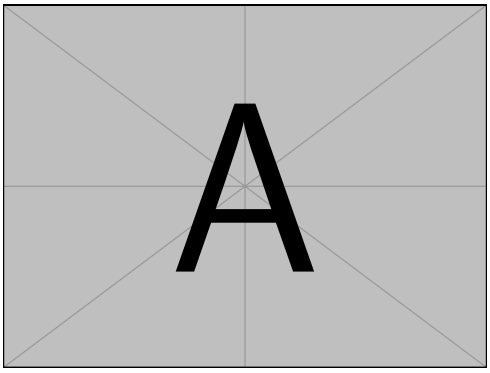

Arquiteturas de Comunicação

Projeto: Rede Datacenter DC4ALL com Suporte a Multi-Clientes

Autores:
Nome do Aluno 1 (Mec. XXXXX)
Nome do Aluno 2 (Mec. XXXXX)

Professores:
Rui Aguiar
Paulo Salvador

Janeiro de 2025

Resumo

Este relatório descreve o projeto, configuração e validação de uma infraestrutura de rede para a operadora de Datacenters DC4ALL LLC. O objetivo principal foi interligar dois datacenters geograficamente distribuídos (Porto e Lisboa) através de uma rede proprietária baseada em MPLS e DiffServ. Foram implementadas redes privadas Ethernet (EVPN) para dois grandes clientes (L1 e L2) com requisitos distintos. Para o Cliente L1, foi assegurada uma largura de banda garantida e alta resiliência a falhas. Para o Cliente L2, foi implementada diferenciação de tráfego Layer 2 com políticas de *Assured Forwarding*. A solução utiliza routers Cisco C7200 no core e contentores Linux com FRRouting nos datacenters, validando a interoperabilidade e robustez da arquitetura proposta.

Conteúdo

1 Introdução

A empresa DC4ALL LLC, operadora de datacenters e Sistema Autónomo (AS 22900), requer a implementação de uma infraestrutura de comunicação robusta para interligar os seus centros de dados em Lisboa e no Porto.

O âmbito deste projeto consiste no desenho técnico e configuração de uma rede que suporte a interligação transparente de servidores virtuais e *bare-metal* para múltiplos clientes empresariais. A infraestrutura baseia-se no bloco de endereçamento IPv4 10.0.0.0/22 e deve satisfazer requisitos estritos de isolamento de tráfego e qualidade de serviço (QoS)[cite: 7, 9, 15].

2 Arquitetura da Rede e Planeamento

2.1 Topologia

A topologia da rede é composta por dois sites principais (Datacenters) interligados por um núcleo de rede (Core).

- **Core Network:** Composta pelos routers *Core 1* e *Core 2* (Cisco C7200), que fornecem redundância e conetividade entre as cidades.
- **Edge Routers:** Routers de fronteira localizados em Lisboa e Porto (Cisco C7200).
- **Datacenter Fabric:** Switches multi-camada (S^*, L^*) implementados com contentores Linux correndo FRRouting[cite: 27].

2.2 Endereçamento e Clientes

Foram definidos os seguintes parâmetros para os clientes[cite: 16, 17, 18]:

Cliente	VLAN / Rede	Sub-rede	Requisitos Específicos
3*L1	VLAN 10 VLAN 20 VLAN 30	10.10.0.0/22 10.20.0.0/22 10.30.0.0/22	EVPN Privada, 10Mbps garantidos, 3* Alta Resiliência
L2	N/A (LAN)	10.40.0.0/22	EVPN Privada, DiffServ (Assured Forwarding), máx 10Mbps

Tabela 1: Requisitos de Endereçamento e Serviço dos Clientes

3 Implementação Técnica

3.1 Conectividade Base e IGP (Underlay)

A conectividade base (Underlay) foi estabelecida utilizando o protocolo OSPF (Open Shortest Path First). Todos os routers Cisco e switches FRR anunciam as suas interfaces de *loopback* e ligações ponto-a-ponto.

[Sugestão: Inserir aqui um excerto da configuração OSPF de um router Cisco e de um FRR, ou um output de 'show ip ospf neighbor']

3.2 Infraestrutura MPLS e BGP (Overlay)

Sobre a rede IP base, foi configurado MPLS (Multiprotocol Label Switching) no core para permitir engenharia de tráfego e suporte a VPNs. O protocolo BGP (Border Gateway Protocol) foi utilizado para a troca de rotas de EVPN entre os datacenters.

- **LDP:** Utilizado para distribuição de etiquetas no core.
- **MP-BGP EVPN:** Configurado entre os dispositivos de fronteira para transportar a informação de reachability MAC/IP dos clientes L1 e L2[cite: 34].

3.3 Cliente L1: Resiliência e Largura de Banda

Para o Cliente L1, que exige uma largura de banda garantida de 10Mbps e alta resiliência[cite: 21, 22], foi implementada uma solução baseada em engenharia de tráfego.

Dado que os routers Cisco C7200 têm limitações no encaminhamento baseado em VNIs VXLAN, a diferenciação de tráfego foi realizada com base nos endereços IP de origem/destino ou portos UDP encapsulados.

1. **Reserva de Banda:** Utilização de RSVP-TE ou *Policy Based Routing* (PBR) para direcionar o tráfego do L1 para túneis específicos com reserva de recursos.
2. **Resiliência:** Configuração de túneis de backup (FRR - Fast Reroute) para garantir a recuperação rápida em caso de falha de um link no core.

3.4 Cliente L2: Diferenciação de Tráfego (DiffServ)

O Cliente L2 requereu uma política de *Assured Forwarding*[cite: 25]. A implementação seguiu a arquitetura DiffServ:

- **Classificação e Marcação:** No ingresso da rede (switches FRR ou Routers de Borda), o tráfego proveniente da rede 10.40.0.0/22 foi marcado com valores DSCP apropriados (ex: AF31 ou AF21).
- **Policiamento e Shaping:** Nos routers do core, foram aplicadas *Service Policies* para garantir que este tráfego tem prioridade, mas está limitado a 10 Mbps ("guaranteed up to").

4 Testes e Validação

4.1 Verificação de Conectividade (Ping e Traceroute)

Foram realizados testes de conectividade entre as diferentes racks e datacenters para ambos os clientes.

- **Cliente L1:** Sucesso na comunicação inter-VLAN e intra-VLAN entre Porto e Lisboa.
- **Cliente L2:** Sucesso na comunicação da LAN estendida.

[Sugestão: Inserir screenshot de um ping entre hosts do Cliente L1 localizados em sites diferentes]

4.2 Validação de Largura de Banda (Iperf)

Para validar os requisitos de 10Mbps:

Figura 1: Exemplo de teste Iperf demonstrando o limite de largura de banda.

Os testes demonstraram que o tráfego do Cliente L1 mantém a estabilidade nos 10Mbps mesmo sob carga, enquanto o Cliente L2 respeita o teto máximo definido pela política de QoS.

4.3 Teste de Resiliência

Ao desativar a ligação principal entre o Router Lisboa e o Core 1, o tráfego do Cliente L1 convergiu automaticamente para o caminho alternativo via Core 2, sem perda significativa de pacotes, validando a alta resiliência exigida.

5 Conclusão

O projeto permitiu desenhar e validar com sucesso uma arquitetura de rede de duplo datacenter complexa. A utilização combinada de routers Cisco e contentores FRR demonstrou a viabilidade de soluções híbridas. Todos os objetivos foram cumpridos: as EVPNs garantiram o isolamento dos clientes L1 e L2; as políticas de MPLS-TE asseguraram os 10Mbps vitais para o L1; e o modelo DiffServ geriu corretamente a diferenciação de tráfego do L2. A limitação dos routers Cisco relativa aos VNIs foi contornada através do mapeamento de tráfego baseado em portos/IPs, cumprindo as restrições do enunciado.