Cloud Computing - Roteiro 1

## **Questões 1**

1. Qual a topologia da sua rede? Quais outras topologias existem?

Nossa rede possui a topologia de estrela, em que todos os servidores estão conectados a um *switch* central. Esta topologia traz como benefícios:

* simplificar a remoção e adição de novos servidores na rede, sem afetar o funcionamento dos outros servidores;
* em caso de falha em algum servidor, a rede pode continuar operando, desde que o *switch* central permaneça ativo;
* aumentar a segurança da rede, já que a única forma de interceptar qualquer tráfego dentro da rede seria através da invasão do *switch* central;
* facilitar o controle de tráfego, uma vez que todas as informações podem ser rapidamente acessadas simplesmente monitorando o fluxo no *switch* central.

Além dela, existem mais 6 topologias: barramento, anel, malha, árvore, daisy-chain e híbrida (que combina várias dessas topologias). Houveram inconsistências sobre *fully-connected* e ponto a ponto serem ou não topologias de rede, com alguns sites mencionando ou não elas como topologias. No meu ponto de vista (e de minha dupla), *fully-connected* é topologia de rede, pois denota quando uma conexão é total, de todos os dispositivos para todos os dispositivos. Contudo, não consideramos ponto a ponto, já que ela é simplesmente uma forma de conexão de entre dois dispositivos, tão trivial que literalmente faz parte de todas as outras topologias.

1. Quais as consequências de utilizar um DNS externo (Por exemplo: 8.8.8.8) em uma rede privada?

O uso de um DNS externo em uma rede privada pode ser uma solução rápida e conveniente para uma empresa visando implementar esse serviço o mais rápido e simples quanto possível. Isso se dá porque o próprio provedor do DNS será responsável por garantir a redundância do sistema, com servidores reserva, mantendo a lista de domínios públicos atualizada, resolvendo nomes de domínios que talvez não seriam previstos caso o servidor fosse confeccionado internamente, e por poder suportar uma maior quantidade de requisições, caso haja uma necessidade de fluxo variável.

Contudo, utilizar um servidor DNS externo pode dificultar a aplicação de políticas de filtragem de conteúdo, especialmente as mais específicas, bem como violar políticas de uso de rede, principalmente em ambientes corporativos, que precisam zelar pela segurança e conformidade da rede. Além disso, por não se ter acesso completo ao servidor DNS, o monitoramento e a capacidade de se gerar relatórios de tráfego pode acabar sendo limitada.

Por fim, utilizar um servidor DNS externo também pode colocar em risco a privacidade e o acesso às informações que são trafegadas, fora da empresa, principalmente se os conteúdos são potencialmente sensíveis.

1. O Switch estava originalmente em qual rede? Quantos IPs tem essa rede?

O switch estava originalmente configurado na rede classe A 10.90.90.90/8, que possui uma quantidade total de 16.777.216 IPs disponíveis, sendo 2 deles não utilizáveis, por serem endereços de rede (10.0.0.0) e de *broadcast* (10.255.255.255). Esta quantidade de IPs foi calculada através da fórmula , sendo correspondente à máscara de sub-rede (que neste caso é 8).

1. Quando acessou o roteador pela primeira vez, ele estava na Classe C. Quantas classes existem e qual é a classe da rede do main?

Existem 5 classes de redes privadas, nomeadas de A a E. A classe A (faixa de IP entre 1.0.0.0 até 126.0.0.0) reserva o primeiro octeto para identificar a rede e os outros 3 para endereçar os dispositivos.

A classe C (faixa de 192.0.0.0 a 223.0.0.0), em que estava o dispositivo durante o 1º acesso, possui 3 octetos para identificação e apenas 1 para endereçamento, uma escolha ideal para redes pequenas.

A classe da rede do main (172.16.0.0/20) não existe, pois a rede do main é descrita como **classless** no inventário. Por outro lado, poderia ser classe do tipo B, se a convenção de classes fosse adotada, já que está no range de classe B. Mas ambas as respostas estão corretas, dada sua respectiva convenção. Não há resposta correta, mas sim pontos de vista sobre esse caso.

## **Questões 2**

1. Quantos IPs utilizáveis estão disponíveis na subrede 10.12.0.0/15? Todos os IP são utilizáveis?

Para calcular a quantidade de domínios disponíveis, utilizamos a fórmula , sendo correspondente à máscara de sub-rede (que neste caso é 15), e menos 2 porque excluímos os endereços 10.12.0.0 (rede) e 10.13.255.255 (broadcast), já que eles não estão disponíveis para uso na sub-rede. Com isso, temos 131.072 IPs disponíveis e 131.070 IPs utilizáveis na sub-rede 10.12.0.0/15.

1. Qual a diferença entre um IP público e um IP privado?

A principal diferença entre IP público e privado é o contexto em que são utilizados, já que o público é acessível a partir de qualquer dispositivo na internet (desde de que atenda às regras de *firewall* e configurações de rede), enquanto o IP privado requer o acesso através de um dispositivo de rede (como roteador) conectado diretamente na rede privada, realizando a tradução dos endereços através da regra NAT daquela rede.

Além disso, os IPs públicos são únicos na internet, enquanto várias redes privadas podem utilizar os mesmos endereços de IP privados, desde que elas estejam isoladas uma da outra. Também vale ressaltar que as redes 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 e 100.64.0.0/10 são reservadas. Esses endereços são destinados ao uso em redes privadas e a alocação de tais endereços não é controlada globalmente por ninguém.

1. Qual a classe utilizada na rede interna do Insper? E na sua rede?

A rede interna do Insper (main) está no endereço de IP 10.102.0.X (conforme informado no "H1 - Diagrama" do roteiro 1), o qual pertence à classe A.

A rede Wi-Fi para os alunos tem endereço de IP 10.102.15.226 (conforme verificado nas configurações de rede de nosso computador durante conexão com o Wi-Fi), o qual pertence à classe A.

A rede utilizada por mim, na aplicação, tem endereço de IP 10.103.0.27, que está na rede 10.103.0.0/20, diferente da rede interna do Insper, 10.102.0.0/20. A conexão entre ambos só é possível a partir de uma regra NAT criada pelos desenvolvedores da matéria, que permitem o acesso ao kit por qualquer wifi do Insper.

## **Questões 3**

1. Por que desabilitar o DHCP do roteador?

Se não desabilitarmos o DHCP do roteador, ele entrará em conflito com o DHCP da sub-rede, gerenciado pelo MaaS, já que dois serviços de DHCP não podem gerenciar a mesma rede. Assim, através do *MaaS* *controller* configuramos o range de IPs entre 172.16.11.1 e 172.16.14.255.

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

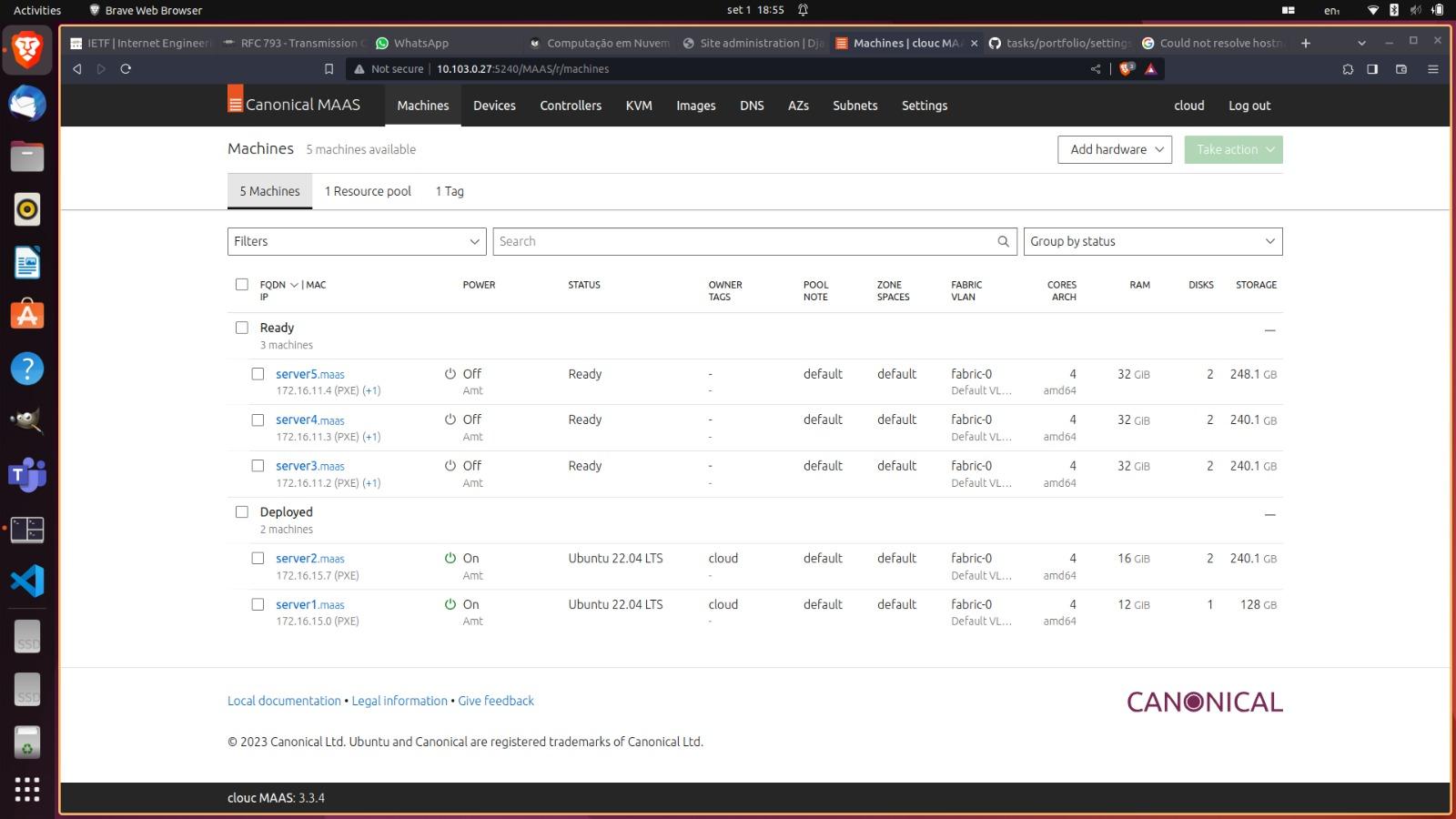
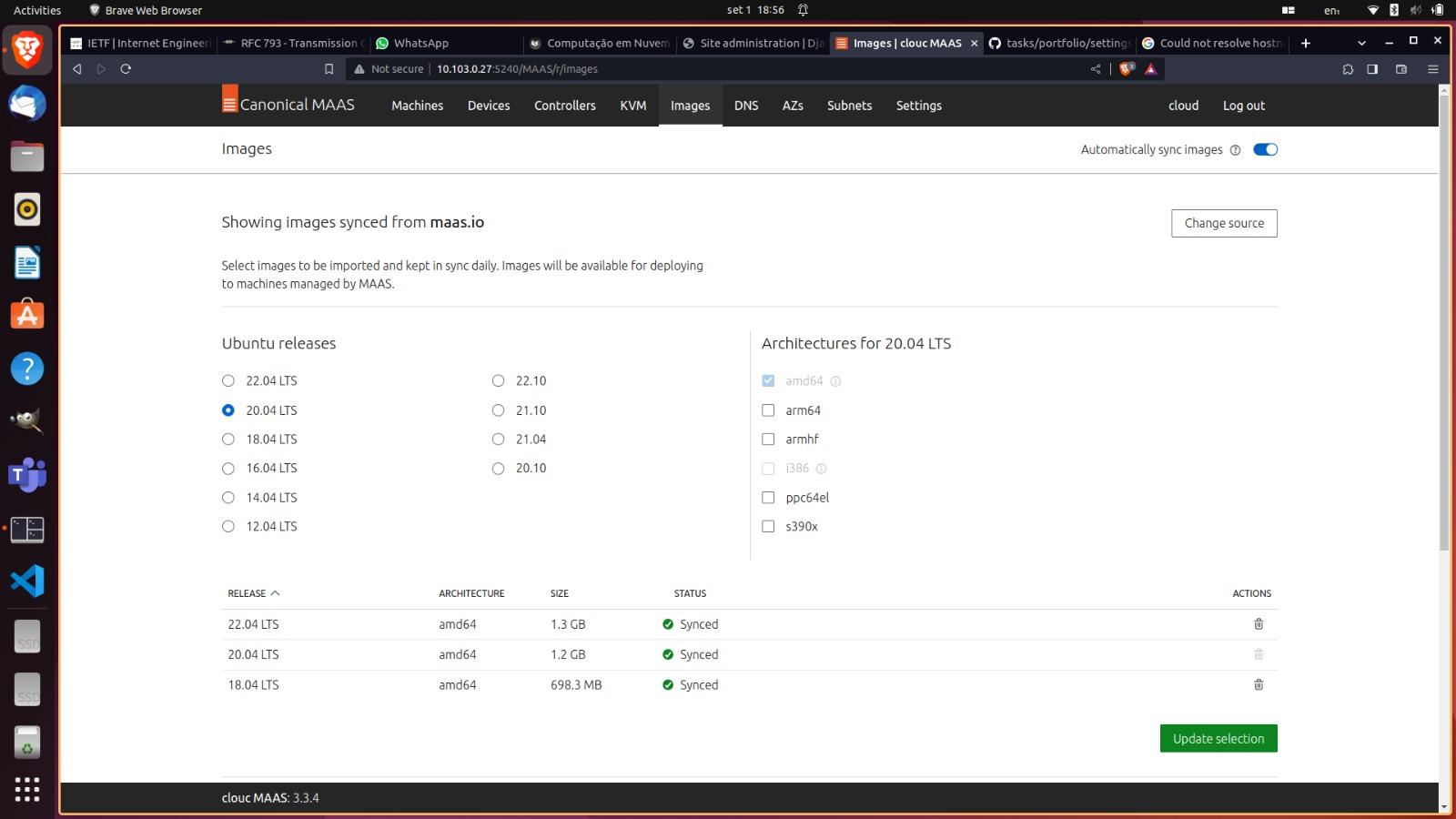
O processo de inicialização PXE (Preboot Execution Environment) é um protocolo que possibilita que os computadores em uma rede sejam inicializados a partir de um servidor remoto. Após a devida configuração dos computadores-alvo, a imagem de inicialização pode ser carregada tanto remotamente quanto localmente, utilizando os recursos disponibilizados pelo PXE em seus clientes habilitados.

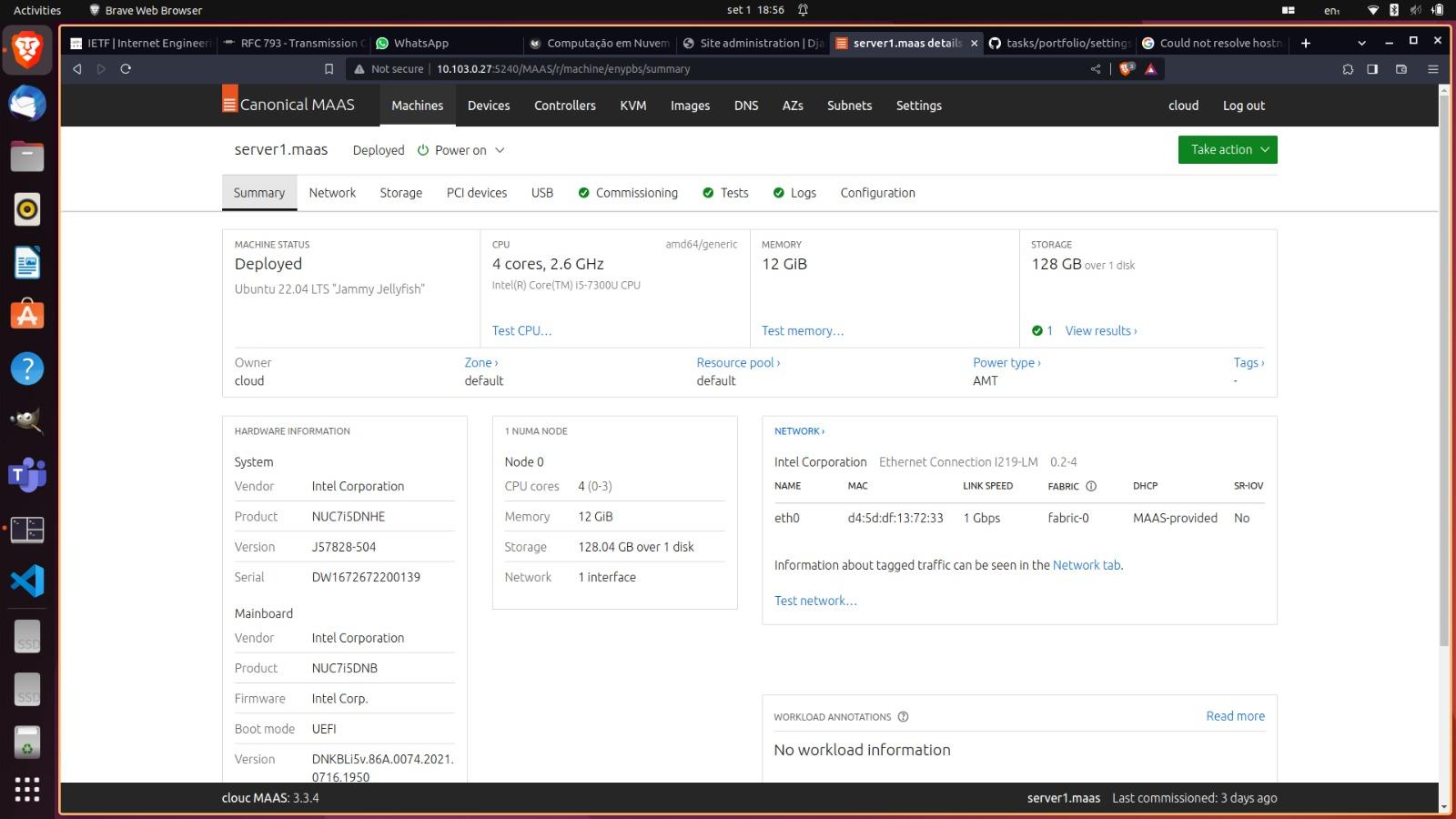
A grande vantagem desse processo em um datacenter real é a automação e eficiência que proporciona. Em uma rede de uma grande empresa, se a inicialização fosse feita manualmente, seria necessário usar um dispositivo de armazenamento em cada máquina e contar com um funcionário para realizar o procedimento de inicialização em cada uma. Usando o PXE, todo o processo é automatizado, reduzindo significativamente a margem de erro humano, envolvendo menos pessoas e centralizando o gerenciamento em um único local. Isso resulta em economia de tempo e recursos, tornando a implantação e manutenção de sistemas operacionais muito mais ágil e eficiente.

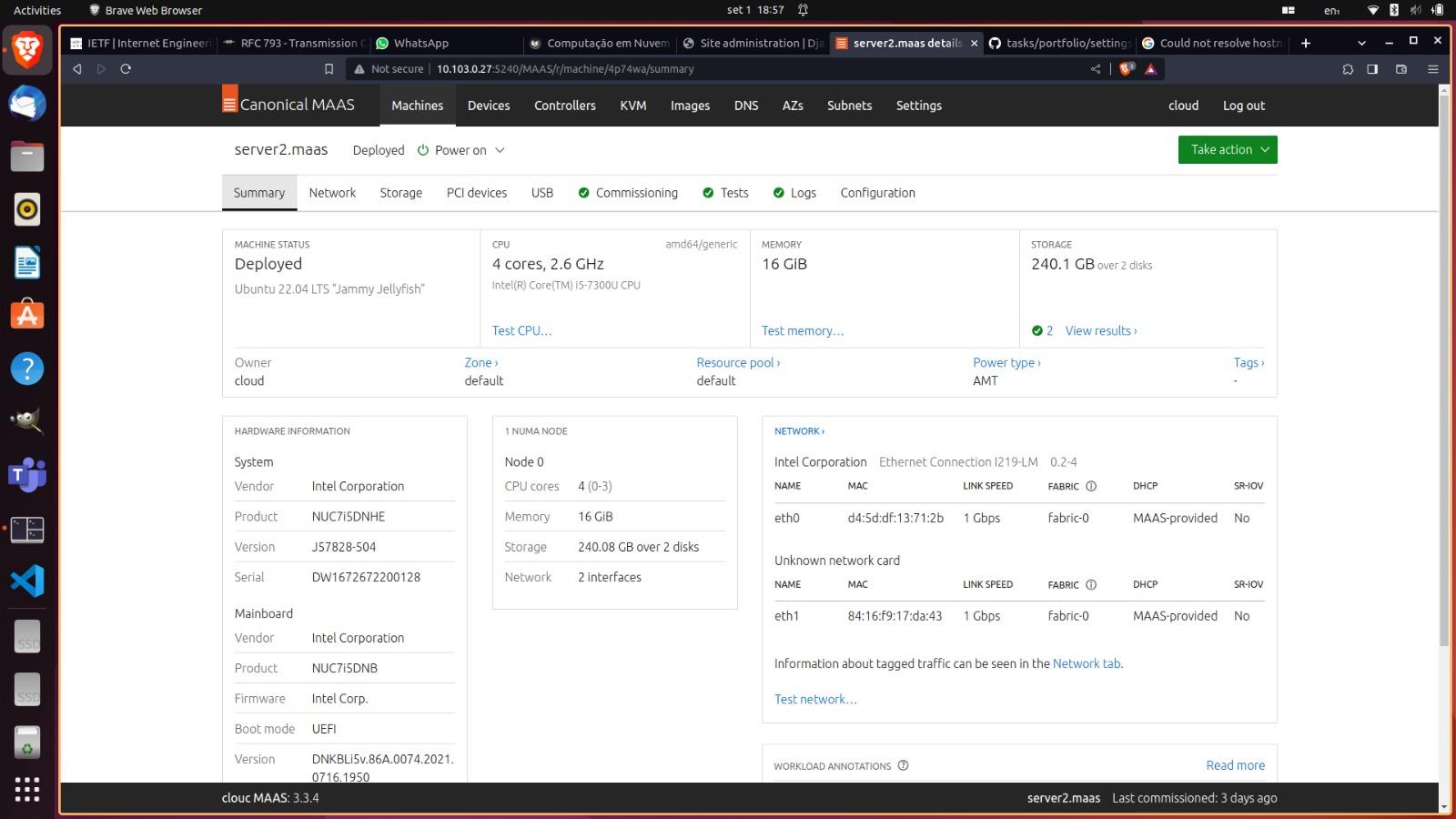
1. Analisando em um aspecto mais amplo, quais outras funcionalidades do MaaS podem ser úteis no gerenciamento de bare metal?

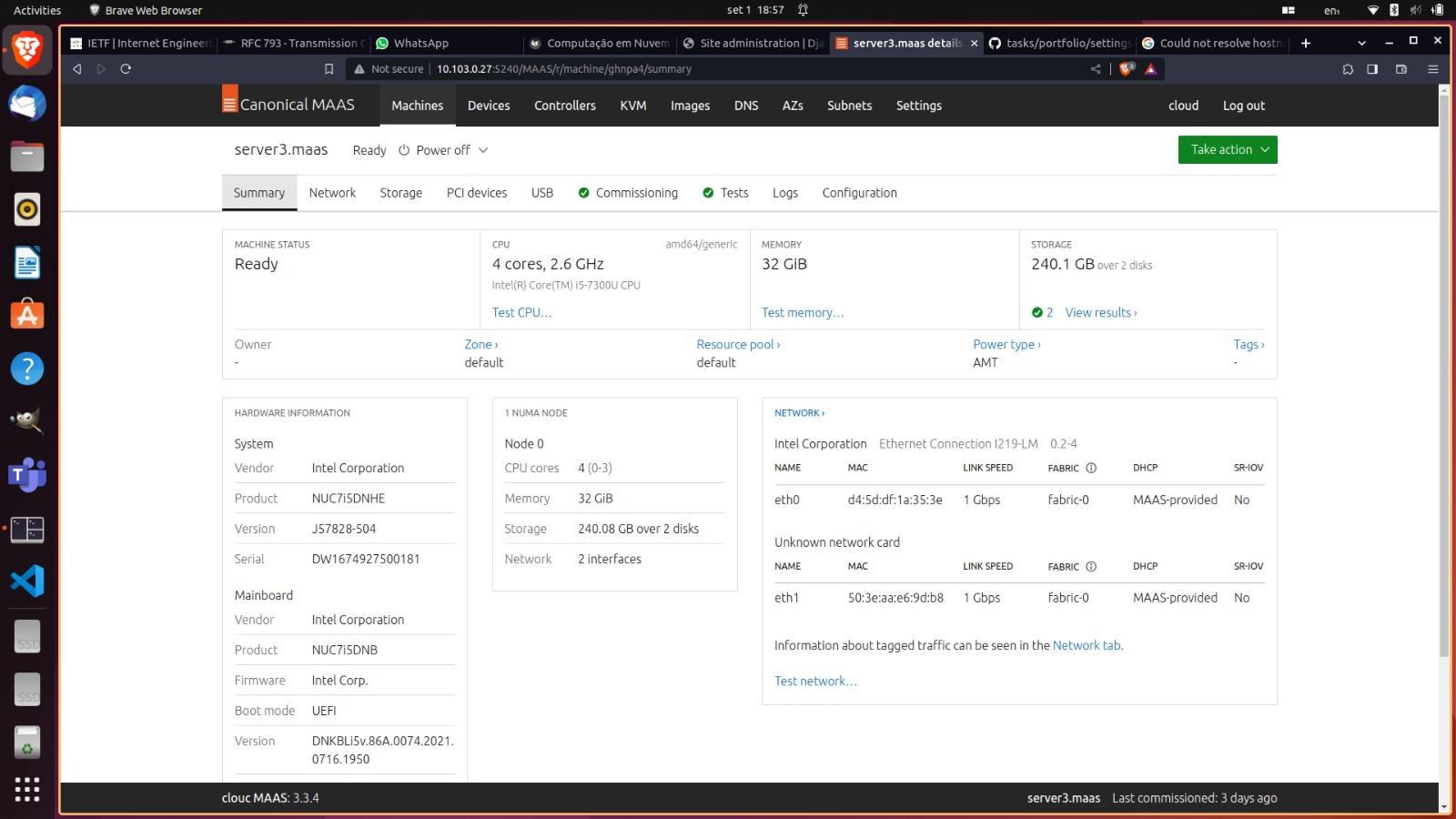
* Automação:
  + Descoberta Automática de Dispositivos: Encontra todos os dispositivos na rede automaticamente, facilitando a identificação de servidores.
  + Operações Remotas com BMC: Permite gerenciar servidores remotamente, mesmo quando estão desligados.
  + APIs para Diversas Tarefas: Facilita a automação de tarefas como configuração de servidores e provisionamento.
* Velocidade:
  + Implantação sem Intervenção: Instala sistemas operacionais automaticamente, economizando tempo.
  + Tempo de Implantação Rápido: Reduz o tempo de instalação para cerca de dois ciclos de inicialização mais dois minutos para a imagem do disco.
* Inventário:
  + Descoberta de Dispositivos: Identifica todos os dispositivos em servidores para um gerenciamento mais eficaz.
  + Inventário Detalhado de Discos: Registra informações sobre discos, facilitando a manutenção.
* Layouts de Armazenamento:
  + Configuração Avançada de Armazenamento: Permite criar configurações de armazenamento personalizadas, como RAID, LVM e ZFS.
  + Automação de Armazenamento: Automatiza a configuração de armazenamento por meio de APIs.
* IPAM, DHCP, DNS:
  + Configuração de Rede Simplificada: Facilita a configuração de redes em servidores com pontes, VLANs e outros recursos.
  + Integração com Serviços de Rede: Integra servidores com serviços de DNS e DHCP de código aberto.
* Teste de Hardware:
  + Verificação de Saúde do Hardware: Avalia o estado de hardware, como discos, memória e CPU, para evitar falhas imprevistas.
* DevOps em Bare Metal:
  + Integração com Ferramentas de Automação: Trabalha em conjunto com ferramentas populares, como Ansible, Chef, Puppet, SALT e Juju, para automatizar tarefas de gerenciamento.
  + APIs e CLI para Automação: Fornece interfaces de programação e linha de comando para automatizar tarefas.
* Monitoramento de Rede:
  + Monitoramento Contínuo: Acompanha o tráfego de rede e identifica dispositivos não autorizados ou desconhecidos.
  + Varredura de Faixas de Rede: Realiza varreduras de endereços de rede para detecção proativa.
* Autenticação e Identidade:
  + Gerenciamento Centralizado de Identidade: Integra-se com sistemas de gerenciamento de identidade como LDAP, Active Directory e SAML.
* Sistemas Componíveis:
  + Compatibilidade com Diversas Plataformas: Oferece suporte para diferentes tipos de hardware, como Cisco UCS, Intel RSD e HP Moonshot.
* Metadados de Nuvem:
  + Reutilização de Operações de Nuvem: Facilita a migração de cargas de trabalho entre servidores físicos e ambientes de nuvem.
* KVM Micro-Cloud:
  + Alocação de Máquinas Virtuais: Permite a criação de máquinas virtuais KVM em servidores físicos para melhor aproveitamento dos recursos.

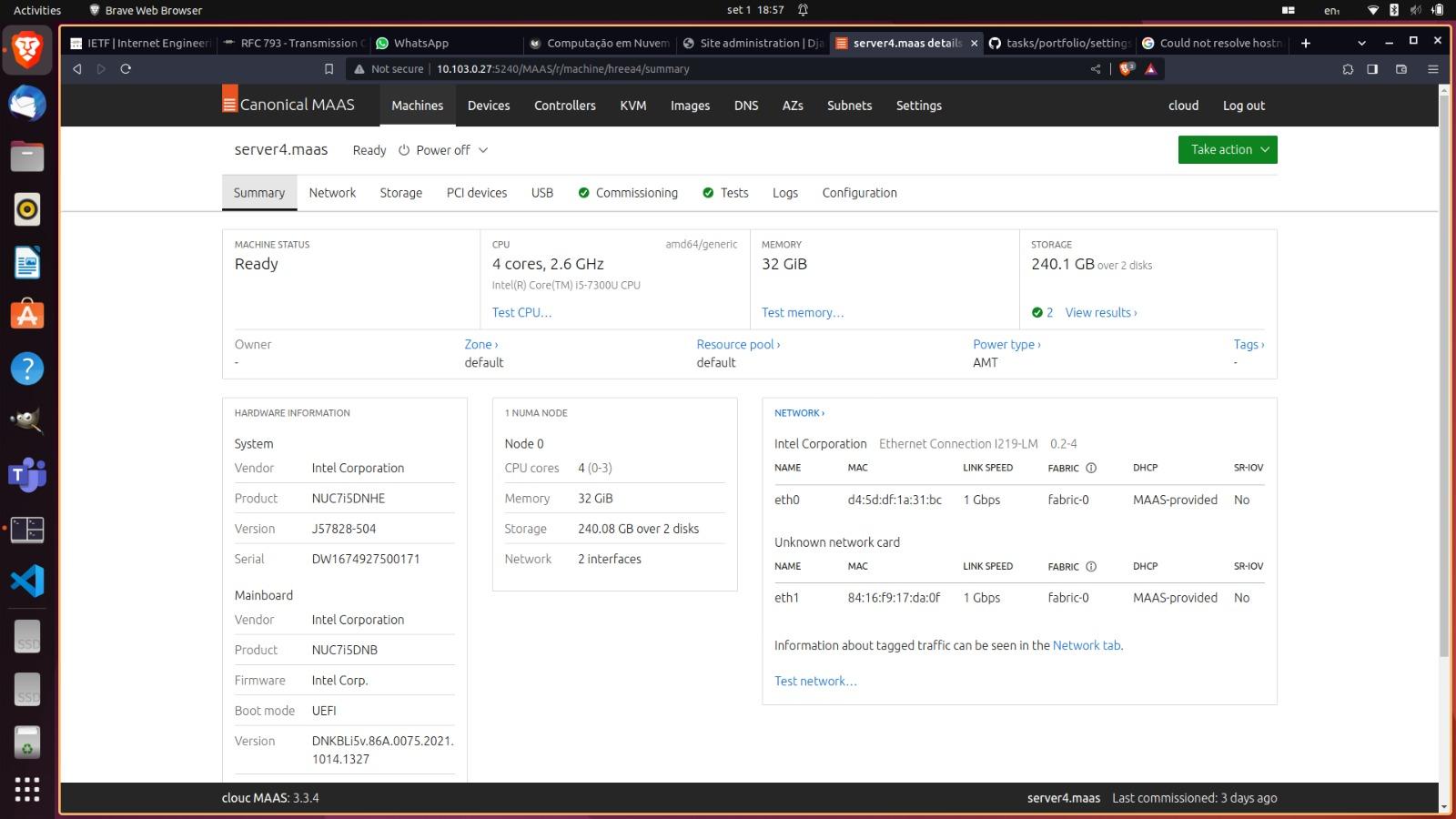
## **Checkpoint 1**

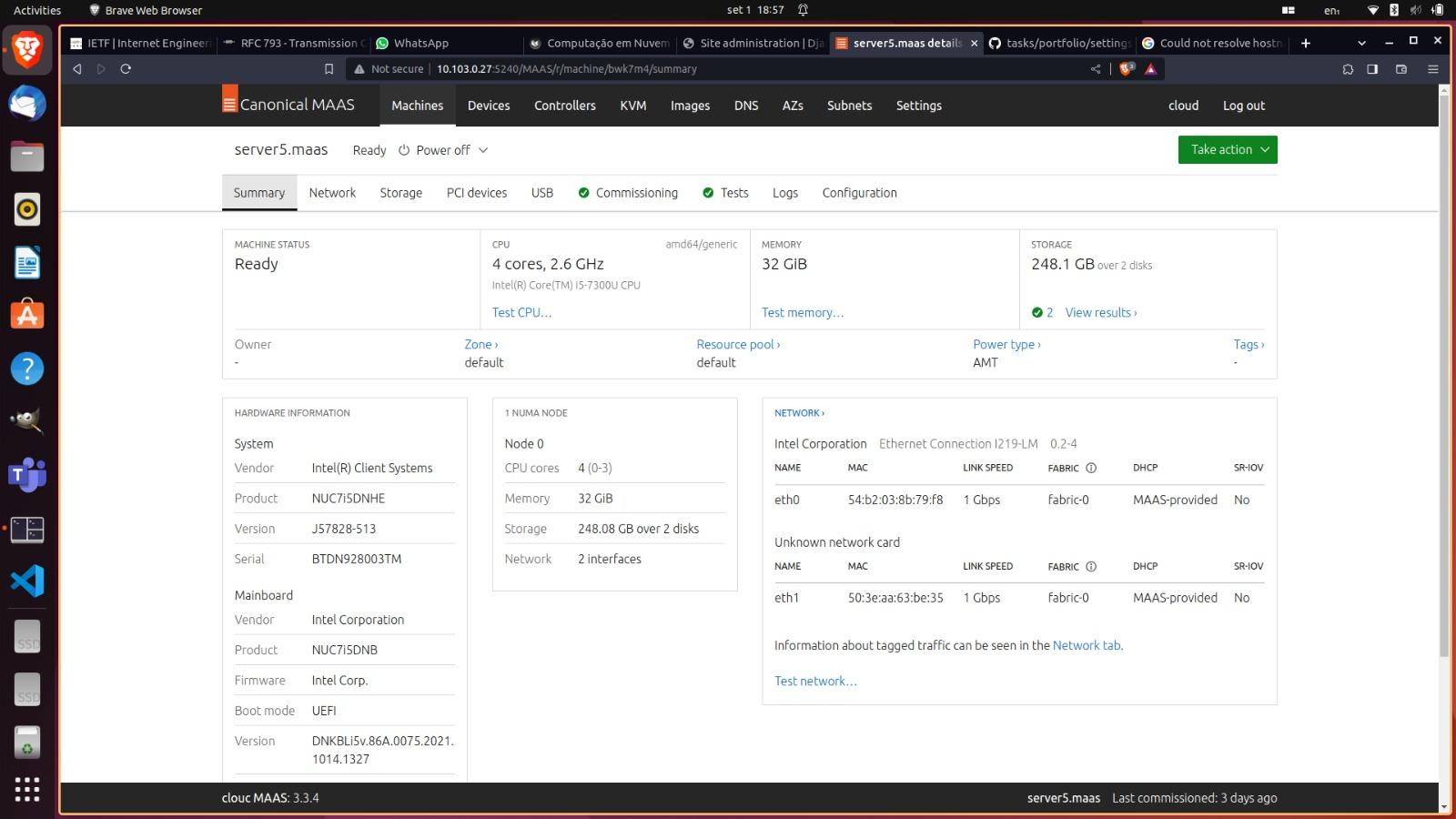
1. Do *dashboard* do **MAAS** com as máquinas. ****
2. Da aba *images*, com as imagens sincronizadas. ****
3. Da aba de cada máquina(5x) mostrando os testes de *hardware* e *commissioning* com Status "OK".

**Server 1**

**Server 2**

**Server 3**

**Server 4**

**Server 5**

## **Questões 4**

1. O que é e como funciona o NAT?

NAT (*Network Address Translation*) é um método que permite que múltiplos dispositivos em uma rede local compartilhem um único endereço IP público para acessar a internet. Ele foi a solução adotada (em maior escala) para resolver a escassez de endereços de IP públicos IPv4.

O NAT atua como intermediário entre a rede local (LAN) e a rede externa (geralmente a *internet*), realizando a tradução de endereços IP e portas de origem dos dispositivos internos quando eles se comunicam com recursos na internet. O roteador que possui NAT é responsável por armazenar uma tabela de tradução de endereços para rastrear qual dispositivo interno enviou a solicitação externa, para que quando chegar a resposta externa, ela seja direcionada ao endereço de IP privado desse dispositivo. Este processo tem o nome de PAT (*Port Address Translation*). O NAT também é capaz de realizar o *Port Forwarding*, processo que traduz também as portas de origem dos dispositivos internos para portas externas únicas quando os dados são enviados para a internet. Isso permite que várias conexões da rede local de um único dispositivo compartilhem do mesmo endereço IP público.

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

LTS significa Long-Term Support e é geralmente utilizado por empresas de software para indicar versões de um software que receberão suporte e manutenção por um tempo prolongado, sem a necessidade de atualizações frequentes que podem afetar a estabilidade ou exigir recursos significativos de migração.

As versões LTS, opostas às versões *Rolling Release*, se tornam importantes para empresas que buscam estabilidade, confiabilidade e segurança em relação ao software que se está utilizando. Isso se torna ainda mais necessário para empresas em serviços de infraestrutura de nuvem, servidores e dispositivos embarcados, onde a estabilidade e a continuidade são fatores críticos.

1. O que é IPv6? Qual a importância da migração?

IPv6 (*Internet Protocol version 6*) é a versão mais recente do protocolo de Internet que define como os dispositivos na rede se comunicam entre si. Ele é o substituto do IPv4 (*Internet Protocol version 4*), amplamente utilizado atualmente.

A migração do IPv6 para o IPv4 é extremamente importante devido à escassez de endereços IP no IPv4, já que ele utiliza endereços IP de 32 bits, permitindo , ou seja, 4.294.967.296 de endereços únicos. Porém, com o crescimento massivo da internet e o aumento sem precedentes de dispositivos únicos conectados por pessoa, essa quantidade logo se tornou insuficiente e se esgotou em maio de 2020. Assim, o IPv6, com endereços IP de 128 bits, proporciona endereços de IP, cerca de 340 undecilhões, que atenderão às demandas de endereçamento por muitos anos.

Vale ressaltar que o IPv6 traz outras importantes funcionalidades, em comparação ao IPv4, como melhorias no suporte a *multicast* (distribuição de dados para grupos de dispositivos), simplificação do cabeçalho de pacotes (facilitando a inspeção e melhorando desempenho), suporte ao protocolo IPsec (que é muito utilizado por sistemas de VPNs, Virtual Private Networks, responsável por autenticar e criptografar pacotes, garantindo comunicação segura entre dois computadores na internet), recurso de auto configuração (que permite com que dispositivos obtenham um endereço IPv6 sem necessidade de configuração de um servidor DHCP), e suporte a novos protocolos, como IoT (*Internet of Things*), e tecnologias emergentes, como NGN (redes de próxima geração). Outra *feature* importante do IPv6 é que o endereço é único para cada dispositivo, de forma análoga ao MAC Address, fazendo com que o dispositivo seja rastreável entre redes.

1. A literatura preconiza que o Modelo de Rede Internet possui 4 camadas, quais são elas e quais camadas foram envolvidas neste capítulo?

As 4 camadas do Modelo de Rede Internet TCP/IP (*Transport Control Protocol / Internet Protocol*) são: Aplicação, Transporte, Internet e Enlace. Apesar do modelo TCP/IP não ser muito utilizado, seus protocolos são amplamente adotados. A camada de **Aplicação** foi envolvida com a instalação do Django. A de **Transporte** com a instalação e funcionamento do MaaS, que fornece comunicação entre os servidores, cada um em sua sub-rede. A camada de **Internet** foi envolvida, por exemplo, com as definições de regras NAT, permitindo que os servidores se conectem à rede do Insper. A comunicação LAN cabeada (e posteriormente, sem fio) através do roteador entre o MaaS e nosso computador confirma o envolvimento da camada de **Enlace** neste roteiro.

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

As 7 camadas do Modelo de Rede OSI (*Open Systems Interconnection*) são: Aplicação, Apresentação, Sessão, Transporte, Rede, Enlace de dados e Física.

Nem todas as camadas do Modelo OSI são explicitamente implementadas no Modelo TCP/IP. A camada Física do OSI é completamente ignorada no TCP/IP e as camadas de Sessão e Apresentação do OSI não são diretamente mapeadas no TCP/IP, sendo a maioria das funcionalidades dessas camadas incorporadas na camada de Aplicação do TCP/IP. Também cabe citar que embora os protocolos associados ao modelo OSI raramente sejam usados atualmente, o modelo em si é bastante adotado, e as características descritas em cada camada continuam muito importantes. Por outro lado, o modelo TCP/ IP tem características opostas: o modelo propriamente dito é considerado "limitado", mas os protocolos são bastante adotados.

1. O que é um MAC address?

*MAC* *address* (*Media Access Control address*) é um identificador local e exclusivo, gravado diretamente na placa de rede, que rotula de forma única um dispositivo em uma rede local, já que utiliza-se o endereço de IP para se comunicar na internet. Ele possui a formatação de um número hexadecimal de 48 bits dividido em pares de dígitos, separados por dois pontos, como "XX:XX:XX:XX:XX:XX". Ele também auxilia na garantia de segurança dentro da rede, já que ele identifica unicamente um dispositivo na rede e o usuário não consegue manipulá-lo facilmente. Um exemplo de utilização do MAC address é no contexto de jogos on-line para banir jogadores (hackers) que desrespeitam os Termos de Uso e Serviços, impedindo que ele consiga conexão com os servidores do jogo através da máquina banida.

1. O que é um IP address? Como ele difere do MAC address?

IP address (*Internet Protocol address*) é um identificador numérico único atribuído a cada dispositivo conectado, permitindo a comunicação em uma rede que utiliza o protocolo internet, seja em uma LAN (rede local) ou rede global. Eles são essenciais no roteamento de pacotes na rede. Cada dispositivo conectado possui um endereço IP exclusivo. Ele também reflete a estrutura hierárquica da topologia de determinada rede. As versões principais do IP são o IPv4 e IPv6, que utilizam, respectivamente, endereços de 32 e 128 bits. O IPv6 busca resolver o problema de escassez de endereços IPv4. Informações mais extensas sobre a aplicação do IP podem ser encontradas nas descrições de DHCP, DNS e NAT.

O MAC address é um identificador local em uma rede privada e não é roteável na internet. Para comunicação na internet, os dispositivos utilizam IP address, e os roteadores realizam a tradução entre IP addresses e MAC addresses, para dados encaminhados entre redes diferentes.

1. O que é CIDR? Qual o papel da sub-rede?

CIDR (*Classless Inter-Domain Routing*) é uma técnica de notação de endereços IP mais flexível, uma alternativa às classes de endereço de IP (A, B, C, D, E). Ela utiliza uma máscara de sub-rede de comprimento variável (VLSM) que altera a proporção entre os bits de rede e de *host* no endereço IP. Isso permite com que os administradores da rede dividam o endereço IP em sub-redes de tamanhos variados. Por isso, um endereço de IP que utiliza CIDR acrescenta um sufixo que informa a contagem de bits do prefixo do endereço de rede, como, por exemplo, em "X.X.0.0/16", onde os 16 primeiros bits representam o endereço de rede, "X.X".

Sub-redes têm o propósito de dividir um único espaço de endereços IP em várias redes menores e isso permite que cada sub-rede opere com uma lógica separada, mesmo que compartilhe da mesma infraestrutura física. Isso também permite que o tráfego seja gerenciado e isolado entre os dispositivos conectados na rede, melhorando o desempenho e a segurança. Sub-redes também desempenham o papel crucial no contexto da internet com adoção em massa do IPv4, onde endereços de IP públicos são extremamente escassos, assim, em vez de alocar uma grande faixa de endereços para uma única rede, você pode dividir essa faixa em várias sub-redes menores, permitindo um uso mais eficiente. Por fim, o terceiro pilar do propósito das sub-redes é que elas auxiliam na escalabilidade da infraestrutura de rede, já que em vez de redesenhar toda a infraestrutura, é mais cômodo adicionar novas sub-redes conforme necessário.

1. O que são DHCP, DNS e gateway?

DHCP (*Dynamic Host Configuration Protocol*) é um protocolo de rede que automatiza a atribuição de configurações de uma rede, o que inclui dados como endereços IP, máscaras de sub-rede, servidores DNS, gateways, entre outros. Seu principal objetivo é facilitar a configuração de redes e tornar mais simples a adição de novos dispositivos na rede. Para executar essa alocação de endereços aos dispositivos, o DHCP possui um *pool de endereços*, que corresponde ao conjunto de endereços IP disponíveis para aquela rede, de onde ele irá atribuir aos dispositivos conforme necessário. Outro ponto fundamental no DHCP é o tempo de concessão, que é atribuído a um dispositivo quando ele solicita a conexão ao servidor, e determina quanto tempo tal dispositivo ficará com aquele endereço de IP fornecido. Essa concessão pode ser renovada antes ou depois do tempo de concessão expirar, ou quando ela expirar, o dispositivo pode também solicitar um novo endereço. Existe também outro recurso dos servidores DHCP, que é o de realizar reservas de endereços IP, sendo configurados para atribuir determinados endereços para dispositivos específicos, baseado em seus endereços MAC.

DNS (*Domain Name System*) é um sistema crucial para o funcionamento da internet, traduzindo os nomes de domínio, como "[www.google.com](http://www.google.com)", para seus respectivos endereços IP, no caso "142.250.219.14". Este papel de tradução é essencial para simplificar a forma com que os usuários se conectam em outras redes na internet. A resolução do nome é o fator primário em um servidor DNS, caso uma solicitação encaminhada por um dispositivo não consiga ser resolvida naquele servidor, ele consultará outros servidores até encontrar o IP associado ao nome de domínio buscado. Outro pilar do DNS é garantir a autenticidade dos sites visitados, contribuindo para evitar ataques do tipo *phishing* e garantindo a comunicação com o servidor correto.

Gateway (do inglês, portão de entrada) é um servidor instalado entre duas redes, com o papel principal de permitir a comunicação entre elas, sejam elas tendo topologias, protocolos ou infraestruturas diferentes. Um gateway também pode ser utilizado como roteador, distribuindo pacotes conforme o IP de destino deles. Outro papel importante dele é na segurança da rede, filtrando e inspecionando o tráfego. Em redes privadas, os gateways costumam realizar NAT para permitir o acesso dos dispositivos à internet, utilizando o IP público do gateway. Também é possível customizar o gateway para redirecionar o tráfego, com base em regras específicas, movendo dispositivos para servidores de balanceamento de cargas e de proxies.