que sai para o **Router** está configurada com uma nova rede [10.10.14.0/24](#).
- Foi configurado o protocolo **RIP** para dar conhecimento das redes que estes estão conectados.

FASE 2 – Apenas permitir pacotes ICMP entre VLANs, restante bloqueado.

Access-List

Para limitar os pacotes que circulam entre VLANs configurei em cada **Router** uma Access-list com as seguintes regras:

- Permite todos os pacotes ICMP, visto que é possível fazer-se **Ping** de umas VLANs para as outras.
- Permitir pacotes TCP em que tenham source na rede de gestão, com qualquer endereço IP de destino e porto de destino 22.
- Permitir pacotes TCP de qualquer endereço IP no porto 22, com endereço IP de destino na rede de gestão.
- Recusar qualquer outro pacote que não respeite as regras acima descritas.

Atribui a cada uma das interfaces de entrada nas VLANs a Access-list acima criada com sentido **inbound**.

FASE 3 – SSH habilitado para todos os equipamentos de rede disponível através de uma rede de gestão.

Para cada um dos equipamentos de rede foi feita a seguinte configuração:

- Foi configurado um **Hostname** e **IP Domain-name**.
- Foi gerada uma chave criptográfica RSA com base no **Hostname** e **IP Domain-name**.
- Foi criado um username e password.
- Foi escolhida também a versão 2 do SSH

FASE 4 – Criar um script para retirar configurações e guardá-las em repositório local automaticamente.

Fiz um script capaz de retirar as configurações de cada um dos dispositivos de rede.

Funcionamento do script:

- Pede os endereços IP de cada um dos dispositivos até ser introduzida a palavra “end”.
- Faz a conexão a cada um dos dispositivos pedindo a password de cada um.
- Renomeia cada um dos ficheiros para o Hostname de cada equipamento.
- Guarda-os na diretoria onde se encontra o script.

FASE 5 – Fazer upload das Configs dos equipamentos num repositório GIT

Adicionei no Github a minha chave pública gerada na máquina com o IP 172.20.170.95.

Fiz depois Git Clone com o link disponível GitHub via SSH.

Funcionamento do script:

- No final do script os ficheiros novos são inseridos no repositório remoto no GitHub (<https://github.com/Freitas512/Desafio>)