
CLOUD
COMPUTING

# Texto base

# 4

# Virtualização de Serviços de rede (Networking) e SDN

Prof. Me. Rodolfo Riyoei Goya

***Resumo***

*Na "Computação em Nuvem", os componentes da infraestrutura de rede de Tecnologia da Informação (T.I.) também se tornam abstratos. Isto inclui conceitos de rede (como redes e endereçamento), dispositivos (como roteadores e firewalls) e serviços (como listas de acesso e tradução de nomes). Abordam-se aqui, como os conceitos listados são lidados.*

## 4.1. Introdução

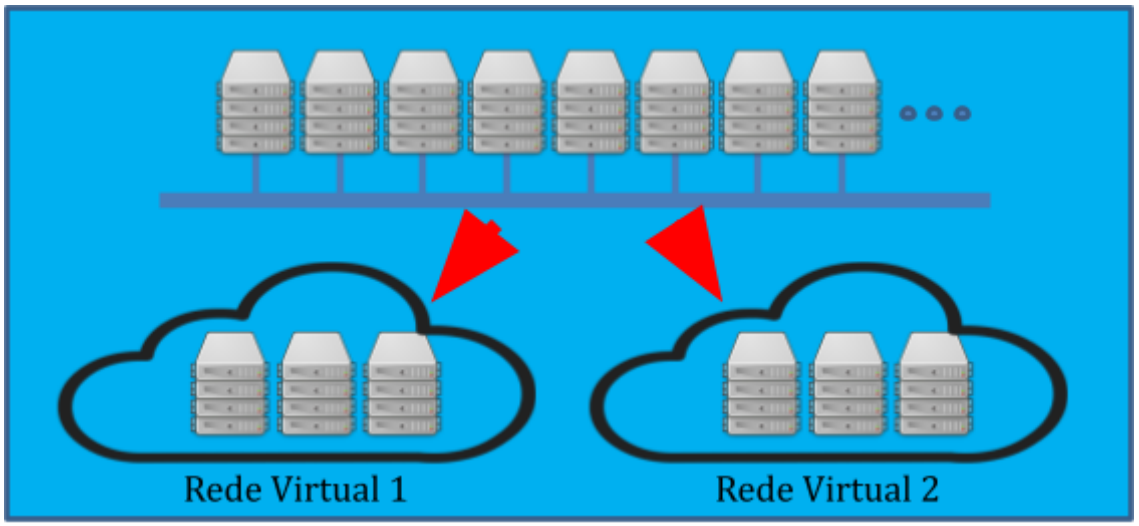
Como ficam as redes e endereços em "Computação em Nuvem"? Como tornar abstratos redes e endereços? "Computação em Nuvem" usa roteadores e switches virtuais? Como trocamos um cabo de um switch para outro para formar redes separadas dentro de uma nuvem? Na "Computação em Nuvem", a configuração de conexão de redes é virtual. Todos os equipamentos são pré-conectados e nenhuma conexão é movida para a formação de redes. Esta virtualização é conhecida como Software-Defined Networking (SDN – Redes Definidas por Software).

### 4.1.1. Redes

Em um ambiente de Datacenter com virtualização para Nuvem múltiplas máquinas com múltiplas CPUs com múltiplos núcleos são montadas em múltiplos racks formando um arranjo fortemente conectado e uniforme com dezenas de milhares de processadores interligados em uma rede única.

Quando se criam redes virtuais, criam-se "abstrações" que aparentam ser redes isoladas das demais. Isso é feito impedindo a comunicação para máquinas virtuais que pertençam a redes virtuais diferentes (permitindo apenas comunicação entre máquinas que pertençam à mesma rede virtual) sem que seja necessário alterar a posição de qualquer cabo de equipamento.

**Figura 1. Redes Virtuais em Ambiente de Nuvem**




**Fonte: do autor, 2022.**

Observe as redes virtuais indicadas na Figura 1. Elas são isoladas entre si apesar de serem interligadas fisicamente. A criação das redes é feita através de configuração (por software, sem que se mova um cabo sequer) e, por esta razão, este tipo de infraestrutura é denominado de "Rede Definida por Software" (Software-Defined Networking - SDN).

A criação de redes permite que provedores de serviços de nuvem isolem um cliente do outro e que clientes possam criar redes organizadas com funcionalidades e requisitos de segurança distintos para cada uma.

Este modelo de criação de rede permite enorme agilidade por permitir a criação de redes sem a necessidade de disponibilizar portas em switches e roteadores ou instalar cabos novos economizando tempo e dinheiro.

Diferentemente do que ocorre com servidores e equipamentos de armazenamento, nas SDNs não são criados switches ou roteadores virtuais configurados com interfaces semelhantes aos dos switches ou roteadores reais comercialmente existentes.

### 4.1.2. Endereçamento IP

Nas SDNs, são definidas faixas de endereços IP para cada rede de acordo com o desejo e necessidade do cliente. Deve-se tomar cuidado pois, uma vez criada, é problemático redimensionar as redes – um planejamento prévio é muito importante.

O endereço de uma rede (aqui trataremos apenas do IP versão 4) é definido na forma a.b.c.d/n (com "a", "b", "c" e "d" sendo números entre 0 e 255) onde a.b.c.d é o endereço de rede (que define o endereço IP inicial da rede) e o /n é a máscara CIDR de rede (que define o tamanho da rede).

É recomendado que o endereço de rede esteja em uma das faixas listadas na Tabela 1. Estes endereços são reservados para uso interno nas empresas e, por isso,

nenhum serviço público ou site de empresa usa estes endereços para serem acessados através da Internet.

**Tabela 1. Endereços IP reservados para redes privadas.**

| Rede | Endereço Inicial | Endereço Final |
|---|---|---|
| 10.0.0.0/8 | 10.0.0.0 | 10.255.255.255 |
| 172.16.0.0/12 | 172.16.0.0 | 172.31.255.255 |
| 192.168.0.0/16 | 192.168.0.0 | 192.168.255.255 |

**Fonte: do autor, 2022.**

Estes endereços são privados e virtuais. Por isso, empresas diferentes podem usar os mesmos endereços sem risco de interferência entre si. Mas deve-se escolher com cuidado os endereços para cada rede dentro de uma mesma empresa, uma vez que redes que apresentam sobreposição de endereços (o mesmo endereço IP podendo aparecer em mais de uma rede diferente) não podem comunicar entre si.

Para a máscara de rede, no IP versão 4, o valor de /n tem "n" variando de 0 a 32 especificando diferentes tamanhos de rede (32 é de tamanho 1 – a menor – e 0 é a maior, dobrando de tamanho para cada valor de "n"). A Tabela 2 mostra alguns tamanhos de rede para diferentes valores de "n" (para "n" abaixo de 15 pode-se extrapolar a tabela).

**Tabela 2. Tamanhos de rede para cada máscara de rede.**

| Máscara | Tamanho | Endereço rede |
|---|---|---|
| /32 | 1 | Múltiplo de 1.1.1.1 |
| /31 | 2 | Múltiplo de 1.1.1.2 |
| /30 | 4 | Múltiplo de 1.1.1.4 |
| /29 | 8 | Múltiplo de 1.1.1.8 |
| /28 | 16 | Múltiplo de 1.1.1.16 |
| /27 | 32 | Múltiplo de 1.1.1.32 |
| /26 | 64 | Múltiplo de 1.1.1.64 |
| /25 | 128 | Múltiplo de 1.1.1.128 |
| /24 | 256 | Múltiplo de 1.1.1.0 |
| /23 | 512 | Múltiplo de 1.1.2.0 |
| /22 | 1.044 | Múltiplo de 1.1.4.0 |
| /21 | 2.048 | Múltiplo de 1.1.8.0 |
| /20 | 4.096 | Múltiplo de 1.1.16.0 |
| /19 | 8.192 | Múltiplo de 1.1.32.0 |
| /18 | 16.384 | Múltiplo de 1.1.64.0 |
| /17 | 32.768 | Múltiplo de 1.1.128.0 |
| /16 | 65.536 | Múltiplo de 1.1.0.0 |
| /15 | 131.072 | Múltiplo de 1.2.0.0 |

**Fonte: do autor, 2022.**

Vamos supor, por exemplo, que se queira uma rede para 1.500 máquinas virtuais. Olhando a Tabela 2 dá para ver que a menor rede capaz de comportar tantos endereços é com máscara /21. Supondo que se queira escolher o endereço de rede na faixa entre 172.16.0.0 e 172.31.255.255 (segunda linha da Tabela 1) é preciso escolher um endereço de rede múltiplo de 1.1.8.0 (linha do /21 da Tabela 2), por exemplo 172.19.24.0 (172 é múltiplo de 1, 19 é múltiplo de 1, 24 é múltiplo de 8 e 0 é múltiplo de 0).

Máquinas virtuais criadas e instaladas dentro de uma dada rede virtual recebem automaticamente um endereço dentro da faixa configurada para esta rede. Este processo dispensa a necessidade de cuidar disso (como fazer alocação estática ou criar infraestrutura de servidores DHCP, por exemplo).

### 4.1.3. Subredes

Redes podem ser subdivididas em redes menores, denominadas subredes. A cada uma delas é atribuída uma faixa de endereços, não podendo haver sobreposição de endereços de uma subrede para outra.

A menos que haja alguma configuração adicional, instâncias só podem se comunicar entre si se estiverem na mesma subrede. Subredes distintas são domínios de colisão e broadcast distintos.

Apesar de subredes se assemelharem às VLANs ou a redes com broadcasts isolados por roteadores das redes convencionais, nenhuma dessas configurações é necessária, nem são implicitamente feitas (nas SDNs todas os servidores são interligados e as redes são formadas por filtragem de tráfego entre eles).

## 4.2. Roteamento

Para permitir e gerenciar a comunicação entre instâncias em redes diferentes, as SDNs permitem configurar roteamento entre redes e subredes. Para isso, são configuradas tabelas de roteamento.

### 4.2.1. Tabelas de Roteamento

Para configurar comunicação entre redes, em SDN se configura tabelas de roteamento. Em uma tabela de roteamento, as redes listadas nela podem se comunicar entre si. No exemplo da Figura 2, há quatro subredes e duas tabelas de roteamento.

**Figura 2. Subredes e Tabelas de Roteamento**

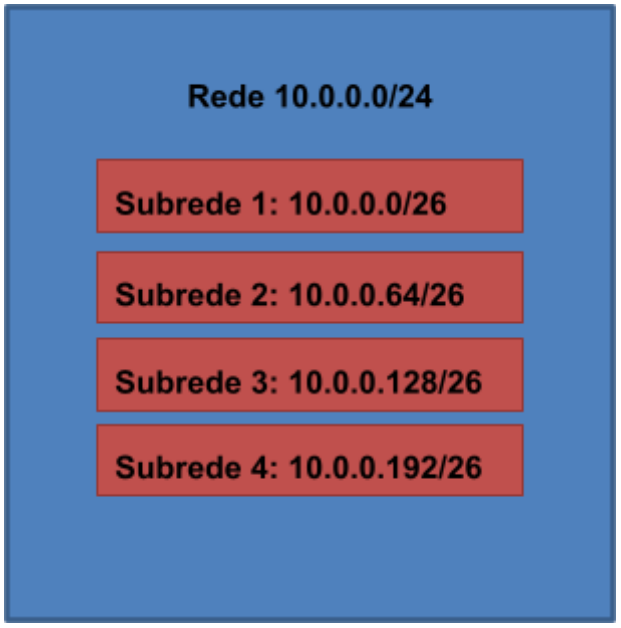



Tabela 1

| Rede | Destino |
|---|---|
| 10.0.0.64/26 | Local |
| 10.0.0.128/26 | Local |

Tabela 2

| Rede | Destino |
|---|---|
| 10.0.0.0/26 | Local |
| 10.0.0.192/26 | Local |
| 10.0.0.128/26 | Local |

**Fonte: do autor, 2022.**

A rede 10.0.0.0/24 (/24 tem 256 endereços: entre 10.0.0.0 e 10.0.0.255) está dividida em quatro subredes sem sobreposição:

**a.** 10.0.0.0/26 (/26 tem 64 endereços: entre 10.0.0.0 e 10.0.0.63)
**b.** 10.0.0.64/26 (/26 tem 64 endereços: entre 10.0.0.64 e 10.0.0.127)
**c.** 10.0.0.128/26 (/26 tem 64 endereços: entre 10.0.0.128 e 10.0.0.191)
**d.** 10.0.0.192/26 (/26 tem 64 endereços: entre 10.0.0.192 e 10.0.0.255)

A tabela de rotas 1 indica que uma instância na subrede 10.0.0.64/26 (por exemplo, uma instância com endereço 10.0.0.100) e uma instância na subrede 10.0.0.128/26 (por exemplo, uma instância com endereço 10.0.0.150) podem se comunicar.

A tabela de rotas 2 indica que instâncias nas subredes 10.0.0.0/26, 10.0.0.128/26 e 10.0.0.192/26 podem se comunicar.

Pela configuração feita, uma instância na subrede 10.0.0.64/26 não pode se comunicar com uma instância nas subredes 10.0.0.0/26 e 10.0.0.192/26 por não haver rotas para isso.

## 4.3. Firewalls e Listas de Acesso

Nas SDN, podem-se configurar conjuntos de regras controlando o tráfego de dados que fluem para as instâncias, subredes e redes. Estes tipos de conjuntos de regras correspondem a dois tipos de serviços de segurança de redes: Firewalls e Listas de acesso.

Cada regra de controle de tráfego é formada por:

a. Autorização: permitir ou negar
b. Protocolo de transporte (por exemplo: TCP, UDP ou ICMP)
c. Porta: (Serviço TCP/UDP ou tipo de ICMP)
d. Endereço de rede: especifica faixa de endereços da origem do tráfego

### 4.3.1. Firewall

Um conjunto de regras de firewall controla as conversações de uma instância.

Conversação é uma comunicação entre uma instância e outro equipamento. Ela é formada por mensagens enviadas da instância para o outro equipamento e por mensagens enviadas do outro equipamento para a instância.

O tipo da conversação da instância é definido por quem a iniciou, podendo ser dois tipos:

a. Entrada, conversação que foi iniciada pela instância.
b. Saída, conversação iniciada pelo outro equipamento com a instância.

Por default, para máxima segurança, todas as conversações de entrada para a instância são negadas e todas as conversações de saída para a instância são permitidas.

Cada regras do firewall especifica permissão para um dado protocolo, porta e endereço de rede de origem.

### 4.3.2. Listas de acesso

Listas de acesso controlam a passagem de tráfego de uma subrede (ou rede) para outra. Listas de acesso de entrada controlam o que entra na subrede e listas de acesso de saída controlam o que sai da subrede.

Cada lista de acesso (entrada ou saída) é formada por um conjunto de regras que permitem ou negam autorização para o tráfego. Estas regras são avaliadas na ordem em que foram definidas. Quando uma regra que se aplica ao tráfego é encontrada, a autorização especificada (permitir ou negar) é aplicada e o restante da lista é ignorado. Assim, a ordem das regras especifica a prioridade de cada regra.

Conversações entre instâncias que estão dentro de uma mesma subrede não estão sujeitas as regras da lista de acesso desta subrede porque o tráfego não está nem entrando nem saindo dela. Assim, mesmo que uma lista de acesso proíba determinado tipo de tráfego, é possível que uma instância use o tipo de tráfego proibido para se comunicar dentro da subrede.

### 4.3.3. Comparando firewalls e listas de acesso

Tanto nos firewalls como nas listas de acesso:

a. Regras incluem protocolo, porta e endereço de rede de origem.
b. A melhor política é autorizar apenas o que é estritamente necessário.
c. Tráfego de tipo não especificado por nenhuma regra é implicitamente negado.

De modo diferente dos firewalls, nas listas de acesso:

a. É irrelevante quem inicia a conversação.
b. Regras podem ser de permissão ou negação (Regras de firewall são sempre de permissão).
c. Regra são definidas com uma ordem de prioridade. Quando uma regra que se aplica a um tráfego é encontrado na lista ordenada, esta regra é usada e as regras seguintes são ignoradas (Nos firewalls não há ordem de prioridade para as regras - todas as regras são verificadas antes de se permitir ou negar um tráfego).
d. Não são tratadas mensagem trocadas dentro de uma subrede.

## 4.4. Serviços de Nomes

Cada interface de máquina ou equipamento em redes TCP/IP exige um endereço IP (como 179.191.78.194) como identificação. Isso não é conveniente para usuários humanos, que preferem nomes (como www.impacta.com.br) a endereços numéricos.

Para acomodar essa situação, foram criados serviços de rede para resolução de nomes. Ele recebe consultas com os nomes, necessários para usuários, os pesquisa em sua base de dados e responde com o endereço numérico IP correspondente a este nome, necessário para a interface correspondente ao nome possa ser alcançada. Além disso, esse serviço administra a quem pertence cada nome, impedindo que interfaces diferentes recebam o mesmo nome, permite organizar uma hierarquia de nomes e provê um banco

de dados distribuído para armazenar os dados sobre os nomes (o que dá escalabilidade para o serviço) e um serviço eficiente de cache que acelera a resposta das consultas. O serviço de nomes mais amplamente usado é o Domain Name System – DNS.

Este serviço é de tamanha importância que se tornou um componente essencial para qualquer infraestrutura de T.I. Sites e domínios de e-mails são o tipo de nomes mais comumente registrados. Os provedores de serviços de nuvem oferecem uma ampla base de serviço de nomes sem que o usuário tenha a necessidade de se criar servidores DNS.

Estes serviços incluem a possibilidade de registrar nomes públicos na Internet (lamento, mas se você quer registrar o nome APPLE.COM, sinto te dizer que este já tem dono). O nome do site que representará a próxima empresa trilhonária está aguardando para ser registrado!

## 4.5. Vamos praticar?

### 4.5.1. Serviços de Nomes

Há vários serviços comerciais que permitem cadastrar nomes na Internet. Navegue no links abaixo e veja o que é possível fazer nestas plataformas.

https://www.godaddy.com/pt-br

https://www.locaweb.com.br/registro-de-dominio/

https://uolhost.uol.com.br/registro-de-dominio.html

https://registro.br/

### 4.5.2. Quanto custa?

Quanta custa registrar um nome na Internet? Dá uma tentação de registrar um nome para si, não? Escolha um nome para seu domínio pessoal. Escolha um nome para sua futura empresa. Veja os sites de registro e verifique o quando custa.

## 4.6. Você quer ler?

Registrou seu nome e quer colocar um site estático na Internet? Veja mais detalhes no link:

<https://docs.aws.amazon.com/pt_br/AmazonS3/latest/userguide/WebsiteHosting.html>
.

## Referências

TAURION, Cezar. **Cloud Computing:** computação em nuvem: transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009.

VELTE, Anthony T.; VELTE, Toby J.; ELSENPRETER, Robert. **Cloud Computing:** a practical approach. EUA:McGraw-Hill, 2010.

MARSHALL, Nick; BROWN, Mike; BLAIR FRITZ, G.; JOHNSON, Ryan. **Mastering VMware vSphere 6.7.** New Jersey: Sybex, 2019. 848p.

SANTOS, Tiago. **Fundamentos da computação em nuvem** (Série Universitária). São Paulo, Editora Senac, 2018. 211p.

ANDREWS, Joshua; HALL, Jon. **VMware Certified Professional Data Center Virtualization on vSphere 6.7 Study Guide:** Exam 2V0-21.19. New Jersey: Sybex, 2020. 640p.

Official Amazon Web Services (AWS) Documentation. **Amazon Elastic Compute Cloud:** User Guide for Linux Instances. Amazon. 2.105p. Disponível em: <https://aws.amazon.com/documentation/ec2/>. Acesso em: 14 jan. 2022.