VxLAN – A nova forma de fazer Metro-Ethernet

Telic
TECHNOLOGIES

We
know
about
network

Telic TECHNOLOGIES

Portfólio de **Soluções**

CGNat

SDWan

Inteligência em **Redes**

Trânsito **IP**

Inteligência em **Anti-DDoS**

Inteligência em **Infraestrutura**

Mitigação **DDoS**

Inteligência em **Monitoramento**

NOC

Agenda

- Motivação
- O que é VXLAN
- Como o Vxlan Funciona?
- Modelo de rede com VXLAN
- VXLAN vs MPLS
- VXLAN em redes Metro Ethernet
- EVPN
- Estudo de caso
- VXLAN para SDwan e mitigação de ataques DDoS

Motivação

Com o aumento da necessidade de transportes em camada 2 e a diminuição do uso comercial das VPN's de camada 3 faz-se necessário uma nova opção para os novos modelos de rede.

Percebendo o falta de conhecimento difundido na maioria dos profissionais de redes, esse trabalho tem como intuito apresentar de maneira simples e objetiva como o VXLAN trabalha e qual seu papel nas redes modernas.

O que é VXLAN?

O VXLAN é um protocolo de encapsulamento que fornece a conectividade usando o tunelamento para estender as conexões de Camada 2 em uma rede de Camada 3.

VXLAN foi criado originalmente para uso em Datacenters, o intuito era interligar no mesmo domínio de broadcast vários servidores, storages e equipamentos em diferentes localidades.

Um exemplo claro de que como VXLAN é feito para datacenter e virtualização é que podemos ver Hypervisors como VMWARE e HyperV, suportando vxlan de maneira nativa.

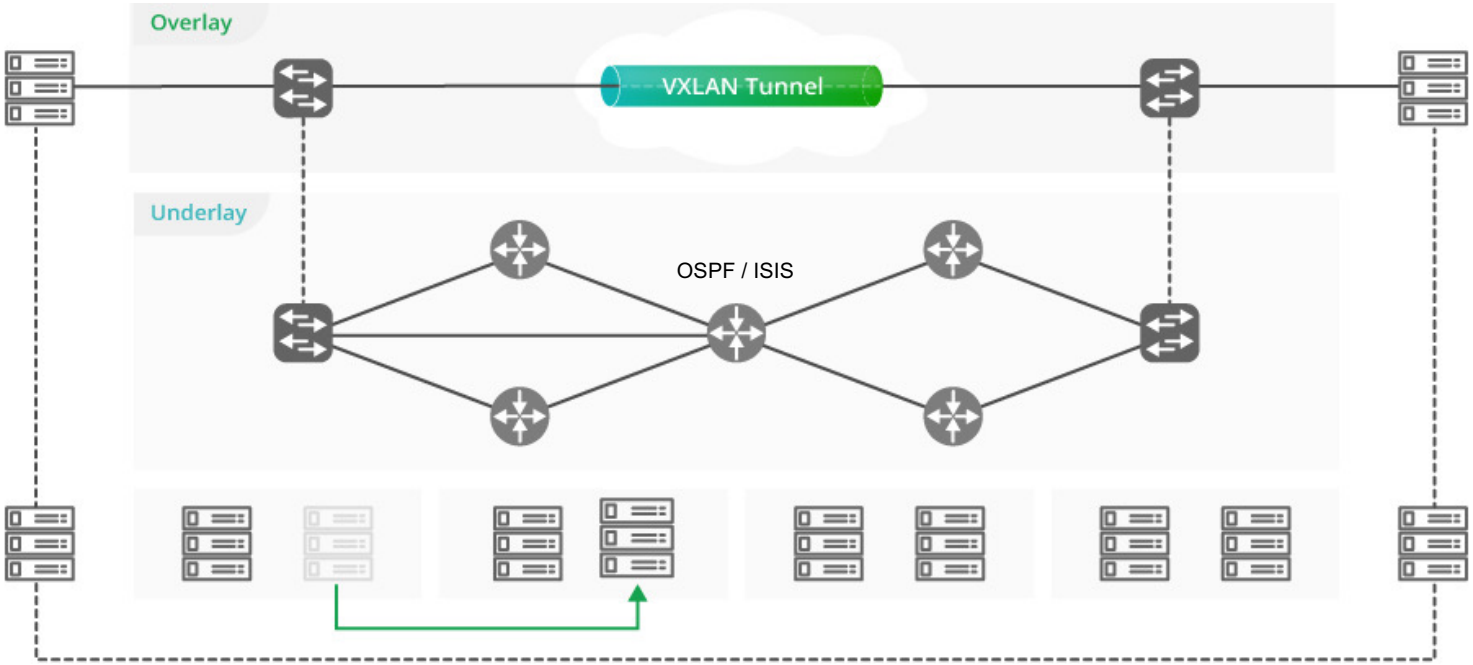
Virtual eXtensible Lan

Como o VXLAN funciona?

É bem simples de entender como VXLAN funciona:

- Encapsula os quadros ethernet em pacotes UDP
- Cada túnel tem um identificador chamado VNI (VXLAN Network Indentifier)
- VNI é similar a Vlan
- Cada elemento da rede que faz o encapsulamento ou desencapsulamento tem o nome de VTEP (Vlan Tunel End Point)
- VTEP é quem recebe ou entrega os pacotes de camada 2.
- Sempre funciona como ponto multi-ponto
- Os VTEP's aprendem MAC address, similar ao VPLS do MPLS
- Basicamente baseado em flood and learning

VXLAN - Modelo



VXLAN em redes Metro Ethernet

Com a evolução dos sistemas operacionais e equipamentos de rede, vários fabricantes e desenvolvedores começaram a incorporar VXLAN em seu código a adicionando essa feature.

- Atualmente VXLAN já é suportado pela maioria dos fabricantes de Switch's e roteadores
- Huawei, Cisco, Juniper, Arista, HP, Mikrotik (v7), etc
- OCNOS, SonicOS, Cumulus, FRR
- Hyper-V, Vmwave
- Datacom ainda não oferece suporte

VXLAN vs MPLS

A comparação com os dois protocolos é um tanto injusta, já que um não substitui o outro. Podemos então fazer um paralelo entre MPLS e Vxlan, já que com os dois podemos estabelecer tuneis de camada 2 sob uma rede camada 3.

VXLAN	MPLS
Possibilita apenas tuneis de camada 2	Tuneis de camada 2 e 3
Depende apenas de uma rede layer 3 onde um VTEP alcance o outro VTEP	Depende de uma malha MPLS, onde todos os equipamentos falem MPLS
Não precisa de protocolos auxiliares	Necessário LDP ou RSVP
Funciona perfeitamente em redes com MTU de 1500	MTU precisa sempre ser maior que 1500
Balanceamento perfeito entre interfaces agregadas	Necessário FAT + DLB na maioria dos equipamentos
Sem possibilidade de engenharia de tráfego inerente ao protocolo	Engenharia de tráfego completa com RSVP-TE
Não precisa de VXLAN em seu núcleo	Depende de label's em todo seu núcleo

EVPN - Ethernet VPN

É a solução de control-plane para distribuir informações de camada 2 e 3 entre os VTEP's em uma rede overlay

- Usa-se o MP-BGP para suportar as extensões de EVPN para o VXLAN
- Não é mandatório para formar tuneis layer2
- Diminui o flooding, já que agora é direcionado
- Podemos fazer um paralelo (a muito grosso modo) entre tuneis MPLS Martini e Kompella

Underlay e Overlay

Underlay basicamente são as redes com protocolos de roteamento como OSPF, IS-IS, EIRGP, etc que permitem caminhos redundantes ao mesmo destino. Overlay (rede sobreposta) basicamente são os túneis que formamos, como o VXLAN. Você ouvirá muito disso ainda.

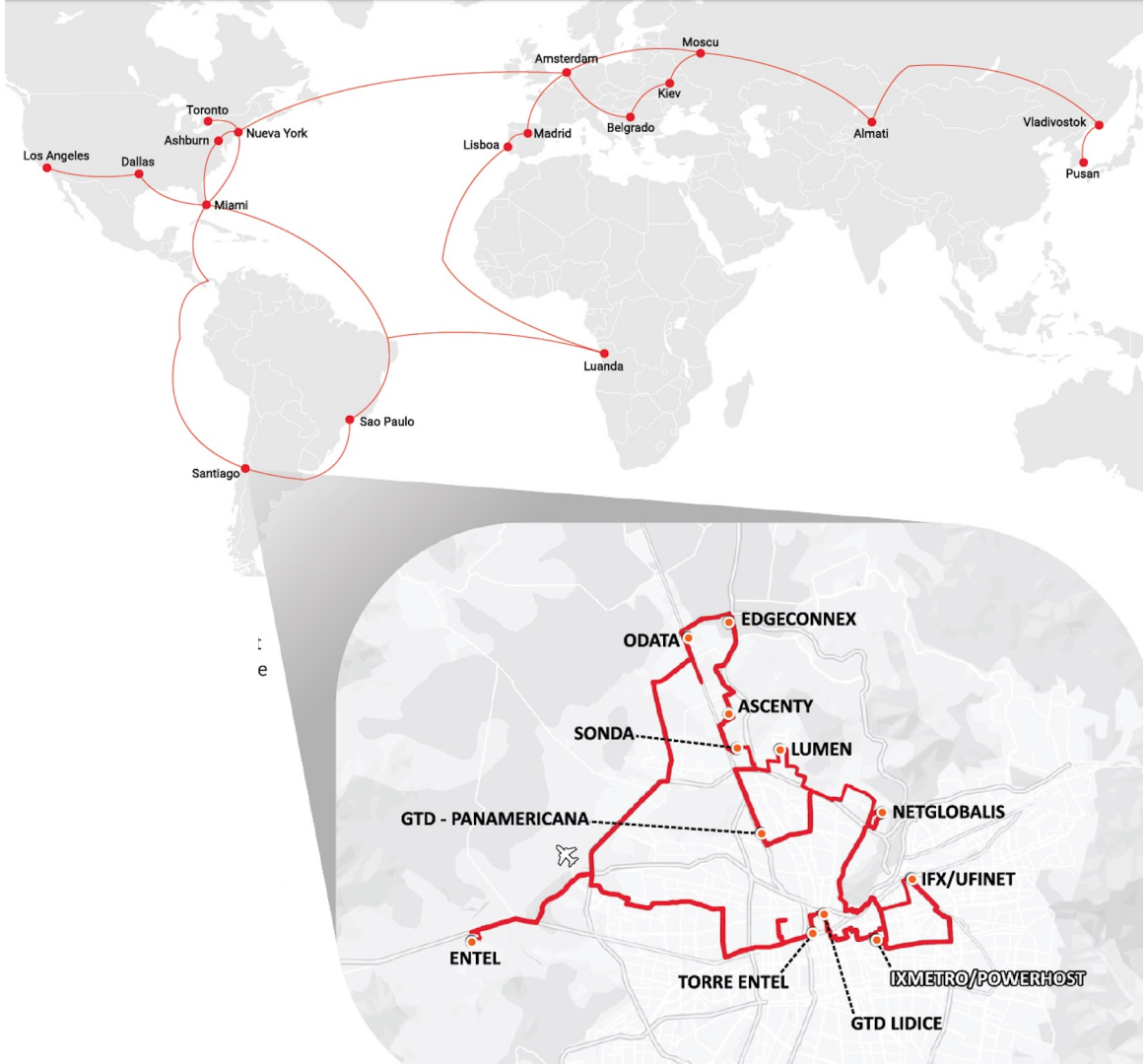
Estudo de caso

IXMETRO

POWERHOST DATACENTER

Cliente Telic, com sua Matriz em Santiago (Chile) focada em serviços de datacenter, IAAS, VPS, colocation, trânsito IP e circuitos ponto a ponto

Mapa de rede IXMETRO



Desafios

Para o cenário proposto, deveríamos:

- Interligar redes em cinco países de dois continentes
- Interligar 13 data-centers dentro de Santiago
- Interligar servidores e storages
- Transportar Circuitos de transito IP e Peering remoto
- Entregar circuitos de Ponto a ponto e ponto multi-ponto

Por que escolhemos VXLAN?

Dentre muitos motivos, os abaixo foram os determinantes na escolha:

- Fabricantes disponíveis no mercado Chileno
- Equipamentos já em uso na infra-estrutura
- Interoperabilidade
- Custo Beneficio
- Praticidade no deploy
- Know-how da equipe já existente

Configuração - Arista

```
interface Loopback0
   ip address 10.51.100.2/32

interface Port-Channel27
   description ENLACE-IFX-01
   no switchport
   network 10.19.0.2/30
   ip ospf network point-to-point

interface Ethernet12/1
   description ACESSO-CLIENTE-XZY-PONTA-Z
   switchport access vlan 234
   switchport mode dot1q-tunnel

router ospf 1
   router-id 10.51.100.2
   redistribute connected
   network 10.19.0.0/30 area 0.0.0.0

interface Vxlan1
   vxlan source-interface Loopback0
   vxlan vlan 234 vni 234
   vxlan flood vtep 10.51.100.4
```

```
interface Loopback0
   ip address 10.51.100.4/32

interface Port-Channel12
   description ENLACE-IFX-01
   no switchport
   network 10.19.0.1/30
   ip ospf network point-to-point

interface Ethernet26/1
   description ACESSO-CLIENTE-XZY-PONTA-A
   switchport access vlan 234
   switchport mode dot1q-tunnel

router ospf 1
   router-id 10.51.100.4
   redistribute connected
   network 10.19.0.0/30 area 0.0.0.0

interface Vxlan1
   vxlan source-interface Loopback0
   vxlan vlan 234 vni 234
   vxlan flood vtep 10.51.100.2
```

Troubleshooting – Arista

```
PE-ABC#show vxlan address-table dynamic vtep 10.51.100.5
          Vxlan Mac Address Table
----------------------------------------------------------------------

Vlan  Mac Address     Type      Prt  Vtep             Moves   Last Move
----  -----------     ----      ---  ----             -----   ---------
1150  0015.ad38.78df  DYNAMIC   Vx1  10.51.100.5      1       53 days, 10:03:18 ago
1150  e468.a3f8.1ece  DYNAMIC   Vx1  10.51.100.5      1       53 days, 10:03:53 ago
Total Remote Mac Addresses for this criterion: 2
```

Mostra todos os MAC's aprendidos de um VTEP

```
PE-ABC#show vxlan address-table vlan 1103
          Vxlan Mac Address Table
----------------------------------------------------------------------

Vlan  Mac Address     Type      Prt  Vtep             Moves   Last Move
----  -----------     ----      ---  ----             -----   ---------
1103  887e.25d3.600b  DYNAMIC   Vx1  10.51.100.8      1       10 days, 19:05:26 ago
1103  887e.25d3.60dd  DYNAMIC   Vx1  10.51.100.8      1       10 days, 19:05:26 ago
Total Remote Mac Addresses for this criterion: 2
```

Mostra todos os MAC's aprendidos em um VNI

Balanceamento em LACP

Mesmo com interfaces agregadas e tuneis VXLAN, não temos problemas com balanceamento.

```
[redacted]#show interfaces po6 | inc rate
  5 minutes input rate 127 Gbps (64.8% with framing overhead), 13664394 packets/sec
  5 minutes output rate 22.9 Gbps (11.9% with framing overhead), 6154975 packets/sec
[redacted]#show interfaces et22/1 | inc rate
  5 minutes input rate 64.0 Gbps (65.1% with framing overhead), 6871765 packets/sec
  5 minutes output rate 11.6 Gbps (12.1% with framing overhead), 3092824 packets/sec
[redacted]#show interfaces et21/1 | inc rate
  5 minutes input rate 63.6 Gbps (64.7% with framing overhead), 6800912 packets/sec
  5 minutes output rate 11.3 Gbps (11.8% with framing overhead), 3065475 packets/sec
```

Resultado:

Então depois de 1 ano em operação, quais os resultados?

- Rede Robusta e resiliente
- Escalabilidade
- Menor custo de operação
- Maior interoperabilidade
- 2tb/s+ de trafego agregado

VXLAN para SDwan e mitigação de ataques DDoS

Se VXLAN é basicamente o encapsulamento de frames ethernet em pacotes UDP, por não usa-lo para outros fins?

- Possibilidade de usar criptografias como IPsec
- Atravessar VLAN's de um ponto a outro via internet
- Fabricantes de SDWAN's já preferem tuneis VXLan a tuneis GRE ou l2tp.
- Podem ser usada no lugar de tuneis GRE para mitigação de ataques DDoS.
- Não necessita de ajustes no TCP-MSS

Contatos **Telic**

+55 17 99711-5311

+55 (11) **4770 0522**

www.**telic**.com.br

Telic
TECHNOLOGIES