Lotic
ARQUITETURA DE SOLUÇÕES

Top Down Network Design para ambientes de Data Center e Cloud Computing

Lotic
ARQUITETURA DE SOLUÇÕES

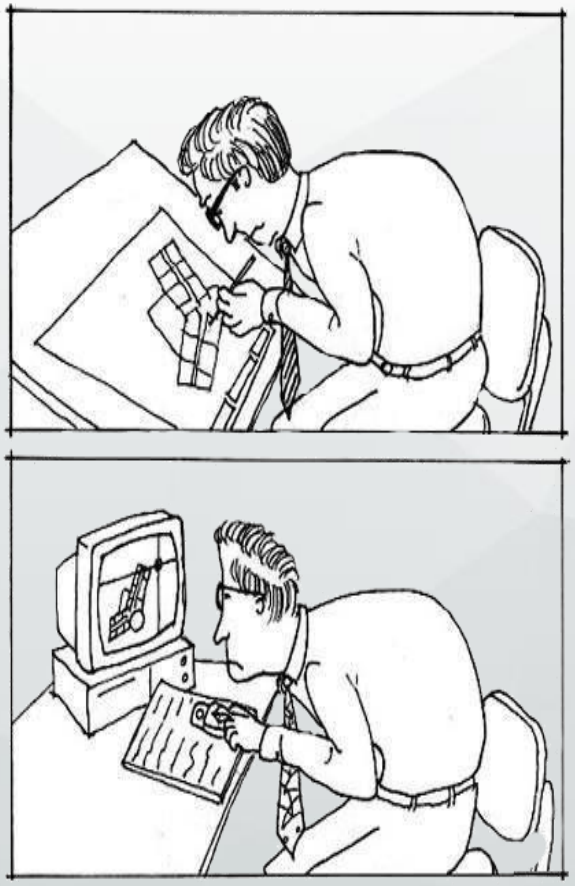
GTER 41 | GTS 27
12 a 14 de maio de 2016, Uberlândia - UniAlgar

Quem Somos

- Nosso time é composto de arquitetos e especialistas de diversas áreas relacionadas à infraestrutura de TI, Data Center e aplicações.

- Construímos soluções com um propósito baseado totalmente em arquitetura e padronização.

- Somos avessos ao *lock-in*, ou seja, nossos projetos procuram seguir protocolos e padrões abertos estimulando assim a concorrência entre fabricantes e a liberdade de escolha.



Lotic
ARQUITETURA DE SOLUÇÕES

GTER 41 | GTS 27
12 a 14 de maio de 2016, Uberlândia - UniAlgar

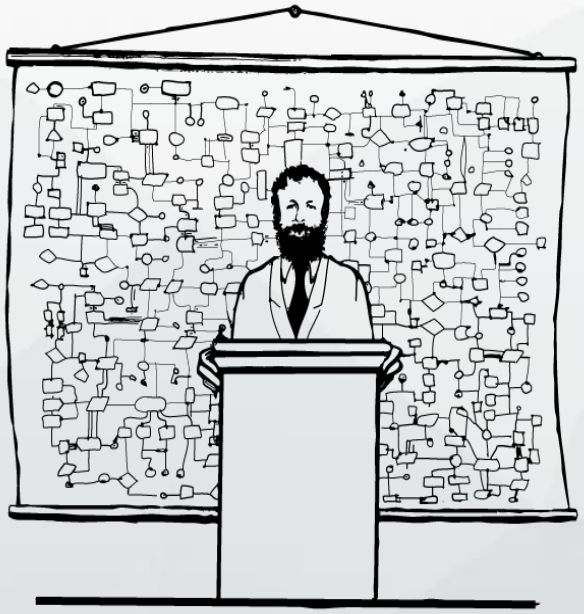
Marcelo Veriato Lima <mlima@lotic.com.br>

Especializado em...

- Infraestruturas de Data Center e Cloud Computing
- Arquitetura de Infraestrutura e aplicações
- Ambientes em alta disponibilidade e altamente escaláveis

Certificações

- Apache CloudStack Certified Professional
- Citrix Certified Professional – Networking (CCP-N)
- F5 System Engineer – LTM/GTM/ASM
- Cisco Certified Internetwork Expert – Data Center (CCIE-DC written)
- Cisco Certified Network Professional – Data Center (CCNP-DC)
- Cisco Certified Network Associate – Data Center (CCNA-DC)
- Cisco Data Center Unified Computing Support Specialist
- Cisco Data Center Unified Computing Design Specialist
- Cisco Data Center Unified Fabric Support Specialist
- Cisco Data Center Unified Fabric Design Specialist



"Now that you have an overview of the system, we're ready for a little more detail"

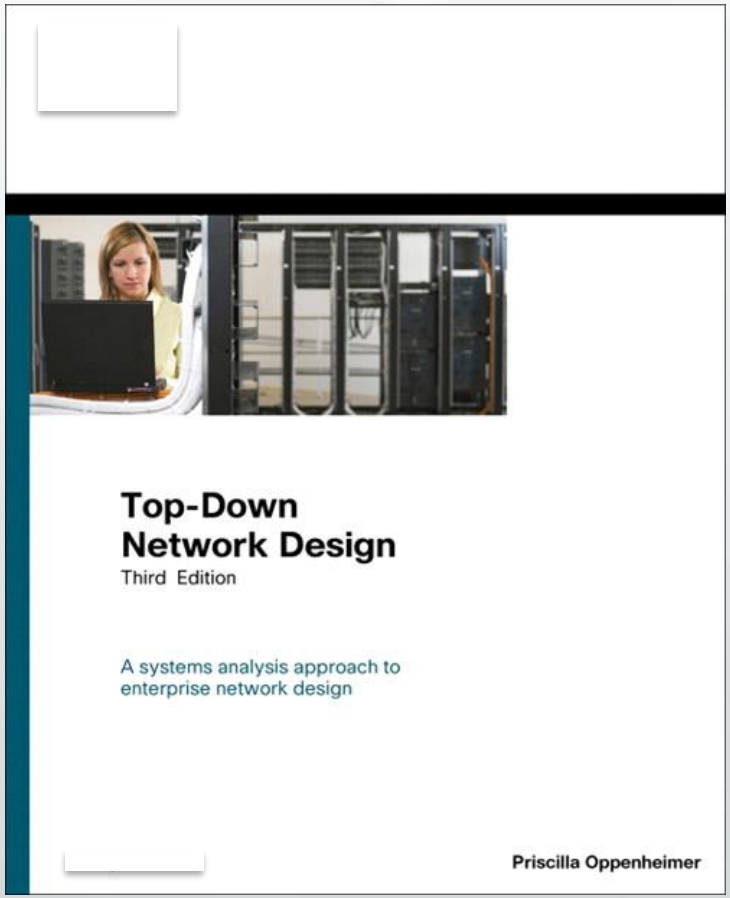
Lotic
ARQUITETURA DE SOLUÇÕES

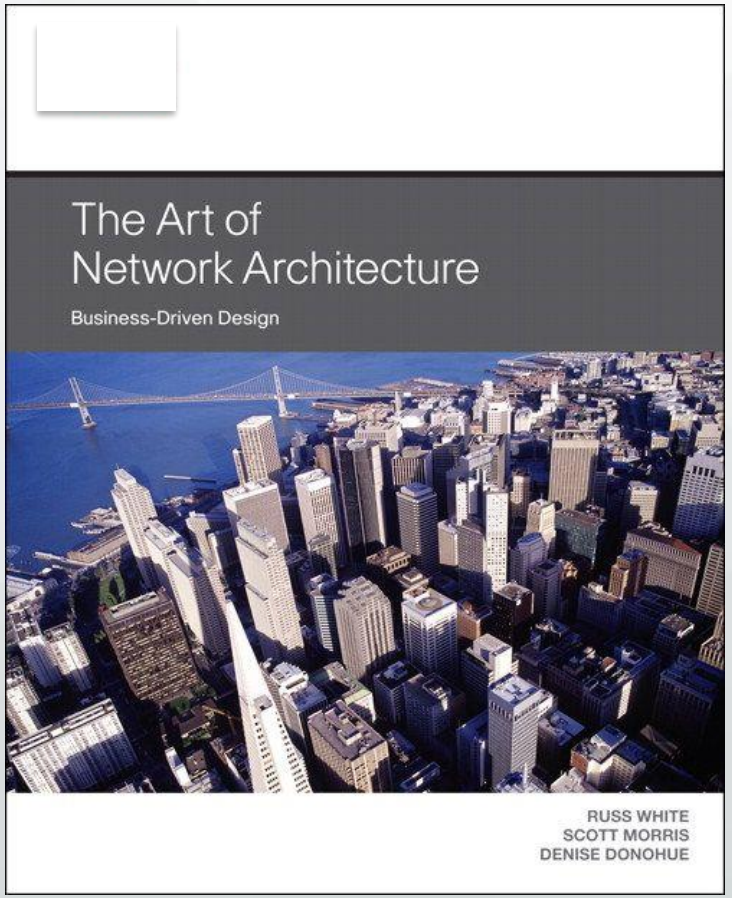
GTER 41 | GTS 27
12 a 14 de maio de 2016, Uberlândia - UniAlgar

Agenda:

- Literatura recomendada
- Top Down Network Design
  - Identificando as necessidades e objetivos do cliente
  - Design da rede lógica
  - Design da rede física
  - Testando, otimizando e documentando o seu projeto
- Montando uma topologia lógica e física

Literatura recomendada





Lotic
ARQUITETURA DE SOLUÇÕES

GTER 41 | GTS 27
12 a 14 de maio de 2016, Uberlândia - UniAlgar

Top Down Network Design

Identificando as necessidades e objetivos do cliente

- Analisando os objetivos de negócio e restrições
- Analisando metas técnicas
- Caracterizando as redes existentes
- Caracterizando o tráfego de rede

Identificando as necessidades e objetivos do cliente

- Analisando os objetivos de negócio e restrições
  - Conhecendo o negócio da empresa
  - Visibilidade ao projeto
  - Entrevistando o cliente
  - Identificando mudanças
  - Identificando escopo
  - Identificando aplicações
  - Identificando as “panelinhas”
  - Limitações orçamentárias
  - Limitações de pessoas
  - Tempo do projeto

Identificando as necessidades e objetivos do cliente

- Analisando metas técnicas
  - Escalabilidade
    - Plano de expansão
    - Expandindo acesso aos dados
    - Restrições de escalabilidade
  - Alta disponibilidade
    - Disaster Recovery
    - Especificando requerimentos de disponiblidade
  - Network performance
    - Optimizando a utilização da rede
    - Throughput

Identificando as necessidades e objetivos do cliente

- Analisando metas técnicas
  - Network Performance
    - Precisão
    - Eficiência
    - Variação de Delay
    - Tempo de resposta
  - Segurança
    - Identificando ativos de rede
    - Analisando riscos de segurança
    - Desenvolvendo requerimentos de segurança

Identificando as necessidades e objetivos do cliente

- Analisando metas técnicas
  - Gerenciamento
  - Usabilidade
  - Adaptatibilidade

Identificando as necessidades e objetivos do cliente

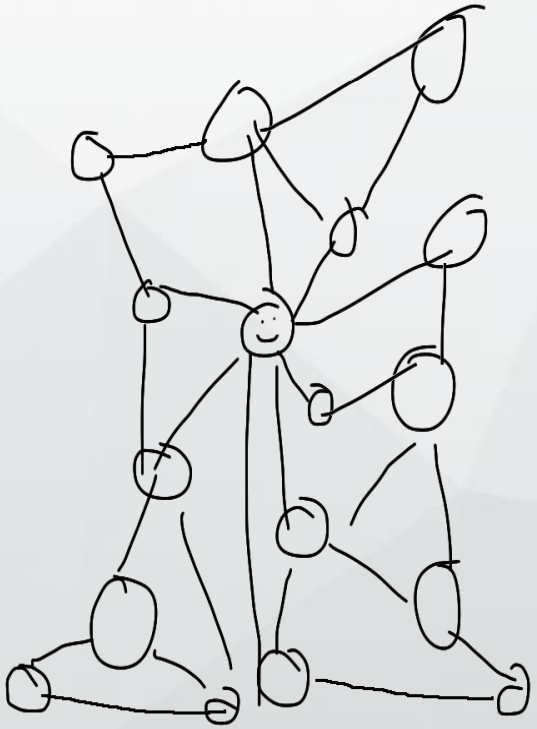
- Caracterizando as redes existentes
  - Desenhando um mapa lógico e físico da rede
  - Levantamento do plano de endereçamento
  - Caracterizando os tipos de cabeamento
  - Analisando disponibilidade da rede
  - Utilização da rede
  - Checando estado de roteadores, switches, firewalls, etc
  - Checando o ambiente físico

Identificando as necessidades e objetivos do cliente

- Caracterizando o tráfego de rede
  - Descobrindo os fluxos
  - Top sources & destinations
  - Caracterizando os tipos de fluxos
  - Levantando a banda consumida por aplicação
  - Analisando fluxos de aplicações
  - Documentando fluxos

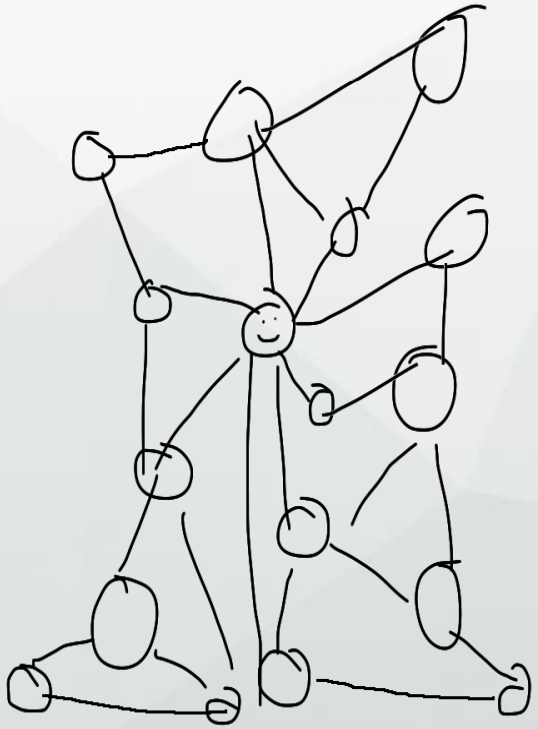
Design da rede lógica

- Desenhando a topologia lógica da rede
- Especificando modelos de endereçamento e sumarização
- Selecionando protocolos de roteamento e features para L3
- Desenvolvendo estratégias de segurança
- Desenvolvendo estratégias de gerenciamento



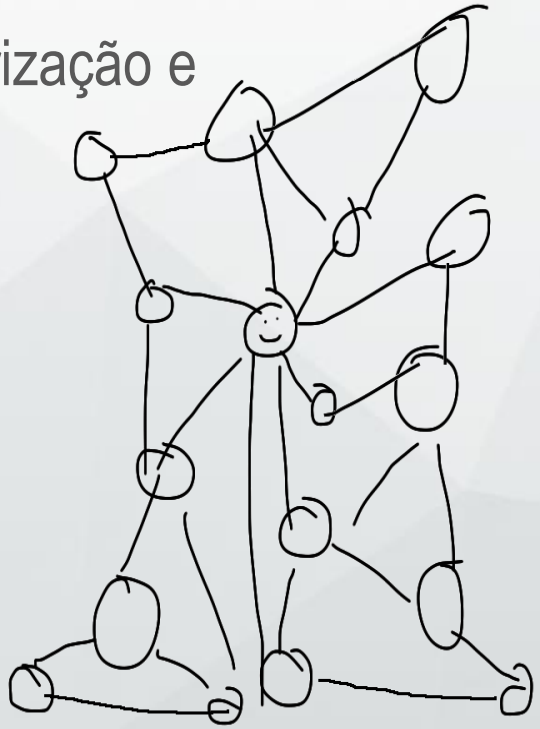
Design da rede lógica

- Desenhando a topologia lógica da rede
  - Pense em criar uma rede modular e simples
  - Borda do Data Center (AS, peering, links)
  - Proteções para a borda (DoS & DDoS, IPS & IDS)
  - Firewalls de borda, perímetros e aplicações
  - Perímetros de gerenciamento, serviços e aplicações
  - Balanceamento local e global
  - Sites remotos (WAN)
  - Acesso remoto (VPN)
  - Segmentação L2 (VLAN ou VxLAN)
  - Segmentação L3 (VRF like)



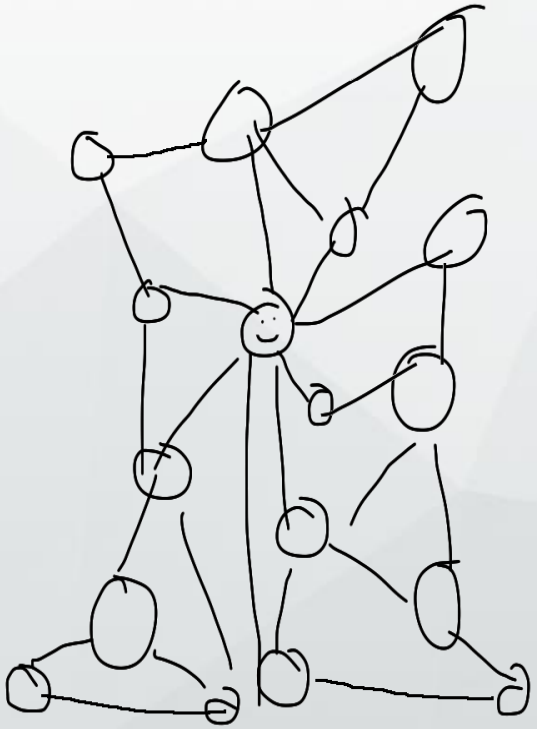
Design da rede lógica

- Especificando modelos de endereçamento, sumarização e nomenclatura
  - IPv4 & IPv6
  - Uso de NAT e PAT
  - Endereçamento estático ou dinâmico
  - Sumarização
  - Redes locais do Data Center
  - Redes de trânsito entre ativos da rede (fw, lb, sw, rt)
  - Servidores DNS



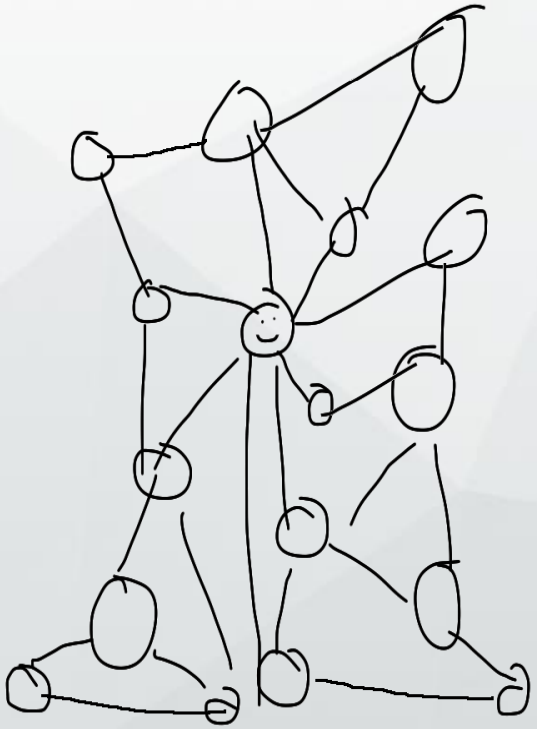
Design da rede lógica

- Selecionando protocolos de roteamento
  - Será que realmente preciso de roteamento dinâmico dentro do Data Center?
  - Sumarizar todo ambiente
  - Sistema autônomo na borda
  - Roteamento entre perímetros
  - WAN
  - BGP ou OSPF, eis a questão



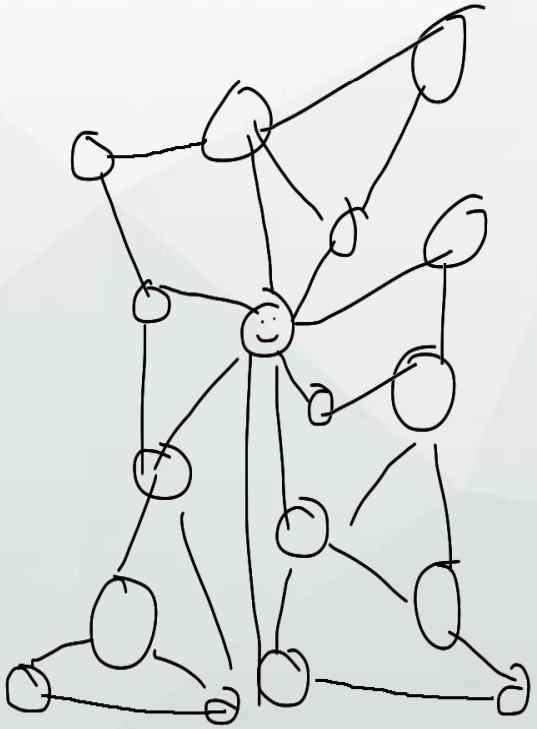
Design da rede lógica

- Desenvolvendo estratégias de segurança
  - Segurança como pré-requisito do ambiente
  - Identificando onde estão os dados valiosos
  - Analisando riscos de segurança
  - Criptografia de dados
  - Auditoria de logs
  - Filtro de pacotes
  - Testes periódicos
  - Sistemas atualizados



Design da rede lógica

- Desenvolvendo estratégias de gerenciamento
  - Processos de gerenciamento
  - Gerência de configuração, autorização e segurança
  - Arquitetura de gerenciamento centralizado e distribuído
  - Gerência in-band ou out-of-band
  - Selecionando protocolos de gerenciamento
  - Selecionando ferramentas de gerenciamento
  - Definindo SLAs e Thresholds



Design da rede física

- Definindo o tipo media e cabeamento
- Selecionando protocolos de swiching
- Desenhando topologia física
- Definindo fabricantes e linhas de equipamentos

Design da rede física

- Definindo o tipo de media e cabeamento
  - Tipo de media, fast, giga, ten giga, etc
  - Fibra ou par trançado
  - Topologia ToR ou EoR
  - Trabalhando com cores
  - Ferramentas para documentação
  - Custos vs Objetivos

Design da rede física

- Selecionando protocolos de switching
  - Fuja do *STP
  - Explore o Link-Aggregation (802.3ad) ou VPC like
  - Sempre pense em Stacking
  - VLAN (802.1q) continuará sendo utilizado
  - Alguns gostam de GVRP/VTP
  - Extensão de VLAN em L2, VPLS/VPWS, OTV like E-VPN e PBB-EVPN
  - Defina o QoS
  - Jumbo Frame
  - Rede SAN (NFS, ISCSI, FC ou FCoE)

Lotic
ARQUITETURA DE SOLUÇÕES

GTER 41 | GTS 27
12 a 14 de maio de 2016, Uberlândia - UniAlgar

Design da rede física

- Desenhando a topologia física
  - Explore o stacking
  - Infra base sempre em pares
  - Explore o HA dos equipamentos
  - Níveis de HA versus Custo
  - CDA ou Spine-Leaf
  - Analise o Oversubscription

Design da rede física

- Definindo fabricantes e linhas de equipamentos
  - Fuja do *lock-in*
  - Escolha sempre baseado nos protocolos utilizados
  - Não confie nos números do Datasheet
  - Solicite prova de conceito
  - Analise o funcionamento do HA
  - Quantidade de portas, pense na expansão
  - Considere o nível do suporte
  - Estimule a concorrência

Lotic
ARQUITETURA DE SOLUÇÕES

GTER 41 | GTS 27
12 a 14 de maio de 2016, Uberlândia - UniAlgar

Testando, otimizando e documentando o seu projeto

- Testando a infraestrutura e aplicações
- Otimizando o Data Center
- Documentando do ambiente

Lotic
ARQUITETURA DE SOLUÇÕES

GTER 41 | GTS 27
12 a 14 de maio de 2016, Uberlândia - UniAlgar

Testando, otimizando e documentando o seu projeto

- Testando a infraestrutura e aplicações
  - Utilizando testes da indústria (Miercom, AppLabs, ICSA, etc)
  - Escrevendo o plano de testes
  - Definindo escopo, objetivos e critérios de aceitação
  - Determinando os tipos de testes
  - Testes automatizados e manuais
  - Implementando o plano de testes
  - Testando em produção a qualquer momento

Testando, otimizando e documentando o seu projeto

- Otimizando o Data Center
  - Otimizando a banda (Borda, LAN e WAN)
  - Reduzindo o Delay
  - Classificando as aplicações críticas
  - Camadas de proxy e cache
  - Balanceadores locais

Testando, otimizando e documentando o seu projeto

- Documentando
  - Toda a empresa deve conhecer o desenho lógico
  - Arquitetura de referência de infraestrutura
  - Arquitetura de referência para aplicações
  - Plano para atender RFPs internas
  - Conteúdo da documentação

Lotic
ARQUITETURA DE SOLUÇÕES

GTER 41 | GTS 27
12 a 14 de maio de 2016, Uberlândia - UniAlgar

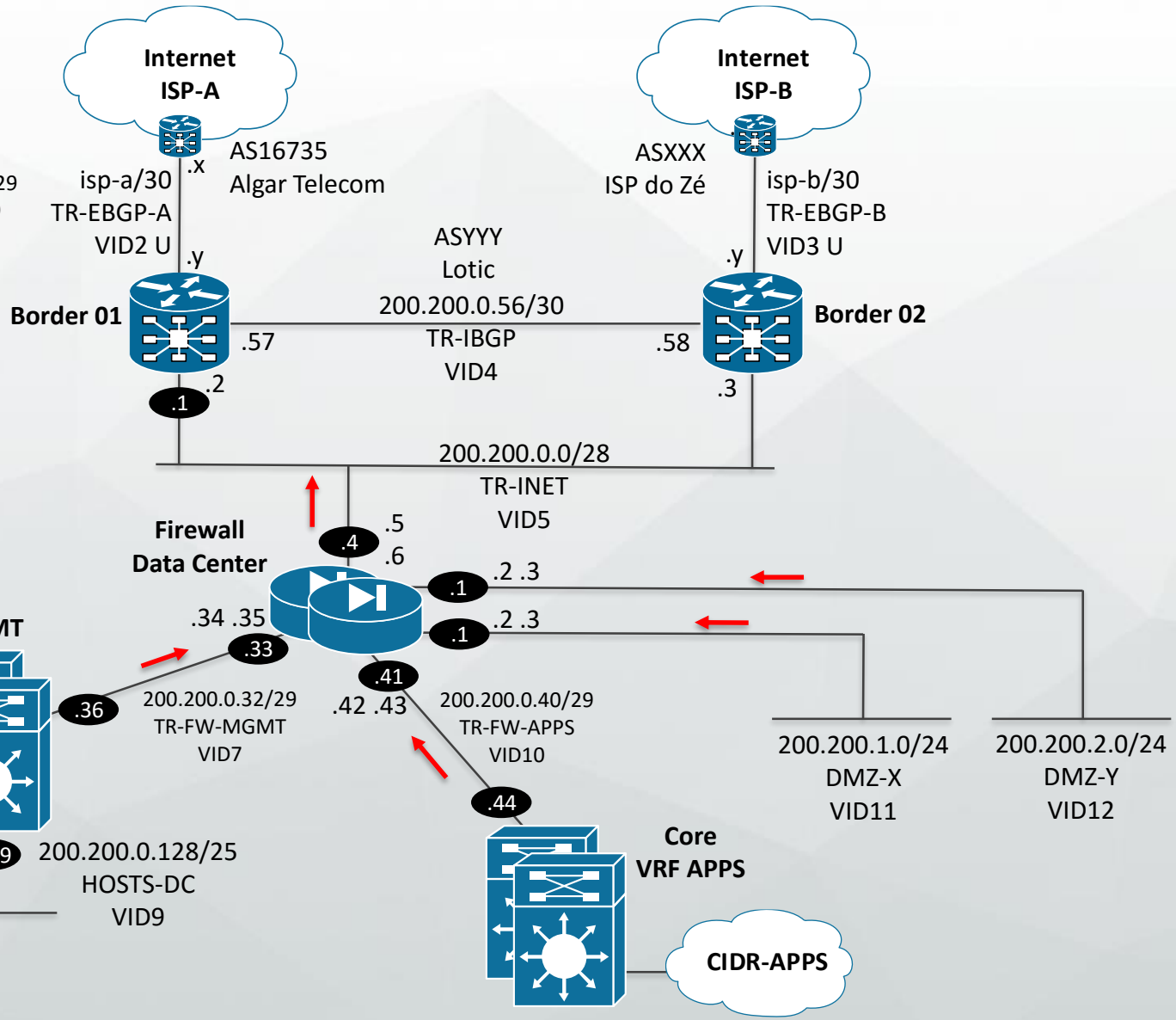
Montando uma topologia lógica e física

Topologia lógica

Super CIDR: 200.200.0.0/22

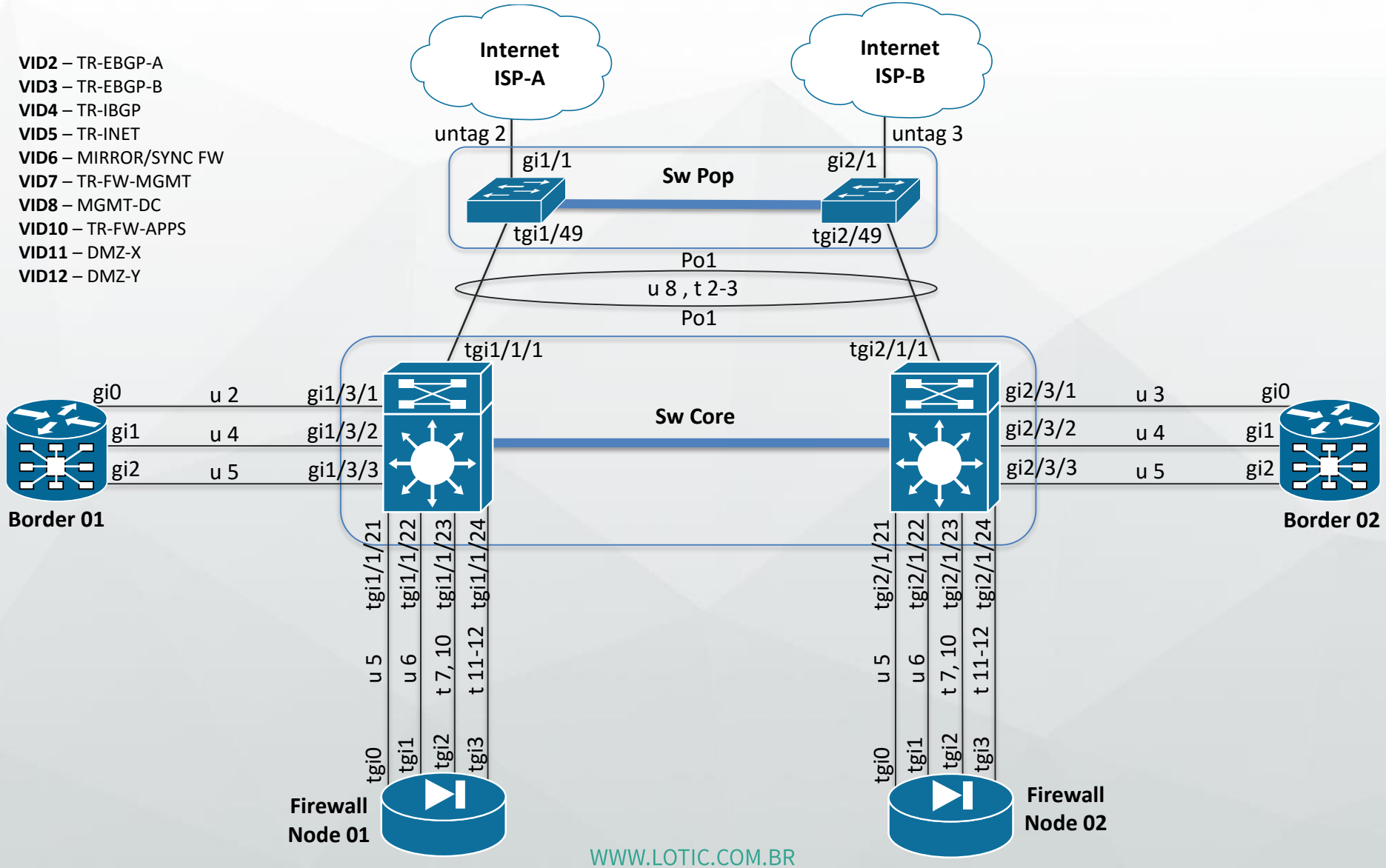
CIDR-TR-MGMT: 200.200.0.0/24
- **CIDR-TR:** 200.200.0.0/26
  - **TR-INET:** 200.200.0.0/28
  - **LIVRE:** 200.200.0.16/28
  - **TR-FW-MGMT:** 200.200.0.32/29
  - **TR-FW-APPS:** 200.200.0.40/29
  - **LIVRE:** 200.200.0.48/29
  - **TR-IBGP:** 200.200.0.56/30
  - **LIVRE :** 200.200.0.60/30
- **MGMT-DC**: 200.200.0.64/26
- **HOSTS-DC**: 200.200.0.128/25

CIDR-APPS: 200.200.1.0/24
DMZ-X: 200.200.2.0/24
DMZ-Y: 200.200.3.0/24



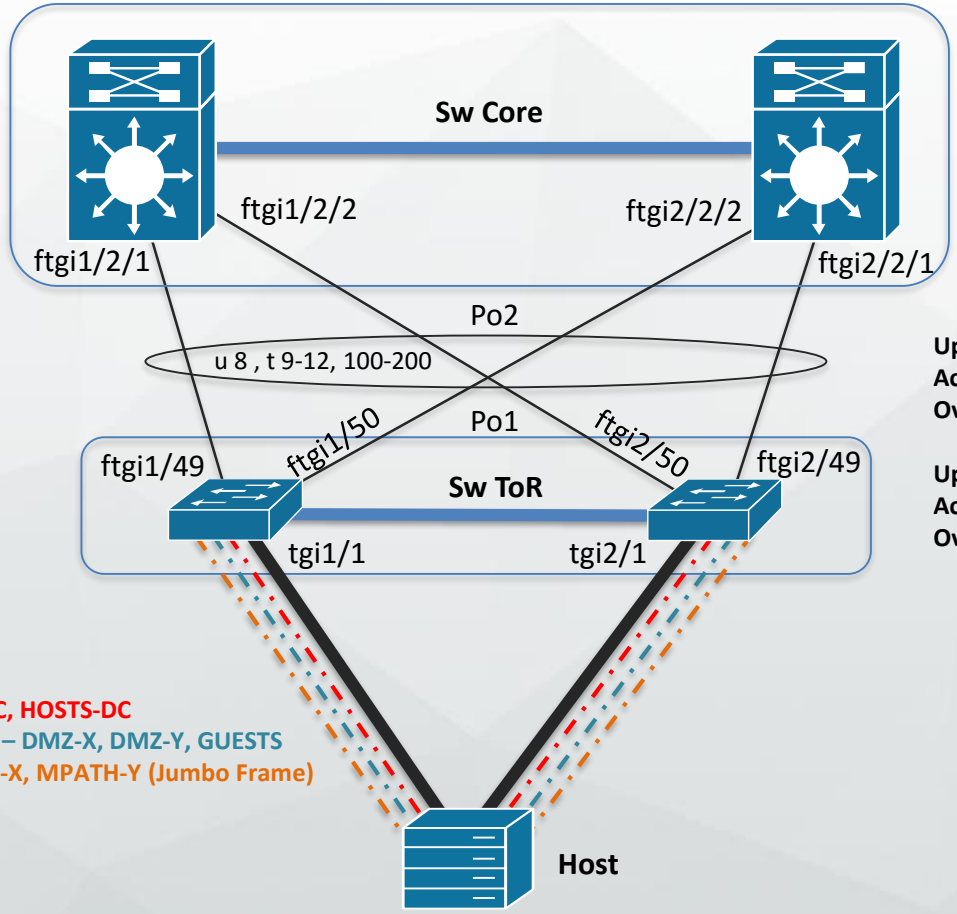
Topologia física

VID2 – TR-EBGP-A
VID3 – TR-EBGP-B
VID4 – TR-IBGP
VID5 – TR-INET
VID6 – MIRROR/SYNC FW
VID7 – TR-FW-MGMT
VID8 – MGMT-DC
VID10 – TR-FW-APPS
VID11 – DMZ-X
VID12 – DMZ-Y



Topologia física

VID2 – TR-EBGP-A
VID3 – TR-EBGP-B
VID4 – TR-IBGP
VID5 – TR-INET
VID6 – MIRROR/SYNC FW
VID7 – TR-FW-MGMT
VID8 – MGMT-DC
VID9 – HOSTS-DC
VID10 – TR-FW-APPS
VID11 – DMZ-X
VID12 – DMZ-Y
VID98 – ISCSI MPATH-X
VID99 – ISCSI MPATH-Y
VID100-200 – GUESTS



Uplink: 4x FortyGigabit = 160 Gpbs
Acesso: 64x TenGigabit = 640 Gbps
Oversubscription = 4,5:1

Uplink: 8x FortyGigabit = 320 Gpbs
Acesso: 64x TenGigabit = 640 Gbps
Oversubscription = 2:1

1+1 GB/VID8-9 – MGMT-DC, HOSTS-DC
4+4 GB/VID11-12, 100-200 – DMZ-X, DMZ-Y, GUESTS
5+5 GB/VID98-99 – MPATH-X, MPATH-Y (Jumbo Frame)

Lotic
ARQUITETURA DE SOLUÇÕES

GTER 41 | GTS 27
12 a 14 de maio de 2016, Uberlândia - UniAlgar

Obrigado!

Marcelo Veriato Lima

mlima@lotic.com.br

Skype: mlimadc


Lotic
ARQUITETURA DE SOLUÇÕES