Redes

O que é redes ?

Redes de computadores referem-se a dispositivos de computação interconectados que podem trocar dados e compartilhar recursos entre si. Esses dispositivos em rede usam um sistema de regras, chamados de protocolos de comunicação, para transmitir informações por meio de tecnologias físicas ou sem fio.

Camadas de redes

Camada de aplicação

Tudo começa no smartphone. A mensagem é escrita em um aplicativo que está em contato direto com a primeira camada de rede chamada aplicação.

Um exemplo de protocolo que atua em conjunto com um aplicativo como o Web Browser é o http.

Camada de transporte

Na sequência, ao clicar no botão de envio da mensagem, ela será preparada para o transporte.

A mensagem será empacotada de forma com que possa ser transportada por meio da rede.

Camada de rede

A camada seguinte é a de rede, que atua no roteador e é responsável por conectar dispositivos diferentes.

O principal protocolo utilizado é o de endereçamento IP. A partir dele é apresentado um cabeçalho, identificando o endereço de origem e o destino.

Assim, é feito o cálculo da rota de tráfego, ou seja, os dispositivos pelos quais esse pacote de informação terá que passar até alcançar o smartphone que queremos enviar a mensagem.

Camada física

A quarta camada é a física e consiste na transmissão dos bits dessa mensagem por meio de dispositivos de rede.

Após trafegar pelos dispositivos da camada física e chegar ao roteador, que está em casa, a mensagem passará pelo processo reverso.

Isso significa que passará pelo desencapsulamento na camada de transporte até que fique disponível no aplicativo do celular da mãe.

É assim que funciona o modelo de camadas de uma rede de computadores, mais precisamente a internet.

Ping e Traceroute

Sabemos que websites não são páginas que existem na nuvem de forma abstrata. São páginas armazenadas em um computador, como um servidor localizado na nossa cidade ou em países diferentes.

Então, logo após o ping digitamos www.alura.com.br e apertamos "Enter".

ping www.alura.com.br

Observe que esse comando envia um pacote com 32 bytes de dados. Esses são dados vazios, apenas para testar se esse pacote está alcançando o destino e com qual velocidade. Também encontramos a latência, ou seja, o tempo que levou para que esse pacote atingisse o endereço de destino.

Repare que, apesar de termos digitado o domínio da Alura, foi indicado o endereço de IP do dispositivo em que esse website está armazenado. Testaremos de outra forma.

Para isso, copiamos o endereço de IP, escrevermos ping e colocarmos em sequência.

ping 104.26.5.131

Ao rodar, percebemos que o processo de envio do pacote de dados ocorre da mesma maneira, obtendo os mesmos resultados. São enviados 4 pacotes. Todos eles foram recebidos, nenhum se perdeu pelo caminho. Além disso, o tempo mínimo, máximo e médio de resposta foi de 8 ms.

Também encontramos uma informação referente ao TTL (Time To Leave), ou seja, o tempo de espera até obter uma resposta do encaminhamento desse pacote. Se o tempo for superior ao TTL, o pacote será considerado perdido na rede.

Podemos fazer testes com outros websites, por exemplo, o youtube.com.

ping youtube.com

Repare que o endereço de IP desse website foi identificado. Novamente foi enviado 32 bytes de dados e o tempo de resposta foi um pouco maior, 119 milissegundos. Já a latência foi menor, de 1 milissegundo. Todos os 4 pacotes enviados foram recebidos e nenhum foi perdido. Esse é o comando ping.

Sabemos que esse pacote não saiu do nosso computador nem foi para um servidor e voltou. Ele, na verdade, passou por dispositivos que estavam no meio do caminho.

Temos um comando que nos permite verificar a rota de tráfego desse pacote de dados, que se chama tracert. Se utilizarmos esse comando seguido de www.alura.com.br, dessa forma:

tracert www.alura.com.br

Ao apertamos "Enter" obtemos a rota de tráfego do pacote que enviamos pela rede até que ele alcance o servidor no qual o site da Alura está armazenado. Também encontramos a informação referente ao número máximo de saltos para identificar o caminho que esse pacote tomou de 30 saltos.

Os saltos se referem ao número de roteadores pelos quais esse pacote de dados passou.

Repare que a primeira linha não apresenta o endereço de IP do dispositivo por questões de segurança. Já no fim, é concluído o rastreamento, identificando diferentes dispositivos pelos quais esse pacote passou até alcançar o endereço de IP onde o website da Alura está armazenado.

Se pegarmos o endereço 104.26.5.131 e aplicarmos o traceroute, teremos um resultado idêntico.

tracert 104.26.5.131

Lembrando que o resultado pode variar conforme o tráfego na rede, por exemplo, pode ser que o pacote tenha passado por outra rota.

O tráfego pelo qual o pacote passará é dinâmico e depende justamente de quão congestionado alguns ramos da rede podem estar em determinado momento.

Cabos de conexão

O padrão de cores e a forma desse conector são padronizados pela Associação Internacional de Telecomunicações, a TIA. Todos os dispositivos que utilizamos, como celular, smart TV, desktop e laptop, possuem algum elemento de hardware dedicado à conexão em rede. No celular, por exemplo, haverá um elemento que estabelecerá a conexão wireless (sem fio). Já no computador, podemos ter uma placa que faz a conexão Wi-Fi e, ao mesmo tempo, uma placa que podemos plugar em um conector Ethernet, que é o caso do RJ45 que vimos na imagem anterior.

Por que temos diferentes fios dentro desse cabo? Na placa de rede, teremos diferentes canais, alguns dedicados ao envio de mensagens e outros à recepção de mensagens. É comum nos computadores que as entradas 1 e 2 da placa de rede sejam destinadas ao envio de dados, e os canais 3 e 6 sejam destinados à recepção de pacotes enviados por outros dispositivos que estão na rede.

Para facilitar a identificação desses diferentes fios e como conectá-los em uma placa de rede, adotamos um padrão de cores, como vemos nesta imagem.

À esquerda, um cabo azul do qual saem 8 fios nas seguintes cores, respectivamente: verde e branco; verde; laranja e branco; azul; azul e branco; laranja; vermelho e branco; e vermelho. À direita, um quadro intitulado "T568A" com os mesmos 8 fios seguidos por uma numeração, sendo: verde e branco para 1; verde para 2; laranja e branco para 3; azul para 4; azul e branco para 5; laranja para 6; vermelho e branco para 7; e vermelho para 8.

Esse padrão, definido pela TIA, é conhecido como T568A. Neste padrão, temos:

na posição 1, um fio verde com branco;
na 2, um fio inteiramente verde;
na 3, um fio laranja com branco;
na 6, um fio inteiramente laranja.

Esses são os canais que utilizamos para o envio e recepção de dados.

Mas como esse cabo vai se conectar no hub que utilizamos no caso que construímos? A placa de rede do hub fará a recepção e a transmissão de dados em canais diferentes da placa de rede no nosso computador. Ou seja, nos canais 1 e 2 ela receberá as informações, enquanto nos canais 3 e 6 fará o envio das informações, utilizando esses canais para enviar pacotes de dados para os dispositivos conectados no hub. Dessa forma, podemos usar um cabo que conhecemos como cabo direto para fazer a conexão entre um dispositivo, como o computador, e o hub.

Mas e se quisermos, por exemplo, conectar um daqueles computadores utilizados no exemplo da manufatura, diretamente com o computador da embalagem? Neste caso, teremos apenas dois computadores, então podemos fazer uma conexão direta, sem um dispositivo de rede intermediário.

Mas há um problema: essas placas de rede utilizam os mesmos canais para fazer a transmissão e recepção de dados. Sendo assim, será que podemos usar o cabo T568A nos dois casos? A resposta é não, porque teríamos um crash. Ou seja, os pacotes se encontrariam, um no sentido direto e outro no sentido inverso, causando uma colisão. Dessa forma, precisamos de outro padrão, de forma que possamos conectar, utilizando uma conexão cabeada, dois dispositivos que estão atuando no mesmo nível da rede.

A solução para isso é o cabo cruzado ou crossover. Vamos pensar na prática como funciona esse cabo. De um lado, temos a conexão do padrão T568A. Dentro do cabo cruzado, vamos inverter a posição dos fios que o constituem, que ficará da seguinte forma:

Quadro intitulado "T568B". Nele, há 8 fios enumerados da seguinte forma: na posição 1, fio laranja com branco; na 2, fio todo laranja; na 4, fio verde com branco; na 4, fio todo azul; na 5, fio azul com branco; na 6, fio todo verde; na 7, fio vermelho com branco; e na 8, fio todo vermelho.

No computador da manufatura (com padrão T568A), os fios laranja com branco e todo laranja, respectivamente nas posições 3 e 6, serão direcionados para os canais 1 e 2 da placa de rede do computador (com padrão T568B), que pode ser da embalagem ou do transporte, também nas cores laranja com branco e todo laranja, respectivamente.

Os cabos 1 e 2, no computador com padrão T568A, de cor verde com branco e todo verde, respectivamente, são destinados ao envio das mensagens, e serão direcionados para os canais 3 e 6 do computador T568B, também de cor verde com branco e todo verde, respectivamente, que farão a recepção dos dados.

Dessa forma, fazemos com que dois dispositivos, usando padrões diferentes, apenas fazendo o cruzamento dos cabos, consigam trocar informações entre si sem haver qualquer tipo de colisão nos pacotes enviados.

IPV4 e classes de ip

Quanto ao limite inferior, não existem endereços de IP negativos, logo, os endereços devem ser superiores à sequência de zero nos quatro octetos (0.0.0.0). Da mesma forma, temos um limite superior: os endereços devem ser inferiores à sequência de 255 em todos os quatro octetos (255.255.255.255).

Classe A

No IPv4, os endereços estão distribuídos em cinco classes diferentes. Vamos começar pela primeira: a classe A. Na classe A, temos endereços de IP que começam o primeiro octeto com sequências que vão de 1 a 126.

Nessa classe, temos como máscara de rede padrão o formato 255.0.0.0. A máscara de rede nos permite identificar, a partir de um endereço de IP da classe, qual é o endereço da rede na qual o dispositivo se encontra.

Vamos analisar um exemplo prático: temos o endereço de IP 123.145.3.3, que pertence à classe A, visto que o primeiro octeto é iniciado com a sequência 123. Qual seria o endereço de rede desse dispositivo?

Basta observar na máscara de rede padrão quais octetos estão ocupados pela sequência de 255. Fazendo a subtração e preenchendo os demais octetos com zero, nós obtemos o endereço de rede na qual esse dispositivo está conectado, ou seja, 123.0.0.0.

O endereço de rede acima não pode ser atribuído a nenhum dispositivo da nossa rede, logo, ele é dedicado à identificação dessa rede específica.

Além do endereço de rede, dedicado à identificação da rede, temos outro endereço: o de broadcast, para o qual o dispositivo envia um pacote de mensagem que quer encaminhar para os demais da mesma rede em que ele está conectado. Inclusive, ao enviar para esse endereço, o próprio dispositivo recebe o pacote de mensagem enviado.

Para obter o endereço de broadcast, basta pensarmos de forma oposta a como obtemos o endereço de rede. Ao invés de preencher os demais octetos com 0, vamos preencher com 255, ou seja, 123.255.255.255.

Assim, conseguimos estabelecer um limite inferior e um limite superior da nossa rede, que são os endereços dedicados primeiro à rede e depois ao broadcast.

Classe B

Temos também a classe B, onde temos os endereços IP que possuem como primeiro octeto uma sequência de 128 até 191. Já a máscara padrão dessa classe é 255.255.0.0. Essa máscara é importante para identificar o endereço da rede de um dispositivo conectado com o endereço IP da classe B e também o endereço de broadcast dessa rede.

Agora, vamos usar como exemplo o seguinte endereço IP da classe B: 135.145.3.3. Qual seria o endereço da rede na qual o dispositivo está conectado?

O exercício é o mesmo, mas agora os dois primeiros octetos são dedicados à identificação da rede e os demais são preenchidos com 0, obtendo 135.145.0.0.

Para encontrar o endereço de broadcast, preenchemos os demais octetos com 255, então obtemos 135.145.255.255.

Dessa forma, identificamos o endereço da rede e de broadcast de um endereço de IP na classe B.

Classe C

Agora, vamos à classe C. Ela é formada por dispositivos que apresentam no seu primeiro octeto uma sequência de 192 até 223. Como máscara de rede padrão, ela possui uma sequência de 255 nos três primeiros octetos, sendo apenas o último octeto utilizado para identificar os dispositivos conectados na rede, então temos 255.255.255.0.

A máscara de rede nos permite analisar quantos dispositivos nós podemos conectar nessa rede específica. No caso da classe C, podemos ter várias redes diferentes e poucos dispositivos conectados em cada uma delas.

Observando a máscara de rede padrão da classe A, temos um único octeto para a identificação da rede, e os demais podem ser utilizados para identificar os dispositivos. Portanto, na classe A, podemos agregar o maior número possível de dispositivos em uma rede.

Então, como descobrir o endereço de rede e o endereço broadcast de um dispositivo conectado com o endereço IP da classe C? Vamos usar o exemplo do endereço 193.168.3.3.

Para encontrar o endereço dessa rede, basta modificar o último octeto para 0, obtendo 193.168.3.0. De modo similar, para encontrar o endereço broadcast da rede, substituímos o último octeto pela sequência 255, ou seja, 193.168.3.255.

Classes D e E

Além das anteriores, temos duas outras classes que são especiais, as quais não utilizamos na identificação dos dispositivos computacionais no dia a dia. São a classes D e E.

A classe D é formada por endereços de IP que apresentam o seu primeiro octeto no intervalo de 224 a 239. Ela é muito utilizada, por exemplo, para multicast, ou seja, para encaminhar mensagens a grupos de dispositivos específicos em uma rede.

Já a classe E é formada por endereços que apresentam o seu primeiro octeto no intervalo de 240 até 255. Essa classe é utilizada para fins de pesquisa e desenvolvimento em redes.

IP público e IP privado

IP público = conexão externa na internet

IP privado = identificação de dispositivos em rede interna

Os endereços IP públicos são usados para estabelecer a conexão externa com a internet, enquanto os endereços IP privados são empregados para identificar dispositivos em redes internas. Dentro de cada classe de endereço IP, existem conjuntos específicos de endereços designados como endereços IP privados.

Conforme vimos, não há nada extremamente confidencial. A única distinção é que esse conjunto de endereços é exclusivamente utilizado para identificar dispositivos em uma rede privada, ou seja, destinado somente para comunicação interna dentro dessa rede.

IP privado
Classe A: 10.0.0.0

Classe B: 172.16.0.0 a 172.31.0.0

Classe C: 192.68.0.0

Dentro da classe A de endereços IP, os endereços IP privados são aqueles em que o primeiro octeto começa com 10. Na classe B, o conjunto de endereços IP privados varia do primeiro octeto 172.16 até a sequência dos dois primeiros octetos 172.31. Já na classe C, temos um conjunto de endereços IP privados em que os dois primeiros octetos começam com 192.68.

Entendemos a distinção entre endereço IP privado e endereço IP público em todas as classes. Podemos, agora, realizar um teste prático para verificar qual é o endereço IP atribuído ao nosso computador e qual endereço IP é visível para dispositivos externos à nossa rede.

Mas como funciona o protocolo STP?

Ele funciona elegendo um switch da malha que vai atuar como principal, e para fazer essa seleção do principal (ou switch root), é necessário ter uma troca de mensagens entre os switches da rede. No contexto de uma rede, sempre que falamos em troca de mensagens, temos um protocolo rodando por trás. Nesse caso, o protocolo BPDU (Bridge Protocol Data Unit).

Para ilustrar o conceito do protocolo BPDU, preparamos o esquema abaixo:

Esquema STP triangular formado por três switches: Switch ADM no topo, Switch MKT na ponta esquerda, e Switch RH na ponta direita. Ao lado dos switches, estão os endereços "MAC 22.22.22.22.22.22", "MAC 33.33.33.33.33.33", e "MAC 11.11.11.11.11.11". Em cada linha de conexão há a inscrição "1 Gps". À direita do esquema, há um retângulo intitulado "BDPU - Bridge Protocol Data Unit", contendo dois retângulos menores dispostos lado a lado, intitulados "Prioridade 32.768" e "Endereço MAC", da esquerda para a direita.

Esse protocolo é acionado quando formamos uma ponte na rede. Essa mensagem tem dois campos, um campo de prioridade e um campo de endereço MAC.

Endereço MAC é o endereço físico que todos os dispositivos que têm uma placa de rede possuem, atribuído por padrão pelo respectivo fabricante.

Nesse protocolo, os dispositivos vão trocar mensagem e a seleção do root será baseada em quem tiver a menor prioridade. No STP, a lógica é "quanto menor, melhor". O switch que tiver a menor prioridade será eleito como root ou switch principal.

Perceba que, no esquema, colocamos o valor de 32.768 na prioridade, e isso não é por acaso. Esse é o valor padrão que vem no switch como prioridade. Se ninguém o alterou, essa é a prioridade padrão, e se todos têm a mesma prioridade, a seleção do switch root será feita por meio da observação do endereço MAC. Como todos os dispositivos possuem endereço MAC diferente, o switch eleito como root será aquele que tiver o menor endereço MAC.

No nosso caso, se observarmos que os switches de ADM, do RH e do MKT têm a mesma prioridade padrão, o switch root, hipoteticamente, seria o Switch RH com o endereço MAC 11.11.11.11.

Mas, nesse caso, ele não é o switch principal, porque temos uma porta desabilitada e esse é um detalhe importante do switch root: ele tem o privilégio de ser o switch principal da rede, ou seja, ele tem a conexão e acaba concentrando todo o tráfego que chega para determinada rede.

Todas as portas do switch root são designadas, portas pelas quais temos um tráfego de dados de entrada e de saída, tanto da rede quanto desse switch para outros switches que estão interligados com ele.

Quantos endereços IP temos disponíveis?

Analisando o último octeto, temos 256 possibilidades de endereços IP, porém, há dois endereços dedicados e reservados: um para o broadcast e outro para a identificação da rede. Podemos considerá-los como limites inferior e superior dos endereços IP disponíveis. Portanto, só temos 254 endereços disponíveis para identificar nossos dispositivos.

Isso traz um problema: precisamos comportar 600 máquinas. Poderíamos pensar em alocar 400 máquinas na VLAN 10 da pesquisa e 400 na VLAN administrativa, por exemplo, de modo a atender a demanda dessas duas VLANs.

Nesse caso, a classe C não nos atenderia e precisaríamos analisar a próxima: a classe B.

Os endereços da classe B começam com o primeiro octeto de 128 a 191, com uma máscara de rede padrão de 255.255.0.0, ou seja, temos dois octetos para identificar os hosts em nossa rede.

Quantos endereços IP teremos disponíveis se utilizarmos a classe B?

Desde o início, utilizamos o termo octeto para nos referir ao endereço IP, composto do primeiro, segundo, terceiro e quarto octeto que constituem um endereço IP para uma máquina, rede ou broadcast. No entanto, temos utilizado sequências de no máximo três dígitos para representar os números em cada octeto. Assim, por que usamos o termo octeto?

Na verdade, usamos a base decimal na identificação dos endereços, pois é a base com a qual estamos mais acostumados no dia a dia, seja para contabilizar nosso rendimento, seja para contar itens que utilizamos frequentemente. Porém, no mundo da computação, a principal linguagem utilizada para representação dos dados é a binária.

Desse modo, a máscara de rede padrão da classe B, 255.255.0.0, na forma binária, é constituída por uma sequência de 1 e 0. Nota-se que 255 é o limite, ou seja, o maior número possível dentro de um octeto. Isso ocorre porque este é o maior número decimal que pode ser representado com oito bits em binário, por uma sequência de 1.

Como obter o valor de um número representado em binário?

Teremos uma atividade no decorrer do curso que permitirá um melhor entendimento, mas podemos adiantar que o valor representado por uma determinada sequência de algarismos em uma base depende da posição em que cada algarismo está na base.

Por exemplo: se convertermos o número 255 para uma soma de potências de 10, será 2 vezes 10 elevado a 2, mais 5 vezes 10 elevado a 1, mais 5 vezes 10 elevado a 0. Se fizermos essa soma, obteremos exatamente o valor 255 representado.

Se fizermos esse cálculo para um binário, começaremos com 1 vezes 2 elevado a 0, mais 1 vezes 2 elevado a 1, e assim sucessivamente, até obter o valor final 255 em uma sequência de 8 bits 1.

Agora que o termo octeto faz sentido para nós, vamos descobrir quantos endereços IP podemos conseguir com um endereço da classe B.

Conforme mencionado anteriormente e bastante estudado no curso 1, em uma máscara de rede, quando temos o número 0 em determinado octeto, indica que esse octeto é dedicado à identificação do host, isto é, das máquinas que podemos conectar na rede.

Analisando a máscara padrão da classe B (255.255.0.0), temos dois octetos destinados à identificação. Preenchemos esses octetos com 0 e os demais com 1, que é o equivalente

em binário. Para descobrirmos quantos dispositivos podemos identificar usando o endereço da classe B, basta contarmos a quantidade de zeros na máscara de rede, ou seja, a quantidade de bits destinados à identificação.

Neste caso, temos 16 bits: 11111111.11111111.00000000.00000000.

Vamos fazer um cálculo rápido: 2 elevado a 16 menos 2. A subtração por 2 corresponde aos dois endereços reservados, o endereço de rede e o endereço de broadcast, ou limite inferior e superior do endereçamento. Obteremos 65.534 endereços IPs disponíveis usando a classe B.

Entendendo o protocolo RIP

Podemos usar o protocolo RIP na rede do provedor de serviços Zoom.

RIP = Routing Information Protocol (Protocolo de informação de roteamento)

Como o protocolo atua? Os roteadores vão compartilhar informações de roteamento entre si, compartilhando quais rotas cada um conhece.

Dessa forma, o roteador A vai saber quais redes o roteador B conhece. Assim, vai poder decidir se vai encaminhar um pacote para o roteador B ou não.

Protocolo BGP

Temos aqui o protocolo BGP - Border Gateway Protocol, ou "Protocolo de roteador de borda", em português. Ele atua no encaminhamento dessas informações entre redes diferentes.

Aqui cabe destacar um conceito importante no contexto do BGP, que é o conceito de sistema autônomo. Um sistema autônomo pode ser entendido como uma coleção de endereços IPs e roteadores que fazem parte de uma rede que está sob a administração de uma única entidade administrativa.

Em outras palavras, é como se tivéssemos um sistema autônomo para o provedor de serviços 1 e um sistema autônomo para o provedor de serviços 2. Para cada sistema autônomo, atribuímos um número de identificação específico, que é o ASN - Autonomous System Number (Número de Sistema Autônomo), que é o número de identificação desse sistema autônomo.