



DESCRIÇÃO

O protocolo de internet versão 4 (IPv4), quarta versão do protocolo desenvolvido originalmente pela Advanced Research Projects Agency Network (ARPANET), o formato do datagrama, o formato do endereço e a escassez dos endereços.

PROPÓSITO

Compreender os conceitos básicos de endereçamento IP é fundamental para entender a forma como as redes se conectam. Além disso, esse conhecimento facilitará o desenvolvimento de projetos, a configuração e a manutenção de redes de computadores.

PREPARAÇÃO

Antes de iniciar este estudo, é recomendado possuir acesso à Internet por meio de um computador com os softwares Packet Tracer, da Cisco, e Wireshark instalados para realizar as simulações

propostas. Você também deve possuir em mãos lápis e caderno para confeccionar cálculos de rede que serão apresentados.

OBJETIVOS

MÓDULO 1

Reconhecer as características do payload e do endereçamento IPv4

MÓDULO 2

Esquematizar o endereçamento de redes e sub-redes IPv4

MÓDULO 3

Reconhecer as soluções temporárias para sanar o esgotamento do endereçamento IPv4

MÓDULO 4

Aplicar ferramentas de análise e troubleshooting do IPv4 e seus protocolos auxiliares

INTRODUÇÃO

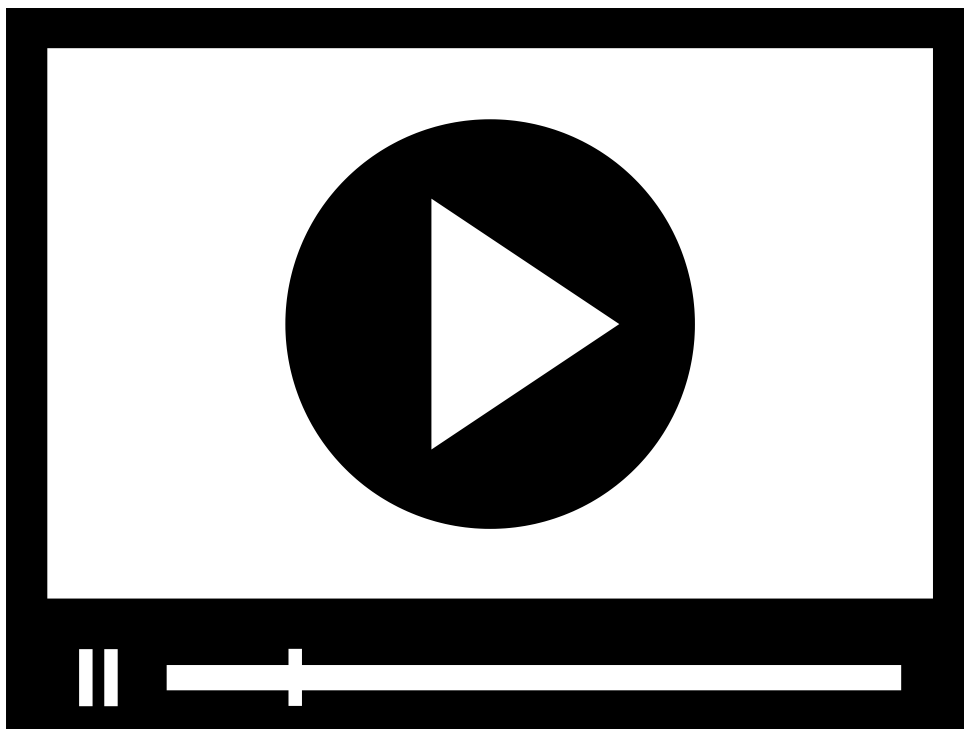
Neste conteúdo, aprenderemos sobre os conceitos fundamentais do principal protocolo empregado na camada de rede, conhecido como IPv4 (Internet Protocol version 4). Para isso, faremos

inicialmente a análise dos elementos componentes de sua estrutura e uma rápida apresentação dos tipos e classes de endereços IPv4.

Apresentaremos em seguida a relação entre o endereço IPv4 e a máscara de rede, que servirá de base para a esquematização de projetos de endereçamento de redes e sub-redes IPv4.

Além disso, identificaremos problemas relacionados ao esgotamento do número de endereços públicos IPv4, necessários ao funcionamento da Internet, e as respectivas soluções encontradas para contornar essas dificuldades.

Por fim, serão apresentados alguns protocolos de rede utilizados por ferramentas com características úteis à análise e troubleshooting de rede de dados. Com essas ferramentas, poderemos observar as características do protocolo IPv4 apresentadas no decorrer deste conteúdo.



O PROTOCOLO IPV4

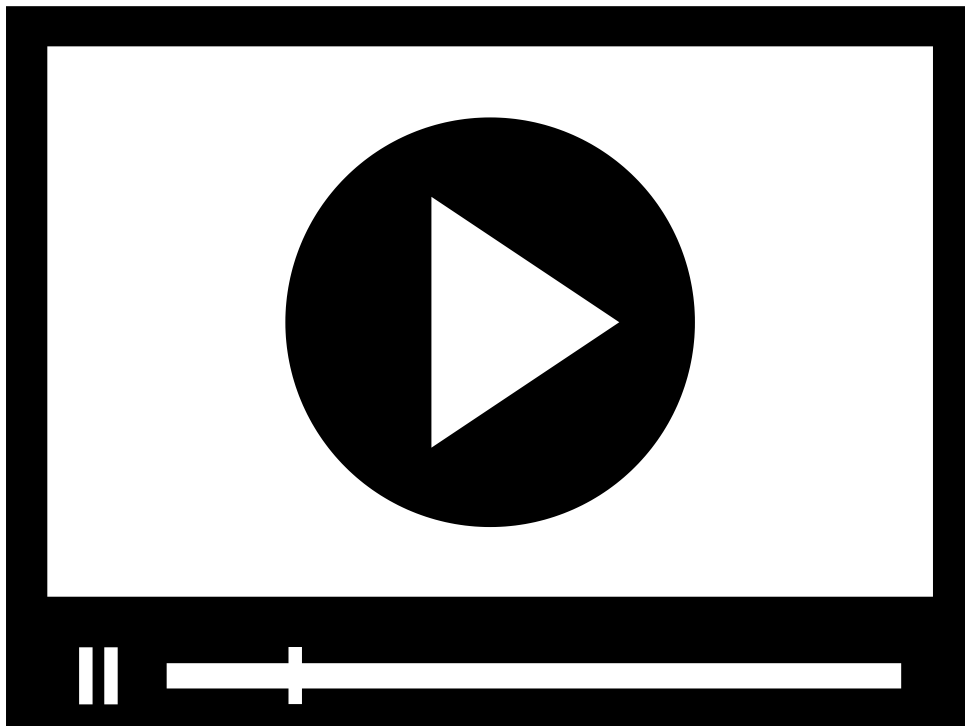
Antes de iniciar seus estudos nos módulos do nosso tema, vamos assistir a um vídeo? Nele, você poderá ver a importância do protocolo IPv4 para permitir a comunicação das aplicações de rede.



MÓDULO 1

🕒 Reconhecer as características do payload e do endereçamento IPv4

A ESTRUTURA DO DATAGRAMA IPV4



O DATAGRAMA IPV4

Neste vídeo, descomplicamos o intrincado formato do datagrama IPv4. Vamos apresentar cada campo, revelando a essência do protocolo que permitiu o roteamento através da internet.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Para melhor entendermos a estrutura do endereço IP versão 4 (IPv4), é necessário relembrar em qual camada do modelo OSI (Interconexão de Sistemas Abertos) ele está inserido.

O quadro a seguir evidencia que o protocolo IP está situado na camada de rede do modelo de OSI, sendo o IP versão 4 e o IP versão 6 (IPv6) os protocolos mais utilizados no processo de roteamento global.

Camadas de redes - Modelo OSI

Número	Nome	Principais protocolos
1	Física	
2	Enlace	
3	Rede	IPv4
		IPv6
4	Transporte	
5	Sessão	
6	Apresentação	
7	Aplicação	

⇒ Utilize a rolagem horizontal

Quadro: Modelo OSI de camadas de rede.

Elaborado por Isaac Santa Rita.

O Protocol Data Unit (PDU) da camada de rede é composto por um cabeçalho IP e as informações contidas na camada superior, normalmente a PDU da camada de transporte, aqui chamada de dados. Esse conjunto, cabeçalho IP e dados, recebe o nome de pacote IP, ou datagrama IP, como podemos observar na imagem a seguir:

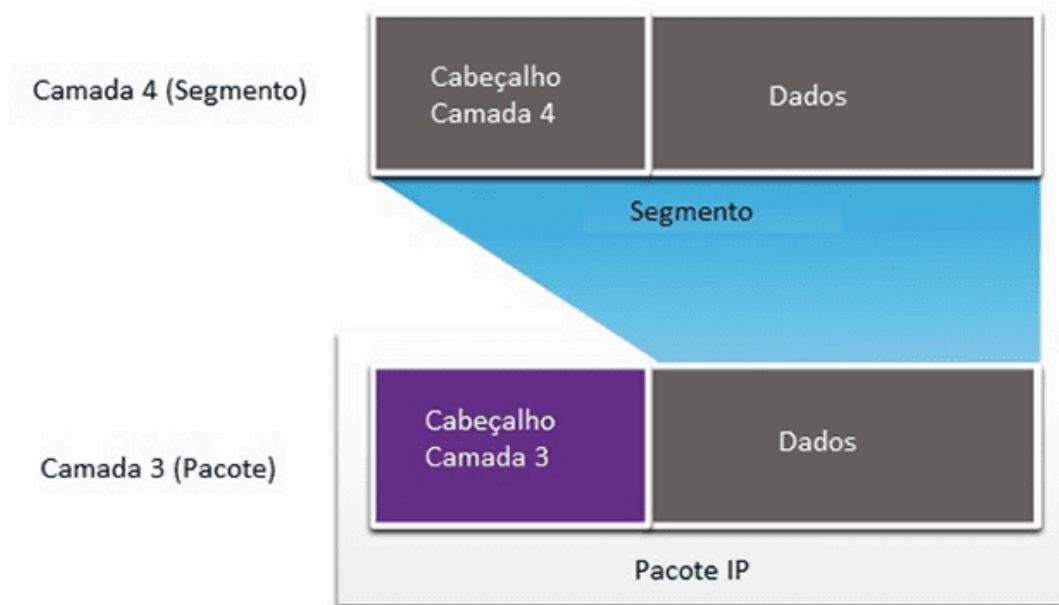


Imagem: Isaac Santa Rita

📷 Pacote IP.

O cabeçalho IP será examinado por todos os dispositivos de camada 3 durante a execução do processo de roteamento. É nele que essas máquinas buscarão o endereço de origem e de destino do pacote em questão, seja ele IPv4 ou IPv6.

📢 ATENÇÃO

O endereço IP, diferentemente do endereço de camada 2, permanece inalterado durante todo o processo de roteamento, desde sua origem até seu destino.

Byte 1		Byte 2		Byte 3		Byte 4	
Versão	Tamanho do Cabeçalho	Serviços Diferenciados		Tamanho Total			
Identificação				Flag	Deslocamento de Fragmento		
Tempo de Vida(TTL)		Protocolo		Checksum de cabeçalho			
Endereço IPv4 de Origem							
Endereço IPv4 de Destino							
Opções							

📷 Quadro: Cabeçalho IPv4.

Elaborado por Isaac Santa Rita

As funções dos campos que compõem o cabeçalho IPv4, ilustradas anteriormente, são definidas da seguinte forma:

VERSÃO

É composto por 4 bits e indicam a versão do protocolo IP (valor 4 para o IPv4 e 6 para o IPv6). É por meio desse número que os roteadores podem definir, por exemplo, qual a tabela de roteamento mais apropriada a se utilizar.

TAMANHO DO CABEÇALHO

É composto por 4 bits que indicam o número de bytes do cabeçalho. O tamanho do cabeçalho IPv4 é variável, pois o campo Opções, presente no cabeçalho IPv4 e demonstrado anteriormente, possui tamanho variável dependendo da informação que carrega. Entretanto, como a maioria dos cabeçalhos IPv4 possuem o campo Opções vazio, o campo Tamanho do cabeçalho normalmente é de 20 bytes.

SERVIÇOS DIFERENCIADOS

Esse campo possui a capacidade de priorizar os datagramas IPv4 conforme suas necessidades, como aqueles que necessitam de baixo atraso, alto fluxo ou confiabilidade. Essa característica é útil para aplicações com necessidades de Qualidade de Serviço (Quality of Service - QoS), por exemplo, dar celeridade ao processamento e encaminhamento de pacotes que contêm informações de voz sobre IP (Voice over IP - VoIP), devido às necessidades de latência dessa aplicação.

TAMANHO TOTAL

Define o tamanho total do pacote em bytes, incluindo o cabeçalho e o campo de dados. Por ser um campo de 16 bits, possui a capacidade de informar tamanho máximo teórico de até 65.535 bytes, entretanto, não é comum pacotes maiores que 1.500 bytes.

IDENTIFICAÇÃO, FLAG E DESLOCAMENTO DE FRAGMENTO

Esses campos estão relacionados à fragmentação do pacote IPv4, necessárias quando a camada de enlace de dados possui tamanho máximo de transporte (Maximum Transport Unit - MTU) incapaz de suportar as informações contidas em um determinado datagrama, fazendo-se necessária a divisão das informações em partes.

TEMPO DE VIDA (TIME TO LIVE – TTL)

Esse campo de 8 bits possui a capacidade de impedir que pacotes sejam indefinidamente roteados, a fim de evitar um problema de loop de roteamento. Ele representa o número máximo de roteadores (saltos) que um pacote pode efetuar antes de ser descartado.

PROTOCOLO

Referência ao protocolo de camada superior que o datagrama IP encapsula. O valor 6 indica que o protocolo da camada de transporte é o TCP (Transmission Control Protocol), já o valor 17, indica que o protocolo da camada de transporte é o UDP (User Datagram Protocol).

CHECKSUM DE CABEÇALHO

Esse campo é utilizado para verificar a integridade do cabeçalho do datagrama IPv4 recebido. Essa verificação é realizada tratando cada 2 bytes do cabeçalho IPv4 como se fosse um número único e somando esses números usando o complemento aritmético de 1, cujo detalhamento está na RFC 791. Cada roteador irá realizar essa verificação para cada datagrama IPv4 recebido e descartará o pacote caso a verificação calculada não seja igual ao valor recebido no campo Checksum de cabeçalho.

ENDEREÇO IPV4 DE ORIGEM

Esse campo contém os 32 bits que compõem a informação de endereço IPv4 de origem.

ENDEREÇO IPV4 DE DESTINO

Esse campo contém os 32 bits que compõem a informação de endereço IPv4 de destino.

OPÇÕES

Esse campo permite que o cabeçalho IPv4 seja alongado para comportar informações de segurança, marcadores de roteamento etc. É o campo que altera o tamanho do cabeçalho, o que confere uma imprevisibilidade ao ponto de início dos dados.

Acerca do funcionamento do campo TTL e dos loops de rede, realiza-se um decremento do valor desse campo por cada roteador que o pacote atravessa durante o processo de roteamento. O TTL

pode possuir um valor inicial máximo de 255 e, caso ele atinja o valor zero durante esse processo, o pacote será descartado, por considerar-se que ele não mais atingirá seu destino. Com isso, evita-se que ele fique eternamente na rede.

❓ VOCÊ SABIA

Loops de rede, normalmente causados por problemas de roteamento, poderiam levar os roteadores à exaustão de processamento. Entretanto, o campo TTL descarta os pacotes em loop, aliviando a sobrecarga dos roteadores até que uma solução definitiva seja realizada.

O campo Checksum de cabeçalho (Header Checksum) é confeccionado pelo remetente, por meio de um algoritmo matemático utilizando as informações que compõem apenas o cabeçalho IPv4. Dessa forma, toda vez que o pacote é analisado por outro equipamento, utilizando-se do mesmo algoritmo matemático, verifica-se a integridade daquele cabeçalho IPv4.

Cada roteador, ao receber um datagrama, irá verificar se o valor carregado no campo Checksum é igual ao que ele calculou. Os roteadores, em geral, descartam os datagramas nos quais foram detectados erros.

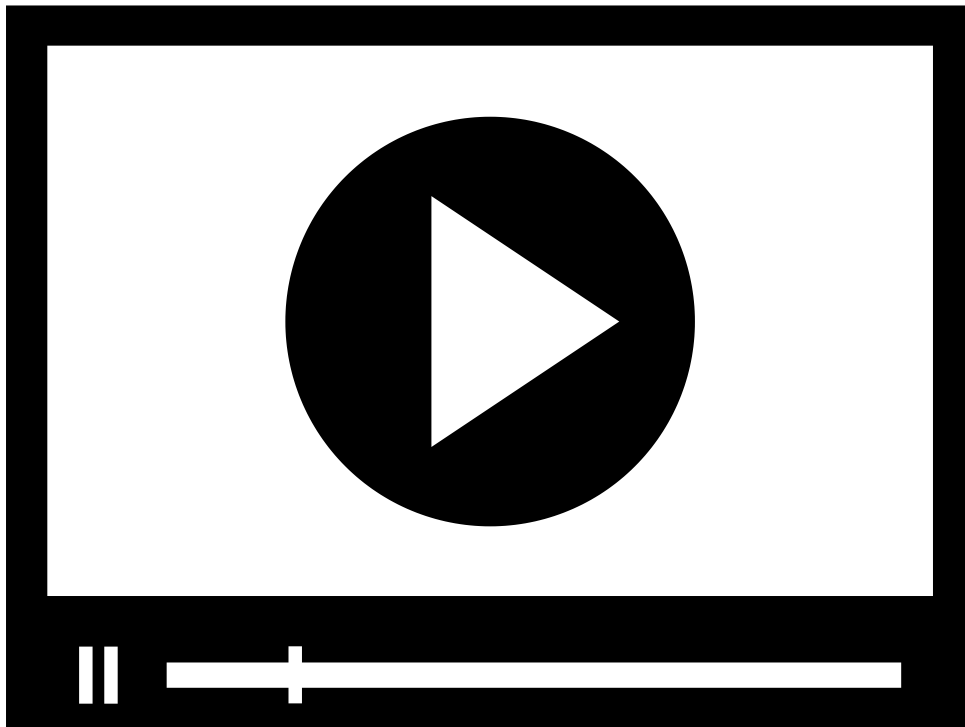
A cada roteador, o campo TTL é modificado, assim como o campo Opções, caso exista, também pode ser modificado. É necessário que, a cada roteador, os valores sejam recalculados e o datagrama IP carregue esses novos valores.

A ESTRUTURA DO ENDEREÇO IPV4

A INFORMAÇÃO DO ENDEREÇO IPV4 DE ORIGEM E DE DESTINO É A INFORMAÇÃO MAIS IMPORTANTE CONTIDA NO CABEÇALHO IPV4, É POR MEIO DELAS QUE O PACOTE É ENCAMINHADO ATÉ SEU DESTINO.

O IPv4 de origem identifica o remetente do pacote, ou seja, permite ao destino identificar o endereço de origem do pacote e, conseqüentemente, confeccionar a resposta ao mesmo, invertendo, no pacote de resposta, a ordem dos IPv4 de origem e destino.

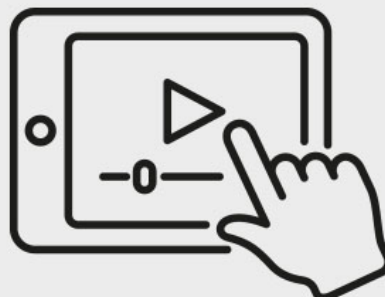
FORMATO DO ENDEREÇO IPV4



O ENDEREÇO IPV4

Neste vídeo, desvendamos a estrutura do endereço IPv4, apresentando as partes que ele é composto e seu papel no processo de roteamento.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Entendida a importância do endereço IPv4 de origem e de destino, **vale observar que ambos possuem 32 bits**, o que permite endereçamentos numéricos compreendidos entre 0 (zero) e 4.294.967.295 ($2^{32}-1$).

A leitura de um endereço IPv4 nesse formato, entretanto, não seria muito agradável. Assim, optou-se por realizar a divisão desses 32 bits em 4 grupos de 8 bits (4 bytes) que, quando transformados para a base decimal, apresentam uma forma mais humanizada para compreendermos o endereço IPv4.

Para exemplificar, observaremos a representação de dois endereços IPv4 a seguir:

Apresentação do IPv4 (representação decimal)				
IPv4 (32 bits)	110000001010100000000000100000010			
IPv4 (4 x 8 bits)	11000000	10101000	00000001	00000010
IPv4 (4 x decimal)	192	168	1	2
IPv4 (apresentação final)	192.168.1.2			

⇒ Utilize a rolagem horizontal

Tabela: Apresentação do IPv4 1/2.

Elaborada por Isaac Santa Rita.

Apresentação do IPv4 (representação decimal)				
IPv4 (32 bits)	11001000000101000111100000000001			
IPv4 (4 x 8 bits)	11001000	00010100	01111000	00000001
IPv4 (4 x decimal)	200	20	120	1
IPv4 (apresentação final)	200.20.120.1			

⇒ Utilize a rolagem horizontal

Tabela: Apresentação do IPv4 2/2.

Elaborada por Isaac Santa Rita.

Uma vez observado o processo de apresentação de um IPv4, fica fácil entender o processo de conversão do IPv4 nos bits que o representam. Para isso, basta transformar a representação decimal de cada octeto em sua respectiva representação binária e, por fim, agrupá-los.

Observe o exemplo do processo de transformação de um IPv4 nos bits que o compõem:

Apresentação do IPv4 (representação binária)				
IPv4 (apresentação final)	172.31.4.1			
IPv4 (4 x decimal)	172	31	4	1
IPv4 (4 x 8 bits)	10101100	00011111	00000100	00000001
IPv4 (32 bits)	10101100000111110000010000000001			

⇒ Utilize a rolagem horizontal

Tabela: Apresentação do IPv4 binário.

Elaborada por Isaac Santa Rita.

PARTES DO ENDEREÇO IPV4

O entendimento da estrutura do endereço IPv4 está intimamente ligado ao entendimento da própria rede de computadores, que nada mais é do que um conjunto de dispositivos conectados por intermédio de um sistema de comunicações, facilitador da troca de dados entre esses equipamentos.

ATENÇÃO

Isso posto, o endereço IPv4 de um dispositivo pode ser dividido em duas partes, uma relacionada ao endereço da rede, comum a todos os dispositivos que pertencem àquela rede, e outra relacionada à identificação desse dispositivo dentro da rede de dados.

A parte relacionada ao endereço comum dos dispositivos em uma rede de dados recebe o nome de endereço de rede ou prefixo de rede, e a parte relacionada à identificação do dispositivo dentro dessa rede recebe o nome de endereço de máquina ou endereço de host. A seguir, essa divisão é ilustrada:

	Endereço de rede / Prefixo de rede			End. de máquina / End. de host
	10	1	12	5
Endereço IPv4	00001010	00000001	00001100	00000101

⇒ Utilize a rolagem horizontal

Tabela: Endereço de rede e de máquina.

Elaborada por Isaac Santa Rita.

O dispositivo com o endereço IPv4 apresentado, IPv4 10.1.12.5, está inserido numa rede de dados na qual todos os demais dispositivos também possuem, na composição de seu endereço IPv4, o mesmo prefixo de rede, o 10.1.12.

COMENTÁRIO

Para que seja inserido um outro dispositivo nessa mesma rede de dados, além de possuir o mesmo prefixo de rede, esse novo equipamento precisa possuir um identificador único de máquina, ou seja, um endereço de host diferente dos demais equipamentos presentes naquela rede até então.

A partir do que foi exposto, os IPv4 10.1.12.1, 10.1.12.6, 10.1.12.200 e 10.1.12.254 são possíveis endereços de outros dispositivos presentes na rede apresentada.

EXERCÍCIO

Agora é a sua vez! Que tal testar cada um dos endereços? Para isso, responda ao exercício a seguir:

1. Para sintetizar o conhecimento apresentado até aqui, indique as opções que apresentam máquinas dentro da mesma rede lógica que a máquina com IPv4 apresentado a seguir.

	Endereço de rede /			End. de máquina /
	Prefixo de rede			End. de host
Endereço IPv4	10	8	5	1
	00001010	00001000	00000101	00000001

⇐ Utilize a rolagem horizontal

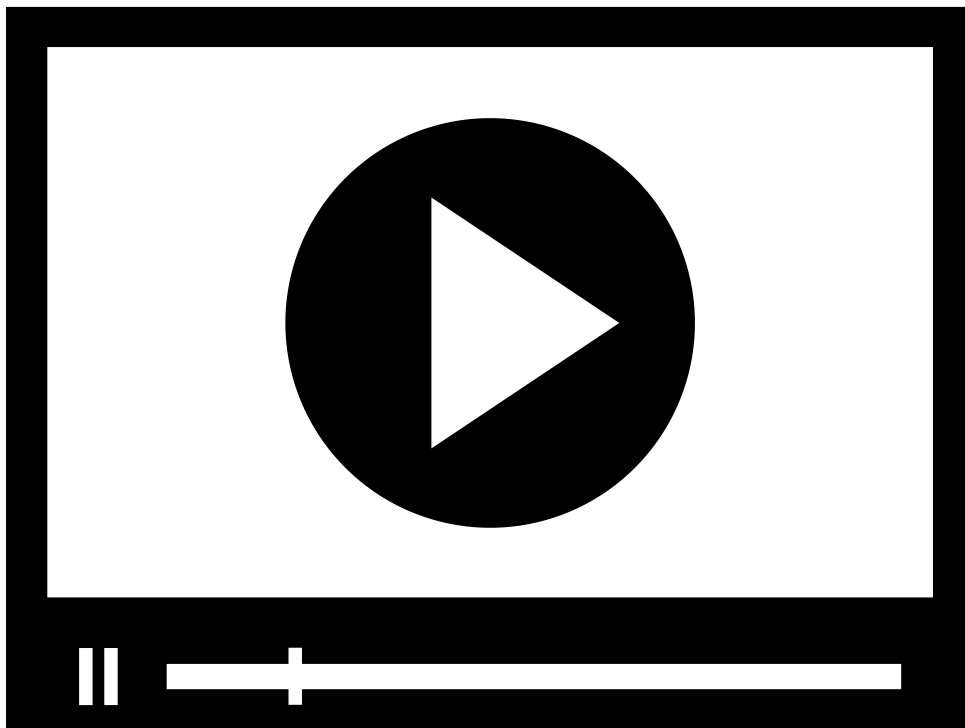
Tabela: Endereço de rede e de máquina.

Elaborada por Isaac Santa Rita.

- a) 10.8.6.1
- b) 10.8.5.2
- c) 10.5.8.15
- d) 10.8.5.255
- e) 10.0.0.1
- f) 10.5.10.10

Observando o endereço informado, foi identificado que os três primeiros bytes pertencem ao prefixo de rede e o último byte pertence ao endereço do host. Portanto, para que outros endereços pertençam à mesma rede lógica, o prefixo de rede deve ser igual, ou seja, os três primeiros bytes devem ser iguais. Assim, as máquinas que estão dentro da mesma rede lógica são as opções B e D.

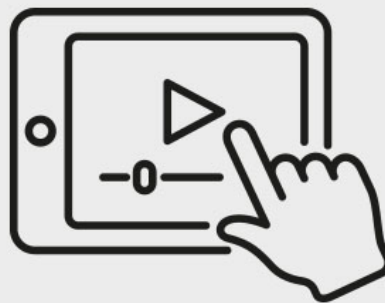
A MÁSCARA DE SUB-REDE



DECIFRANDO A MÁSCARA DE SUB-REDE

Neste vídeo, desmistificamos a função crucial da máscara de sub-rede no endereçamento IPv4. Uma análise direta dos bits que moldam a segmentação de redes, essencial para entender a eficiência da comunicação na era digital.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Como vimos anteriormente, o endereço IPv4 é composto por uma parte referente ao endereço de rede e outra ao endereço de host.

Nos perguntamos, então, quem é o responsável pela delimitação entre a parte de rede e a parte do host.

RESPOSTA

A resposta a essa pergunta é a máscara de sub-rede. É ela quem determina onde é o ponto de divisão entre essas duas partes. Por consequência, é a responsável por determinar o tamanho de uma rede de computadores, pois quanto maior for a parte do endereço de máquina, maior será a quantidade de IPv4 (máquinas) disponíveis para essa rede.

Para exemplificar, observe a apresentação a seguir de dois IPv4 em duas redes diferentes. Na rede 1, existem 16 bits que compõem o prefixo de rede, deixando outros 16 bits para a parte dos hosts. Já na rede 2, são 8 bits utilizados pelo prefixo de rede, restando 24 bits para a parte de hosts.

Endereço de rede 1		Endereço de máquina 1	
172	16	0	1
101010100	00010000	00000000	00000001

Endereço de rede 2		Endereço de máquina 2	
10	0	0	1
11000000	00000000	00000000	00000001

⇒ Utilize a rolagem horizontal

Tabela: Máscara de sub-rede.

Elaborada por Isaac Santa Rita.

Assim, observada a premissa de que o prefixo de rede é fixo, fica disponível para cada uma das redes apresentadas as seguintes quantidades de IPv4:

REDE 1

$$2^{16} = 65.536 \text{ IPv4}$$

REDE 2

$2^{24} = 16.777.216$ IPv4

Com isso, observamos que a máscara de sub-rede, que possui as mesmas características do IPv4, é capaz de determinar a quantidade de máquinas que podem ser inseridas dentro de uma rede de dados por meio da delimitação do tamanho do prefixo de rede.

Essa delimitação é realizada mediante a quantidade de bits “1” presentes na parte mais significativa da máscara de redes. A seguir, são apresentadas algumas máscaras de sub-rede e suas respectivas identificações.

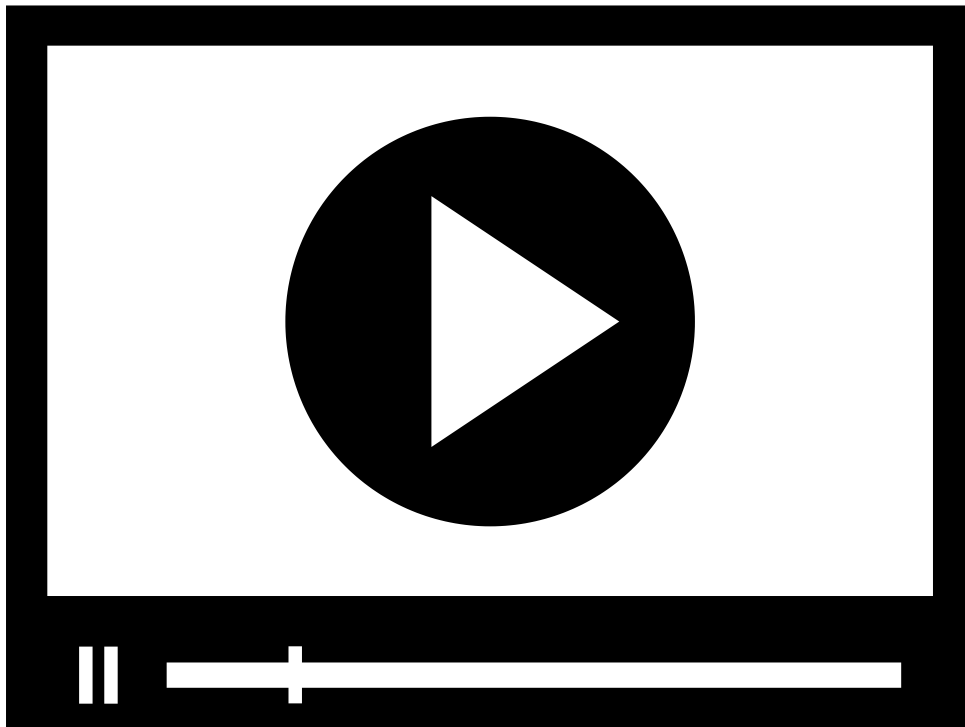
Endereço de 32 bits de máscara de sub-rede	Identificação da máscara de sub-rede
11111111.00000000.00000000.00000000	255.0.0.0
11111111.11111111.00000000.00000000	255.255.0.0
11111111.11111111.11111111.00000000	255.255.255.0
11111111.11111111.11111111.10000000	255.255.255.128
11111111.11111111.11111111.11000000	255.255.255.192
11111111.11111111.11111111.11110000	255.255.255.240
11111111.11111111.11111111.11111100	255.255.255.252

⇒ Utilize a rolagem horizontal

Tabela: Identificação de máscara de sub-rede.

Elaborada por Isaac Santa Rita.

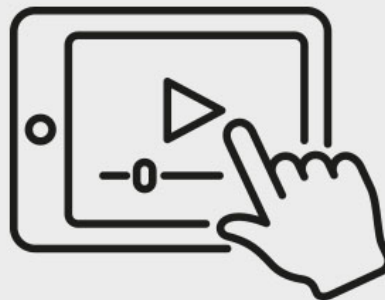
ENDEREÇOS ESPECIAIS



ENDEREÇOS ESPECIAIS NO IPV4

Neste vídeo, exploramos os endereços de rede e broadcast no IPv4. Compreenda o papel crucial desses números na comunicação de dados, desvendando a arquitetura que sustenta a conectividade digital em redes locais e globais.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



ENDEREÇO DE REDE

Quando desejamos nos referir a uma determinada rede utilizando uma numeração, devemos fazê-lo pelo endereço de rede daquela rede. A identificação do endereço de rede é realizada por meio da operação lógica AND bit-a-bit entre o endereço IPv4 em questão e a respectiva máscara de rede. Veja, a seguir, o resultado da operação lógica AND bit-a-bit:

Operação lógica AND		
Bit A	Bit B	AND
0	0	0
0	1	0
1	0	0
1	1	1

⇒ Utilize a rolagem horizontal

Tabela: Operação lógica AND.
Elaborada por Isaac Santa Rita.

Em seguida, podemos observar a obtenção do endereço de rede 192.168.1.0, por intermédio da operação AND bit-a-bit descrita anteriormente, para o conjunto IPv4/máscara 192.168.1.1/255.255.255.0 de um dispositivo pertencente a essa rede.

IPv4 (192.168.1.1)	192	168	1	1
	11000000	10101000	00000001	00000001
Máscara de sub-rede (255.255.255.0)	255	255	255	0
	11111111	11111111	11111111	00000000
	OPERAÇÃO AND BIT-A-BIT			

Endereço de rede	192	168	1	0
	11000000	10101000	00000001	00000000

⇒ Utilize a rolagem horizontal

Tabela: Obtenção do endereço de rede.

Elaborada por Isaac Santa Rita.

Como o IPv4 de rede é o IP que dá nome para a rede de dados, ele não pode ser utilizado em nenhum dispositivo nessa rede. Ele é normalmente utilizado no processo de roteamento que levará os pacotes até essa rede de dados.

EXERCÍCIO

Vamos testar seus conhecimentos mais uma vez? Responda ao exercício proposto:

2. Para sintetizar o conhecimento apresentado até aqui, determine o IP da rede que contém uma máquina com o grupo IPv4/máscara 192.168.10.30/255.255.255.248.

Para identificar a que rede o endereço pertence, é necessário realizar a operação AND, bit a bit, entre o endereço e a máscara de sub-rede. A tabela abaixo detalha a operação, obtendo o resultado 192.168.10.24 para o endereço da Rede.

IPv4 (192.168.1.1)	192	168	10	30
	11000000	10101000	00001010	00011110
Máscara de sub-rede (255.255.255.0)	255	255	255	248
	11111111	11111111	11111111	11111000
OPERAÇÃO AND BIT-A-BIT				

Endereço de rede	192	168	10	24
	11000000	10101000	00001010	00011000

⇒ Utilize a rolagem horizontal

Tabela: Obtenção do endereço de rede.

Elaborada por Isaac Santa Rita.

ENDEREÇO DE BROADCAST

O endereço de broadcast é um endereço IPv4 que permite que a informação seja enviada para todas as máquinas presentes numa rede de dados.

Para essa finalidade, foi reservado o último endereço de cada rede. Por isso, assim como o endereço de rede, o último endereço IPv4 de cada rede, que é o endereço de broadcast, também não pode ser atribuído a nenhum dispositivo.

Utilizando o IPv4/máscara do exemplo anterior, 10.1.15.10/255.255.252.0, determinaremos qual é o IPv4 de broadcast dessa rede.

Para isso, devemos preservar o prefixo de rede e preencher os bits da parte do endereço de máquina, evidenciado em vermelho, com bits 1, conforme apresentado a seguir.

Endereço de rede	10	1	12	0
	00001010	00000001	00001100	00000000
Endereço de broadcast	10	1	15	255
	00001010	00000001	00001111	11111111

⇒ Utilize a rolagem horizontal

Tabela: Obtenção do endereço de broadcast.

Elaborada por Isaac Santa Rita.

Verificamos, assim, que o endereço de broadcast para a rede 10.1.12.0/255.255.252.0 é o IPv4 10.1.15.255.

EXERCÍCIO

Agora é com você. Teste seus conhecimentos respondendo ao exercício:

3. Para sintetizar o conhecimento apresentado até aqui, determine o IP de broadcast da rede que contém uma máquina com o grupo IPv4/máscara 192.168.10.30/255.255.255.248.

Para identificar o endereço de broadcast, que é o último da sub-rede, devemos identificar os bits de máquina, marcados em vermelho, e colocar todos valendo 1. A tabela abaixo detalha a operação, obtendo o resultado 192.168.10.31.

IPv4 (192.168.1.1)	192	168	10	30
	11000000	10101000	00001010	00011110
Máscara de Sub rede (255.255.255.0)	255	255	255	248
	11111111	11111111	11111111	11111000
Endereço de Broadcast	192	168	10	31
	11000000	10101000	00001010	00011111

⇒ Utilize a rolagem horizontal

Tabela: Obtenção do endereço de broadcast.

Elaborada por Isaac Santa Rita.

ENDEREÇO DE HOST

Uma vez entendido o motivo pelo qual não se pode utilizar os endereços de rede e de broadcast para configuração de dispositivos numa rede, restam os demais endereços para compor a configuração dos equipamentos. Para esses endereços, utilizamos a nomenclatura de endereços de host ou endereços úteis.

É fácil identificar a máxima quantidade de equipamentos que podem fazer parte de uma determinada rede.

★ EXEMPLO

Como exemplo, vamos determinar a quantidade de máquinas suportadas pela rede 10.1.12.0/255.255.252.0.

Bits 1 no prefixo de rede = 22

Bits na parte de hosts = 10

N.º total de IPv4 = $2^{10} = 1024$

N.º máximo de máquinas = N.º total de IPv4 – IPv4 de rede – IPv4 de broadcast

N.º máximo de máquinas = $1024 - 1 - 1 = 1024 - 2 = 1022$ máquinas

N.º máximo de máquinas = $2^{(32-N)} - 2$

Em palavras, numa rede com máscara de rede 255.255.252.0, é possível a colocação de 1.022 máquinas, incluindo o equipamento roteador que, normalmente, é o default gateway da rede.

EXERCÍCIO

Vamos testar seus conhecimentos mais uma vez? Então responda ao exercício proposto:

4. Dentre os IPv4 apresentados abaixo, indique aqueles que podem ser inseridos na rede 192.168.10.24/255.255.255.248.

192.168.10.24

192.168.10.25

192.168.10.26

192.168.10.29

192.168.10.30

192.168.10.31

Como já vimos anteriormente, para que um endereço pertença a uma sub-rede é necessário que ele possua o mesmo prefixo de rede. Para podermos descobrir é necessário realizar a operação AND bit a bit, de cada endereço informado, com a máscara de sub-rede. Se o resultado da operação for o prefixo de rede informado, ele poderá ser utilizado por uma máquina.

Vamos fazer o exemplo b) 192.168.10.25? Veja na tabela abaixo os endereços na forma binária e o resultado da operação AND. Como o resultado é 192.168.10.24, o endereço pertence a sub-rede e pode ser utilizado, assim como as opções C, D e E.

As opções a) e f), apesar de darem como resultado na operação AND o endereço 192.168.10.24, não podem ser utilizadas porque são, respectivamente, o endereço da rede e o endereço de broadcast.

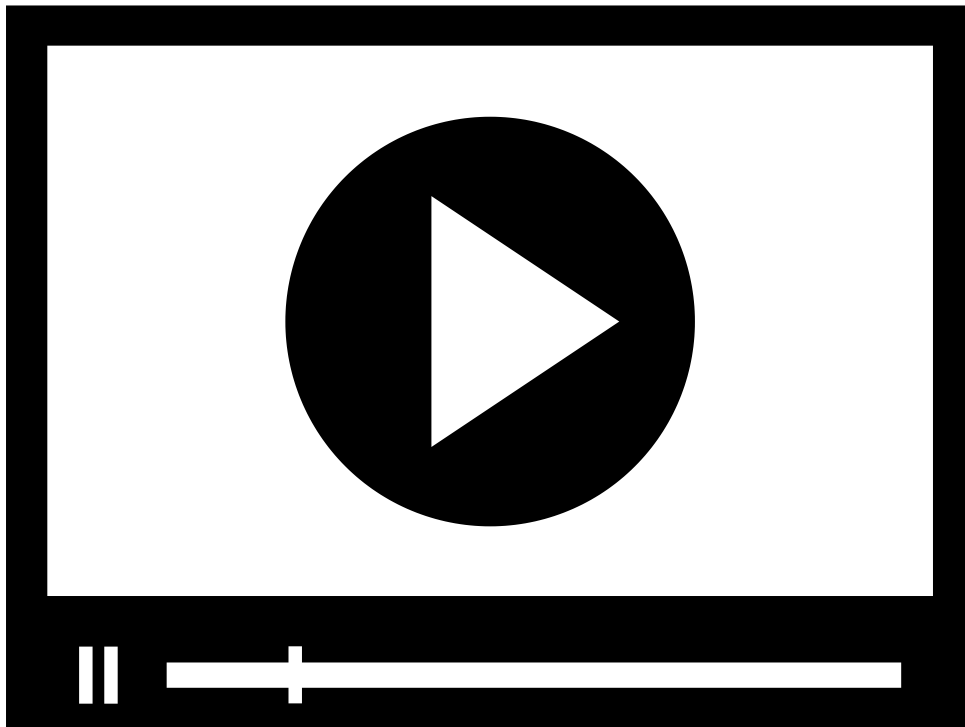
IPv4 (192.168.1.1)	192	168	10	25
	11000000	10101000	00001010	00011001
Máscara de sub-rede (255.255.255.0)	255	255	255	248
	11111111	11111111	11111111	11111000
	OPERAÇÃO AND BIT-A-BIT			
Endereço de rede	192	168	10	24
	11000000	10101000	00001010	00011000

⇐ Utilize a rolagem horizontal

Tabela: Obtenção do endereço de broadcast.

Elaborada por Isaac Santa Rita.

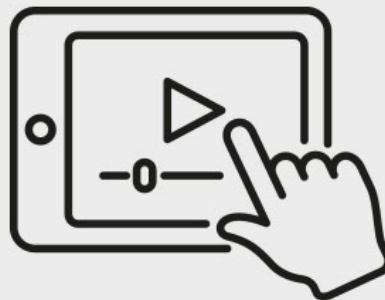
ENDEREÇOS CLASSIFICADOS



CLASSES DE ENDEREÇO IPV4

Neste vídeo, descomplicamos as classes de endereço no IPv4. Descubra como a divisão nas classes A, B e C influencia a estrutura da rede, fornecendo a base para uma comunicação eficiente na internet.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



A RFC 790, de 1981, definiu cinco classes de endereçamento IPv4. Elas abrangem toda a faixa de IPv4, e a ideia inicial era a alocação das faixas de endereço respeitando as classes disponíveis, fato que ficou conhecido como endereçamento classfull (classe cheia). A seguir, apresentamos a distribuição dos endereços IPv4 em suas respectivas faixas de rede.

DISTRIBUIÇÃO DE ENDEREÇOS EM CLASSES

Classe	1º octeto	Faixa de rede / IP	Finalidade: redes com máscara
A	0XXXXXX	0.0.0.0/8 até 127.0.0.0/8	255.0.0.0
B	10XXXXXX	128.0.0.0/16 até 191.255.0.0/16	255.255.0.0
C	110XXXXX	192.0.0.0/24 até 223.255.255.0/24	255.255.255.0
D	1110XXXX	224.0.0.0 até 239.255.255.255	Endereços multicast
E	1111XXXX	240.0.0.0 até 255.255.255.255	Uso experimental

⇒ Utilize a rolagem horizontal

Tabela: Distribuição de endereços IPv4 em classes.

Elaborada por Isaac Santa Rita.

VERIFICANDO O APRENDIZADO

1. O PROTOCOLO IPV4 É UM DOS PROTOCOLOS MAIS UTILIZADOS GLOBALMENTE. PARA A REPRESENTAÇÃO BINÁRIA A SEGUIR, APRESENTE O ENDEREÇO IPV4 CORRESPONDENTE:

IPV4 (BINÁRIO) = 11110000.10101010.00001111.11001100

- A) 224.170.240.11
- B) 240.170.15.204
- C) 200.160.15.11
- D) 224.32.47.0
- E) 240.150.15.202

2. OS ENDEREÇOS IPV4 NORMALMENTE SÃO APRESENTADOS NA SUA FORMA DECIMAL. OS ROTEADORES, ENTRETANTO, ANALISAM A SUA FORMA BINÁRIA, COM O OBJETIVO DE DETERMINAR O MELHOR CAMINHO PARA O DESTINO DESEJADO. DENTRE AS ALTERNATIVAS A SEGUIR, INDIQUE A QUE REPRESENTA A COMPOSIÇÃO BINÁRIA DO IP 172.16.10.10.

- A) 11000000.10101000.10100000. 10100000



Atenção! Para visualização completa da equação utilize a rolagem horizontal

- A)
- B) 10101010.10101000.10000001. 10000001



Atenção! Para visualização completa da equação utilize a rolagem horizontal

- B)
- C) 10101100.00100000.00001010.00001010



Atenção! Para visualização completa da equação utilize a rolagem horizontal

- C)
- D) 10101100.00010000.10100000.10100000



Atenção! Para visualização completa da equação utilize a rolagem horizontal

- D)
- E) 10101100.00010000.00001010.00001010



Atenção! Para visualização completa da equação utilize a rolagem horizontal

- E)

GABARITO

1. O protocolo IPv4 é um dos protocolos mais utilizados globalmente. Para a representação binária a seguir, apresente o endereço IPv4 correspondente:

IPv4 (Binário) = 11110000.10101010.00001111.11001100

A alternativa **"B "** está correta.

O endereço IP binário apresentado possui seus octetos apresentados na resposta B. Para encontrar o endereço IP, basta converter a representação binária para a representação decimal, separando de 8 em 8 bits.

2. Os endereços IPv4 normalmente são apresentados na sua forma decimal. Os roteadores, entretanto, analisam a sua forma binária, com o objetivo de determinar o melhor caminho para o destino desejado. Dentre as alternativas a seguir, indique a que representa a composição binária do IP 172.16.10.10.

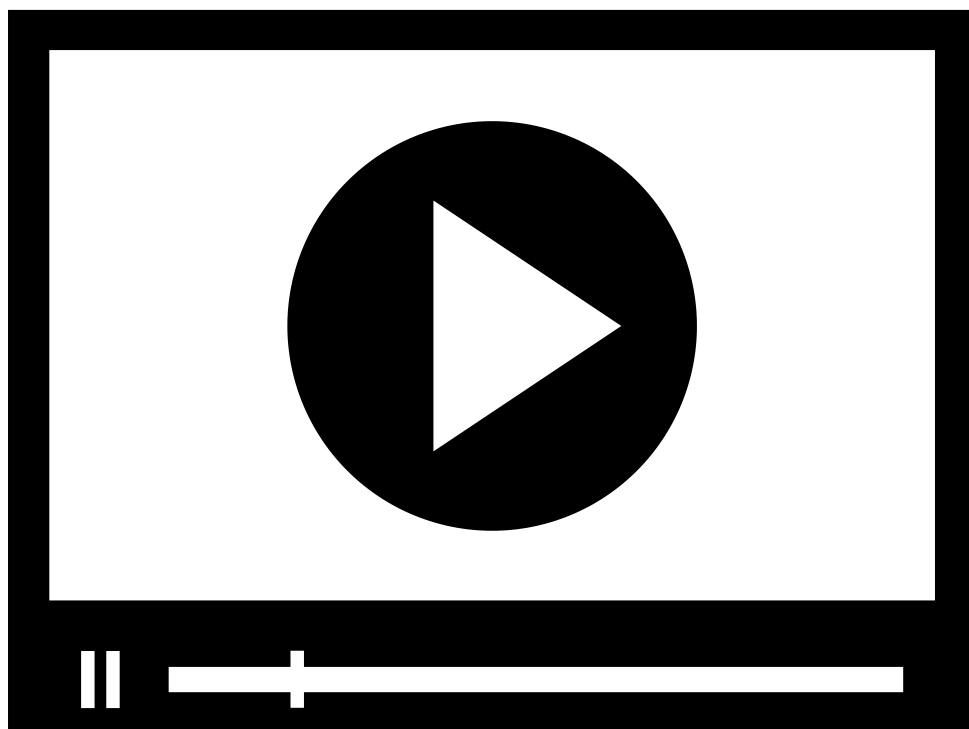
A alternativa **"E "** está correta.

Para encontrar os octetos que representam o IPv4 da questão, é necessário transformá-los em sua forma binária, convertendo para bits. Obtêm-se, assim, a composição da alternativa E.

MÓDULO 2

⦿ **Esquematizar o endereçamento de redes e sub-redes IPv4**

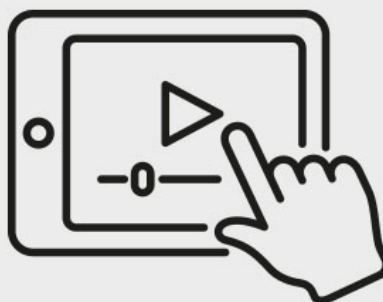
SEGMENTAÇÃO DE REDE



SEGMENTAÇÃO DE REDES IPV4

Neste vídeo, exploramos a Segmentação de Rede e as técnicas CIDR e VLSM. Descubra como essas práticas fundamentais aprimoram a gestão de endereços, otimizando a comunicação e facilitando a administração de redes.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



As redes de classe cheia, classfull, caíram em desuso devido ao grande desperdício de IPv4 e à necessidade de reduzir os impactos negativos de redes muito grandes, como a difusão excessiva de pacotes broadcast, entre outros.

Nesse sentido, surgiu a necessidade de ajuste do tamanho das redes às suas reais demandas de endereços, sem prejuízo ao processo de roteamento.

A esse conceito damos o nome de Classless Inter Domain Routing (CIDR), que nada mais é do que a utilização de redes com máscaras variadas, sem classe (classless) aliada à manutenção do processo de roteamento.

Ao processo de ajuste de máscaras às demandas de endereçamento, damos o nome de Variable Length Subnet Mask (VLSM), que nos permite trabalhar com redes das mais diversas máscaras sem observar o uso imperativo das classes de rede “A”, “B” e “C”.

A partir desse conceito, uma rede com necessidade de 20 endereços IPv4 deixou de utilizar uma rede classe C (255.255.255.0), com capacidade de hospedar 254 máquinas, e passou a utilizar, por exemplo, uma rede com máscara 255.255.255.224, com capacidade de hospedar 30 (2^5-2) máquinas.

COMENTÁRIO

Para facilitar o entendimento do processo VLSM, podemos utilizar a contagem do número de bits 1 presentes na máscara de sub-redes para identificá-la e utilizar a notação “/ (Quantidade de bits 1)”.

A fim de entendermos melhor o processo VLSM, apresentamos a seguir três exemplos de segmentação da rede 192.168.1.0/24 em grupos de redes com outras máscaras, já utilizando a notação de máscara de sub-rede citada:

SEGMENTAÇÃO DA REDE 192.168.1.0/24

Exemplo	Rede original	Segmentação	Bits (último octeto)
1	192.168.1.0/24	192.168.1.0/25	00000000
		192.168.1.128/25	10000000
2	192.168.1.0/24	192.168.1.0/26	00000000
		192.168.1.64/26	01000000
		192.168.1.128/26	10000000

SEGMENTAÇÃO DA REDE 192.168.1.0/24

		192.168.1.192/26	11000000
3	192.168.1.0/24	192.168.1.0/27	00000000
		192.168.1.32/27	00100000
		192.168.1.64/27	01000000
		192.168.1.96/27	01100000
		192.168.1.128/27	10000000
		192.168.1.160/27	10100000
		192.168.1.192/27	11000000
		192.168.1.224/27	11100000

⇒ Utilize a rolagem horizontal

Tabela: Divisão da rede 192.168.1.0/24.

Elaborada por Isaac Santa Rita.

Nesse processo, é importante observar que a divisão da rede 192.168.1.0/24 preserva os bits do prefixo dessa rede, realizando apenas o empréstimo de bits da parte de host às novas máscaras. Para evidenciar, vejamos em seguida a composição dos bits da divisão da rede 192.168.1.0/24 nas redes /27.

Rede original	Prefixo de rede original (bits)	Empréstimo (bits)	Parte de host (bits)	Sub-rede /27 derivada
192.168.1.0/24	11000000.10101000.00000001.	000	00000	192.168.1.0/27

Rede original	Prefixo de rede original (bits)	Empréstimo (bits)	Parte de host (bits)	Sub-rede /27 derivada
	11000000.10101000.00000001.	001	00000	192.168.1.32/27
	11000000.10101000.00000001.	010	00000	192.168.1.64/27
	11000000.10101000.00000001.	011	00000	192.168.1.96/27
	11000000.10101000.00000001.	100	00000	192.168.1.128/27
	11000000.10101000.00000001.	101	00000	192.168.1.160/27
	11000000.10101000.00000001.	110	00000	192.168.1.192/27
	11000000.10101000.00000001.	111	00000	192.168.1.224/27

⇒ Utilize a rolagem horizontal

Tabela: Composição binária de sub-redes.

Elaborada por Isaac Santa Rita.

Uma vez observada possibilidade de uma rede ser decomposta no somatório de sub-redes menores, apresentaremos como pode ser realizada a decomposição de uma rede /16 emprestando bits para a composição de novas sub-redes.

Cálculo de sub-rede

Máscara de rede original	N.º de bits emprestados	Nova máscara de sub-rede	N.º de sub-redes		N.º Endereços IPv4 na sub-rede	N.º Endereços IPv4 úteis em cada sub-rede
/16	1	/17	2 ¹	2	32768	32766

Cálculo de sub-rede

	2	/18	2^2	4	16384	16382
	3	/19	2^3	8	8192	8190
	4	/20	2^4	16	4096	4094
	5	/21	2^5	32	2048	2046
	6	/22	2^6	64	1024	1022
	7	/23	2^7	128	512	510
	8	/24	2^8	256	256	254
	9	/25	2^9	512	128	126
	10	/26	2^{10}	1024	64	62
	11	/27	2^{11}	2048	32	30
	12	/28	2^{12}	4096	16	14
	13	/29	2^{13}	8192	8	6
	14	/30	2^{14}	16384	4	2
	15	/31	2^{15}	32768	2	0

⇒ Utilize a rolagem horizontal

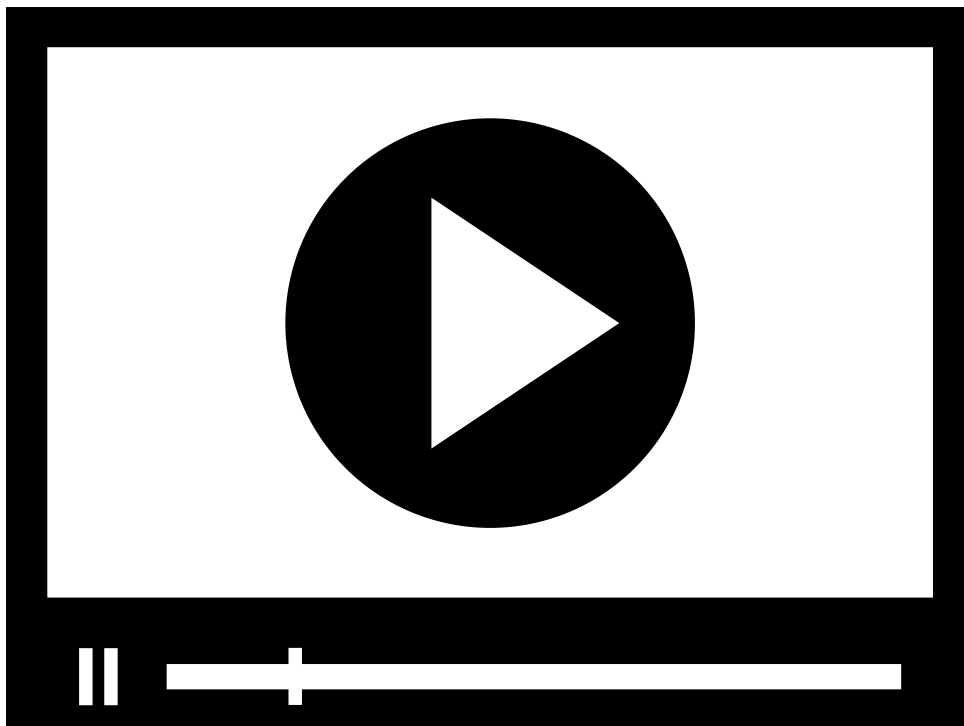
Tabela: Decomposição de uma rede /16 em sub-redes.

Elaborada por Isaac Santa Rita.

ATENÇÃO

Nessa apresentação, fica evidente que uma rede /16, com capacidade inicial de $2^{16} - 2$ dispositivos, pode ser decomposta de diversas formas em redes com diferentes máscaras. Essas sub-redes, utilizando-se da mesma lógica, podem ser decompostas novamente, para melhor ajuste a um determinado projeto.

PROJETOS DE REDE: REDES INDEPENDENTES



PROJETO DE REDES IPV4

Neste vídeo, abordamos estratégias essenciais para o projeto de redes IPv4. Explore métodos eficazes de design, garantindo uma infraestrutura robusta e eficiente para suportar a comunicação na era digital.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Focaremos, nesta seção, na quantidade de dispositivos necessários a um projeto de rede IPv4. Nesse contexto, devemos recordar como calcular o número máximo de máquinas que uma rede pode comportar.

RELEMBRANDO

Para uma rede com máscara de sub-rede /N, podemos comportar:

N.º máximo de máquinas = N.º total de IPv4 – endereço IPv4 de rede – endereço IPv4 de broadcast

N.º máximo de máquinas = $2^{(32-N)}$

Dessa forma, uma rede com máscara de sub-rede 255.255.255.0 (/24) pode comportar:

$$N_{\max} = 2^{(32-N)} - 2 = 2^{(32-24)} - 2 = 2^{(8)} - 2 = 256 - 2 = 254 \text{ máquinas}$$

 **Atenção!** Para visualização completa da equação utilize a rolagem horizontal

Assim, para determinar a máscara de sub-rede necessária ao suporte de uma determinada quantidade de máquinas, basta encontrar o menor “N” que satisfaz a inequação exponencial apresentada a seguir:

$$2^{(32-N)} - 2 \geq (\text{N.º de máquinas desejado})$$

 **Atenção!** Para visualização completa da equação utilize a rolagem horizontal

Para exemplificar, vamos criar uma rede com capacidade de suportar a operação de 120 máquinas.

$$2^{(32-N)} - 2 \geq (\text{N.º de máquinas desejado})$$

$$2^{(32-N)} - 2 \geq 120$$

$$2^{(32-N)} \geq 120 + 2$$

$$2^{(32-N)} \geq 122$$

$$32 - N = 7$$

$$N = 32 - 7$$

$$N = 25 \quad (255.255.255.128)$$



Atenção! Para visualização completa da equação utilize a rolagem horizontal

Utilizando uma faixa de rede aleatória, podemos criar a seguinte rede de dados para comportar as 120 máquinas demandadas pelo problema.

Máscara de sub-rede: /25 (255.255.255.128)

IP de rede: 192.168.1.0

IP de broadcast: 192.168.1.127

Nº de Endereços IPs úteis: $2^{(32-N)} - 2 = 2^7 - 2 = 128 - 2 = 126$

IPv4 úteis: do IPv4 192.168.1.1 até o IPv4 192.168.1.126

EXERCÍCIO

Agora chegou a vez de você verificar se compreendeu os projetos de rede. Realize o exercício proposto e confira a resposta:

1. Apresente os parâmetros solicitados abaixo para uma rede de dados com capacidade de suportar 728 máquinas (utilizar o IP de rede 192.168.0.0).

Máscara de sub-rede:

IP de rede:

IP de broadcast:

Nº de Endereços IPs úteis:

IPv4 úteis:

Máscara de sub-rede: /22 (255.255.252.0)

IP de rede: 192.168.0.0

IP de broadcast: 192.168.3.255

N.º de IPs úteis: $2^{(32-N)} - 2 = 2^{10} - 2 = 1024 - 2 = 1022$

IPv4 úteis: Do IPv4 192.168.0.1 até o IPv4 192.168.3.254

PROJETOS DE REDE: DIVISÃO DE REDES EM SUB-REDES

Normalmente, os projetos de redes são confeccionados a partir de uma faixa de rede predefinida. Essa delimitação obriga os administradores a criarem sub-redes dessa rede predefinida para atender às suas necessidades.

Para melhor compreensão, temos como o exemplo a necessidade de um administrador que precisa compor um projeto de rede a partir da rede 172.16.1.0/24. Nessa demanda, ele terá que criar 4 redes com capacidade de até 60 máquinas cada.

Demonstramos a seguir as capacidades de cada uma das possíveis sub-redes criadas a partir da rede 172.16.1.0/24, até que possamos definir as mais adequadas a esse projeto.

Cálculo de sub-rede para rede /24

Máscara de rede original	N.º de bits emprestados	Nova máscara de sub-rede	N.º de sub-redes		N.º Endereços IPv4 na sub-rede	N.º Endereços IPv4 úteis em cada sub-rede
/24	1	/25	2 ¹	2	128	126
	2	/26	2 ²	4	64	62

⇒ Utilize a rolagem horizontal

Tabela: Decomposição de uma rede /26 em sub-redes.

Elaborada por Isaac Santa Rita.

Podemos observar que a divisão da rede /24 em 4 unidades de rede /26 atende às necessidades do projeto em questão, uma vez que poderemos ter em cada sub-rede até 62 máquinas.

Desse modo, o administrador de rede pode confeccionar seu projeto utilizando a máscara de rede /26. Explicitamos, na sequência, a solução de endereçamento IPv4 para o projeto em questão.

Rede original	N.º da sub-rede	IP de rede /26	IP de broadcast	N.º máx. de máquinas
172.16.1.0/24	1	172.16.1.0/26	172.16.1.63	62
	2	172.16.1.64/26	172.16.1.127	62
	3	172.16.1.128/26	172.16.1.191	62
	4	172.16.1.192/26	172.16.1.255	62

⇒ Utilize a rolagem horizontal

Tabela: Discriminação da rede 172.16.1.0/24 em 4 redes /26.

Elaborada por Isaac Santa Rita.

EXERCÍCIO

Vamos testar seus conhecimentos mais uma vez? Para isso, realize o exercício a seguir:

2. Apresente os parâmetros solicitados abaixo para a subdivisão da rede 10.1.12.0/22 em oito sub-redes com capacidades idênticas.

Rede original	N.º da sub-rede	IP de rede /26	IP de broadcast	N.º máx. de máquinas
10.1.12.0/22	1			
	2			
	3			
	4			
	5			

Rede original	N.º da sub-rede	IP de rede /26	IP de broadcast	N.º máx. de máquinas
	6			
	7			
	8			

⇒ Utilize a rolagem horizontal

Tabela: Subdivisão da rede 10.1.12.0/22 em oito sub-redes.

Elaborada por Isaac Santa Rita.

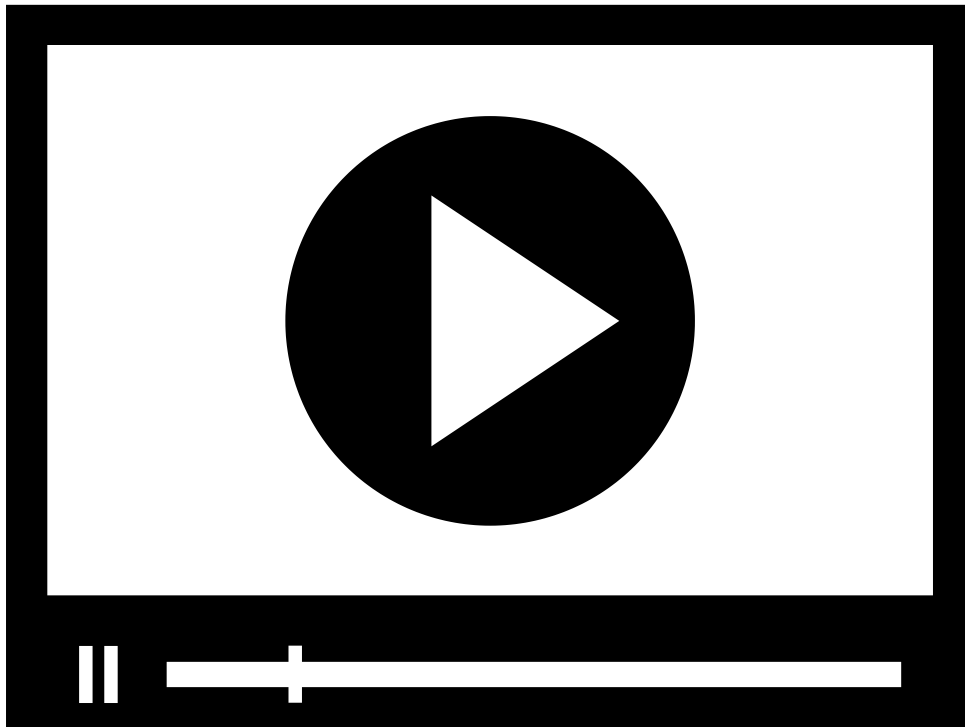
Rede original	N.º da sub-rede	IP de rede /26	IP de broadcast	N.º máx. de máquinas
10.1.12.0/22	1	10.1.12.0/25	10.1.12.127	126
	2	10.1.12.128/25	10.1.12.255	126
	3	10.1.13.0/25	10.1.13.127	126
	4	10.1.13.128/25	10.1.13.255	126
	5	10.1.14.0/25	10.1.14.127	126
	6	10.1.14.128/25	10.1.14.255	126
	7	10.1.15.0/25	10.1.15.127	126
	8	10.1.15.128/25	10.1.15.255	126

⇒ Utilize a rolagem horizontal

Tabela: Subdivisão da rede 10.1.12.0/22 em oito sub-redes.

Elaborada por Isaac Santa Rita.

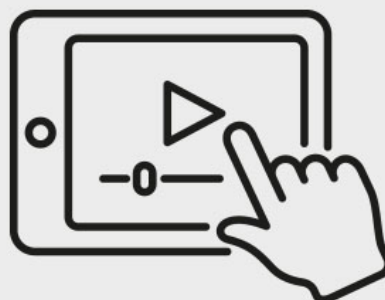
PROJETOS DE REDE: DIVISÃO DE REDES EM SUB-REDES HETEROGÊNEAS



DIVISÃO DE REDES EM SUBREDES HETEROGÊNEAS

Neste vídeo, exploramos a prática da divisão de redes em subredes heterogêneas. Descubra como essa abordagem estratégica otimiza a gestão de recursos, promovendo eficiência na comunicação e adaptabilidade nas redes.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Nesta parte, vamos estudar a adequação de projetos de rede a condições mais próximas da realidade, nas quais cada rede necessita de uma quantidade específica de equipamentos, condicionado ao uso de uma faixa de IP predefinida.

A título de exemplo, vamos confeccionar um projeto no qual dispomos da rede 10.10.10.0/24 para compor três redes com necessidades específicas:

A Rede A, com necessidade de 120 endereços IPv4 úteis

A Rede Ligação, com necessidade de 2 endereços IPv4 úteis

A Rede B, com necessidade de 35 endereços IPv4 úteis

Essas exigências estão demonstradas a seguir.

REDE DISPONÍVEL: 10.10.10.0/24



📷 Necessidades do projeto IPv4.

Captura de tela do software Packet Tracer.

Nesse projeto, inicialmente levantaremos a mínima máscara capaz de atender cada uma das três redes apresentadas.

🔄 RELEMBRANDO

Para isso, lembraremos que a quantidade de dispositivos permitidos por uma rede “/N” é expresso pela fórmula $2^{(32-N)} - 2$.

A fim de encontrar a máscara de rede mais ajustada a cada uma das três redes apresentadas, devemos encontrar o menor número “N” inteiro que satisfaz as seguintes condições:

$$\text{Rede A: } 2^{(32-N)} - 2 \geq 120 \Rightarrow N = 25 \text{ Rede /25}$$

$$\text{Rede Ligação: } 2^{(32-N)} - 2 \geq 2 \Rightarrow N = 30 \text{ Rede /30}$$

$$\text{Rede B: } 2^{(32-N)} - 2 \geq 35 \Rightarrow N = 26 \text{ Rede } /26$$

Como é impositiva a utilização da faixa 10.10.10.0/24 na composição das três redes, efetuaremos um planeamento IPv4 tomando por base essa rede e os conhecimentos aprendidos na decomposição de redes em sub-redes.

Vejamos a seguir uma demonstração dessa etapa do referido projeto:

Rede	Nº de Sub-Rede	Decomposição /25	Rede atendida
10.10.10.0/24	1	10.10.10.0/25	Rede A
	2	10.10.10.128/25	Disponível
Rede	Nº de Sub-Rede	Decomposição /26	Rede atendida
10.10.10.128/25	1	10.10.10.128/26	Rede B
	2	10.10.10.192/26	Disponível
Rede	Nº de Sub-Rede	Decomposição /30	Rede atendida
10.10.10.192/26	1	10.10.10.192/30	Rede Ligação
	2	10.10.10.196/30	Disponível
	3	10.10.10.200/30	Disponível
	4	10.10.10.204/30	Disponível
	5	10.10.10.208/30	Disponível
	6	10.10.10.212/30	Disponível
	7	10.10.10.216/30	Disponível
	8	10.10.10.220/30	Disponível
	9	10.10.10.224/30	Disponível
	10	10.10.10.228/30	Disponível
	11	10.10.10.232/30	Disponível
	12	10.10.10.236/30	Disponível
	13	10.10.10.240/30	Disponível
	14	10.10.10.244/30	Disponível
	15	10.10.10.248/30	Disponível
	16	10.10.10.252/30	Disponível

Imagem: Isaac Santa Rita

📷 Planejamento IPv4 do projeto.

Assim, para a realização desse projeto, vamos decompor a rede 10.10.10.0/24 da seguinte forma:

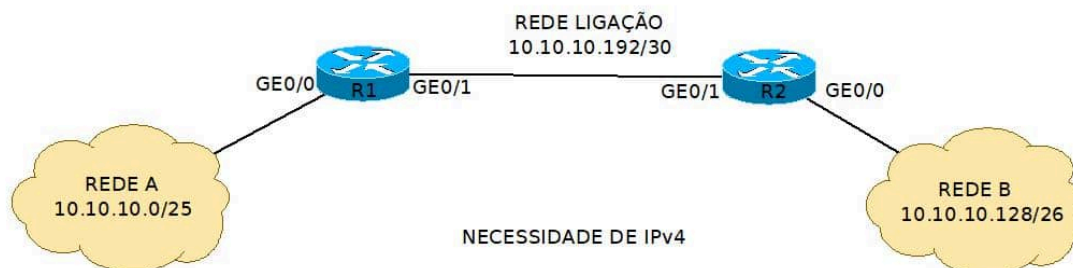
Rede A: 10.10.10.0/25

Rede B 10.10.10.128/26

Rede Ligação: 10.10.10.192/30

A seguir, o resultado do projeto:

REDE DISPONÍVEL: 10.10.10.0/24



VERIFICANDO O APRENDIZADO

1. O PLANEJAMENTO DE ENDEREÇOS IPV4 É FUNDAMENTAL AO DESENVOLVIMENTO DE PROJETOS DE REDE IPV4. PARA A REDE IPV4 172.17.0.0/27, ASSINALE A OPÇÃO QUE APRESENTA A QUANTIDADE DE DISPOSITIVOS DISPONÍVEIS, O IP DE REDE E O IP DE BROADCAST DESSA REDE, RESPECTIVAMENTE.

A) 32; 172.17.0.0; 172.17.0.255.

B) 30; 172.17.0.0; 172.17.0.63.

C) 27; 172.17.0.31; 172.17.0.255.

D) 30; 172.17.0.0; 172.17.0.31.

E) 32; 172.17.0.0; 172.17.0.31.

2. UM PROJETO DE REDE PERMITE QUE POSSAMOS DIVIDIR A REDE EM DIVERSAS SUB-REDES. CONSIDERANDO ENDEREÇO DE REDE 10.10.10.0/24, ASSINALE A ALTERNATIVA QUE APRESENTA CORRETAMENTE A DIVISÃO EM DUAS SUB-REDES COM MÁSCARA /25 E A QUANTIDADE DE MÁQUINAS DISPONÍVEIS EM CADA SUB-REDE.

A)

Rede original	N.º da sub-rede	IP da rede /25	IP do broadcast	N.º máx. de máquinas
10.10.10.0/24	1	10.10.10.0	10.10.10.127	128
	2	10.10.10.128	10.10.10.255	128

A)

B)

Rede original	N.º da sub-rede	IP da rede /25	IP do broadcast	N.º máx. de máquinas
10.10.10.0/24	1	10.10.10.0	10.10.10.127	126
	2	10.10.10.128	10.10.10.255	126

⇒ Utilize a rolagem horizontal

B)

C)

Rede original	N.º da sub-rede	IP da rede /25	IP do broadcast	N.º máx. de máquinas
10.10.10.0/24	1	10.10.10.1	10.10.10.126	128
	2	10.10.10.129	10.10.10.254	128

⇒ Utilize a rolagem horizontal

C)

D)

Rede original	N.º da sub-rede	IP da rede /25	IP do broadcast	N.º máx. de máquinas
10.10.10.0/24	1	10.10.10.0	10.10.10.126	126
	2	10.10.10.127	10.10.10.255	126

⇒ Utilize a rolagem horizontal

D)

E)

Rede original	N.º da sub-rede	IP da rede /25	IP do broadcast	N.º máx. de máquinas
10.10.10.0/24	1	10.10.10.1	10.10.10.126	126

Rede original	N.º da sub-rede	IP da rede /25	IP do broadcast	N.º máx. de máquinas
	2	10.10.10.129	10.10.10.254	126

⇒ Utilize a rolagem horizontal

E)

GABARITO

1. O planejamento de endereços IPv4 é fundamental ao desenvolvimento de projetos de rede IPv4. Para a rede IPv4 172.17.0.0/27, assinale a opção que apresenta a quantidade de dispositivos disponíveis, o IP de rede e o IP de broadcast dessa rede, respectivamente.

A alternativa "D " está correta.

N.º de máquinas: $2^{(32-n)} - 2 = 2^{(32-27)} - 2 = 2^5 - 2 = 32 - 2 = 30$

IP rede 172.17.0.(00000000)₂

IP broadcast 172.17.0.(00011111)₂ = 172.17.0.31

2. Um projeto de rede permite que possamos dividir a rede em diversas sub-redes. Considerando endereço de rede 10.10.10.0/24, assinale a alternativa que apresenta corretamente a divisão em duas sub-redes com máscara /25 e a quantidade de máquinas disponíveis em cada sub-rede.

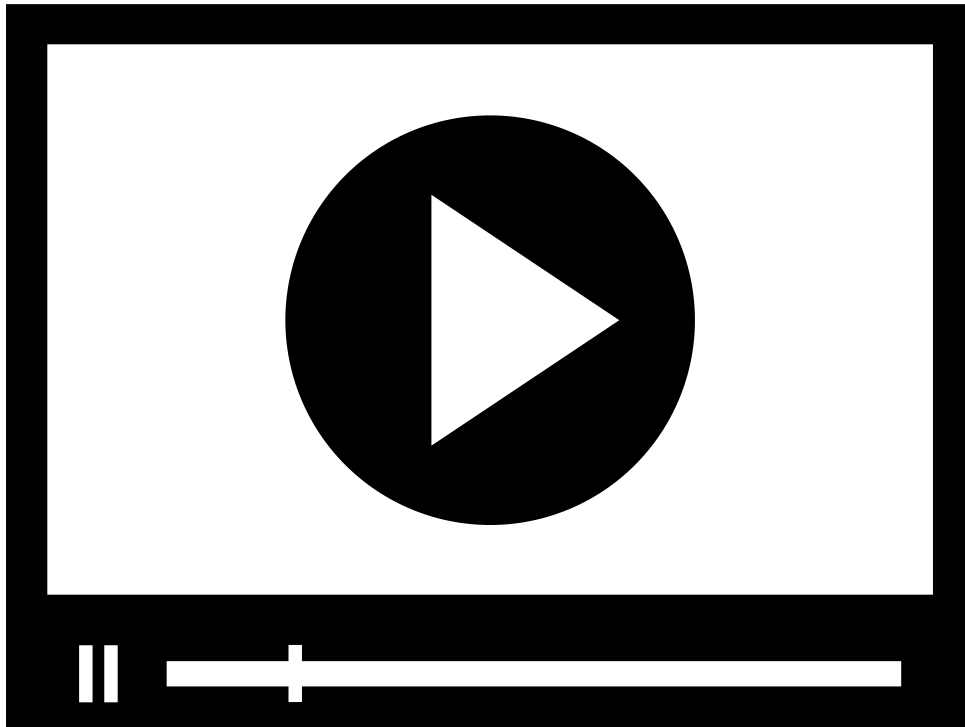
A alternativa "B " está correta.

Para que seja possível realizar a divisão em duas sub-redes, o primeiro bit que era destinado à estação passou a ser considerado como parte da rede, portanto, passando a máscara de /24 para /25. Assim, a rede foi dividida em duas, de acordo com o quadro da alternativa B.

MÓDULO 3

⦿ Reconhecer as soluções temporárias para sanar o esgotamento do endereçamento IPv4

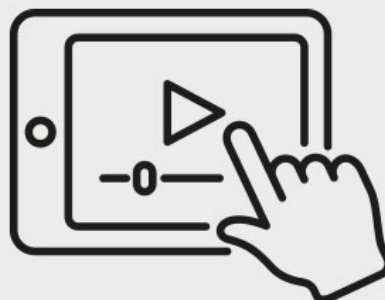
ORIGEM E EVOLUÇÃO DO PROTOCOLO IP



DESAFIOS E SOLUÇÕES: ESGOTAMENTO DE ENDEREÇOS IPV4

Neste vídeo, discutimos os desafios enfrentados com o esgotamento de endereços IPv4 e apresentamos soluções criadas para lidar com essa questão, garantindo a continuidade da conectividade na era digital.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



NOS ANOS INICIAIS DA INTERNET, FOI ESPECIFICADO QUE CADA DISPOSITIVO QUE VIESSE A FAZER PARTE DESSA REDE

DEVERIA POSSUIR UM ENDEREÇO ÚNICO, O IP. O IPV4 FOI A SOLUÇÃO ENCONTRADA PARA ATENDER A ESSA NECESSIDADE.

Composto por 32 bits, possui a capacidade de endereçar até 4.294.967.296 (2^{32}) dispositivos, o que para a época parecia ser inesgotável.

Mas isso mudou. Acompanhe:



Com a explosão da Web comercial, a chegada dos smartphones conectados e, principalmente, com o avanço da Internet das Coisas (Internet of Things – IoT), todo tipo de máquina passou a estar conectada e a quantidade de IPs disponíveis em sua versão 4 deixou de atender à demanda de endereçamento global.

Dessa forma, a Internet Assigned Numbers Authority (IANA), entidade responsável pela coordenação global do DNS raiz, do endereçamento IP, do protocolo de internet e outros recursos, foi obrigada a buscar alternativas ao esgotamento dos endereços IPv4.



A solução definitiva foi o desenvolvimento, em 1995, da versão 6 do protocolo IP, o IPv6, que possui em sua composição 128 bits de endereçamento e capacidade de endereçar aproximadamente $3,4 \times 10^{38}$ dispositivos.

Essa versão do protocolo IP foi padronizada pela RFC 2460 em 1998 e está em processo de implantação desde o ano 2000.



❓ VOCÊ SABIA

O eminente esgotamento dos endereços IPv4 na primeira década deste século, aliado ao atraso do início da operação do IPv6, demandaram soluções que permitissem uma sobrevivência ao IPv4, até que seu substituto estivesse totalmente operacional.

Nesse contexto, podemos listar diversas iniciativas como o desenvolvimento do processo Classless Inter Domain Routing (CIDR), que nada mais é do que a utilização de redes com máscaras variadas, sem classe (**classless**) , aliada à manutenção do processo de roteamento.

Outra solução desenvolvida em decorrência da escassez de IPv4 foi a alocação dinâmica de IPv4 por meio do DHCP (Dynamic Host Configuration Protocol), que também confere às redes de dados grande economia de endereços mediante o reuso.

★ EXEMPLO

Como exemplo do emprego do DHCP como solução auxiliar ao esgotamento de endereço, podemos imaginar um ambiente público, como uma cafeteria, um aeroporto, supermercado, ou qualquer outro ambiente que forneça acesso à rede.

Antes dos DHCP, qualquer estação que desejasse utilizar a rede receberia um endereço por um tempo indeterminado. É fácil imaginar que, em uma situação dessas, rapidamente haveria o esgotamento dos endereços, porque uma estação entraria na rede, sairia, e o endereço continuaria alocado.

O DHCP acrescentou o conceito de alocação temporária (aluguel ou lease), fornecendo o endereço para uma estação apenas durante um tempo, permitindo, portanto, o reuso dos endereços.

Além dessas soluções, destaca-se o uso de faixas de endereçamento não roteadas na Internet, aliadas à utilização de processos de tradução desses endereços àqueles com capacidade de trânsito na rede mundial de computadores, que estudaremos mais detalhadamente.

ENDEREÇOS PÚBLICOS E PRIVADOS

A vasta maioria dos endereços IPv4 são endereços públicos.

Esses endereços são únicos e capazes de serem roteados na Internet, ou seja, devem ser atribuídos aos pacotes egressos de máquinas conectadas à Internet, para que a rede mundial de computadores possa encaminhá-los ao destino e fazer com que retornem ao remetente.

COMENTÁRIO

Logicamente, em toda faixa IPv4, existem pequenos blocos destinados a fins específicos que não estão contemplados dentro dos objetivos deste estudo.

Assim, um dos artifícios utilizados para contornar o problema da escassez dos endereços públicos IPv4 está definido na RFC 1918, que introduz, entre outros, faixas de IPv4 privados.

Os IPv4 privados são blocos comuns de endereços usados internamente pelas organizações para atribuição de endereços IPv4 a seus dispositivos, mas que não possuem a capacidade de serem roteados na Internet.

Os endereços privados não são únicos, e dessa forma, podem ser reutilizados em diversas instituições ao mesmo tempo, bastando para isso que não haja conexão direta entre essas redes.

As faixas de IPv4 privados definidas dela RFC 1918 são apresentadas a seguir:

ENDEREÇOS PRIVADOS	
Endereço de rede	RFC 1918 – intervalo de endereços privados
10.0.0.0/8	10.0.0.0 até 10.255.255.255
172.16.0.0/12	172.16.0.0. até 172.31.255.255
192.168.0.0/16	192.168.0.0 até 192.168.255.255

⇒ Utilize a rolagem horizontal

Tabela: Faixas de IPs privados.

Elaborada por Isaac Santa Rita.

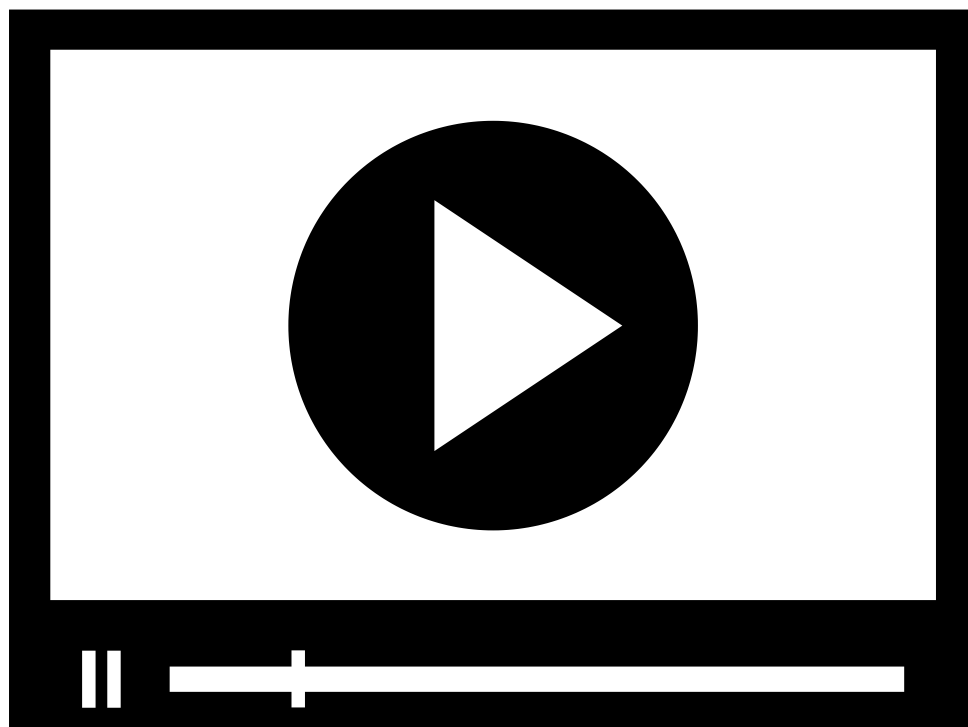
A seguir, estão demonstradas as três instituições que utilizam a mesma faixa de IPv4 para compor seus respectivos parques computacionais. Como elas não possuem conexão direta, é totalmente viável sua coexistência, sem qualquer problema de multiplicidade de IPv4. Observe:



📷 Redes isoladas com mesma faixa IPv4.

Captura de tela do software Packet Tracer.

TRADUÇÃO DE ENDEREÇOS IPV4



TRADUÇÃO DE ENDEREÇOS IPV4

Neste vídeo, abordamos a tradução de endereços IPv4. Exploraremos como esse recurso permitiu que as redes IPv4 permanecessem em operação até hoje, promovendo a interoperabilidade e eficiência no cenário digital atual.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

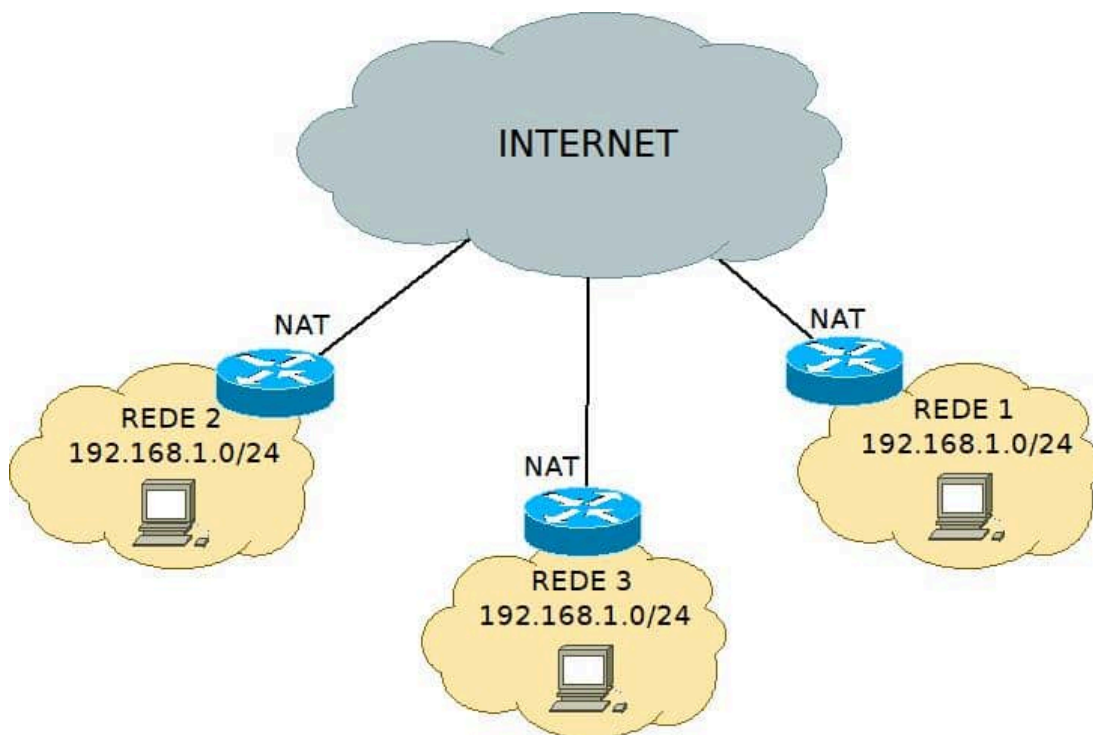


ATENÇÃO

A tradução de endereços IPv4 é o método mais utilizado para conectar redes que utilizam as faixas privadas de endereçamento, uma vez observada a necessidade dessas instituições conectarem seus parques de máquinas à rede mundial de computadores.

Essa tradução de endereço de rede recebe o nome de Networking Address Translation (NAT), que consiste na substituição do endereço IPv4 de determinado pacote para viabilizar a navegação dentro de uma outra rede de dados, normalmente a Internet.

A partir desse processo, é possível que as redes de instituições que utilizam a mesma faixa de rede privada se comuniquem por meio de uma outra rede, como a Internet, conforme ilustrado:



📷 Redes privadas conectadas por meio da Internet pelo NAT.

Captura de tela do software Packet Tracer.

Esse NAT é normalmente realizado pelo equipamento de borda dessas instituições. Eles possuem a capacidade de trocar o endereço IPv4 privado por um endereço IPv4 público durante o processo de roteamento, conforme exemplo.

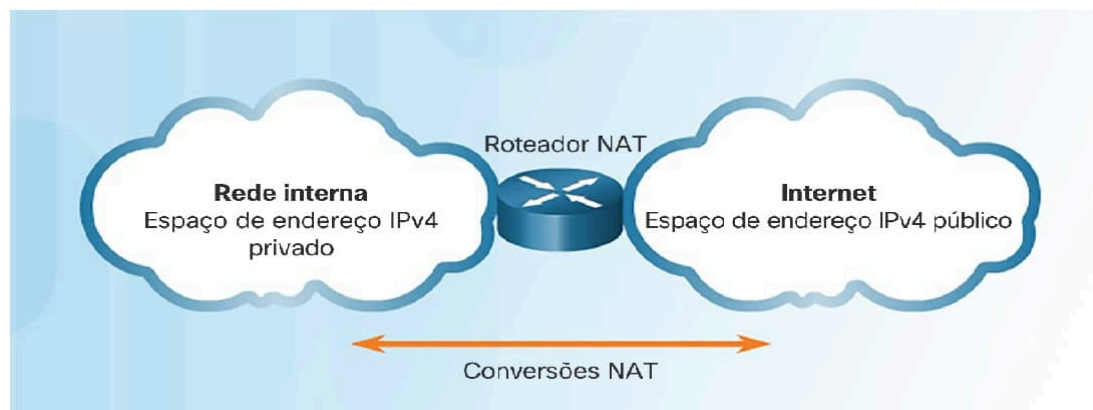
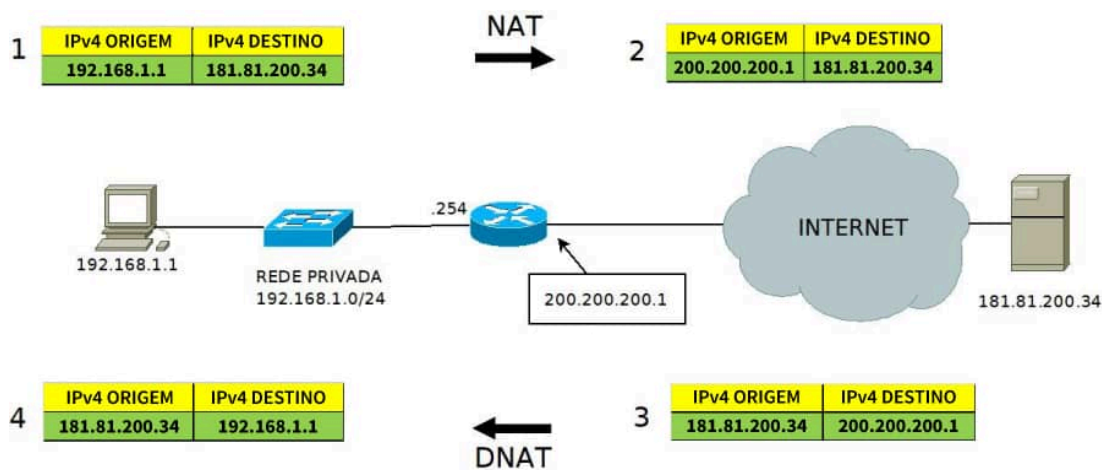


Imagem: Isaac Santa Rita

📷 Redes isoladas com mesma faixa IPv4.

No exemplo a seguir, apresentaremos a tradução de endereço de uma máquina interna a uma rede privada, durante o acesso a uma página web disponível na Internet sob um IPv4 público.



📷 Tradução de IPv4.

Captura de tela do software Packet Tracer.

Os passos 1, 2, 3 e 4, indicados na imagem, representam a sequência de tradução dos IPv4 envolvidos no processo de acesso da máquina 192.168.1.1 ao servidor web sob IPv4 público 181.81.200.34.

Essas etapas podem ser discriminadas da seguinte forma:

ETAPA 1

Formação do pacote IPv4 com endereços de origem (192.168.1.1) e destino (181.81.200.34) originais.

ETAPA 2

Tradução (NAT) do IPv4 privado de origem para o IPv4 público de origem 200.200.200.1. Esse IPv4 público permite que o pacote retorne do website até o roteador de borda da instituição em questão.

ETAPA 3

Retorno do pacote IPv4 ao destino. Evidencia-se a inversão da ordem dos IPv4 de origem e de destino: o IPv4 181.81.200.34 passa a ser de origem; o IPv4 200.200.200.1, de destino.

ETAPA 4

Tradução (Destination NAT) do IPv4 de destino 200.200.200.1 para o IPv4 de destino 192.168.1.1.

COMENTÁRIO

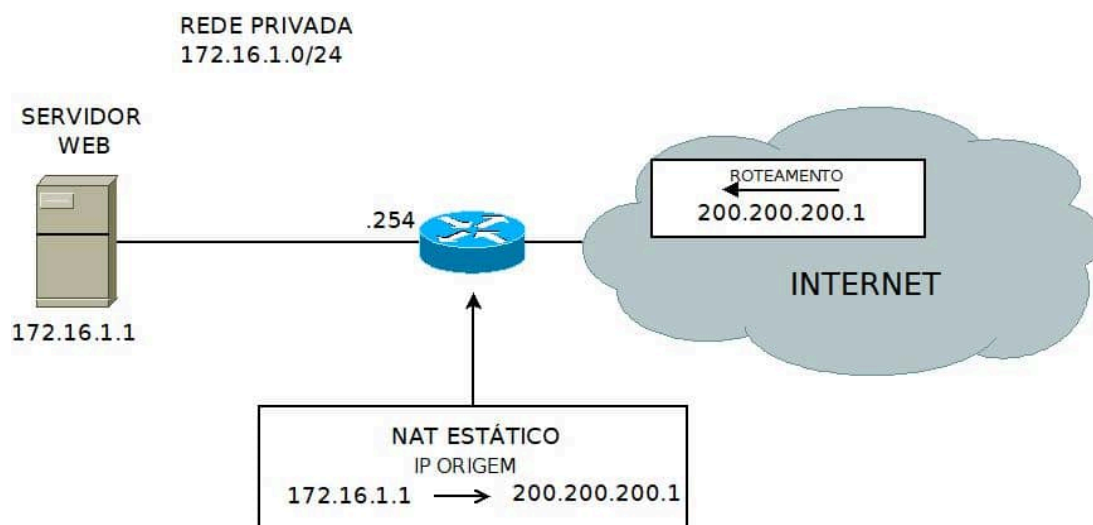
Duas formas são bastante utilizadas para o processamento do NAT pelos equipamentos de borda, são elas o NAT estático e o NAT dinâmico, que possuem características adequadas aos cenários que serão apresentados.

NAT ESTÁTICO

O NAT estático, como o próprio nome sugere, realiza a tradução estática de um IPv4 privado para um IPv4 público.

Essa forma de tradução normalmente é utilizada para publicar serviços que devem ficar disponíveis permanentemente na Internet, mas estão hospedados em uma rede privada.

Observaremos um exemplo da tradução estática do IPv4 privado (172.16.1.1) de um servidor web, que deve estar acessível na Internet sob o IPv4 público 200.200.200.1.



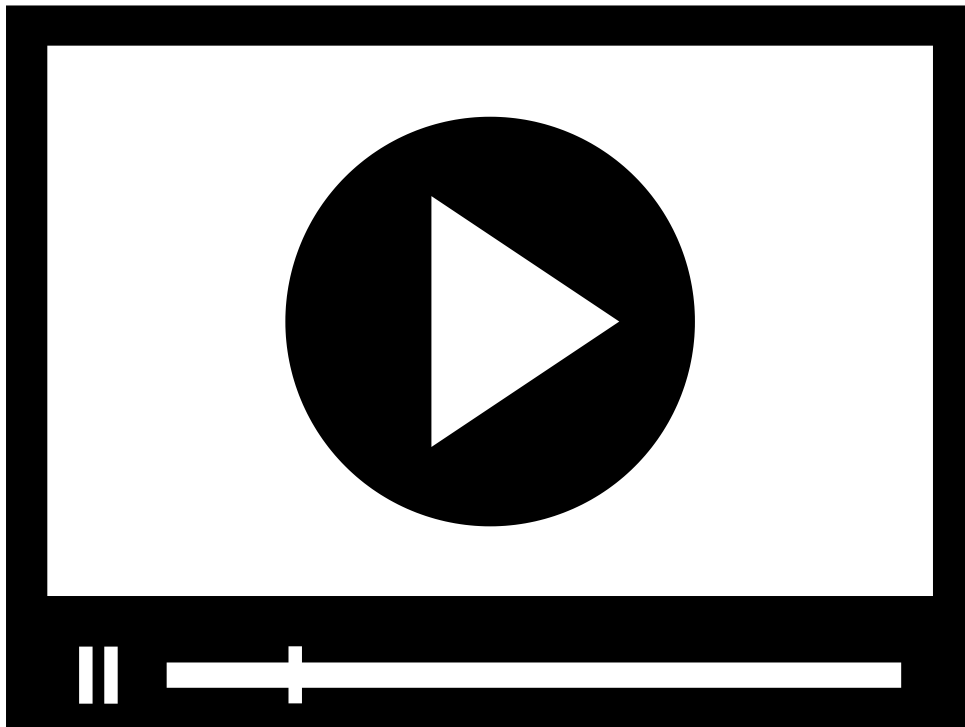
📷 Tradução de IPv4.

Captura de tela do software Packet Tracer.

Cabe destacar que a configuração realizada no roteador apresentado na imagem efetua a troca do IP de origem 172.16.1.1 para o IPv4 de origem 200.200.20.1, de forma fixa.

Além disso, toda vez que se efetua um NAT num roteador, como o exemplificado anteriormente, há automaticamente o tratamento do retorno do pacote traduzido. Desse modo, na operação em questão, está implícita a tradução de retorno, que consiste na troca do IPv4 de destino 200.200.200.1 para o IPv4 de destino 172.16.1.1.

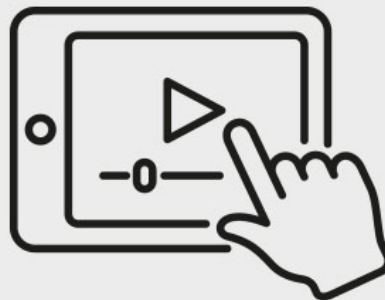
CONFIGURAÇÃO DE NAT ESTÁTICO



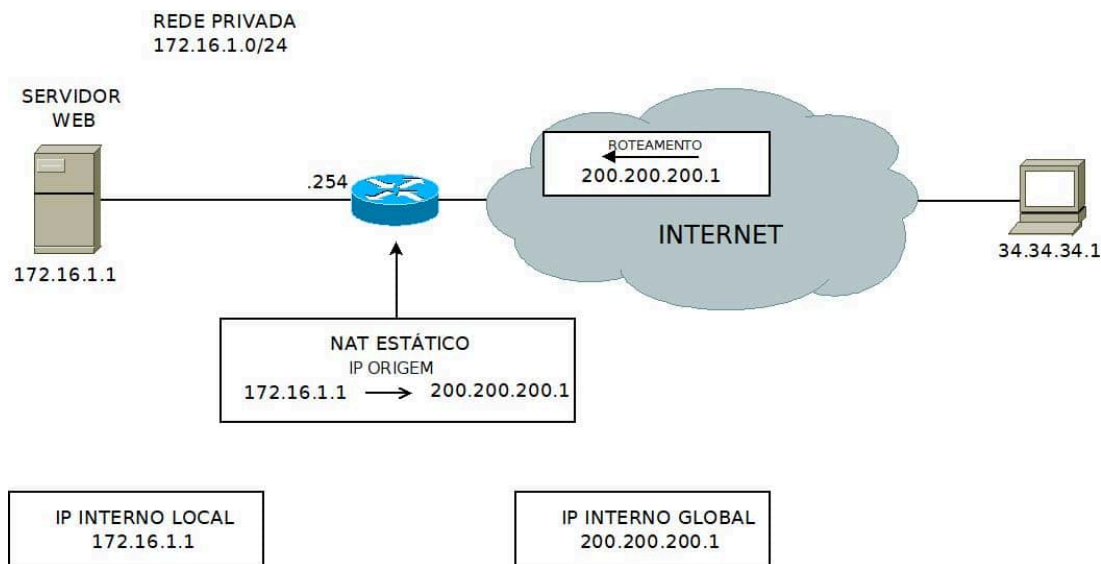
CONFIGURAÇÃO DE NAT ESTÁTICO

Neste vídeo, mostramos passo a passo como implementar o NAT estático de maneira prática. Explore as configurações essenciais para otimizar a comunicação entre redes, garantindo uma conexão eficiente e segura.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Com o objetivo de melhor compreendermos a configuração do NAT estático vejamos a rede que será apresentada. Posteriormente, devemos realizar a publicação do servidor web na Internet sob o IP 200.200.200.1 apresentado.



📷 Configuração NAT estático de IPv4.

Captura de tela do software Packet Tracer.

A configuração do roteador Cisco necessária à publicação do servidor na Internet sob o IP 200.200.200.1 está apresentada a seguir.

R1#

R1# conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)# interface gigabitethernet 0/0

R1(config-if)# ip nat inside (Define a interface voltada para a rede privada)

R1(config-if)# exit

R1(config)# interface gigabitethernet 0/1

R1(config-if)# ip nat outside (Define a interface voltada para a rede pública)

R1(config-if)# exit

R1(config)# ip nat inside source static 172.16.1.1 200.200.200.1

R1(config)# end

R1#

EXERCÍCIO

Agora vamos praticar o que você aprendeu até aqui? Realize a atividade proposta a seguir:

1. Por meio do no software Packet Tracer, vamos configurar o NAT estático apresentado anteriormente e verificar a tradução sendo realizada. Para você realizar a sua atividade, você pode baixar o arquivo pré-configurado **Mod 4 Sec 3 Nat Estatico.pkt**.

Siga as seguintes etapas:

Configurar o NAT conforme orientação.

Acessar o servidor web em seu PC por meio de seu navegador web.

Efetuar o comando “R1#sh ip nat translations” no roteador do laboratório.

Padrão de resposta para o último comando

Ao acessar o servidor web por meio do PC, será criada uma tabela de conversão similar à que segue. Ressalta-se que, quanto mais acessos forem realizados, diferentes valores poderão aparecer.

Pro	Inside Global	Inside Local	Outside Local	Outside Global
---	200.200.200.1	172.16.1.1	---	---
Tcp	200.200.200.1:80	172.16.1.1:80	34.34.34.1:1028	34.34.34.1:1028

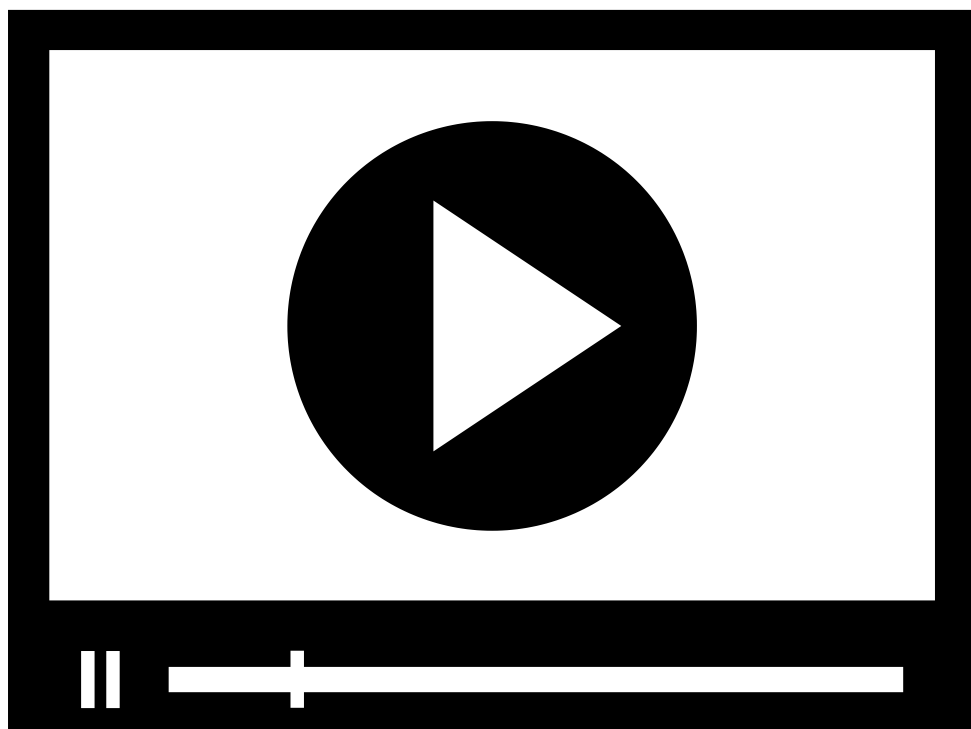
⇨ Utilize a rolagem horizontal

Elaborada por Isaac Santa Rita.



Atenção! Para visualização completa da equação utilize a rolagem horizontal

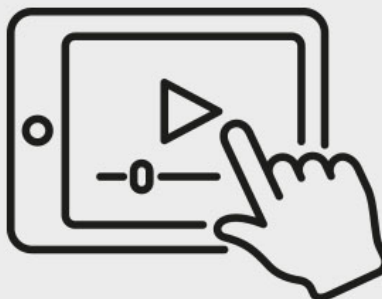
NAT DINÂMICO



NAT DINÂMICO E PORT ADDRESS TRANSLATION

Neste vídeo, vamos simplificamos a implementação do NAT Dinâmico e Port Address Translation. Aprenda de forma prática a dinamizar e gerenciar endereços, otimizando a comunicação entre redes com eficiência.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



O NAT dinâmico, como o próprio nome sugere, realiza a tradução dinâmica de um grupo de endereços IPv4 privados para um grupo de endereços IPv4 públicos.

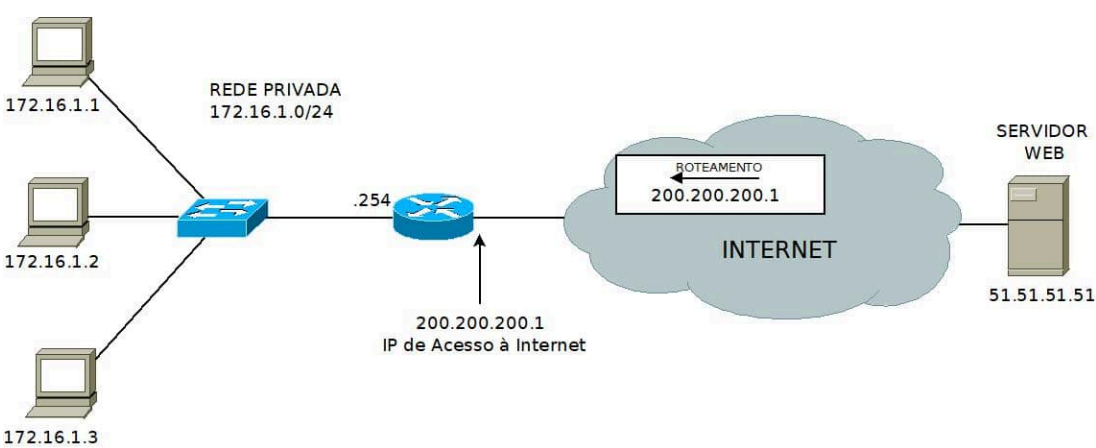
Os endereços privados a serem traduzidos nesse processo são limitados ao número de IPs públicos disponíveis para essa tradução, uma vez que a tradução é realizada observando a proporção de um IPv4 privado para cada IPv4 público disponível.

A fim de contornar esse problema e conferir grande vantagem numérica no processo de tradução de endereços IP, surgiu o Port Address Translation (PAT), que permite a tradução de diversos dispositivos de uma rede privada por meio de um único IPv4 público.

📢 ATENÇÃO

Para realizar essa tarefa, o PAT, também conhecido como NAT overload, utiliza a informação de porta da camada de transporte do modelo OSI no processo de tradução.

Com o objetivo de entendermos melhor esse processo, observaremos a imagem na qual três máquinas de uma rede privada acessam um servidor de páginas web, disponível na Internet, utilizando-se de um único IPv4 público (200.200.200.1).



📷 PAT IPv4.

Captura de tela do software Packet Tracer.

Vejamos a seguir o processo PAT para no acesso das três máquinas da rede privada ao servidor web.

PAT – Port Address Translation

IP origem: porta origem	IP origem traduzido: porta origem	IP destino: porta destino	IP destino: porta destino
172.16.1.1:2567	200.200.200.1:2567	51.51.51.51:80	51.51.51.51:80
172.16.1.2:2376	200.200.200.1:2376	51.51.51.51:80	51.51.51.51:80

PAT – Port Address Translation

172.16.1.3:4558	200.200.200.1:4558	51.51.51.51:80	51.51.51.51:80
------------------------	---------------------------	----------------	----------------

⇒ Utilize a rolagem horizontal

Tabela: Conversão PAT.

Elaborada por Isaac Santa Rita.

Nesse processo, cabe evidenciar que os IPs privados das três máquinas que compõem a rede dessa instituição tiveram seus IPs substituídos pelo mesmo IP público disponível. Isso foi possível devido à utilização da informação de porta na tradução, o que permitirá ao equipamento tradutor realizar o processo inverso de tradução quando o pacote retornar.

Ressalta-se que, quando duas máquinas utilizam a mesma porta de origem no acesso a um IP externo, o roteador realiza o PAT com o valor da próxima porta disponível.

Veja a seguir o processo PAT anterior com esta coincidência explicitada:

PAT – Port Address Translation

IP origem: porta origem	IP origem traduzido: porta origem	IP destino: porta destino	IP destino: porta destino
172.16.1.1:2567	200.200.200.1:2567	51.51.51.51:80	51.51.51.51:80
172.16.1.2:2567	200.200.200.1:2568	51.51.51.51:80	51.51.51.51:80

⇒ Utilize a rolagem horizontal

Tabela de conversão PAT com mesma porta de origem.

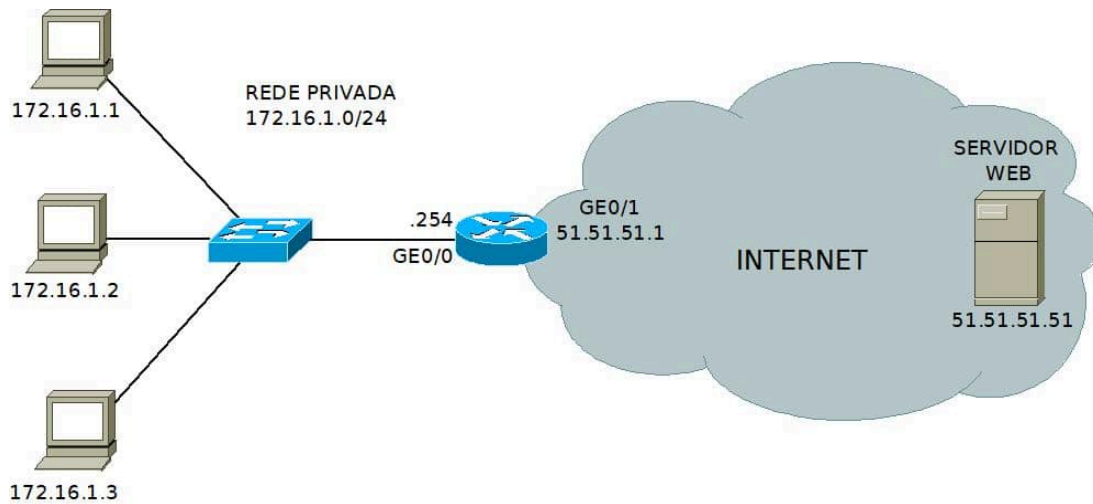
Elaborada por Isaac Santa Rita.

CONFIGURAÇÃO DE PAT

A seguir, apresentaremos dois cenários de configuração para o PAT. No primeiro, iremos realizar a configuração de uma rede acessando a Internet por meio do IP público da interface do roteador conectado à Internet. No segundo cenário, realizaremos a configuração do acesso à Internet por intermédio de uma faixa de IP pública, disponível para utilização.

CENÁRIO 1

Neste cenário, as três máquinas da instituição em questão possuem IPv4 privado e acessarão a Internet utilizando o IPv4 público da interface GigabitEthernet 0/1 do roteador R1.



📷 Cenário PAT 1.

Captura de tela do software Packet Tracer.

A configuração do roteador Cisco de borda necessária à situação descrita no cenário 1 é apresentada abaixo.

```
R1# conf t
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip nat inside
R1(config-if)# interface gigabitEthernet 0/1
R1(config-if)# ip nat outside
R1(config-if)# exit
R1(config)# access-list 1 permit 172.16.1.0 0.0.0.255 (Lista com autorização de tradução)
R1(config)# ip nat inside source list 1 interface gigabitEthernet 0/1 overload (Configuração do NAT)
R1(config)# end
R1#
```

EXERCÍCIO

É hora de praticar mais uma vez os seus conhecimentos. Realize o exercício a seguir:

2. No software Packet Tracer, configure o NAT dinâmico para interface única apresentada na imagem anterior e verifique a tradução sendo realizada por meio das etapas apresentadas a seguir. Para você realizar a sua atividade, você pode baixar o arquivo pré-configurado **Mod 4 Sec 6 PAT 1.pkt**.

Configurar o NAT conforme orientação.

Acessar o servidor web pelo PC por meio de seu navegador web.

Efetuar o comando “R1#sh ip nat translations” no roteador do laboratório.

Padrão de resposta para o último comando

Ao acessar o servidor web por meio das máquinas 1, 2 e/ou 3, será criada uma tabela de conversão similar à que segue. Ressalta-se que, quanto mais acessos forem realizados, diferentes valores poderão aparecer.

Pro	Inside Global	Inside Local	Outside Local	Outside Global
Tcp	51.51.51.1:1024	172.16.1.2:1025	51.51.51.51:80	51.51.51.51:80
Tcp	51.51.51.1:1025	172.16.1.1:1025	51.51.51.51:80	51.51.51.51:80
Tcp	51.51.51.1:1026	172.16.1.3:1025	51.51.51.51:80	51.51.51.51:80

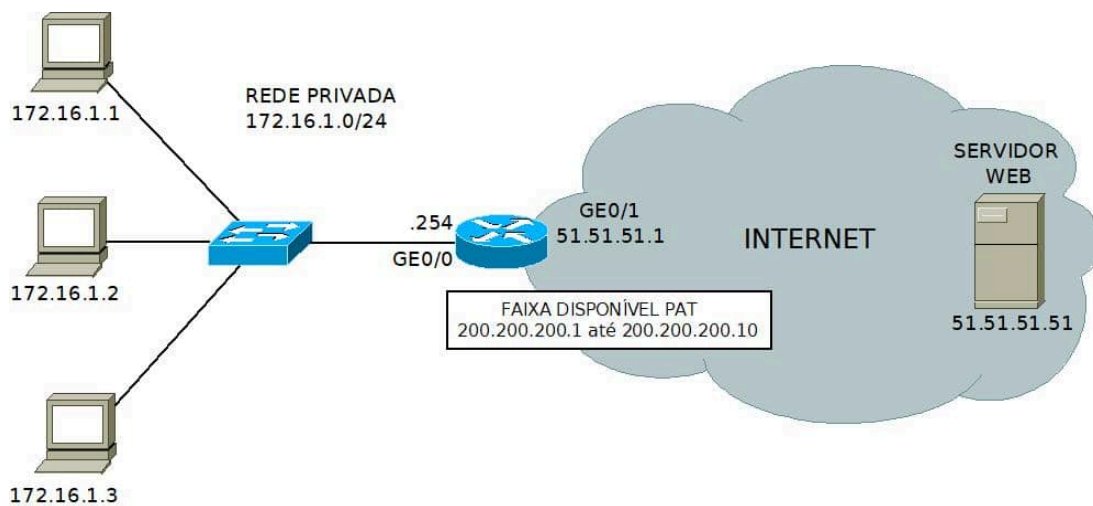
⇒ Utilize a rolagem horizontal

Elaborada por Isaac Santa Rita.

CENÁRIO 2

Represente pela imagem a seguir, na qual as três máquinas da instituição em questão, que possuem IPv4 privado, farão acesso à Internet utilizando uma faixa de IPv4 pública disponível.

Logicamente, o roteamento da Internet encaminha essa faixa de IP pública para o roteador de borda da instituição em questão.



📷 Cenário PAT 2.

Captura de tela do software Packet Tracer.

A configuração do roteador de borda Cisco, necessária para permitir o acesso dessas máquinas à Internet por meio da faixa de IPv4 pública disponível, está apresentada a seguir.

R1#

R1# conf t

R1(config)# interface gigabitEthernet 0/0

R1(config-if)# ip nat inside

R1(config-if)# interface gigabitEthernet 0/1

R1(config-if)# ip nat outside

R1(config-if)# exit

R1(config)# access-list 1 permit 172.16.1.0 0.0.0.255 (Lista com autorização de tradução)

R1(config)# ip nat pool FAIXA 200.200.200.1 200.200.200.10 netmask 255.255.255.0 (Definição de IPs públicos a serem utilizados)

R1(config)# ip nat inside source list 1 pool FAIXA overload (Configuração do NAT)

R1(config)# end

R1#

EXERCÍCIO

Chegou a hora de praticar o último cenário!

3. No software Packet Tracer, configure o NAT dinâmico para uma faixa de IP apresentada na imagem anterior e verifique a tradução sendo realizada por meio das etapas demonstradas a seguir. Para você realizar a sua atividade, você pode baixar o arquivo pré-configurado **Mod 4 Sec 6 PAT 2.pkt**.

Configurar o NAT conforme orientação.

Acessar o servidor web pelo PC por meio de seu navegador web.

Efetuar o comando “R1#sh ip nat translations” no roteador do laboratório.

Padrão de resposta para o último comando

Ao acessar o servidor web por meio das máquinas 1, 2 e/ou 3, será criada uma tabela de conversão similar à que segue. Ressalta-se que, quanto mais acessos forem realizados, diferentes valores poderão aparecer.

Pro	Inside Global	Inside Local	Outside Local	Outside Global
Tcp	1.51.51.1:1024	172.16.1.2:1025	172.16.1.2:80	172.16.1.2:80
Tcp	1.51.51.1:1025	172.16.1.1:1025	172.16.1.2:80	172.16.1.2:80
Tcp	1.51.51.1:1026	172.16.1.3:1025	172.16.1.2:80	172.16.1.2:80

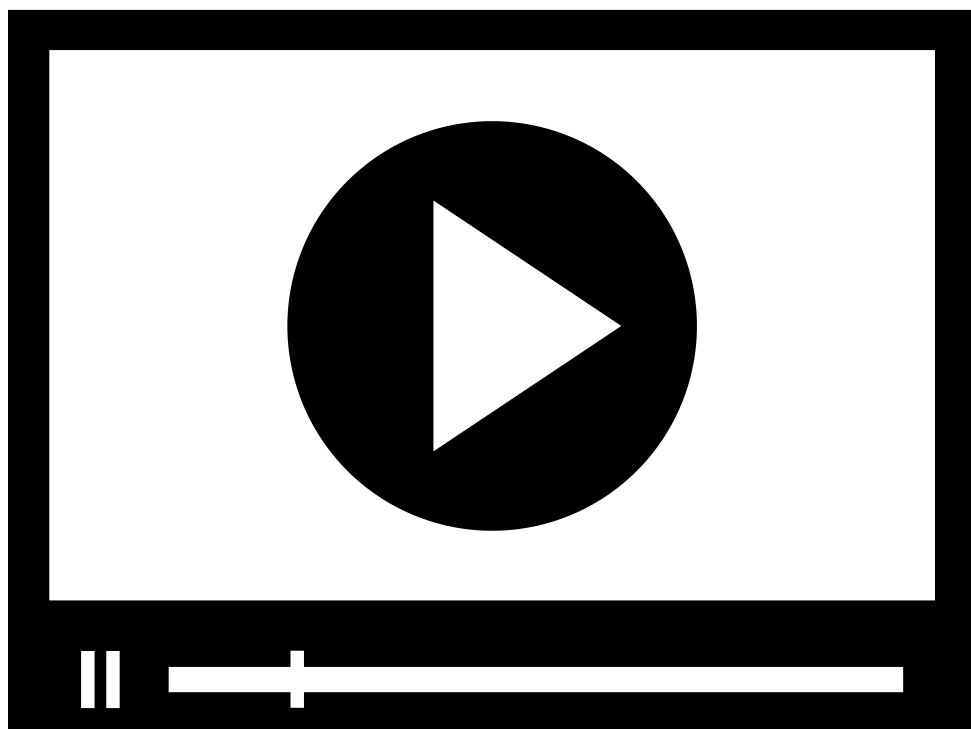
⇒ Utilize a rolagem horizontal

Elaborada por Isaac Santa Rita.



Atenção! Para visualização completa da equação utilize a rolagem horizontal

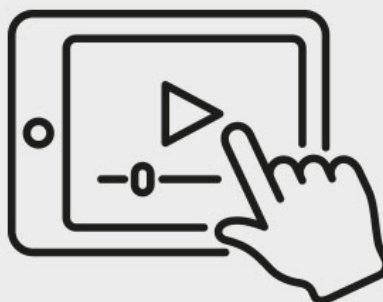
CARRIER GRADE NETWORK ADDRESS TRANSLATION (CGNAT)



CGNAT

Neste vídeo, desvendamos o CGNAT, revelando como esse recurso impulsiona a conectividade em larga escala. Entenda como ele auxilia no processo de man, aprimorando a comunicação na era digital.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



O Carrier Grade Network Address Translation (CGNAT ou CGN) é mais uma solução adotada para prover sobrevida ao IPv4 até que seja completamente substituído pelo IPv6.

 **ATENÇÃO**

Consiste num intermediário entre a rede doméstica e a Internet, implementada a nível de provedor de acesso. Ou seja, é uma solução de NAT, a nível do Internet Service Provider (ISP).

Antes da escassez de IPv4, existiam dois tipos de consumidores:

AQUELES COM UM IP DINÂMICO

Que recebiam um endereço para seus dispositivos a cada conexão.

AQUELES COM UM IP FIXO

Que pagavam mais caro, mas tinham sempre o mesmo endereço IP e poderiam, se assim o desejassem, hospedar serviços de internet.

Fato comum entre os dois, ambos contavam com um IP público exclusivo para sua conexão.

Entretanto, o CGNAT permite aos ISPs atribuir o mesmo endereço IP para diferentes usuários ao mesmo tempo, diferenciando-os pelas diferentes portas, em processo semelhante ao Port Address Translation (PAT).

A RFC 6598, publicada pelo IETF (Internet Engineering Task Force), detalha o espaço de endereço para uso do CGNAT, que pode manipular os mesmos prefixos de rede. A IANA (Internet Assigned Numbers Authority) alocou o bloco de endereço 100.64.0.0/10 para essa finalidade.

A imagem a seguir ilustra como são realizadas as implementações CGNAT pelos ISP.

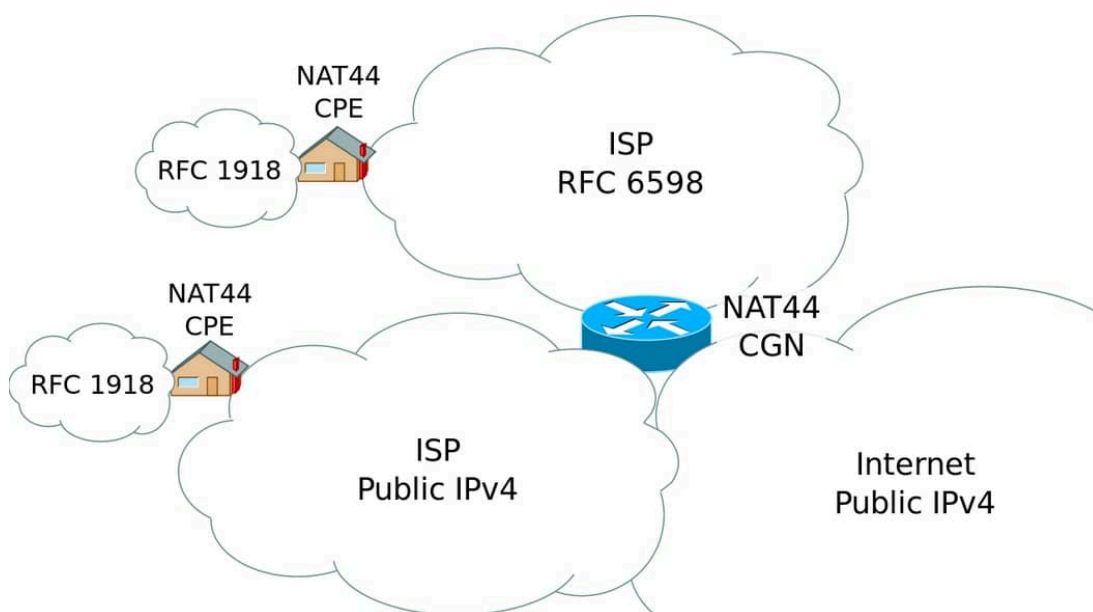


Imagem: Mro / Wikimedia Commons / CC BY-SA 3.0

📷 CGNAT.

VERIFICANDO O APRENDIZADO

1. NO CONTEXTO DAS FAIXAS DE IPV4 PRIVADAS E PÚBLICAS, IDENTIFIQUE QUAL DAS ALTERNATIVAS ABAIXO NÃO PERTENCE A NENHUMA DAS FAIXAS DE REDE PRIVADA DEFINIDAS PELA RFC 1918.
- A) 192.168.1.12
- B) 172.27.1.200
- C) 10.0.0.0
- D) 172.15.1.1
- E) 192.168.200.1
2. NO CONTEXTO DO PROCESSO DE TRADUÇÃO DE IP NETWORKING ADDRESS TRANLATION (NAT), E SUAS DERIVAÇÕES, COMO O PORT ADDRESS TRANLATION (PAT), QUAL DAS ALTERNATIVAS ABAIXO MELHOR REPRESENTA A PORTA ALOCADA PARA A TRADUÇÃO EM EVIDÊNCIA, NO PROCESSO PAT APRESENTADO NA TABELA ABAIXO?

PAT - PORT ADDRESS TRANSLATION

IP LOCAL INTERNO: PORTA ORIGEM	IP GLOBAL INTERNO: PORTA ORIGEM	IP LOCAL EXTERNO: PORTA DESTINO	IP GLOBAL EXTERNO: PORTA DESTINO
172.16.1.1:2567	200.200.200.1:2567	51.51.51.51:80	51.51.51.51:80
172.16.1.2:2567	200.200.200.1:XXXX	51.51.51.51:80	51.51.51.51:80

PAT - PORT ADDRESS TRANSLATION

172.16.1.3:4558	200.200.200.1:4558	51.51.51.51:80	51.51.51.51:80
-----------------	--------------------	----------------	----------------

⇒ UTILIZE A ROLAGEM HORIZONTAL

ELABORADA POR ISAAC SANTA RITA.

A) 2567

B) 4558

C) 2563

D) 0000

E) 2568

GABARITO

1. No contexto das faixas de IPv4 privadas e públicas, identifique qual das alternativas abaixo não pertence a nenhuma das faixas de rede privada definidas pela RFC 1918.

A alternativa "D " está correta.

Os IPs das alternativas A e E pertencem à rede 192.168.0.0/16; o da alternativa B, à rede 172.16.0.0/12; o da alternativa C, à rede 10.0.0.0/8. O IP 172.15.1.1 não pertence a nenhuma faixa de rede privada definida na RFC 1918.

2. No contexto do processo de tradução de IP Networking Address Translation (NAT), e suas derivações, como o Port Address Translation (PAT), qual das alternativas abaixo melhor representa a porta alocada para a tradução em evidência, no processo PAT apresentado na tabela abaixo?

PAT - Port Address Translation

IP local interno: porta origem	IP global interno: porta origem	IP local externo: porta destino	IP global externo: porta destino
-----------------------------------	------------------------------------	------------------------------------	--

PAT - Port Address Translation

172.16.1.1:2567	200.200.200.1:2567	51.51.51.51:80	51.51.51.51:80
172.16.1.2:2567	200.200.200.1:XXXX	51.51.51.51:80	51.51.51.51:80
172.16.1.3:4558	200.200.200.1:4558	51.51.51.51:80	51.51.51.51:80

⇨ Utilize a rolagem horizontal

Elaborada por Isaac Santa Rita.

A alternativa "E " está correta.

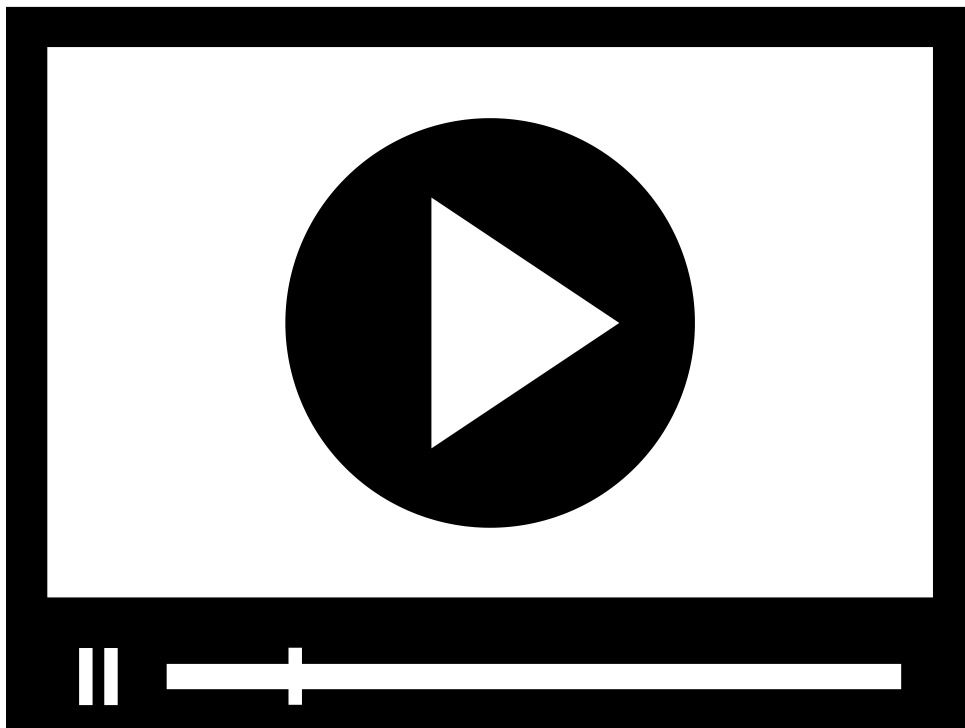
Quando duas máquinas utilizam a mesma porta de origem no acesso a um IP externo, o roteador realiza o PAT com o valor da próxima porta disponível.

$$2567 + 1 = 2568$$

MÓDULO 4

🕒 Aplicar ferramentas de análise e troubleshooting do IPv4 e seus protocolos auxiliares

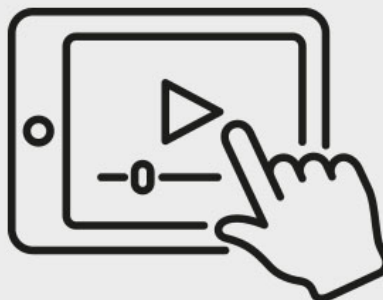
PROTOCOLOS ARP E ICMP



PROTOCOLOS ARP E ICMP

Neste vídeo, exploramos os fundamentos dos protocolos ARP e ICMP. Descubra como essas peças-chave facilitam a comunicação e resolvem problemas de conectividade, garantindo uma compreensão prática no mundo das redes.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Problemas de rede são normalmente causados pela falha de algum tipo de processo. Seguindo um roteiro, uma ordem ou um fluxograma, esses problemas podem ser solucionados por qualquer pessoa.

Em sua grande maioria, as causas raiz são identificadas por meio de um processo de eliminação (troubleshooting) que passa por todas as fases de um determinado processo.

Existem várias ferramentas, em redes de computadores, que nos auxiliam na eliminação de seus problemas mais comuns. Grande parte dessas ferramentas está baseada em dois protocolos de rede: o **ARP** (Address Resolution Protocol) e o **ICMP** (Internet Control Message Protocol).

O PROTOCOLO ARP

O ARP é definido pela RFC 826 e utilizado na associação de endereços (conversão) da camada de enlace de dados com endereços de rede, ou seja, é usado para descobrir um endereço MAC associado a um endereço IP.

Essa associação pode ser obtida, em máquinas com sistema operacional Windows por meio do comando “arp -a”. A imagem que segue apresenta a tabela ARP de uma máquina com essas características.

```
C:\Users\PC>arp -a

Interface: 192.168.56.1 --- 0xf
Endereço IP      Endereço físico    Tipo
192.168.56.255    ff-ff-ff-ff-ff-ff  estático
224.0.0.22        01-00-5e-00-00-16  estático
224.0.0.251       01-00-5e-00-00-fb  estático
224.0.0.252       01-00-5e-00-00-fc  estático
239.255.255.250   01-00-5e-7f-ff-fa  estático
255.255.255.255   ff-ff-ff-ff-ff-ff  estático

Interface: 192.168.0.17 --- 0x17
Endereço IP      Endereço físico    Tipo
192.168.0.1       74-3a-ef-dc-52-58  dinâmico
192.168.0.15      6c-ad-f8-29-66-ad  dinâmico
192.168.0.255     ff-ff-ff-ff-ff-ff  estático
224.0.0.22        01-00-5e-00-00-16  estático
224.0.0.251       01-00-5e-00-00-fb  estático
224.0.0.252       01-00-5e-00-00-fc  estático
239.255.255.250   01-00-5e-7f-ff-fa  estático
255.255.255.255   ff-ff-ff-ff-ff-ff  estático

C:\Users\PC>
```

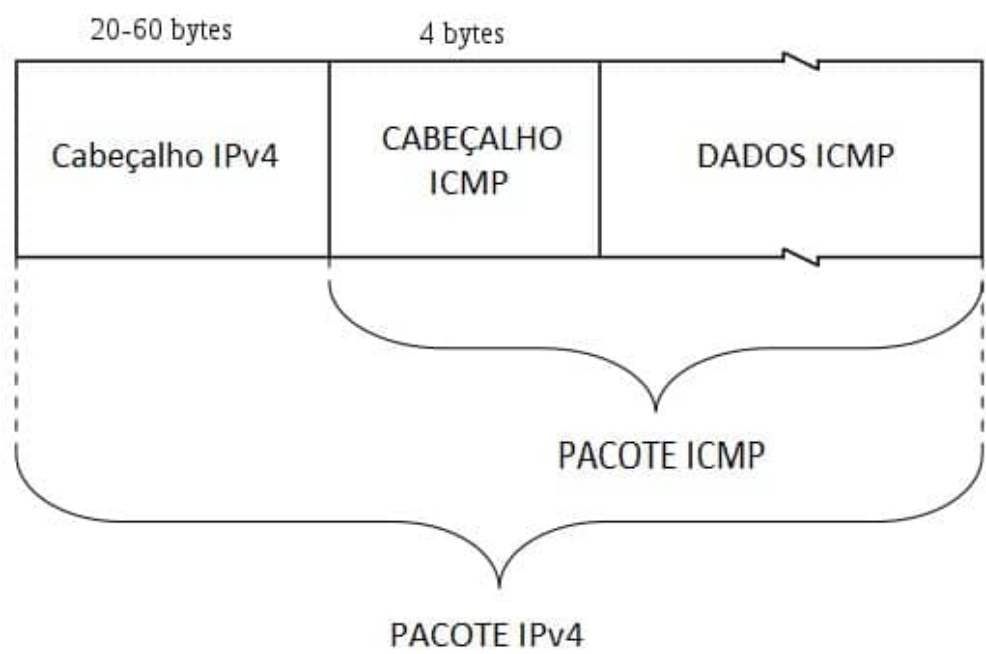
📷 ARP.

Captura de tela com o comando “arp” no Prompt de Comando do Windows.

Cabe ressaltar que, por meio da observação da tabela ARP de uma máquina, é possível, entre outras coisas, identificar o endereço MAC do default gateway de uma rede. Na imagem apresentada, podemos verificar que o endereço MAC do default gateway (192.168.0.1) dessa rede é o 74-3a-ef-dc-52-58.

O PROTOCOLO ICMP

O ICMP (Internet Control Message Protocol) é um protocolo da camada de rede do modelo OSI, definido pela RFC 792, normalmente utilizado para fornecer relatórios de erros ao remetente. Esse protocolo está inserido no campo de dados do pacote IP, conforme imagem a seguir:



📷 ICMP.

O ICMP apresenta a estrutura ilustrada no quadro que segue, cujos campos têm a seguinte finalidade:

Byte	0	1	2	3
0	Tipo	Código	Checksum	
32	Resto do Cabeçalho (Rest of Header)			

⇒ Utilize a rolagem horizontal

Quadro: Estrutura do ICMP

Elaborado por Isaac Santa Rita.

TIPO

Especifica o tipo de mensagem ICMP.

CÓDIGO

Especifica o código (subtipo) de mensagem ICMP.

CHECKSUM

Verificação da integridade de dados.

RESTO DO CABEÇALHO

Dependente do tipo e código do ICMP.

O quadro a seguir apresenta a relação entre os principais tipos do ICMP e seus respectivos códigos.

Tipo	Código	Descrição
0 – Echo Reply	0	Resposta Echo (usado para fazer ping)

Tipo	Código	Descrição
1 and 2		Reservado
3 – Destination Unreachable	0	Rede de destino inacessível
	1	Máquina de destino inacessível
	2	Protocolo de destino inacessível
	3	Porta de destino inacessível
	4	Fragmentação necessária, mas impossível devido à bandeira (flag) DF
	5	Falha na rota de origem
	6	Rede de destino desconhecida
	7	Máquina de destino desconhecida
4 – Source Quench	0	Source quench (Controle de Congestionamento)
5 – Redirect Message	0	Redirecionamento do datagrama para a rede
	1	Redirecionamento do datagrama para a máquina
	2	Redirecionamento do datagrama para o ToS & rede
	3	Redirecionamento do datagrama para o ToS & máquina

Tipo	Código	Descrição
8 – Echo Request	0	Solicitação de resposta (ping)
9- Router Advertisement		Anúncio do roteador
10 – Router Solicitation	0	Descoberta de roteador/solicitação
11 – Time Exceeded	0	TTL expired in transit

⇒ Utilize a rolagem horizontal

Quadro: Principais tipos e códigos ICMP.

Elaborado por Isaac Santa Rita.

RESUMINDO

As mensagens ICMP, em resumo, permitem verificar:

A acessibilidade do host.

Destino ou serviço inalcançável.

Tempo excedido.

Quanto à acessibilidade, as mensagens do tipo Echo permitem o teste de capacidade de acesso a uma determinada máquina na rede de dados.

As mensagens de destino ICMP inacessível podem ser usadas para notificar o remetente sobre um dos motivos da inacessibilidade. Os códigos de inacessibilidade mais comuns estão evidenciados no quadro que segue:

Tipo	Código	Descrição
3 – Destination Unreachable	0	Rede de destino inacessível

Tipo	Código	Descrição
	1	Máquina de destino inacessível
	2	Protocolo de destino inacessível
	3	Porta de destino inacessível

⇒ Utilize a rolagem horizontal

Quadro: Códigos tipo 3 do ICMP.

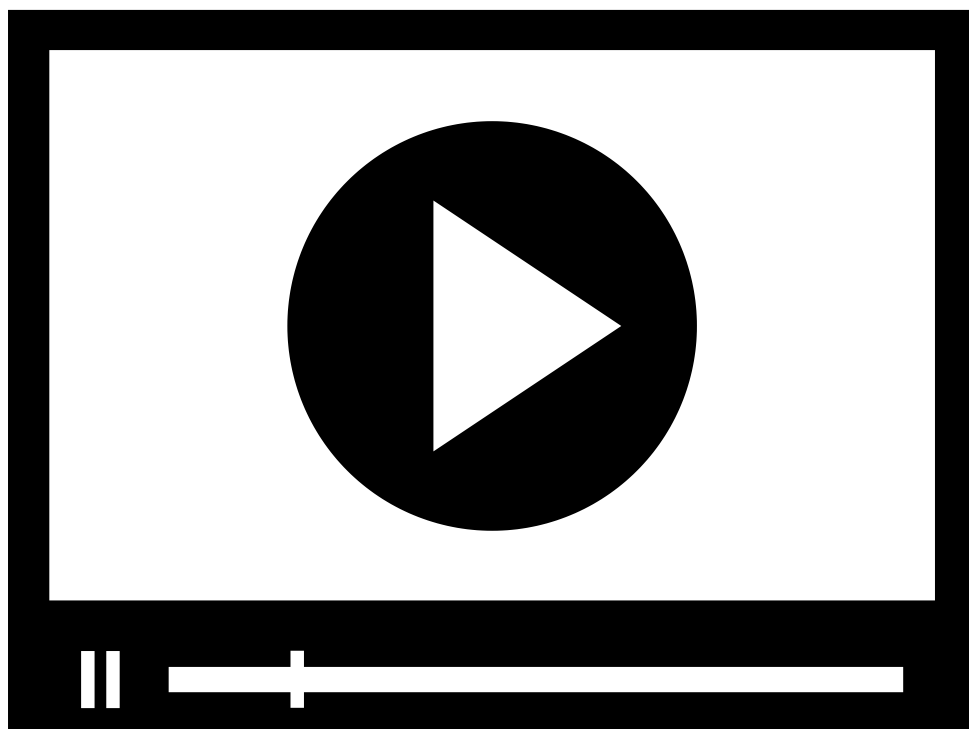
Elaborado por Isaac Santa Rita.

Em relação ao tempo excedido, toda vez que o tempo de vida (TTL) do pacote IP for reduzido a zero, uma mensagem tipo 11 (Time Exceeded) ICMP será enviada ao remetente.

É possível perceber, portanto, que o ICMP possui grande capacidade de auxiliar na realização de troubleshooting de rede. Nesse sentido, foram desenvolvidas diversas ferramentas com essa finalidade, destacando-se aqui o ping e o traceroute.

WIRESHARK

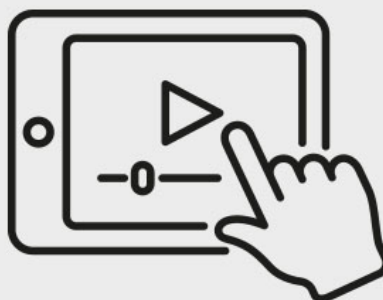
O Wireshark é o analisador de protocolo de rede mais utilizado no mundo. Ele permite visualizar o que está acontecendo na sua rede em um nível microscópico.



ANALISANDO A TROCA DE TRÁFEGO IP

Estamos quase finalizando o nosso conteúdo. Antes de prosseguir, assista ao vídeo a seguir em que explicamos, passo a passo, a troca de mensagens e as informações mais relevantes.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



O desenvolvimento do Wireshark foi iniciado em 1998 e atualmente é realizado por meio de contribuições voluntárias de especialistas em rede de todo o mundo.

Com essa ferramenta, é possível observar todas as características dos protocolos das diversas camadas do modelo OSI. A imagem a seguir apresenta a captura de um pacote ICMP, na qual podem ser verificadas as seguintes informações úteis:

IPv4 de origem: 192.168.0.17

IPv4 de destino: 8.8.8.8

Tipo de protocolo: ICMP

Time to Live: 128

Type: 8 (Echo Request)

Código: 0

Wireshark packet capture showing ICMP Echo (ping) request and reply. The packet list shows a request from 192.168.0.17 to 8.8.8.8 with TTL=128. The packet details show the ICMP Echo (ping) request with Type 8 and Code 0. The packet bytes show the raw data of the ICMP request.

ESCOLHA DO PACOTE ANALISADO

ANALISE DO PACOTE

📷 Wireshark.

Captura de tela do software Wireshark, adaptado por Isaac Santa Rita.

PING

O ping é uma ferramenta de teste de conectividade que utiliza o ICMP como base, mais especificamente as mensagens ICMP tipo 8 (Echo Request) e tipo 0 (Echo Reply). Além disso, ela é capaz de informar a taxa de sucesso e o tempo médio de ida até o destino e volta.

📣 ATENÇÃO

Caso a mensagem ICMP não receba a resposta esperada, a ferramenta ping apresenta uma mensagem informando que a resposta não foi recebida.

A imagem a seguir apresenta os testes de conectividade executados por uma máquina com sistema operacional Microsoft Windows, e outra com o sistema operacional Cisco IOS.

PING Maq Windows

```
C:\Users\>
C:\Users\>ping 192.168.0.1

Disparando 192.168.0.1 com 32 bytes de dados:
Resposta de 192.168.0.1: bytes=32 tempo=9ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=17ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=8ms TTL=64
Resposta de 192.168.0.1: bytes=32 tempo=15ms TTL=64

Estatísticas do Ping para 192.168.0.1:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 8ms, Máximo = 17ms, Média = 12ms

C:\Users\>
```

PING Maq Cisco IOS

```
S1#ping 192.168.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

📷 Ping em Windows e Cisco IOS.

Captura de tela com o comando “ping” no Prompt de Comando do Windows e no Cisco IOS.

TESTE DE CONEXÃO LOCAL

O ping pode ser utilizado para testar a conectividade local, basta efetuar o comando para qualquer IPv4 da rede 127.0.0.0/8. É comum, entretanto, a utilização do IPv4 127.0.0.1 ou do nome localhost para essa finalidade.

A imagem que segue ilustra o teste de rede de conectividade local efetuado utilizando o nome localhost. É possível observar a tradução do nome localhost para o IPv4 127.0.0.1.

```
C:\>
C:\>ping localhost

Pinging localhost with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time=6ms TTL=128
Reply from 127.0.0.1: bytes=32 time=2ms TTL=128
Reply from 127.0.0.1: bytes=32 time=1ms TTL=128
Reply from 127.0.0.1: bytes=32 time=2ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 6ms, Average = 2ms

C:\>
```

📷 Ping: teste de conexão local.

Captura de tela com o comando ping no Prompt de Comando do Windows.

TESTE DE CONEXÃO COM O GATEWAY

O gateway padrão de um dispositivo é o equipamento que dá acesso deste dispositivo a outras redes além de sua rede local. É através dele que os pacotes podem, por exemplo, chegar à Internet.

Por isso, testar a conectividade entre um dispositivo e seu gateway é o primeiro passo para garantir o acesso de um dispositivo às redes remotas.

Uma vez observado o IP do default gateway de um dispositivo, é possível testar a conexão entre eles por meio do comando ping, como ilustrado a seguir.


```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Link-local IPv6 Address.....:
FE80::2D0:BAFF:FE1E:B0C
    IP Address.....: 192.168.0.1
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: 192.168.0.254

Bluetooth Connection:

    Link-local IPv6 Address.....: ::
    IP Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: 0.0.0.0

C:\>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:

Reply from 192.168.0.254: bytes=32 time<1ms TTL=255
Reply from 192.168.0.254: bytes=32 time<1ms TTL=255
Reply from 192.168.0.254: bytes=32 time<1ms TTL=255
Reply from 192.168.0.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>|
```

📷 PING Teste Gateway.

Captura de tela com o comando “ipconfig” e “ping” no Prompt de Comando do Windows.

EXERCÍCIO

Vamos verificar a troca de pacotes no ping por meio de uma captura?

1. Você pode efetuar uma captura por intermédio do Wireshark, realizando o ping para o default gateway da sua rede. Você também pode baixar o arquivo pcap **Teste Ping Gw** com uma captura já pronta.

Para você visualizar os pacotes ICMP, você pode digitar ICMP no filtro ou filtrar pelo endereço IP do roteador, digitando: **ip.addr == (IP do seu default gateway)**.

Padrão de resposta

Nas imagens que seguem, podemos visualizar a captura que foi disponibilizada, filtrada pelo protocolo ICMP. Na primeira imagem, podemos verificar a mensagem de Echo do ICMP; na segunda mensagem, a mensagem de reply do ICMP.

No.	Time	Source	Destination	Protocol	Length	Info
6	3.345356	192.168.0.17	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=6273/33048, ttl=128 (reply in 7)
7	3.356655	192.168.0.1	192.168.0.17	ICMP	74	Echo (ping) reply id=0x0001, seq=6273/33048, ttl=64 (request in 6)
8	4.355020	192.168.0.17	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=6274/33304, ttl=128 (reply in 9)
9	4.369131	192.168.0.1	192.168.0.17	ICMP	74	Echo (ping) reply id=0x0001, seq=6274/33304, ttl=64 (request in 8)
10	5.366541	192.168.0.17	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=6275/33560, ttl=128 (reply in 11)
11	5.377750	192.168.0.1	192.168.0.17	ICMP	74	Echo (ping) reply id=0x0001, seq=6275/33560, ttl=64 (request in 10)
12	6.379459	192.168.0.17	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=6276/33816, ttl=128 (reply in 13)
13	6.390954	192.168.0.1	192.168.0.17	ICMP	74	Echo (ping) reply id=0x0001, seq=6276/33816, ttl=64 (request in 12)

> Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F329805E-C33D-479F-8935-D80E8F75EF73}, id 0

> Ethernet II, Src: IntelCor_11:e2:7f (dc:53:60:11:e2:7f), Dst: Kaonmedi_dc:52:58 (74:3a:ef:dc:52:58)

> Internet Protocol Version 4, Src: 192.168.0.17, Dst: 192.168.0.1

> Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

[Checksum: 0x34da [correct]]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 6273 (0x1881)

Sequence Number (LE): 33048 (0x8118)

[Request frame: 7]

> Data (32 bytes)

No.	Time	Source	Destination	Protocol	Length	Info
6	3.345356	192.168.0.17	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=6273/33048, ttl=128 (reply in 7)
7	3.356655	192.168.0.1	192.168.0.17	ICMP	74	Echo (ping) reply id=0x0001, seq=6273/33048, ttl=64 (request in 6)
8	4.355020	192.168.0.17	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=6274/33304, ttl=128 (reply in 9)
9	4.369131	192.168.0.1	192.168.0.17	ICMP	74	Echo (ping) reply id=0x0001, seq=6274/33304, ttl=64 (request in 8)
10	5.366541	192.168.0.17	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=6275/33560, ttl=128 (reply in 11)
11	5.377750	192.168.0.1	192.168.0.17	ICMP	74	Echo (ping) reply id=0x0001, seq=6275/33560, ttl=64 (request in 10)
12	6.379459	192.168.0.17	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=6276/33816, ttl=128 (reply in 13)
13	6.390954	192.168.0.1	192.168.0.17	ICMP	74	Echo (ping) reply id=0x0001, seq=6276/33816, ttl=64 (request in 12)

> Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F329805E-C33D-479F-8935-D80E8F75EF73}, id 0

> Ethernet II, Src: Kaonmedi_dc:52:58 (74:3a:ef:dc:52:58), Dst: IntelCor_11:e2:7f (dc:53:60:11:e2:7f)

> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.17

> Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

[Checksum: 0x3cda [correct]]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 6273 (0x1881)

Sequence Number (LE): 33048 (0x8118)

[Request frame: 6]

[Response time: 11,299 ms]

> Data (32 bytes)

Capturas de tela do software Wireshark.

TESTE DE CONEXÃO COM EQUIPAMENTO REMOTO

O ping também pode ser utilizado para testar a comunicação com um equipamento remoto, pois os roteadores possuem a capacidade de rotear pacotes ICMP até o seu destino.

COMENTÁRIO

Cabe ressaltar, entretanto, que muitos administradores de rede e dispositivos finais proíbem a entrada de pacotes ICMP, o que pode resultar num teste de conectividade sem resposta.

A imagem a seguir ilustra um teste de conexão remota entre um computador em uma rede privada e o DNS do Google, que está disponível na Internet e sob o IPv4 8.8.8.8 ou 8.8.4.4.

```
C:\Users\>
C:\Users\>ping 8.8.8.8

Disparando 8.8.8.8 com 32 bytes de dados:
Resposta de 8.8.8.8: bytes=32 tempo=23ms TTL=117
Resposta de 8.8.8.8: bytes=32 tempo=25ms TTL=117
Resposta de 8.8.8.8: bytes=32 tempo=19ms TTL=117
Resposta de 8.8.8.8: bytes=32 tempo=21ms TTL=117

Estatísticas do Ping para 8.8.8.8:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 19ms, Máximo = 25ms, Média = 22ms

C:\Users\>ping 8.8.4.4

Disparando 8.8.4.4 com 32 bytes de dados:
Resposta de 8.8.4.4: bytes=32 tempo=20ms TTL=117
Resposta de 8.8.4.4: bytes=32 tempo=16ms TTL=117
Resposta de 8.8.4.4: bytes=32 tempo=16ms TTL=117
Resposta de 8.8.4.4: bytes=32 tempo=19ms TTL=117

Estatísticas do Ping para 8.8.4.4:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 16ms, Máximo = 20ms, Média = 17ms

C:\Users\>
```

📷 Ping: teste host remoto.

Captura de tela com o comando “ping” no Prompt de Comando do Windows.

EXERCÍCIO

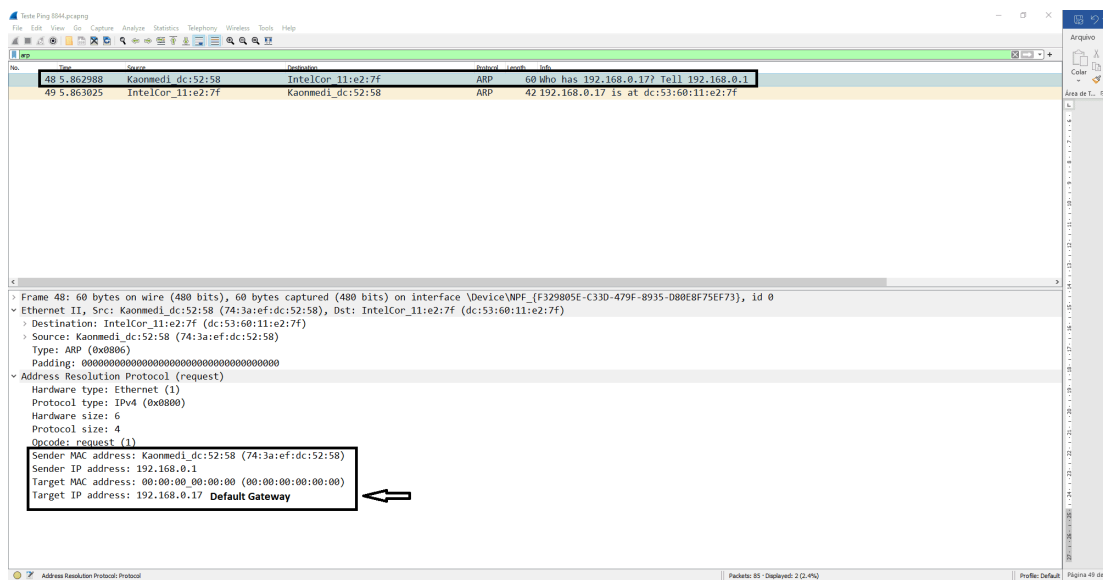
Você está pronto para praticar mais uma vez? Acompanhe o exercício:

2. Faremos agora uma captura realizando um ping para um endereço externo à sua rede. Você pode realizar uma nova captura ou baixar uma captura pronta com teste de conexão com o IP 8.8.4.4 em **Teste Ping 8844**.

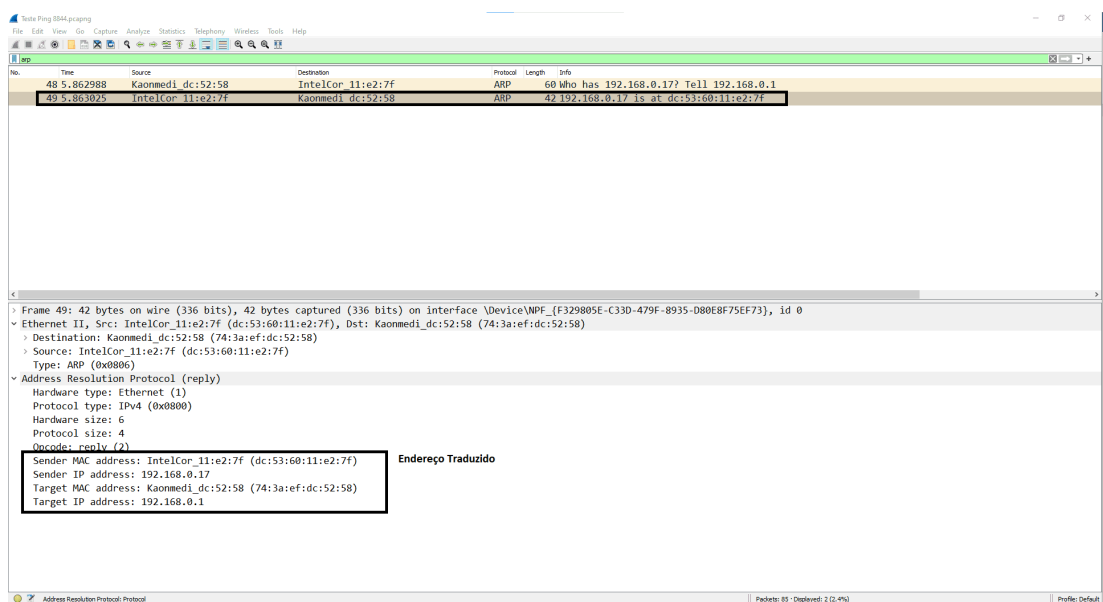
Para você visualizar os pacotes ICMP, você pode digitar ICMP no filtro ou filtrar pelo endereço IP do endereço externo que você utilizou, digitando: **ip.addr == (IP do seu default gateway)**. Para a captura disponibilizada, o filtro foi **ip.addr == 8.8.4.4**

Padrão de resposta

Nas imagens abaixo, podemos visualizar a troca de mensagens do protocolo ICMP com uma máquina externa à rede. Observe nas duas primeiras imagens que, inicialmente, o protocolo ARP é utilizado para realizar a descoberta do endereço físico (MAC) do default gateway.

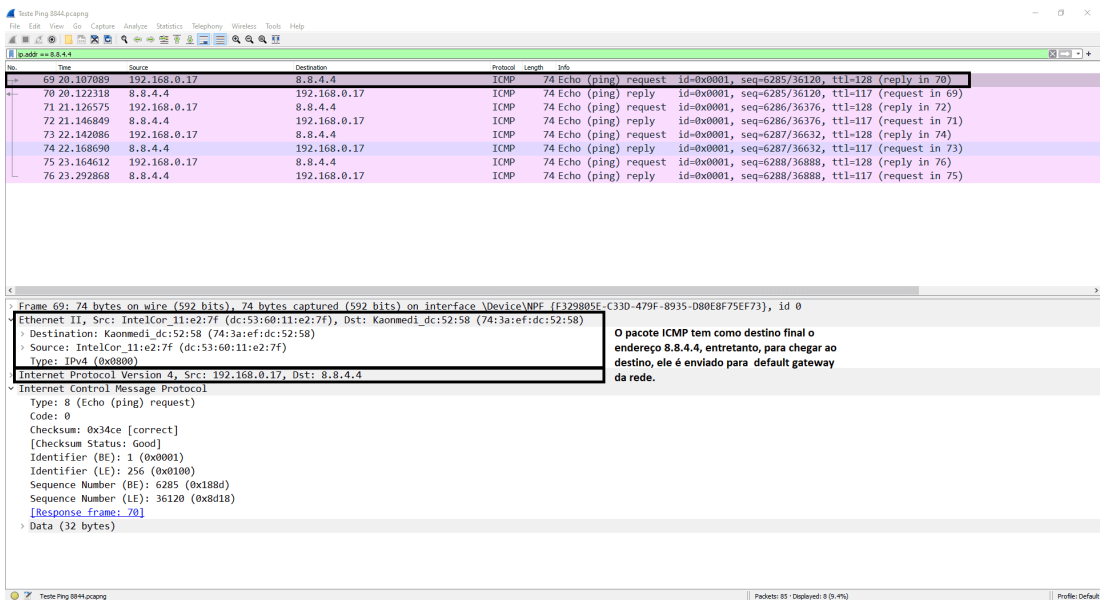


📷 Captura de tela do software Wireshark.

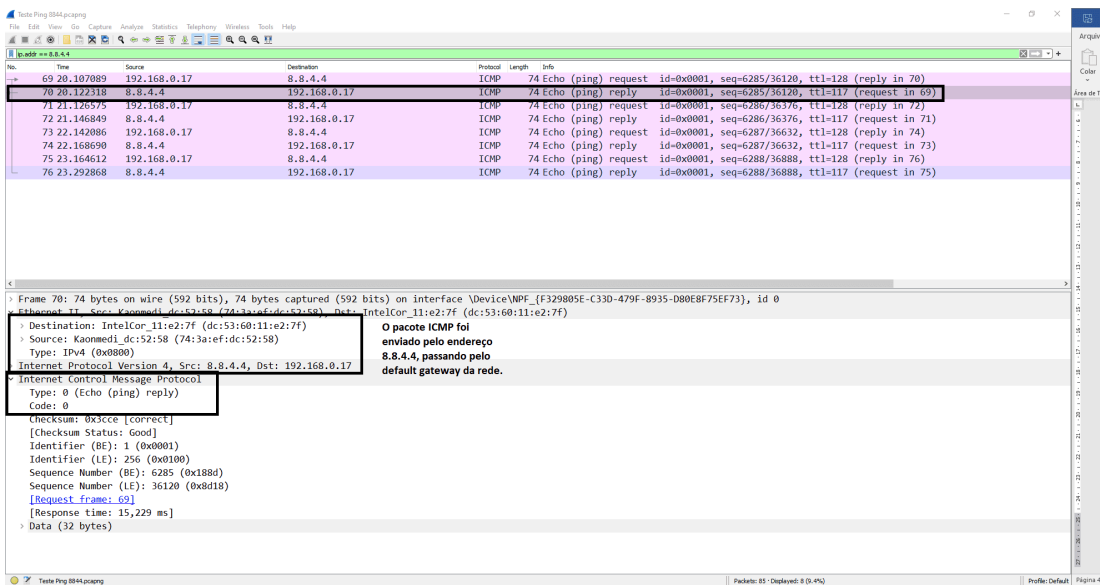


📷 Captura de tela do software Wireshark.

Após a descoberta do endereço físico do gateway, os pacotes ICMP são enviados, com o endereço IP de destino sendo o 8.8.4.4 e o endereço físico de destino sendo o default gateway da rede.



📷 Captura de tela do software Wireshark.



📷 Captura de tela do software Wireshark.

TRACEROUTE

O traceroute, também conhecido como tracert, é uma ferramenta utilizada para testar o caminho entre dois dispositivos. Nesse teste, ele é capaz de mostrar os equipamentos roteadores envolvidos no processo de encaminhamento do pacote até seu destino.

Outra facilidade apresentada pelo traceroute é a capacidade de fornecer o tempo de ida e volta até cada um dos roteadores envolvidos no processo. Um asterisco (*) é usado para indicar um pacote perdido ou não respondido.

As informações fornecidas pelo traceroute podem ser usadas para localizar um roteador com problemas ou identificar problemas de roteamento, como o loop de rede.

A imagem a seguir ilustra um traceroute entre um computador em uma rede privada e o DNS do Google. Nesse teste, é possível identificar todos os roteadores que um pacote irá percorrer até chegar naquele DNS.

```
C:\Users\ >tracert -d 8.8.8.8

Rastreando a rota para 8.8.8.8 com no máximo 30 saltos

 1    9 ms    10 ms    10 ms    192.168.0.1
 2   16 ms    19 ms    22 ms    100.84.64.1
 3   21 ms    58 ms    25 ms    201.17.9.173
 4   28 ms    24 ms    66 ms    201.17.5.48
 5   85 ms    31 ms    21 ms    201.17.34.197
 6   19 ms    16 ms    19 ms    201.17.34.146
 7   49 ms    22 ms    22 ms    201.17.31.202
 8   43 ms    16 ms    46 ms    142.250.39.113
 9   19 ms    21 ms    22 ms    142.251.48.163
10   40 ms    21 ms    25 ms    8.8.8.8

Rastreamento concluído.
C:\Users\ >
```

Traceroute.

Captura de tela com o comando tracert no Prompt de Comando do Windows.

Para realizar essa tarefa, o traceroute envia a primeira mensagem ao destino com valor de campo TTL igual a 1. Isso faz com que o TTL atinja o tempo limite no primeiro roteador. Em seguida, esse roteador responde com uma mensagem de tempo excedido ICMP, quando é identificado pela ferramenta.

Na sequência, o traceroute aumenta progressivamente o campo TTL (2, 3, 4 e assim por diante) das mensagens subsequentes. Isso permite à ferramenta identificar o endereço IP de cada salto à medida que o TTL de cada pacote atinge o valor zero ao longo do caminho.

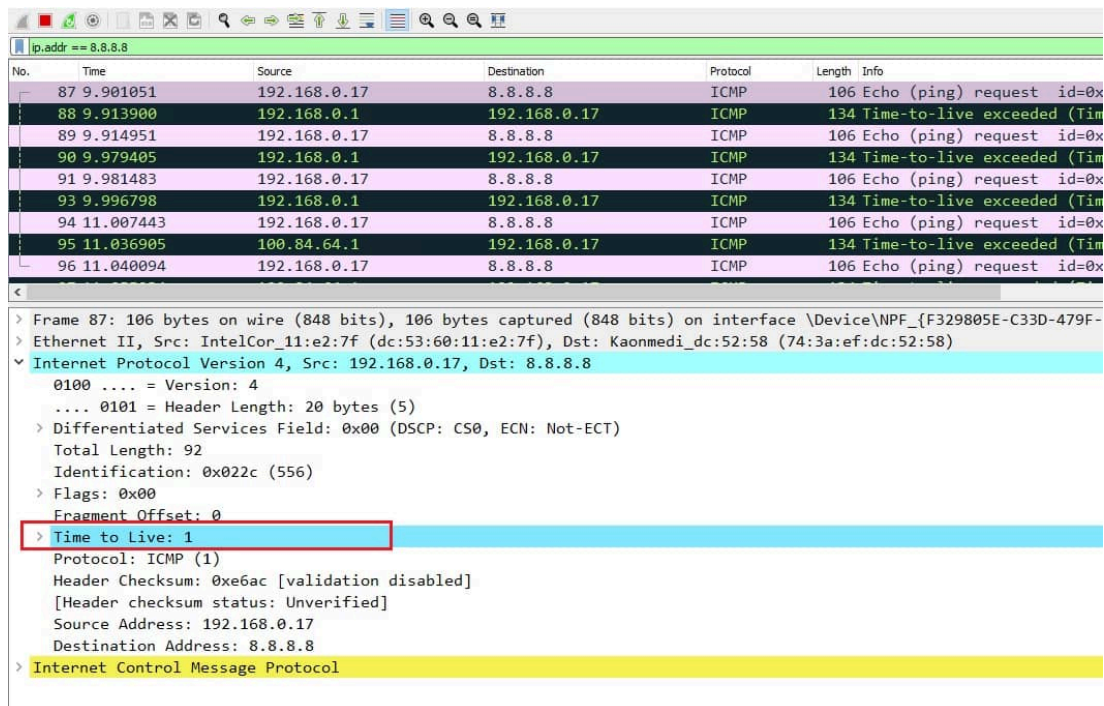
EXEMPLO

Vamos à nossa última atividade?

3. Efetue a captura de pacotes ICMP com teste de traceroute para o IPv4 8.8.4.4. Observe as respostas com ICMP Tipo 11 (Time-to-Live Exceeded). Você também pode baixar uma captura pronta em **Teste Traceroute 8844**. Para este arquivo, utilize o filtro: **ip.addr == 8.8.4.4**.

Padrão de resposta

A imagem abaixo apresenta a captura de tela de um traceroute realizado para o IPv4 8.8.4.4. Nessa captura, evidencia-se o envio de um pacote ICMP com TLL com valor unitário.



No.	Time	Source	Destination	Protocol	Length	Info
87	9.901051	192.168.0.17	8.8.8.8	ICMP	106	Echo (ping) request id=0x...
88	9.913900	192.168.0.1	192.168.0.17	ICMP	134	Time-to-live exceeded (Tim...
89	9.914951	192.168.0.17	8.8.8.8	ICMP	106	Echo (ping) request id=0x...
90	9.979405	192.168.0.1	192.168.0.17	ICMP	134	Time-to-live exceeded (Tim...
91	9.981483	192.168.0.17	8.8.8.8	ICMP	106	Echo (ping) request id=0x...
93	9.996798	192.168.0.1	192.168.0.17	ICMP	134	Time-to-live exceeded (Tim...
94	11.007443	192.168.0.17	8.8.8.8	ICMP	106	Echo (ping) request id=0x...
95	11.036905	100.84.64.1	192.168.0.17	ICMP	134	Time-to-live exceeded (Tim...
96	11.040094	192.168.0.17	8.8.8.8	ICMP	106	Echo (ping) request id=0x...

> Frame 87: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{F329805E-C33D-479F-...}

> Ethernet II, Src: IntelCor_11:e2:7f (dc:53:60:11:e2:7f), Dst: Kaonmedi_dc:52:58 (74:3a:ef:dc:52:58)

> Internet Protocol Version 4, Src: 192.168.0.17, Dst: 8.8.8.8

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 92

Identification: 0x022c (556)

Flags: 0x00

Fragment Offset: 0

> Time to Live: 1

Protocol: ICMP (1)

Header Checksum: 0xe6ac [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.0.17

Destination Address: 8.8.8.8

> Internet Control Message Protocol

📷 ICMP TTL 1.

Captura da tela do software Wireshark.

VERIFICANDO O APRENDIZADO

1. ACERCA DAS FERRAMENTAS DE TROUBLESHOOTING PARA O PROTOCOLO IPV4, IDENTIFIQUE DENTRE AS ALTERNATIVAS APRESENTADAS AQUELA QUE APRESENTA O IP DE ORIGEM DO PACOTE ANALISADO.

No.	Time	Source	Destination	Protocol	Length	Info
8027	89.059900	192.168.0.17	192.168.0.1	HTTP	387	GET /assets/img/logo-claro.jpg HTTP/1.1
8036	89.082317	192.168.0.17	192.168.0.1	HTTP	440	GET /assets/fonts/futuram.woff2 HTTP/1.1
8037	89.082612	192.168.0.17	192.168.0.1	HTTP	439	GET /assets/fonts/futult.woff2 HTTP/1.1
8053	89.097391	192.168.0.17	192.168.0.1	HTTP	426	GET /header_disable_ui.html HTTP/1.1
8058	89.107516	192.168.0.1	192.168.0.17	HTTP	1113	HTTP/1.1 200 Ok (image/jpeg)
8079	89.131427	192.168.0.1	192.168.0.17	HTTP	289	HTTP/1.1 200 Ok (text/html)
8094	89.139763	192.168.0.1	192.168.0.17	HTTP	972	HTTP/1.1 200 Ok (text/html)
8140	89.341868	192.168.0.1	192.168.0.17	HTTP	1470	HTTP/1.1 200 Ok (text/html)
8147	89.373055	192.168.0.17	192.168.0.1	HTTP	445	GET /assets/fonts/irone-net.ttf HTTP/1.1

> Frame 8053: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits) on interface \Device\NPF_{F329805E-C33D-479F-8935-D80E8F75EF73}, id 0
 > Ethernet II, Src: IntelCor_11:e2:7f (dc:53:60:11:e2:7f), Dst: Kaonmedi_dc:52:58 (74:3a:ef:dc:52:58)
 > Internet Protocol Version 4, Src: 192.168.0.17, Dst: 192.168.0.1
 > 0100 = Version: 4
 > 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 > Total Length: 412
 > Identification: 0x56c7 (22215)
 > Flags: 0x40, Don't fragment
 > Fragment Offset: 0
 > Time to Live: 128
 > Protocol: TCP (6)
 > Header Checksum: 0x2132 [validation disabled]
 > [Header checksum status: Unverified]
 > Source Address: 192.168.0.17
 > Destination Address: 192.168.0.1
 > Transmission Control Protocol, Src Port: 65472, Dst Port: 80, Seq: 1, Ack: 1, Len: 372
 > Hypertext Transfer Protocol

📷 PACOTE ANALISADO.

CAPTURE DA TELA DO SOFTWARE WIRESHARK.

- A) 192.168.0.1
- B) 172.16.0.1
- C) 192.168.0.17
- D) 192.168.1.17
- E) 8.8.8.8

2. SOBRE O AS FERRAMENTAS DE TRACEROUTE E SUAS POSSIBILIDADE DE AJUDA NO PROCESSO DE TROUBLESHOOTING DE REDES, IDENTIFIQUE DENTRE AS ALTERNATIVAS APRESENTADAS AQUELA QUE APRESENTA O NÚMERO DE SALTOS (ROTEADORES) QUE A MÁQUINA DE ORIGEM PASSA ATÉ ATINGIR SEU OBJETIVO (IPV4 200.244.19.141).


```
C:\Users\>tracert -d 200.244.19.141

Rastreando a rota para 200.244.19.141 com no máximo 30 saltos

 1  13 ms    19 ms    11 ms    192.168.0.1
 2  40 ms    23 ms    50 ms    100.84.64.1
 3  61 ms    122 ms   21 ms    201.17.9.173
 4  79 ms    120 ms    30 ms    201.17.5.48
 5  72 ms    61 ms    21 ms    200.179.69.121
 6  152 ms   27 ms    19 ms    200.244.19.141

Rastreamento concluído.

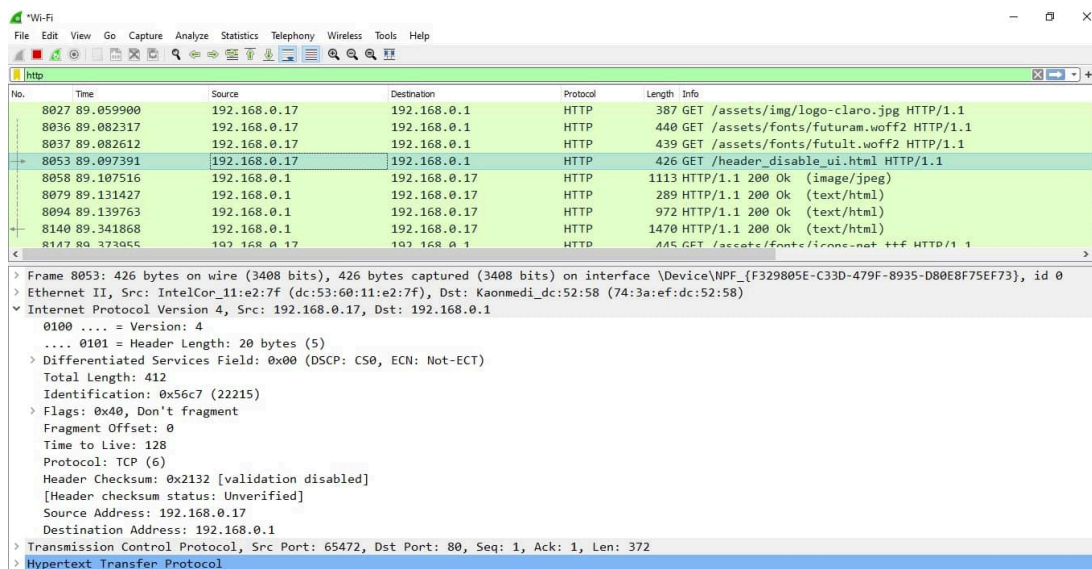
C:\Users\>
```

📷 CAPTURA DO COMANDO TRACERT NO PROMPT DE COMANDO DO WINDOWS.

- A) 6 roteadores
- B) 5 roteadores
- C) 4 roteadores
- D) 3 roteadores
- E) 2 roteadores

GABARITO

1. Acerca das ferramentas de troubleshooting para o protocolo IPv4, identifique dentre as alternativas apresentadas aquela que apresenta o IP de origem do pacote analisado.



📷 Pacote analisado.

Captura da tela do software Wireshark.

A alternativa "C" está correta.

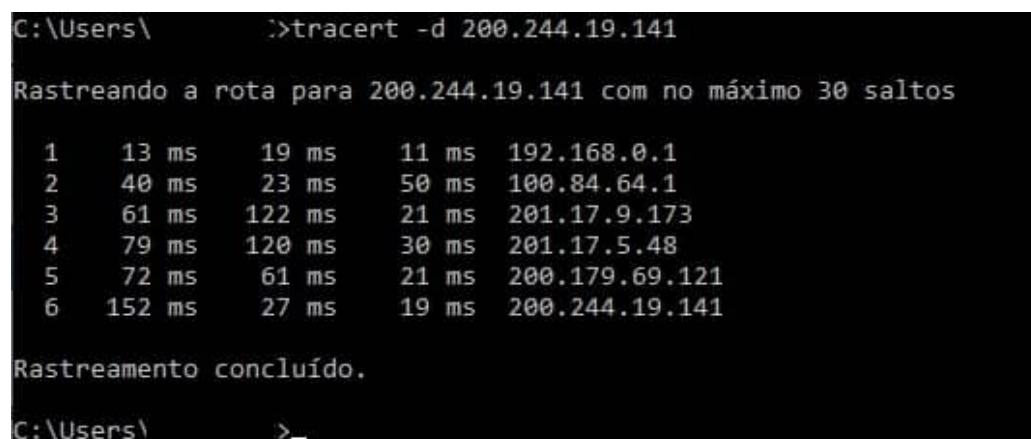
IPv4 de origem: 192.168.0.17

IPv4 de destino: 192.168.0.1

Tipo de protocolo: HTTP

Time to Live: 128

2. Sobre o as ferramentas de traceroute e suas possibilidade de ajuda no processo de troubleshooting de redes, identifique dentre as alternativas apresentadas aquela que apresenta o número de saltos (roteadores) que a máquina de origem passa até atingir seu objetivo (IPv4 200.244.19.141).



📷 Captura do comando tracert no Prompt de Comando do Windows.

A alternativa "B" está correta.

Serão cinco roteadores, sendo eles:

192.168.0.1

100.84.64.1

201.17.9.173

201.17.5.48

200.179.69.121

A última linha corresponde ao endereço do destino a ser alcançado: 200.244.19.141.

CONCLUSÃO

CONSIDERAÇÕES FINAIS

Neste estudo, vimos os conceitos básicos do protocolo de rede IPv4 e como ele pode nos auxiliar na criação de redes IPv4 dos mais variados tamanhos por meio do emprego da máscara de rede.

Mostramos que existem faixas numéricas de IP destinadas à navegação na Internet e outras dedicadas à comunicação interna das instituições.

Ainda, reconhecemos os mecanismos utilizados para que os dispositivos internos das instituições possam usufruir dos benefícios da navegação na rede mundial de computadores. Entendemos como os técnicos de rede podem utilizar ferramentas para realizar troubleshooting em suas redes de computadores.

A partir deste momento, é necessário aprofundar o estudo nos outros protocolos da camada de rede do modelo OSI, para aperfeiçoar o entendimento do processo de endereçamento e roteamento nas redes de computadores.

Para ouvir um *podcast* sobre o assunto, acesse a versão online deste conteúdo.



Podcast sobre o assunto

REFERÊNCIAS

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet**: uma abordagem top-down. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2011.

EXPLORE+

Para se aprofundar no assunto, procure na Internet as RFC do protocolo IPv4 comentadas neste estudo.

CONTEUDISTA

Isaac Newton Ferreira Santa Rita

 **CURRÍCULO LATTES**