ROTEIRO 1

Alunos: Bernardo Cunha Capoferri e Lívia Sayuri Makuta.

QUESTÕES-1

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

Primeiramente, tem-se que a topologia de uma rede está relacionada com a forma como os elementos de uma rede de comunicação estão organizados. Assim, as topologias de rede são essenciais para ter mais organização, performance e usabilidade, que atualmente são características necessárias ao implementar uma rede de computadores.

E esse conceito é aplicado tanto de uma maneira física como de maneira lógica. Dessa forma, existem dois tipos de topologias: **a física e a lógica**. A primeira – **física** – representa **como as redes são conectadas fisicamente com os cabos, e o meio de conexão dos dispositivos das redes como os nós** (switches), logo, é por meio das estratégias de organização, cabeamento e disposição das máquinas que a topologia física pode ser definida. Por sua vez, **a topologia lógica** diz respeito ao modo que os sinais agem sobre os meios de rede, ou seja, **como os dados são transmitidos através da rede a partir de um dispositivo para outro**, mas sem levar em consideração a interligação física dos dispositivos, **considerando mais os ajustes que dependem de uma interface como softwares, recursos de nuvem, roteadores**, entre outros, com o objetivo de conectar os nós a rede com um tráfego menor e mais eficiente.

Dentro da categoria de topologia física, temos as seguintes opções: **estrela, anel, árvore, barramento, híbrida, malha e ponto a ponto**. Cada uma delas será explicada abaixo.

A mais comum dentre essas é a topologia estrela, que utiliza cabos de par trançado e um concentrador que é um ponto central da rede, sendo que esse ponto retransmite todos os dados para todas as estações, tendo a vantagem de tornar a localização de problemas mais fácil, já que caso um dos cabos, ou uma das portas do concentrador ou placa de rede estiver com problemas, apenas o nó ligado ao componente defeituoso será afetado. E essa é a

topologia da nossa rede, já que o roteador pode ser visto mais como um servidor, já que apenas conecta redes diferentes e tem duas interfaces (WAN e LAN). Assim, **temos um switch conectado com 6 servidores em uma topologia de estrela.**

Outra topologia importante é a topologia de anel que conecta os dispositivos em série formando um circuito fechado, como se fosse um anel. Dessa forma, os dados são transmitidos em uma única direção de nó por nó até chegar em seu destino ou na sua estação fonte. Com isso, todos os computadores acessam a rede da mesma forma e caso aumentem os usuários da rede a performance não será muito impactada. Porém, caso um dispositivo falhe, todos os outros serão afetados, o que dificulta até mesmo encontrar onde está o problema.

Já a topologia árvore, também chamada de estrela estendida, é basicamente como se fosse um conjunto de ramos conectados a um dispositivo central. Basta pensar que no laboratório seria o equivalente ao switch estar conectado a outros switches, assim, teríamos um switch na barra central que está conectado aos seus servidores e a partir dele outros switches que também estão conectados a outros servidores, formando ramos. A desvantagem dela é que pela conexão se propagar por caminhos distintos, as velocidades de propagação e os sinais refletidos também serão distintos, sendo que no geral, a taxa de transmissão dessa topologia é menor do que as redes em barra comum.

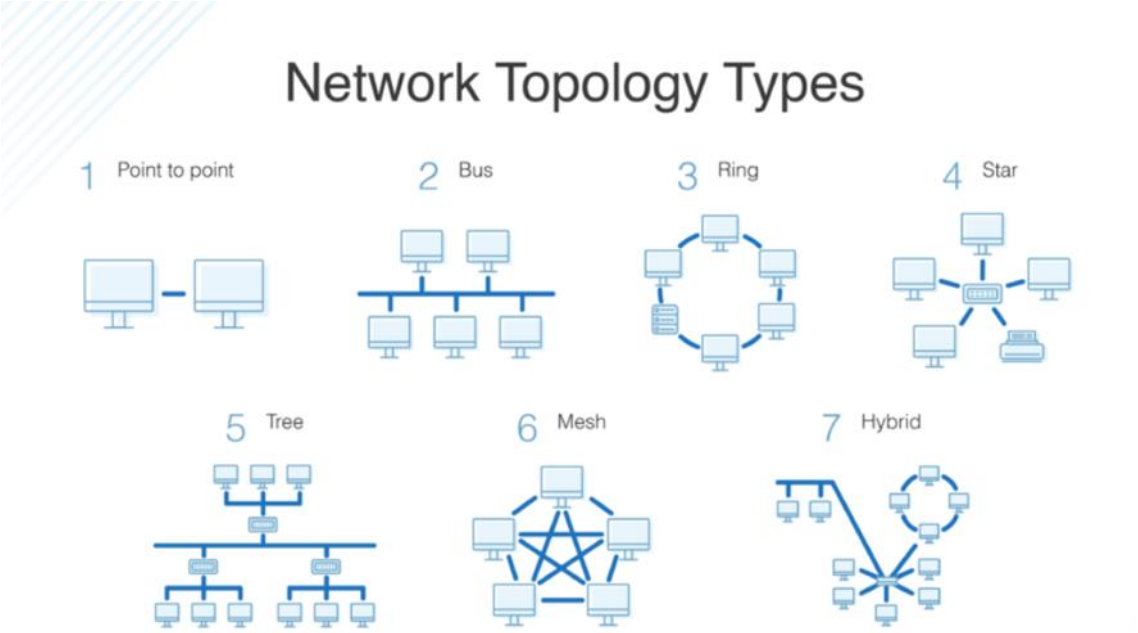
Por sua vez, a topologia de barramento permite que todos os dispositivos sejam ligados em um mesmo barramento físico de dados. Assim, embora os dados não passem por dentro de cada nó, todas as máquinas irão escutar e recolher os dados que forem destinados para elas, sendo que apenas uma pode escrever no barramento por vez. Então se um computador estiver transmitindo um sinal e outro tentar enviar, vai haver uma colisão e a transmissão vai ter que ser reiniciada.

Em relação a topologia de malha, tem-se que nela todos os nós estão conectados com todos os outros nós, como se fossem entrelaçados. Assim, há vários caminhos possíveis onde a informação pode fluir da origem até o destino. Ou seja, nessa topologia há redundância e maior confiabilidade e há uma facilidade de diagnóstico, porém a instalação acaba sendo custosa.

Uma das mais simples, por outro lado, é a ponto a ponto, onde cada um dos pontos da rede funciona tanto como cliente quanto como servidor, o que possibilita compartilhar serviços e dados sem precisar de um servidor central.

Por fim, existe a topologia híbrida, que mescla duas ou mais topologias de rede, o que dependendo da integração pode desfrutar de vantagens de cada uma das topologias, sendo muito utilizada nas grandes redes, exatamente por se adequar ao ambiente em que está inserida.

Abaixo há uma imagem que mostra como são organizados os tipos de topologias físicas (retirado de https://www.heavy.ai/technical-glossary/network-topology):



2. Quais casos uma rede ter mais de 1 gateway?

Para termos uma rede interligada, é preciso uma rede que tem gateways, sendo um exemplo de gateway o roteador, que conecta a rede local com as redes externas. E nesse contexto, é possível termos mais de 1 gateway. Um exemplo é pensar em um e-commerce quando há vários servidores para serviços replicados a fim de atender uma demanda maior e para evitar que falhas aconteçam. Nesse caso podemos ter gateways - roteadores - de diferentes operadores e redes para não ficar à mercê de instabilidades, principalmente quando o número de requisições aos servidores é muito grande.

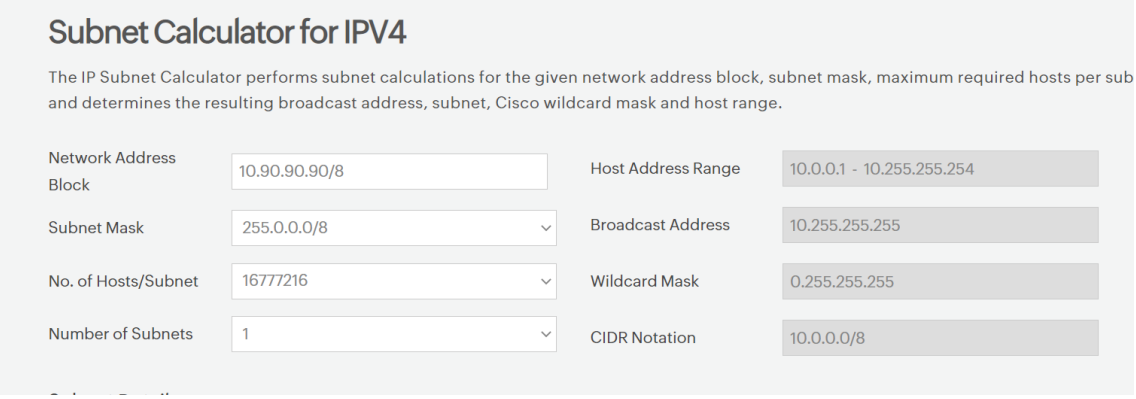
3. Quais as consequências de utilizar um DNS externo (Por exemplo: 8.8.8.8) em uma rede privada?

Ao utilizar um DNS externo em uma rede privada há a possibilidade de relevar o IP para externos possibilitando assim que seja atacada, além disso, também existe a possibilidade da comunicação ser bloqueada caso a rede local proíba o uso de um DNS externo. Entretanto a manutenção desse sistema não fica mais à mercê da própria rede, sendo

manejada pelo provedor do serviço externo, o que possivelmente pode evitar erros causados por mudanças de servidores, como aconteceu no Insper no ano passado, quando o git mudou o endereço de ip e isso não tinha sido atualizado pelo DNS do Insper que consequentemente apontava para um ip que não existia mais, o que impossibilitava acessar o site do git. Outro problema que pode surgir é que por utilizar um sistema externo, o acesso a outros pontos na rede local pode ser impossível, por exemplo, caso haja um sistema de autenticação de usuários local, utilizar um DNS externo impede que a rede local seja acessada para autenticação.

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

O switch estava originalmente na rede 10.0.0.0/8, no endereço de ip: 10.90.90.90/8. Logo, a máscara aplicada à essa rede em binário seria: 11111111 00000000 00000000 00000000 ou no formato CIDR 255.0.0.0/8. Dessa forma, tem-se 8 bits separadas para endereçar redes e 24 bits utilizados para hosts. Assim, podemos concluir que a rede tem: 2^24 IPs, ou 16.777.216. Entretanto, sempre o primeiro e o último IPs da rede são excluídos por serem, respectivamente, o ip da rede e o ip do broadcast, restando apenas 16.777.214 que estão no seguinte intervalo de ips: 10.0.0.1 a 10.255.255.254.



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

As classes de rede foram criadas para dar suporte a números específicos de redes e hosts, que contemplam capacidades diferentes e que dividem de maneira organizada e bem definida o espaço dos endereços IP. Dentre elas, temos três classes principais que são as mais comuns: A, B e C. A primeira, a classe A, há possibilidade de existirem cerca de 16

milhões de endereços IPs por rede (16.777.214), mas com somente 126 redes. Já a classe B, contempla aproximadamente 65.000 endereços IP (65.534) e 16.382 redes. Por fim, a classe C possui apenas 254 endereços IP e 2.097.150 redes. Logo, o intervalo de IPs de cada classe é:

A : 1.0.0.0 - 127.0.0.0

B: 128.0.0.0 - 191.255.0.0:

C: 192.0.0.0 - 223.255.255.0

Em geral, a classe A é utilizada por grandes empresas e instituições, a B para empresas de médio porte e a C, que por ser mais numerosa, é provavelmente a mais encontrada atualmente.

Há ainda a classe D que é reservada para endereços Multicast, que são usados para transmitir pacotes à mais de um endereço simultaneamente e que também é conhecido como broadcast seletivo, já que transmite somente para hosts determinados ao invés de transmitir para todos os hosts do segmento. E também existem outras duas classes: a classe E - utilizada para pesquisas, e a classe *classless* (em português: “sem classe”). Essa última surgiu por conta do problema de alocação e da falta de flexibilidade ao utilizar somente as faixas de IPs pré-definidas nas três classes principais, assim, esse conceito traz a novidade de que a faixa de IPs pode ser dividida de acordo com as necessidades da rede não mais obedecendo às classes definidas como A, B ou C. Assim, uma rede é formada pelo número de bits que são utilizados para a representação do endereço de rede e pelos outros bits da direita deste que poderão ser utilizados para endereçar hosts ou sub-redes.

Assim, como o ip do main server é 192.168.0.3/20 , podemos concluir que ele é da classe *classless*, isso porque a máscara é /20 ou 255.255.240.0/20, ou seja, ele foge do padrão das máscaras das classes tradicionais A, B, C;

Classe	Primeiro Octeto	Parte da rede (N) e parte para hosts (H)	Máscara	Nº Redes	Endereços por rede
A	1-127	N.H.H.H	255.0.0.0	**126** (2^7-2)	**16,777,214** (2^{24}-2)
B	128-191	N.N.H.H	255.255.0.0	**16,382** (2^{14}-2)	**65,534** (2^{16}-2)
C	192-223	N.N.N.H	255.255.255.0	**2,097,150** (2^{21}-2)	**254** (2^8-2)
D	224-239	Multicast	NA	NA	NA
E	240-255	experimental	NA	NA	NA

QUESTÕES-2

1. Quantos IPs utilizáveis estão disponíveis na sub-rede 192.168.0.0/20? Todos os IP são utilizáveis?

A sub-rede 192.168.0.0 usa máscara /20, que em binário seria: 11111111 11111111 11110000 00000000 ou no formato CIDR 255.255.240.0/20. Dessa forma, tem-se 16 bits separados para endereçar redes, 4 bits utilizados para identificar sub-redes e 12 bits utilizados para hosts. Assim, podemos concluir que a rede tem: 2^12 hosts possíveis, ou 4096. Entretanto, sempre o primeiro e o último IPs da rede são excluídos por serem, respectivamente, o ip da rede e o ip do broadcast, restando apenas 4094 que estão no seguinte intervalo de ips: 192.168.0.1/20 a 192.168.15.254/20.

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

Primeiro, vamos entender as implicações de cada um. O IP público é aquele que podemos acessar diretamente pela internet e que é atribuído ao roteador de rede por meio do provedor de serviços de internet. Assim, ao utilizar um IP público para acessar a internet é como se utilizássemos uma caixa postal ao invés de informar nosso endereço residencial para os correios. É um pouco mais seguro, mas é muito mais visível.

Já um endereço de IP privado é aquele que o roteador de rede atribui ao dispositivo, ou seja, cada dispositivo que está conectado na mesma rede recebe um endereço de IP privado que é exclusivo, o que permite que os dispositivos conectados em uma mesma rede se comuniquem entre si sem se conectar a toda a internet. É o endereço de IP local que permite que ao pesquisar o roteador retorne os resultados da pesquisa para o meu computador e não para outro dispositivo conectado à essa mesma rede.

Dessa forma, a principal diferença entre endereços de IP públicos e privados é o alcance e ao que estão conectados. O endereço de IP público possibilita nos identificar na internet para que todas as informações cheguem até nós, enquanto o endereço de IP privado é utilizado em uma rede privada para se conectar aos outros dispositivos da rede com segurança.

Um diagrama que exemplifica bem isso e que foi retirado do seguinte site: https://www.avast.com/pt-br/c-ip-address-public-vs-private#:~:text=Um%20endere%C3%A7o%20IP%20p%C3%BAblico%20te,um%20endere%C3%A7o%20 IP%20 privado%20 exclusivo , pode ser visto abaixo.

Nele, um celular, um tablet, um laptop e um PC estão conectados na mesma rede local (192.168.0.0) e acessam a internet por meio do roteador que possui um endereço de IP público.

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

A rede do Insper é a seguinte :10.102.0.0/19. Essa rede utiliza uma máscara que em binário é 11111111 11111111 11100000 00000000 ou no formato CIDR 255.255.224.0/19 e está em um intervalo que vai de 10.102.0.1/19 até 10.102.31.254/19 com 8.190 hosts utilizáveis.

Por sua vez, a rede do nosso main server é a 192.168.0.0/20. Essa rede utiliza uma máscara que em binário é 11111111 11111111 11110000 00000000 ou no formato CIDR 255.255.240.0/20 e está em um intervalo que vai de 192.168.0.1/20 até 192.168.15.254/20 com 4094 hosts utilizáveis.

Ambas pertencem à mesma classe de rede que é a classless, isso porque as máscaras que utilizam não fazem parte das classes A, B e C.

QUESTÕES-3

1. Por que desabilitar o DHCP do roteador?

É necessário desabilitar o DHCP do roteador porque é o DHCP que faz com que as máquinas obtenham um endereço de IP automaticamente e esses endereços mudam. Nesse caso o DHCP que determinava o IP do server main era o do roteador, mas como o servidor main foi configurado no Maas para distribuir serviços como sistema operacional para as outras máquinas, é ideal que ele tenha um ip estático para que esse servidor que entrega os serviços seja confiável. Além disso, a gente também habilitou o DHCP do Maas que depois passa a ser quem distribui os endereços de IP para as máquinas comissionadas, e não mais o roteador.

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

O PXE Boot é um padrão de boot remoto que foi primeiro desenvolvido pela Intel e que consiste em um software que é gravado na memória ROM da placa de rede e que possibilita com que um computador inicialize através da rede, o que irá carregar todo o software necessário, como imagem do PC ou sistemas operacionais, através de um servidor que foi configurado para esse fim. Ou seja, ele fornece serviços de pré-inicialização no firmware dos dispositivos para que eles possam baixar os programas de inicialização de rede.

Isso é extremamente vantajoso para datacenters, isso porque cada datacenter de cada região tem pelo menos um rack, e esse rack terá servidores, serviços e máquinas. Dessa forma, imagine se fosse preciso subir um sistema operacional em cada uma dessas máquinas e servidores de maneira não automatizada, seria muito trabalhoso e pouco eficiente. É por isso que o PXE pode ser usado, pois ele vai procurar um serviço PXE que irá trazer os protocolos de rede básicos para conectar a máquina a um servidor que irá permitir com que aquela máquina obtenha uma imagem de sistema operacional.

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

O Maas, além de ter as funcionalidades um gerenciador bare metal como criar um inventário de todos os discos reconhecidos de cada servidor e ter um banco de dados de cada modelo de máquina e suas características físicas (memória RAM, MAC Address, entre outras) ele também testa esses discos e permite identificar problemas nas máquinas.

Ademais, o Maas permite trabalhar com serviços de contingência, já que ao cadastrar os racks podemos trabalhar com réplica de serviços, criando uma relação entre eles o que torna possível que o rack gerencie máquinas que estão em outros switches e até mesmo em outros racks.

Por fim, o Maas permite que um sistema operacional possa ser subido para outras máquinas cadastradas no Maas, que foi uma das tarefas que fizemos: subimos o Linux para os três servidores. Além disso, quando um usuário termina de usar uma máquina ele pode liberá-la de volta e pedir ao Maas para garantir que o disco da máquina seja completamente limpo e sempre terá informações sobre os estados da máquina, como a informação de se ela está pronta assegurando que o usuário pode começar a usar aquela máquina de novo e alocar ou até refazer o deploy com um sistema operacional novo e atualizado.

QUESTÕES-4

1. O que é e como funciona o NAT?

A tradução de endereços de rede (NAT, em inglês: “Network Address Translation”) é um processo que permite que um endereço exclusivo IP possa representar um conjunto de computadores. E isso surgiu por conta da necessidade de que na internet cada dispositivo deve ter um endereço de IP único, e por conta da limitação desse endereçamento no protocolo IPv4 a NAT veio com o objetivo de conservar o número de endereços de IPs públicos em uso para fins de segurança e também econômicos - lembrando que a NAT surgiu antes do IPv6.

Assim, um roteador ou firewall NAT atribui um endereço público a um computador ou computadores dentro de uma rede privada, e por meio da NAT é possível que um único dispositivo atue como intermediário entre a rede local privada e a rede pública que é a internet. Dessa forma, quando um dispositivo na rede interna quer conectar com a rede externa, ele manda mensagens e pacotes para o roteador ou firewall NAT que irá substituir o endereço do dispositivo original pelo seu e que depois enviará esses pacotes para a internet. E, quando a

resposta é retornada, esse dispositivo NAT retira o seu próprio endereço e o substitui pelo endereço do dispositivo original que fez a requisição, e envia a resposta para a rede interna.

E existem três tipos de NAT:

NAT Estático: é o mapeamento um-para-um de um endereço IP privado para um IP público, que é útil quando um dispositivo e que está dentro de uma rede privada precisa de acesso a internet.

NAT Dinâmico: é o mapeamento de um conjunto de endereços públicos, também chamados de pool, que as máquinas que usam endereços privados podem usar. Dessa forma, o endereço IP público é retirado de um conjunto de endereços que já está configurado no roteador final.

NAT Sobrecarga: também conhecido como PAT, é outro tipo de NAT dinâmico. A diferença é que ele mapeia vários endereços de IP privado em um único IP público, e isso é possível graças à utilização de portas que identificam univocamente cada pedido das máquinas locais para a rede exterior.

2. O que é e como funciona a VPN?

A VPN (“Virtual Private Network” ou rede virtual privada em português) é um serviço que cria um túnel criptografado para os dados do usuário e protege a sua identidade na internet ocultando seu endereço de IP e permitindo que esse usuário possa utilizar pontes de acesso de Wi-Fi públicos de maneira segura.Logo, é por meio desse túnel que é possível que um usuário no Brasil consiga utilizar recursos de um site disponíveis em outro país, por exemplo, eu poderia utilizar uma VPN para acessar o catálogo da NetFlix da Coreia do Sul e assistir filmes e séries que estão disponíveis apenas lá, e isso porque no processo o host da Coreia age como um gateway para a internet. Importante ressaltar que a VPN não tem apenas esse uso, ela também é muito utilizada em redes de grandes corporações privadas e também para transferir com segurança arquivos entre dispositivos.

3. O que deveria ser feito para você conseguir acessar o Maas da sua casa sem VPN?

O roteador do Insper sabe qual é o endereço de ip do main que é o servidor do Maas, mas o roteador da minha casa não, logo, para acessar as máquinas de lá seria necessário ter um encadeamento de serviços NAT para traduzir o IP privado do main para uma rede pública. Assim, deveríamos ter um NAT no Insper e outro em casa.

Inclusive poderíamos utilizar o tipo de NAT Overload (PAT) que permite que por meio de um endereço público (ou um pequeno range de IP's) seja possível fazer sair várias máquinas, como numa relação de 1 para N. E isso é possível pelo fato de que o NAT Overload utiliza portas que identificam cada pedido das máquinas locais para o exterior. Assim, por meio de um IP único (que é o do server main que está configurado no Maas) poderíamos acessar as várias máquinas comissionadas no Maas por meio de diferentes portas.

QUESTÕES-COMPLEMENTARES

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

LTS ("Long-term support" ou suporte de longo prazo em português) é uma variação de um software que tem como objetivo proporcionar estabilidade para os usuários. Esse é um conceito muito visto em projetos de código aberto, como o sistema operacional Linux, frameworks e IDEs de desenvolvimento, e isso porque certos programas têm a demanda de serem estáveis por longos períodos de tempo. Isso significa que durante toda a vida de uma versão de software haverá o compromisso de atualizá-lo, corrigi-lo e mantê-lo, e isso porque sem o suporte de longo prazo, o software pode se tornar um risco de segurança. As vulnerabilidades se desenvolvem ao longo do tempo e sem mecanismos para corrigi-las ou atualizá-las, os sistemas ficam expostos e quanto mais tempo ficam desatualizados, pior é o desempenho. Por outro lado, também existem desvantagens, pois se os usuários ficarem com a mesma versão por muito tempo, seu sistema vai ficar para trás, pois embora alguns recursos-chave sejam normalmente portados para versões antigas, normalmente o que é mais recente é melhor.

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

O IPv6 é um protocolo da camada de rede que identifica computadores e garante que informações irão chegar nos destinos corretos, assim, os arquivos empacotados em uma camada anterior vão ser recebidos e anexados ao IP da máquina que enviará e receberá

arquivos e a partir disso serão enviados pela internet e irão para outra camada. É como se fosse um entregador, sendo que o IPv6 transfere endereços com 128 bits. E a necessidade do IPv6 ter sido criado deve-se ao fato do IPv4 suportar 4,29 bilhões de IPs pelo mundo, mas não mais que isso, enquanto o IPv6 suporta um número de cerca de 340 undecilhões de endereços, ou seja, com ele o crescimento da demanda de internet é facilmente suportado por muitos anos. Logo, a migração para o IPv6 é importante pois ela permitirá a escalabilidade ao longo do tempo, além de facilitar o surgimento de novos aplicativos e serviços em várias plataformas e também de mitigar riscos para empresas que não podem desacelerar o crescimento de seus negócios por conta do esgotamento de endereços de rede.

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

O modelo de rede de internet que possui 5 camadas é chamado de TCP/IP e suas camadas são: a camada física, a camada de enlace, a de internet, a de transporte e a de aplicação.

A camada física trata da transmissão de bits por um canal de comunicação, de maneira a garantir que quando um lado manda um bit 1, esse bit deve ser recebido do outro lado como um bit 1, além de se preocupar com o tempo que um bit deve durar, se a transmissão é simultânea nos dois sentidos, como a comunicação será iniciada, estabelecida e finalizada, etc. Ou seja, é mais sobre interfaces mecânicas, elétricas e de sincronização. Importante lembrar que essa camada os autores de livros de rede acabam colocando, mas no protocolo TCP/IP não é necessário por ser um problema de telecomunicação, há inclusive profissionais da área que afirmam que é mais para facilitar a compreensão.

Já a camada de enlace, transforma um canal de transmissão normal em uma linha que parece não ter erros de transmissão já que trata esses erros e perdas no meio do caminho de envio de dados. Além disso, ela regula o fluxo de dados de modo que um host mais rápido não sobrecarregue um mais lento e também realiza o mapeamento entre um endereço que identifica o nível de rede para um endereço físico.

Por sua vez, a camada de internet vem para manter toda a arquitetura unida, como se correspondesse à camada de rede do modelo OSI. E sua tarefa é permitir que hosts coloquem pacotes em qualquer rede e garantir que esses pacotes irão trafegar de maneira independente até o destino – podendo ser até em uma rede diferente. É como se fosse um sistema de correio, em que uma pessoa pode deixar várias cartas internacionais em uma caixa de correio

em um país e irá esperar que essas cartas sejam entregues no endereço correto no país de destino. Por conta disso as cartas provavelmente vão passar por centros de triagem ao longo do caminho e isso será transparente para os usuários, também sendo orientado pelo padrão de cada país em relação aos selos, tamanhos de envelope, regras de entrega, etc.

Em relação à camada de transporte, tem-se que essa camada irá permitir que as entidades pares dos hosts de origem e destino mantenham uma conversação, e para isso conta com o auxílio de dois protocolos: o TCP e o UDP. O TCP é o protocolo de controle de transmissão e é orientado a conexões confiáveis permitindo a entrega de um fluxo de bytes sem erros – e para isso fragmenta o fluxo de bytes de entrada em mensagens discretas e passa cada uma delas para a camada de internet, sendo que é no destino que o processo TCP receptor volta a montar as mensagens recebidas. Por sua vez, o protocolo UDP é um protocolo sem conexões, não confiável e para aplicações que não desejam a sequência ou o controle de fluxo do TCP. Ele é usado mais para consultas isoladas com solicitação e resposta (tipo cliente-servidor), e em aplicações em que a entrega imediata é mais importante do que a entrega precisa, como na transmissão de voz ou vídeo.

Por fim, a camada de apresentação contém todos os protocolos de nível mais alto, dentre eles temos: o protocolo de terminal virtual (TELNET), o protocolo de transferência de arquivos (FTP) e o protocolo de correio eletrônico (SMTP). Além desses, outros foram incluídos com o decorrer dos anos como o DNS – que mapeia os nomes de hosts para seus respectivos endereços da camada de internet - , o HTTP (protocolo usado para buscar páginas na World Wide Web, e o RTP (protocolo para entregar mídia em tempo real como voz ou vídeo).

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

O modelo de rede OSI possui 7 camadas: a camada física, de enlace, de rede, de transporte, de sessão, de apresentação e de aplicação. Sendo que dessas camadas, as camadas de aplicação,a apresentação e sessão estão representando uma comunicação dentro de um próprio computador. E é a partir da camada de transporte que há uma separação dessas aplicações do usuário, para entrar na camada de rede – onde já não está mais dentro do computador do usuário e onde há de fato comunicação com a rede, com pacotes e informações sendo encaminhadas pela rede.

Agora, já no modelo TCP/IP essas camadas de aplicação, apresentação, e sessão foram juntadas em uma única: a camada de aplicação. Já a camada de rede se tornou a camada de internet, e as outras camadas de transporte, enlace e física se mantêm. Detalhe que no modelo TCP/IP original as camadas de enlace e física eram juntadas em uma única: acesso aos meios, mas depois da atualização desse modelo, as camadas de enlace e física se mantiveram separadas para uma melhor compreensão.

Vale notar que o modelo de referência OSI foi gerado antes dos protocolos correspondentes terem sido criados. Isso significa que o modelo não teve influência de um determinado conjunto de protocolos para a criação de suas camadas, tendo uma formulação bem genérica. Entretanto, a desvantagem dessa ordenação foi que os projetistas não tinham muita experiência no assunto nem muita noção sobre a funcionalidade que deveria ser incluída em cada camada. Como consequência, podemos citar, por exemplo, a camada de enlace de dados que lidava originalmente com redes ponto a ponto e que com o surgimento das redes de broadcast teve que criar uma nova subcamada no modelo. Além disso, quando as pessoas começaram a criar redes reais com base no modelo OSI e nos protocolos existentes, descobriu-se que essas redes não eram compatíveis com as especificações de serviço exigidas

Com o TCP/IP, ocorreu exatamente o contrário: como os protocolos vieram primeiro, o modelo realmente foi criado como uma descrição dos protocolos existentes. Não houve problemas para os protocolos serem adaptados ao modelo, mas o problema foi o modelo não se adaptar a outras pilhas de protocolos. Consequentemente, ele não tinha muita utilidade para descrever outras redes que não faziam uso do protocolo TCP/IP.

Por fim, outra diferença está na área da comunicação não orientada a conexões e comunicação orientada a conexões. A camada de rede, no modelo OSI, é compatível com a comunicação não orientada a conexões e também com a comunicação orientada a conexões; já na camada de transporte, o modelo aceita apenas a comunicação orientada a conexões, onde de fato ela é mais importante (pois o serviço de transporte é visível para os usuários). Por sua vez, o modelo TCP/IP só tem um modo de operação na camada de rede (não orientado a conexões), mas aceita ambos os modos na camada de transporte, oferecendo aos usuários a possibilidade de escolha. Essa escolha é especialmente importante para os protocolos simples de solicitação/ resposta.

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

Um gerenciador de Bare Metal detecta e coloca no inventário todos os discos reconhecidos de cada servidor, assim, através desse comissionamento o usuário terá um banco de dados de cada modelo de máquina e suas características físicas como informações da CPU, MAC Address, memória RAM, interface de rede, entre outras. Além disso, o gerenciador de Bare Metal também testa os discos e aprende sobre o seu desempenho e permite ver se uma máquina foi reconhecida ou não, o que também ajuda a identificar problemas nas máquinas ou saber se elas estão prontas e sem problemas caso todos os testes tenham passado.

6. O que é um MAC address?

Um endereço MAC (“Media Access Control” ou Controle de Acesso de Mídia em português) é um endereço físico associado a interfaces de comunicação que são usadas em dispositivos de rede. Ou seja, é uma identificação gravada em hardware por fabricantes de placas de rede que depois se tornam partes de computadores, roteadores, celulares, tablets, entre outros equipamentos. E essa identificação é única, sendo usada para fazer o que é chamado de “controle de acesso” em vários tipos de redes de computadores. Importante salientar que apesar de ser único e gravado em hardware existem formas de alterar esse endereço que inclusive são muito utilizadas em ataques. Além disso, sempre que a rede utiliza uma identificação baseada em software como o protocolo TCP/IP, o endereço MAC é utilizado.

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

O endereço de IP (Internet Protocol Address ou endereço de protocolo da internet em português) é um endereço exclusivo que identifica um dispositivo na rede local ou em uma rede de internet, e isso é baseado em um conjunto de regras que irão reger o formato dos dados enviados em uma rede externa ou interna. Assim, é o endereço IP que identifica e que permite que informações sejam enviadas entre dispositivos conectados em uma rede, e isso porque ele contém informações da rede e do host.

A diferença entre o endereço IP e o endereço MAC está na função de cada um, enquanto o MAC identifica exclusivamente um dispositivo que quer participar de uma rede e que é um endereço do aparelho que é usado para manter um registro de todos os aparelhos que já se conectaram à rede, o IP vai definir exclusivamente uma conexão de uma rede com

a interface de um dispositivo. Basicamente podemos pensar no endereço MAC como o nome permanente de um dispositivo, enquanto o IP seria uma instrução para outros dispositivos o encontrarem, assim, é como dizer que o dispositivo tem um endereço MAC X que pode ser encontrado com o endereço de IP Y.

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

O CIDR (“Classless Inter-Domain Routing”) é um método usado para rotear e para repartir os endereços IP. Ele surgiu em 1993 através da Internet Engineering Task Force com o objetivo de desacelerar o crescimento das tabelas que continham os roteadores da rede, e desde então tem substituído a arquitetura anterior que fazia o endereçamento de redes. Assim, é por meio desse método que aquele sistema de classes A, B e C ganhou mais flexibilidade e o conceito de sub-rede foi criado. Sendo que o papel de uma sub-rede é subdividir uma rede grande em redes menores o que resulta num tráfego menor e em uma melhor performance da rede, bem como simplifica a administração.

Além disso, o CIDR possui uma notação que é extremamente compacta e que identifica o endereço IP e qual o seu prefixo de roteamento que está associado. Sua notação é construída através de um endereço IP, uma barra (/) e, por último, um número decimal. O número final será composto pela contagem dos bits 1 iniciais que está na máscara de roteamento, e esse número normalmente é conhecido como a máscara de rede que é quem denota o que é a rede, o que é a sub-rede, e o que é o host.

9. O que são DHCP, DNS e gateway?

O DNS (Domain Name System) é um sistema de nomes de domínios que foi criado em 1983. Assim como existem diversas maneiras de comunicar algo, como por exemplo na música, em que temos partituras que são como textos de notas musicais para serem tocadas, o computador também funciona de maneira diferente por dentro. Bem no fundo tudo é um conjunto de números, principalmente os uns e zeros. Mas então, por que quando queremos acessar sites nós digitamos nomes ao invés de números? Isso porque existe o que é chamado de DNS, Domain Name System em inglês ou Sistema de Nomes de Domínio em português, que localiza e traduz para números IP os endereços que digitamos nos navegadores. Assim como no caso das ruas, uma forma de representá-las é através do CEP, que também é um conjunto de números, mas já pensou se para todas as ruas que você quisesse ir tivesse que

chamá-las por números ao invés dos nomes? Pois é, seria uma confusão. E é por isso que o DNS foi criado, continuamos com os nomes, e esse trabalho de tradução para a máquina entender o que queremos, é feito por esse sistema - um esquema hierárquico de atribuição de nomes baseado no domínio e de um sistema de banco de dados distribuído para implementar esse esquema de nomenclatura. Ele é mais usado para mapear nomes de hosts em endereços IP, mas também pode servir para outros objetivos. Além disso, existem diferentes tipos de DNS, os públicos e os privados. No caso de um DNS público significa que está disponível para a população em geral que que normalmente vem do seu provedor de serviços de internet ou de um provedor DNS dedicado. Já um DNS privado é normalmente usado por empresas para fornecer aos funcionários acesso mais fácil a sites ou endereços IP internos.

Já o DHCP (Dynamic Host Configuration Protocol ou Protocolo de Configuração Dinâmica de Endereços de Rede em português) é um protocolo utilizado em redes de computadores que permite que as máquinas obtenham endereços de IP de forma automática. Isso facilitou muito a distribuição de endereços IP, pois quanto mais máquinas em uma rede, se isso precisasse ser feito manualmente levaria muito tempo. Assim, por meio de um servidor que já tem um intervalo endereços de IP pré-definido e configurado , esses endereços diferentes são distribuídos para todos os computadores da rede à medida que eles solicitam a conexão. Assim, sempre que uma máquina for desconectada da rede, o IP que ela utilizou ficará disponível para ser utilizado por outra máquina.

Por fim, um gateway é um conceito usado para descrever uma máquina que faz conexão entre duas ou mais redes e que oferece a conversão necessária em termos de hardware e software. Sendo que, há diferentes tipos de gateways, que são distinguidos através da camada em que estão operando na hierarquia de protocolos.

De maneira geral, a vantagem de ter uma rede interligada é a possibilidade de conectar computadores pelas redes, assim não queremos um gateway em muito baixo nível, caso contrário não poderemos fazer conexões entre diferentes tipos de redes. Além disso, também não queremos usar um gateway em um nível muito alto, pois senão a conexão só vai funcionar para determinadas aplicações. Logo, o nível do meio é o mais apropriado – camada de rede – e um roteador é um gateway que comuta pacotes nessa camada. Assim, para ter uma rede interligada, é preciso uma rede que tem roteadores (que tem gateways). Entretanto vale lembrar que gateways não se limitam a roteadores, os firewalls de hardware e software também são gateways, por exemplo.