

Filipe Borba e Gabriel Moreira

## R1 - Bare Metal

### **Material**

#### **1) Como foi feito para identificar as NUCs corretamente sem um sistema operacional?**

Para identificá-las, foi necessário entrar na BIOS de cada NUC e verificar suas especificações de hardware, além do MAC address. Com as especificações em mãos, nomeamos cada NUC de acordo com o roteiro.

### **Rede**

#### **1) Quais IPs são fixos e quais são flutuantes? Qual a subrede?**

Os IPs fixos são do Roteador (192.168.0.1), do Switch (192.168.0.2) e de Broadcast (192.168.0.255). Os endereços entre 192.168.0.3 e 192.168.15.254 são flutuantes, dentro da subrede 192.168.0.0/20 de máscara 255.255.240.0.

#### **2) Existe um DHCP server na sua rede? Aonde?**

O DHCP server da nossa rede é o Switch, pois ele é o responsável pela atribuição de IPs na nossa rede.

#### **3) Existe um DNS server na sua rede? Aonde?**

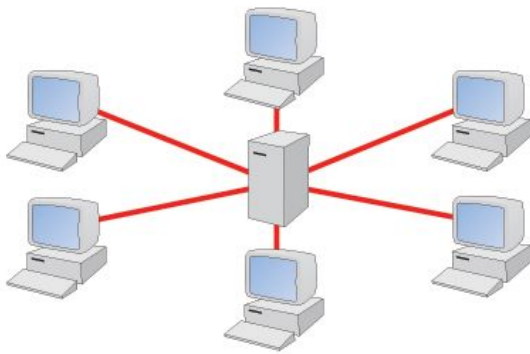
O DNS server não está presente na rede, pois utilizamos o DNS server do Google (8.8.8.8).

#### **4) Existe um gateway? Aonde?**

O gateway da nossa rede é o Roteador, pois é responsável por conectar os vários NUCs à rede do Insper.

#### **5) Qual a topologia da sua rede?**

A topologia da nossa rede é Estrela, visto que o nosso switch está conectando todas as NUCs.



## **Lapidando o projeto**

### **1. Quantos IPs utilizáveis estão disponíveis na subrede 192.168.0.0/20? Todos os IP são utilizáveis?**

Não são todos os IPs que são utilizáveis, pois alguns deles ficam estáticos e são essenciais, como o de Broadcast. Os endereços entre 192.168.0.3 e 192.168.15.254 estão disponíveis para uso, totalizando 4094 possíveis hosts.

### **2. Qual a diferença entre um IP público e um IP privado?**

Quando assinamos um provedor de internet, temos um IP público designado para nós. Este IP é visível para qualquer site ou aplicação e permite que você realize ações na rede. O IP público pode ser estático ou dinâmico e é designado por região (um IP do Brasil é diferente dos EUA, que é diferente da Espanha...). Já o IP privado é o IP interno ou local do seu dispositivo, ou seja, não é designado pelo provedor de internet. Ao invés disso, seu roteador designa um IP privado para cada dispositivo conectado à rede, assim, eles conseguem se comunicar na LAN.

### **3. Qual a classe utilizada na rede interna do Insper? E na sua rede? Quantas classes existem?**

A classe utilizada na rede do Insper provavelmente é a B, enquanto que na nossa é a C, dado o número de conexões necessárias. Existem 5 classes: A, B, C, D e E.

Class	Leading bits	Size of network number bit field	Size of rest bit field	Number of networks	Addresses per network	Total addresses in class	Start address	End address	Default subnet mask in dot-decimal notation	CIDR notation
Class A	0	8	24	128 ( $2^7$ )	16,777,216 ( $2^{24}$ )	2,147,483,648 ( $2^{31}$ )	0.0.0.0	127.0.0.0 <sup>[a]</sup>	255.0.0.0	/8
Class B	10	16	16	16,384 ( $2^{14}$ )	65,536 ( $2^{16}$ )	1,073,741,824 ( $2^{30}$ )	128.0.0.0	191.255.0.0	255.255.0.0	/16
Class C	110	24	8	2,097,152 ( $2^{21}$ )	256 ( $2^8$ )	536,870,912 ( $2^{29}$ )	192.0.0.0	223.255.255.0	255.255.255.0	/24
Class D (multicast)	1110	not defined	not defined	not defined	not defined	268,435,456 ( $2^{28}$ )	224.0.0.0	239.255.255.255	not defined	not defined
Class E (reserved)	1111	not defined	not defined	not defined	not defined	268,435,456 ( $2^{28}$ )	240.0.0.0	255.255.255.255	not defined	not defined

[https://en.wikipedia.org/wiki/Classful\\_network](https://en.wikipedia.org/wiki/Classful_network)

## **MaaS**

### **1. Descreva como foram evitados ou resolvidos os problemas de roteamento e resolução de nomes.**

Não tivemos que resolver nenhum problema para pingar as urls fornecidas, mas para evitá-los, tivemos de configurar o Gateway e o DNS da máquina. O Gateway fornecido foi o IP do roteador, que estava conectado à rede do Insper. Após a configuração do Gateway, utilizamos o DNS externo '8.8.8.8' para realizar a resolução de nomes.

## **Chaveando o DHCP**

### **1. Por que Desabilitar o do roteador?**

Desabilitamos o DHCP do roteador para não conflitar com o DHCP server do MaaS.

### **2. Como funciona o ataque DHCP rogue? Como evitar?**

Um servidor DHCP rogue é um servidor DHCP em uma rede que não está sob o controle administrativo do dono da rede. Geralmente é algum dispositivo como um modem ou roteador conectado na rede por um usuário sem intenção ou para realizar ataques de rede (como "man in the middle"). Quando um cliente conecta na rede, tanto o rogue DHCP quanto o servidor DHCP legal oferecem um IP, assim como o gateway padrão, DNS, etc. Se a informação que o rogue DHCP oferece difere da informação real, os clientes que aceitam os IPs podem sofrer problemas de acesso à rede, incluindo quedas de velocidade e falhas para se conectar a alguns hosts. O usuário dono do DHCP rogue pode até setar como default gateway um IP de uma máquina, permitindo que possa monitorar todo o tráfego de informações (man in the middle). O resultado final disso pode ser que uma grande parte da rede não esteja conectada à internet e uma parte do domínio sem acesso algum.

Para evitar este ataque, deve-se utilizar sistemas de detecção de intrusos com assinaturas apropriadas ou pelo chamado “DHCP snooping”, que basicamente é ignorar mensagens de DHCP servers que não são confiados ou assinados.

## **Comissioning Nodes**

### **1. Descreva o processo PXE Boot? Qual a sua grande vantagem em um datacenter real?**

O PXE Boot é uma opção de boot que acontece via rede, administrado pelo client. Normalmente o boot pode ser feito de acordo com o IPv4 e IPv6. No caso do roteiro, o boot foi feito por IPv4 e o client é a NUC na qual está instalada o MAAS.

Tal boot pode ser útil pensando em um data center com milhares de máquinas. Em uma situação como essa, seria muito trabalhoso bootar todas as máquinas uma por uma a partir de um pen drive, por isso a opção de apenas uma máquina orquestrar o boot de todas as outras é uma vantagem.

### **2. Analisando em um aspecto mais amplo, quais outras funcionalidades do MaaS pode ser útil no gerenciamento de bare metal?**

O MaaS oferece uma dashboard para gerenciar o bare metal, assim, é possível monitorar e controlar cada máquina de maneira remota e simples. O Node Comissioning permite que a instalação de novas máquinas seja muito mais tranquila, visto que o MaaS realiza alguns testes antes de deixá-la como Ready. Ainda, o MaaS pode permitir que um usuário trabalhe com máquinas que já estejam com status Ready, assim como fazer o release dela quando o usuário tiver terminado seu trabalho.

## **Finalizando a rede para acesso “externo”**

### **1. Qual o nome e como funciona a ferramenta utilizada?**

A ferramenta utilizada para finalizar a rede para acesso “externo” se chama Redirecionamento de Portas. Essa ferramenta permite redirecionar uma porta da rede para outro nó da rede, possibilitando que um usuário alcance um IP privado dentro da rede mesmo estando fora dela. Assim, é possível disponibilizar publicamente serviços internos, sem abrir mão da segurança de portas fechadas.

### **2. O que deveria ser feito para você conseguir acessar o Maas da sua casa?**

Para acessar o Maas de casa, deve ser feito um redirecionamento de portas na rede do Inspér, como foi feito com o roteador. Feito isso, quando acessarmos uma porta específica

da rede do Insper, o endereço será redirecionado para a porta 22 do roteador, que por sua vez será redirecionado para a porta 22 da máquina do MAAS por exemplo.

## **Questões Complementares**

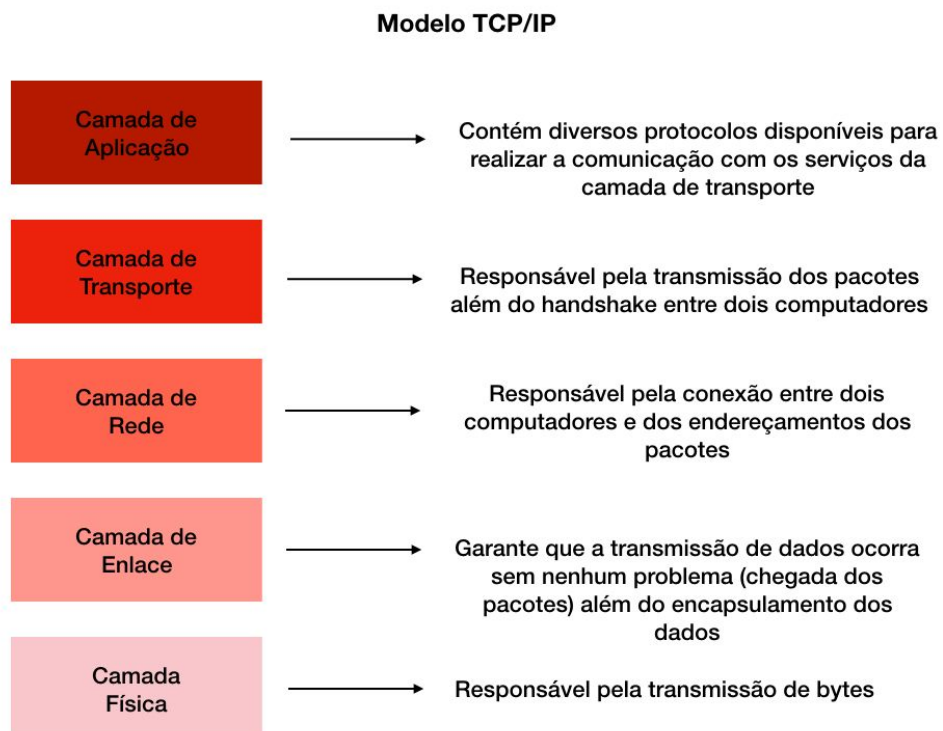
### **1. O que significa LTS? Por que isso importa para uma empresa?**

LTS (Long Term Support) é um tipo de versionamento de software (normalmente software livre) que indica que o software terá suporte por um período maior de tempo. Isso é bom para a empresa porque o software irá continuar sendo atualizado por mais tempo que o normal, além de mobilizar grande parte da comunidade para achar erros e vulnerabilidades, contribuindo para novos patches.

### **2. O que é IPv6? Qual a importância da migração?**

IPv6 é uma nova versão do IP (Internet Protocol) que define os endereços virtuais de cada máquina conectada na rede. A migração do IPv4 para o IPv6 é de grande importância uma vez que o número de dispositivos conectados à rede é maior que a quantidade de endereços que o protocolo suporta, o que pode causar problema na identificação do usuário e problemas de rotas para transferência de pacotes.

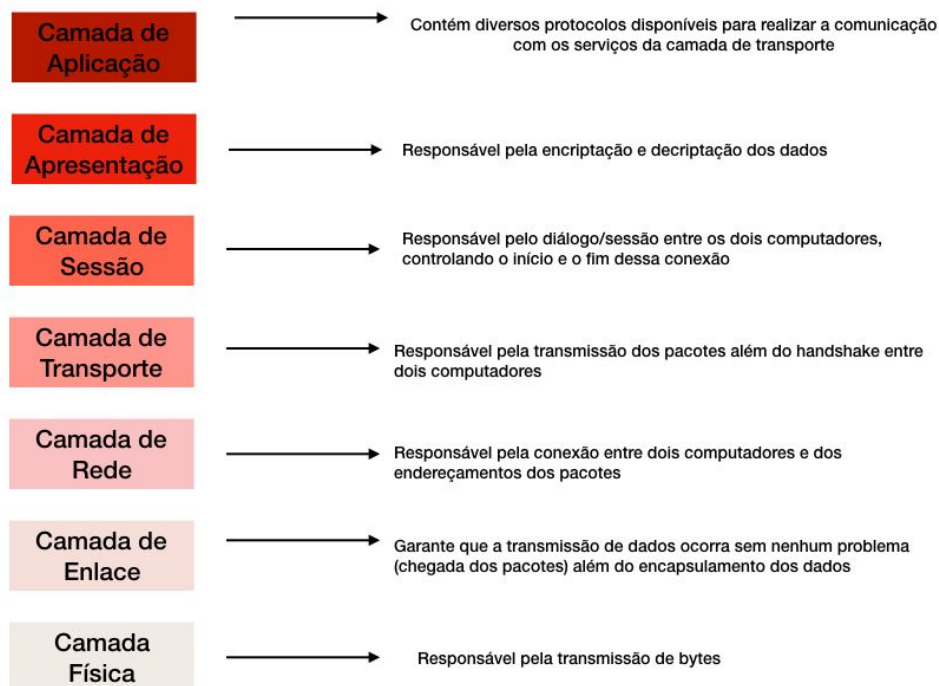
### **3. A literatura preconiza que o Modelo de Rede Internet possui 5 camadas, quais são elas e quais camadas foram envolvidas neste capítulo?**



Neste capítulo foram envolvidas as camadas de aplicação (IP, DHCP), rede (DNS, gateway), e física (NICs, roteador, switch, cabos de rede).

**4. A literatura mais antiga discorre sobre o Modelo de Rede OSI de 7 camadas. Explique a diferença entre os dois modelos.**

### Modelo OSI



A diferença mais visível é o número de camadas, o modelo TCP/IP junta a camada de Aplicação, de Apresentação e de Sessão em uma só, chamada de Aplicação. Isto se dá porque a definição do modelo OSI veio antes mesmo da invenção dos protocolos que ele se refere, por isso existem mais camadas do que protocolos. Já o modelo TCP/IP veio depois da existência dos protocolos, por isso a relação entre o número de camadas e protocolos é a mesma.

## Concluindo

### 1. O que é e para que serve um gerenciador de Bare Metal?

Um gerenciador de Bare Metal é uma máquina física com um software como o MaaS instalado que gerencia as outras máquinas de um rack. Ele pode fazer deploys de maneira

segura, monitorar as máquinas, teste de hardware, DevOps, permitir acesso de usuários externos, entre outras funcionalidades que são utilizadas num serviço de Cloud.

## **2. O que é um MAC address?**

Um endereço MAC (Media Access Control) é um endereço físico que identifica a interface de rede (geralmente uma placa de rede) de um dispositivo conectado à rede. É um endereço de deveriam ser únicos, mas acabam sendo reutilizados pelos fabricantes. Além disso, o MAC Address possui informações do fabricante em parte do seu código.

## **3. O que é um IP address? Como ele difere do MAC address?**

Um IP Address é um endereço virtual utilizado na internet ou numa rede local para identificar uma máquina e endereçar os conteúdos a serem enviados e recebidos. O IP difere do MAC principalmente por ser virtual, variável e único para cada dispositivo dentro de uma rede, enquanto que o MAC é físico, fixo e pode estar presente em mais de um dispositivo.

## **4. O que é CIDR? Qual o papel da subrede?**

CIDR (Classless Inter Domain Routing) é uma subrede que possui uma máscara que não é característica de nenhuma classe (A, B C ou D) como 255.255.240.0 por exemplo.

O papel da subrede é dividir um IP em segmentos de redes com o intuito de indentificar mais dispositivos e possibilitar a conexão internet sobre o mesmo endereço de IP.

## **5. O que é são DHCP, DNS e gateway?**

DHCP: significa Dynamic Host Configuration Protocol e trata-se de um protocolo responsável por distribuir IPs automaticamente à diferentes computadores da rede.

DNS: significa Domain Name System e são servidores responsáveis em transformar o endereço dos sites como "[www.google.com](http://www.google.com)" em seus respectivos endereços IPs (74.126.224.72).

Gateway: é um nó numa rede de computadores por onde passam dados para e de outras redes. Por causa do gateway é que conseguimos enviar e receber os dados, porque ele é

responsável por conduzir esses dados. Geralmente, um gateway é um modem ou roteador numa rede de computadores.

**Conclusão: Descreva como o MaaS poderia ser utilizado em um datacenter real (com muitos servidores) e como seria um processo alternativo sem essa ferramenta. Ainda, é possível e SIMPLES realizar a implantação de uma aplicação usando o MaaS?**

Num datacenter real, o MaaS funcionaria como um 'orchestrator', ou seja, um gerenciador das máquinas presentes na rede. A máquina com o MaaS instalado seria o centro de todo o datacenter, convergindo todo o processo de deployments, monitoramento, etc. para essa máquina, facilitando o trabalho do responsável pelo datacenter.

Configurar um datacenter real, com muitos servidores sem a utilização da ferramenta MaaS seria muito trabalhoso, pois o MaaS já configura diversos serviços essenciais (DNS server, NTP server, PXE, etc.) de maneira automática, permitindo, ainda, a utilização de uma interface web. Sem o MaaS, todos esses serviços essenciais teriam de ser construídos e configurados manualmente.

Ainda, sim, é possível realizar a implantação de aplicações usando o MaaS, mas não seria simples; por causa disso, usamos o Juju para gerenciar o deploy de aplicações.