

Unidade 2 - Webaula 6 - Camada de Rede - Protocolos

Olá! Tudo bem?

Seja bem-vindo(a) à Webaula 6 de **Redes de Computadores**.

INTRODUÇÃO

Introdução à Webaula 6

TÓPICO 1

Protocolos de Rede

Atividade de Passagem

TÓPICO 2


Endereços de Rede

Atividade de Passagem

RESUMO

Resumo da Webaula 6

REFERÊNCIAS

 **Referências**

 **Créditos**

Introdução à Webaula 6

Olá!

Quando você está navegando pela internet, já parou para pensar como é possível navegar por qualquer canto do mundo com apenas um click? Pois é graças à camada de rede do modelo TCP/IP que isso é possível, pois é ela que é responsável por encontrar o melhor caminho desde um equipamento de origem até qualquer um de destino para encaminhar os pacotes gerados a partir dos dados da camada de transporte, independentemente da tecnologia de transmissão utilizada (KUROSE; ROSS, 2013).

Antes de analisar como é que a camada de rede avalia qual o melhor caminho a ser seguido pelos pacotes para que cheguem ao destino, nesta aula serão apresentados os protocolos utilizados nessa camada que são utilizados para transportar os dados ao longo desse percurso de rede.

E então, vamos começar?

CONTINUE

Protocolos de Rede

O elemento que mantém a internet unida é o protocolo de camada de rede, o IP (*Internet Protocol*), definido no padrão IETF RFC 791, nas versões **IPv4** e **IPv6**. A tarefa do IP é fornecer a melhor forma de transportar pacotes entre equipamentos da origem até um destino, independentemente de eles estarem em uma mesma rede ou em redes distintas (KUROSE; ROSS, 2013).

Um pacote IPv4 consiste em duas partes: cabeçalho e dados. O cabeçalho tem uma parte fixa de 20 bytes e uma parte opcional de tamanho variável. O formato da parte fixa do cabeçalho está mostrado na Figura 1.

Figura 1 - Formato do Cabeçalho Fixo do IPv4

1	1	2	2	2	1	1	2	4	4
Versão	Tipo	Compr.	Id.	Offset	Tempo	Protoc.	Soma	Origem	Destino

Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

Observe atentamente a função de cada um desses campos e perceba a quantidade de informação que o cabeçalho IPv4 carrega. Os campos fixos deste cabeçalho são:

- **versão:** controla a versão do protocolo IP e o tamanho do seu cabeçalho (parte fixa mais a parte opcional) para determinar onde começam os dados do pacote;
- **tipo:** define o ToS (*Type of Service*), que permite distinguir os diferentes tipos de pacotes IPv4: baixo atraso ou alta taxa de transferência;
- **comprimento:** comprimento de tudo o que há no pacote: cabeçalho e dados. O tamanho máximo normal de um pacote IP é de 1500 bytes;
- **Identificação:** permite que o equipamento de destino determine a qual pacote pertence um determinado fragmento (todos os fragmentos de um mesmo pacote devem conter um mesmo valor) quando estiver habilitada a fragmentação de pacotes;
- **offset:** informa a que posição, múltipla de 8 bytes, do pacote atual pertence o fragmento quando estiver habilitada a fragmentação de pacotes;
- **tempo:** (TTL – *Time to Live*) contador utilizado para limitar a vida útil do pacote através de um decremento deste valor a cada equipamento por que o pacote passa (quando o contador chega a zero, o pacote é descartado);
- **protocolo:** usado quando o pacote chega ao seu destino, especifica a presença de cabeçalhos opcionais ou o processo de transporte que deverá ser aplicado à porção de dados do pacote (por exemplo ICMP, IGMP, TCP, UDP, que ainda serão estudados);
- **soma:** soma de verificação, de 2 bytes, apenas para os bytes do cabeçalho;
- **origem:** endereço IPv4, de 4 bytes, do equipamento de origem;
- **destino:** endereço IPv4, de 4 bytes, do equipamento de destino final.

A partir de 1990, o IETF (*Internet Engineering Task Force*) começou a trabalhar em uma nova versão de IP, capaz de impedir o esgotamento dos endereços e de ajustar e ampliar outros aspectos do IPv4, tornando-o mais flexível e mais eficiente: o **IPv6**, definido nos padrões IETF RFC 2373 e RFC 2460 (KUROSE; ROSS, 2013).

Basicamente, em relação ao IPv4, cujos endereços são compostos por 4 bytes (32 bits), o IPv6 é composto por endereços de 16 bytes (128 bits) e possui um cabeçalho bem mais simples de ser tratado e mais eficiente, com apenas 8 campos.

Reflita

Supondo que não houvesse restrições de uso, você saberia dizer quantos endereços IPv4 seriam possíveis de serem criados com endereços de 32 bits? E quantos IPv6 com endereços de 128 bits? Você percebe o impacto dessa evolução na internet atual e do futuro?

Um pacote IPv6 consiste em duas partes: cabeçalho e dados. O cabeçalho tem um tamanho fixo de 40 bytes e uma parte opcional de tamanho variável. O formato da parte fixa do cabeçalho está mostrado na Figura 2.

Figura 2 - Formato do Cabeçalho Fixo do IPv6

1	3	2	1	1	16	16
Versão/Tipo	Fluxo	Comprimento	Protocolo	Tempo	Origem	Destino

Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

Observe atentamente a função de cada um desses campos e perceba que, apesar do comprimento desse cabeçalho ter aumentado em relação ao cabeçalho do IPv4, a quantidade de informação que o cabeçalho IPv6 carrega é menor. Os campos deste cabeçalho são:

- **versão/tipo:** controla a versão do protocolo IP e define o ToS (*Type of Service*), que permite distinguir os diferentes tipos de pacotes IPv6: baixo atraso, alta taxa de transferência ou confiabilidade;
- **fluxo:** permite identificar pacotes que pertençam a fluxos específicos para os quais o remetente requisita tratamento especial, tal como serviço de qualidade não padrão ou um serviço de tempo real;
- **comprimento:** comprimento de tudo o que há no pacote menos os 40 bytes da parte fixa do cabeçalho: cabeçalho opcional e dados;
- **protocolo:** (*next header*) usado quando o pacote chega ao seu destino, especifica a presença de cabeçalhos opcionais ou o processo de transporte que deverá ser aplicado à porção de dados do pacote (ICMPv6, TCP, UDP);
- **tempo:** (*hop limit*) contador utilizado para limitar a vida útil do pacote através de um decremento deste valor a cada equipamento por que o pacote passa (quando o contador chega a zero, o pacote é descartado);
- **origem:** endereço IPv6, de 16 bytes, do equipamento de origem;
- **destino:** endereço IPv6, de 16 bytes, do equipamento de destino final.

Mas para passar a usar o IPv6 ao invés do IPv4, devemos “desligar” o IPv4? Não, pois foi previsto que ambas as versões do protocolo IP deverão coexistir e a transição deverá ser gradativa, o que não significa que seja simples. Essa transição do IPv4 para o IPv6 deve lidar, portanto, com um problema: enquanto os novos sistemas habilitados para IPv6 podem ser inversamente compatíveis, isto é, podem enviar, rotear e receber pacotes IPv4, os sistemas habilitados para IPv4 não podem tratar pacotes IPv6.

Para contornar o problema de migração do protocolo IPv4 da internet para o protocolo IPv6, o IETF descreve duas abordagens para a integração gradual de equipamentos IPv4 ao mundo IPv6:

Pilha dupla

As interfaces dos equipamentos IPv6 devem ter também uma implementação IPv4, podendo enviar qualquer uma das versões de IP de acordo com a capacidade de tratá-la ao longo do caminho entre os nós;

Tunelamento IPv4

Quando houver nós IPv4 no caminho entre nós IPv6, os pacotes IPv6 devem ser encaminhados através de túneis IPv4, tornando os segmentos de rede IPv4 transparentes para os equipamentos IPv6.

Apesar da migração da infraestrutura de rede para o IPv6 estar sendo transparente para os usuários, os aplicativos de rede precisam ser reescritos para que se adaptem à necessidade de tratamento de novos parâmetros para o estabelecimento de conexões IPv6.

A operação da internet é monitorada pelos vários tipos de equipamentos de rede. Quando algo inesperado ocorre em uma rede IPv4, um evento é reportado através de uma mensagem **ICMP** (*Internet Control Message Protocol*), definida na RFC 792. Este tipo de mensagem também é usado para testar o acesso a equipamentos da internet (TANENBAUM; WETHERALL, 2011).

Saiba Mais

Clique [aqui](#) para saber quais são os tipos de mensagens ICMP.

Apesar de o ICMP ser o protocolo de controle da camada de rede, ele não é um protocolo independente, mas usa o próprio protocolo IP para ser transmitido: cada tipo de mensagem ICMP é carregado como dado de um pacote IP.

Já quando algo inesperado ocorre em uma rede IPv6, um evento é reportado através de uma mensagem **ICMPv6** (Internet Control Message Protocol version 6), definida na RFC 2463. O ICMPv6 implementa para o IPv6 as funcionalidades divididas entre vários protocolos de controle utilizados no IPv4, tais como ICMP (Internet Control Message Protocol) e IGMP (Internet Group Management Protocol), e faz algumas simplificações ao eliminar tipos de mensagens do ICMP que não são utilizados

Saiba Mais

Clique [aqui](#) para saber quais são os tipos de mensagens ICMPv6.

Da mesma forma que o ICMP, o ICMPv6 usa o protocolo IPv6 para ser transmitido: cada tipo de mensagem ICMPv6 é carregado como dado de um pacote IPv6.

2

Segurança na Camada de Rede

Quando a segurança é disponibilizada pela camada de rede, os pacotes (portanto as aplicações) que utilizarem o protocolo estarão se beneficiando dos serviços de segurança desta camada.

A segurança na camada de rede é obtida por um protocolo denominado **IPsec** (*IP security*), definido nas normas IETF RFC 2401 e RFC 2411. Para prover sigilo na camada de rede, todos os dados enviados por um pacote IP devem estar criptografados. Em princípio, a criptografia pode ser feita através de chaves secretas, chaves públicas ou chaves de sessão negociadas através de chaves públicas (KUROSE; ROSS, 2013).

A especificação do IPsec prevê o uso de dois tipos de cabeçalhos adicionais para serem incluídos no final do cabeçalho dos pacotes IPv4 ou IPv6:

- **AH** (*Authentication Header*), que implementa integridade e autenticação;
- **ESP** (*Encapsulation Security Payload*), que implementa sigilo, integridade e autenticação.

AH (*Authentication Header*)

Que implementa integridade e autenticação;

ESP (Encapsulation Security Payload)

Que implementa sigilo, integridade e autenticação.

Caso o IPsec já estivesse sendo amplamente utilizado, todos os dados enviados por um equipamento para outro, incluindo correio eletrônico, páginas web, transferência de arquivos, controle, gerência etc. seriam sigilosos, o que tornaria todo o tráfego da internet significativamente mais seguro.

Além do sigilo, o IPsec também provê a autenticação do equipamento de origem dos pacotes, eliminando assim a possibilidade de ataques de *spoofing* de IP.

Saiba Mais

Clique [aqui](#) para saber mais sobre *spoofing* de IP.

CONTINUE

Atividade de Passagem

(ENADE) Um administrador de redes de computadores implementou uma solução para a utilização do IPv6 em sua rede corporativa. A solução desenvolvida pelo administrador permitiu a transmissão de pacotes IPv6 através da infraestrutura IPv4 já existente, encapsulando o conteúdo do pacote IPv6 em um pacote IPv4. Qual é a técnica de coexistência e transição do IPv6 para IPv4 que o administrador de rede utilizou?

- ☐ Técnica de pilha dupla
- ☐ Técnica de roteamento
- ☐ Técnica de tradução
- ☐ Técnica de store-and-forward
- ☐ Técnica de tunelamento

SUBMIT

(ENADE) O protocolo IPv6 foi desenvolvido para substituir o IPv4, tendo sua implementação ocasionado várias mudanças importantes, como a capacidade de endereçamento expandida, o cabeçalho aprimorado de 40 bytes e a rotulação de fluxo e prioridade. Considerando essas afirmações, avalie as afirmações a seguir, relativas à descrição dos campos do cabeçalho IPv6.

- I. Em "endereço de origem" e "endereço de destino" cada campo possui 64 bits, tendo sido expandidos os 32 bits usados no IPv4.
- II. Em se tratando do cabeçalho IPv6, insere-se o valor 32 no campo "versão", de 4 bits que é usado para identificar a versão do protocolo IP.
- III. O campo "próximo cabeçalho" identifica o protocolo ao qual os dados presentes no datagrama serão entregues, por exemplo, TCP ou UDP.
- IV. No IPv6, o campo "classe de tráfego", de 8 bits, é semelhante ao campo "tipo de serviço" do IPv4, ambos utilizados para diferenciar os tipos de pacotes IP.
- V. O valor do campo "limite de saltos" é diminuído em um para cada roteador que repassa o pacote; caso a contagem do limite de salto chegue a zero, o pacote será descartado.

É correto apenas o que se afirma em:

☐

II e IV.

☐

I, II e III.

☐

I, III e V.

☐

III, IV e V.

☐

I, II, IV e V.

SUBMIT

CONTINUE

Endereços de Rede

Na internet, cada equipamento tem um endereço IP que codifica seu **número de rede** e seu **número de equipamento**, sendo que dois equipamentos em uma mesma rede não poderão ter nunca o mesmo número de equipamento, ou seja, o mesmo endereço IP.

No caso da internet, os endereços IP são administrados pelos **RIRs** (Regional Internet Registry), coordenados mundialmente pelo **NRO** (Number Resource Organization – www.nro.net), o organismo do **ICANN** (Internet Corporation for Assigned Names and Numbers – www.icann.org) responsável pela gestão global da distribuição de endereços IP para a internet. Os cinco RIRs são (KUROSE; ROSS, 2013):

(Clique nas abas e na seta lateral para acessar os conteúdos)

AFRINIC	APNIC	ARIN	LACNIC	
African Network Information Centre – www.afrinic.net				

AFRINIC	APNIC	ARIN	LACNIC	
----------------	--------------	-------------	---------------	--

Asia Pacific Network Information Centre – www.apnic.net

AFRINIC

APNIC

ARIN

LACNIC

American Registry for Internet Numbers – www.arin.net

AFRINIC

APNIC

ARIN

LACNIC

Latin American and Caribbean Network Information Centre – www.lacnic.net

AFRINIC

APNIC

ARIN

LACNIC

Réseaux IP Européens Network Coordination Centre – www.ripe.net

Um endereço IPv4 é formado por 4 bytes (32 bits). Os 4 bytes de um endereço IPv4 são escritos em notação decimal separados por pontos, como no seguinte exemplo:

200.10.150.20

O endereçamento IPv4 permite três tipos de endereços:

(Clique nos cartões para acessar os conteúdos)

Ponto a Ponto

Corresponde a uma interface de um equipamento;

Multidifusão

Corresponde a múltiplas interfaces de um grupo de equipamentos;

Difusão

Corresponde a todas as interfaces dos equipamentos de uma mesma rede.

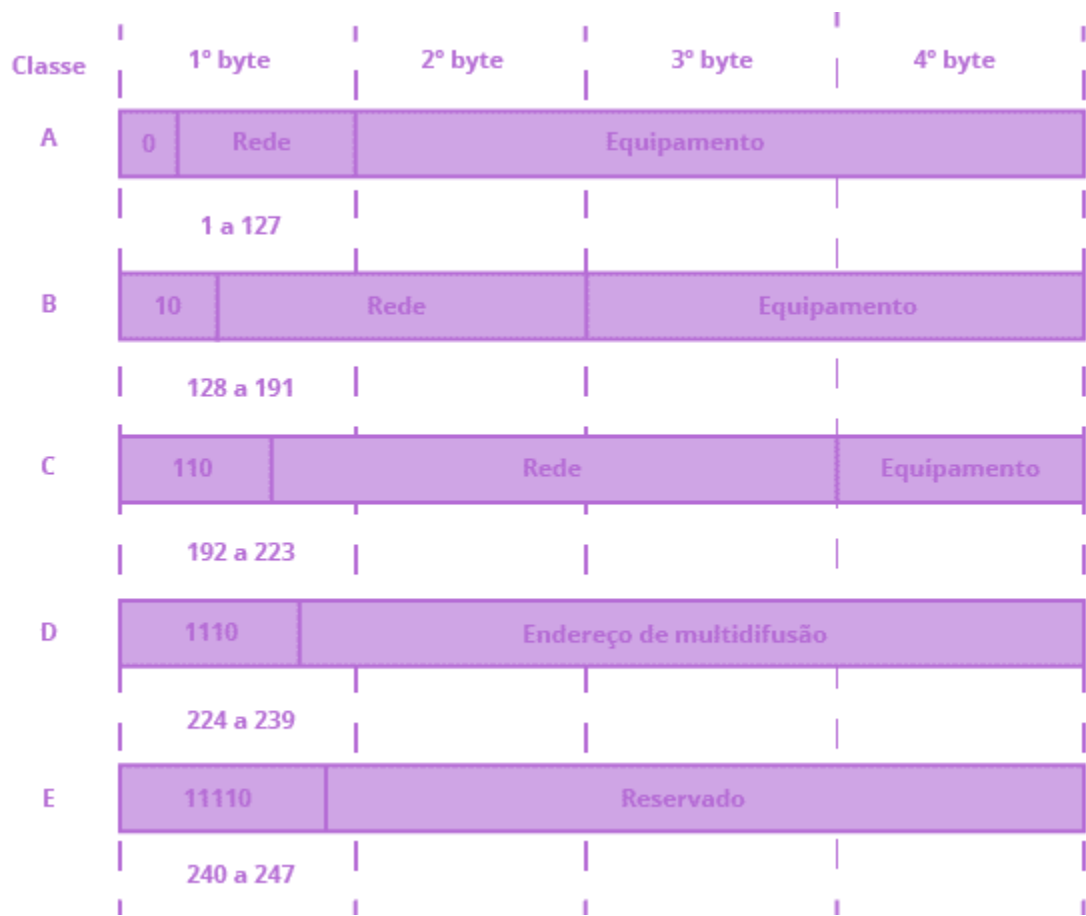


Saiba Mais

Veja [aqui](#) quais foram os endereços IPv4 entregues para cada um dos 5 RIRs.

Para que um equipamento de rede possa enviar dados por uma rede é preciso que ele seja capaz de extrair o número de rede e de equipamento do endereço IP, ou seja, determinar quantos/quais bytes do endereço representam o número de rede e quantos/quais bytes do endereço representam o número de equipamento. Com este propósito, os possíveis endereços IPv4 foram divididos em cinco faixas distintas, chamadas **classes de endereço IPv4**, identificadas através dos primeiros bits do endereço, conforme apresentado na Figura 3.

Figura 3 - Classes de Endereçamento IPv4

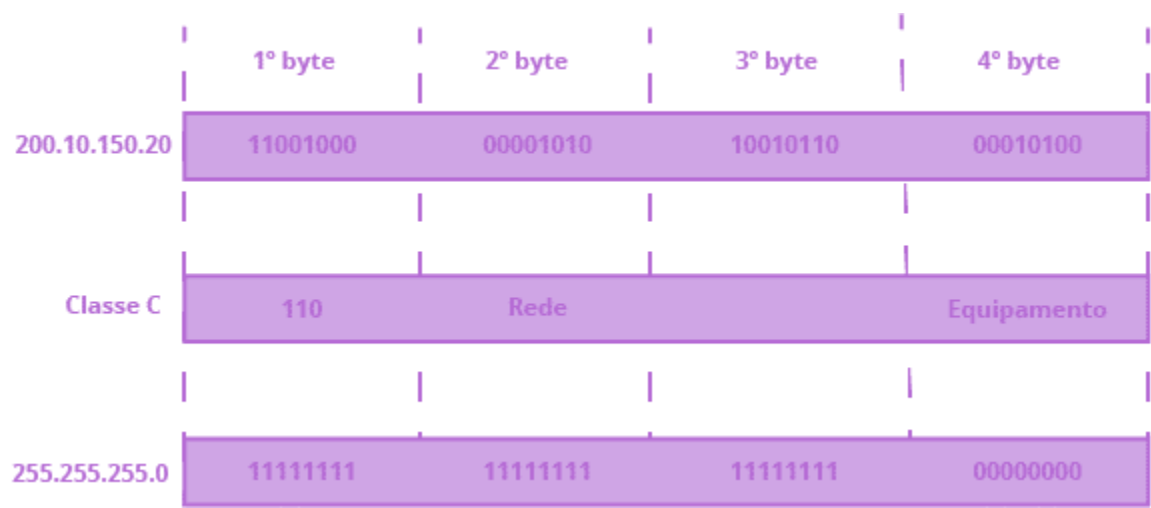


Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

Além da divisão dos endereços IPv4 em classes, utiliza-se um número IPv4 especial chamado **máscara de sub-rede padrão**. Uma máscara de sub-rede é um número IPv4 que identifica com bits 1 a parte de um endereço IPv4 que representa o número de rede e com bits 0 a parte de um endereço IPv4 que representa o número de equipamento (KUROSE; ROSS, 2013).

Dessa forma, uma máscara de sub-rede padrão para um endereço IPv4 de uma determinada classe indica quais bytes do endereço representam o número de rede e quais bytes do endereço representam o número de equipamento. No caso do exemplo do endereço IPv4 200.10.150.20 (Figura 4), tem-se que, em função dos 3 primeiros bits, trata-se de um endereço da classe C e, portanto, a sua máscara de sub-rede padrão é 255.255.255.0, já que um endereço da classe C é composto por 3 bytes para indicar o número de rede e 1 byte para indicar o número de equipamento.

Figura 4 - Exemplo de Máscara de Sub-rede Padrão Classe C



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

Para cada uma das três primeiras classes de endereços IPv4, são definidas algumas faixas de endereços IP para uso específico. Em relação aos endereços IPv4 da **classe A**, tem-se que:

- a máscara de sub-rede padrão é **255.0.0.0**, ou seja, 8 bits (1 byte) definem o número da rede e 24 bits (3 bytes) definem o número do equipamento;
- a faixa de endereços é de **1.*.*.* a 127.*.*.***: **127** redes com 16777216 endereços cada;
- a faixa de endereços **10.*.*.*** (1 endereço de rede) é restrita para equipamentos de redes privadas que utilizem endereços classe A;
- a faixa de endereços **127.*.*.*** é reservada e representa o próprio equipamento de rede (*loopback*).

Da forma equivalente, em relação aos endereços IPv4 da **classe B**, tem-se que:

- a máscara de sub-rede padrão é **255.255.0.0**, ou seja, 16 bits (2 bytes) definem o número da rede e 16 bits (2 bytes) definem o número do equipamento;
- a faixa de endereços é de **128.0.*.* a 191.255.*.***: 16384 redes com 65536 endereços cada;
- a faixa de endereços **172.16.*.* a 172.31.*.*** (16 endereços de rede) é restrita para equipamentos de redes privadas que utilizem endereços classe B;
- a faixa de endereços **169.254.*.*** é reservada e serve para configuração automática de equipamentos de um mesmo segmento de rede (**local link**) quando nenhum mecanismo de configuração estiver disponível.

De forma equivalente, em relação aos endereços IPv4 da **classe C**, tem-se que:

- a máscara de sub-rede padrão é **255.255.255.0**, ou seja, 24 bits (3 bytes) definem o número da rede e 8 bits (1 byte) definem o número do equipamento;
- a faixa de endereços é de **192.0.0.* a 223.255.255.***: 2097152 redes com 256 endereços cada;
- a faixa de endereços **192.168.0.* a 192.168.255.*** (256 endereços de rede) é restrita para equipamentos de redes privadas que utilizem endereços classe C.

Qualquer organização que precisar utilizar endereços de alguma das faixas restritas para redes privadas poderá fazê-lo sem contatar um sistema de registro da internet, pois estes endereços nunca são introduzidos no sistema de roteamento da internet. Mas este sistema faz com que a organização precise utilizar um mecanismo de conversão de endereços de rede privados em endereços globais para permitir o acesso à internet.

Os endereços IP correspondentes a um determinado número de rede possuem dois endereços especiais que não podem ser utilizados para identificar nenhum equipamento de rede específico: os que possuem somente bits 0 como número de equipamento e os que possuem somente bits 1 como número de equipamento.

Os endereços IP que possuem somente bits 0 como número de equipamento servem para identificar o endereço da própria rede. Por exemplo, na Figura 5, o endereço IPv4 200.10.150.0 é o endereço de uma rede classe C. Os endereços que possuem somente bits 1 como número de equipamento permitem a difusão de pacotes numa rede, ou seja, é o endereço de difusão (*broadcast*) daquele endereço de rede. Por exemplo, o endereço IPv4 200.10.150.255 refere-se a todos os equipamentos da rede 200.10.150.0 classe C.

Figura 5 - Exemplo de Endereços de Rede e de Difusão de Classe C

	1° byte	2° byte	3° byte	4° byte
200.10.150.20 endereço	11001000	00001010	10010110	00010100
255.255.255.0 máscara	11111111	11111111	11111111	00000000
200.10.150.0 rede	11001000	00001010	10010110	00000000
200.10.150.255 broadcast	11001000	00001010	10010110	11111111

Fonte: Elaboração própria (2022).

Arte/Diagramação: DME/FURB (2023).

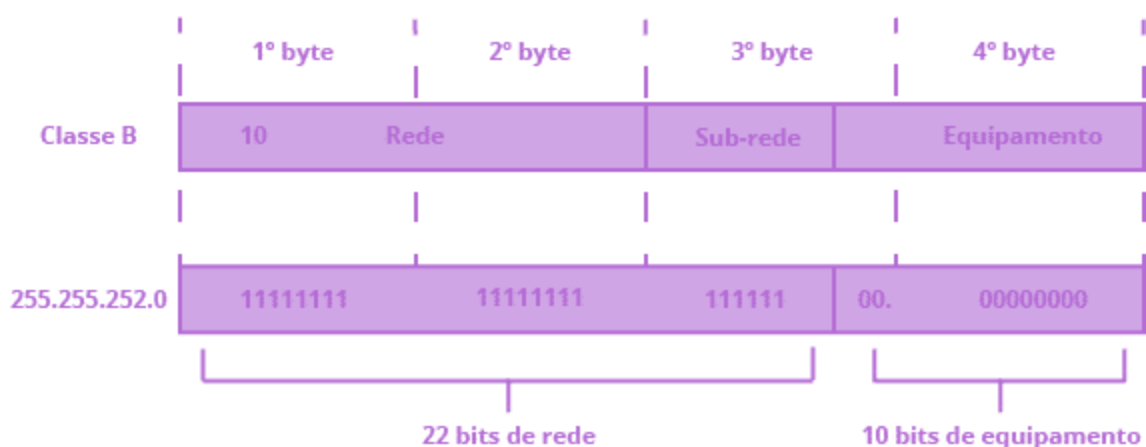
Todos os equipamentos de uma rede devem ter o mesmo número de rede. Esta propriedade do endereçamento IP causa problemas à medida que o número de redes cresce continuamente.

No caso do IPv4, criou-se uma solução para esse problema permitindo-se que, em vez de se definirem os números de rede e de equipamento pela divisão de faixas de endereços IPv4 em classes de endereços, o número de equipamento seja dividido em diversas partes para uso interno, mas externamente continue a funcionar como uma única rede: essas partes foram denominadas **sub-redes**. A esta solução deu-se o nome de **CIDR** (*Classless Interdomain Routing*).

A consequência de se dividir o número de equipamento em diversas sub-redes é que, em vez de os equipamentos de rede terem que descobrir quantos dos 4 bytes de um endereço IPv4 definem o número de rede e quantos o número de equipamento, os equipamentos de rede têm que descobrir quantos dos 32 bits do endereço IPv4 definem o número de rede e quantos definem o número de equipamento (KUROSE; ROSS, 2013).

Por exemplo, seja um endereço IPv4 de classe B, onde o número de equipamento de 16 bits foi dividido em um número de sub-rede de 6 bits e um número de equipamento de 10 bits, o que permite 64 sub-redes (2^6 sub-redes) para cada endereço de rede, com 1022 equipamentos cada uma ($2^{10} - 2$ equipamentos, pois o primeiro, 00.00000000, é o endereço da rede, e o último, 11.11111111, é o endereço de difusão, os quais não podem ser usados para endereçar nenhum equipamento específico), como apresentado na Figura 6.

Figura 6 - Exemplo de Máscara de Sub-rede de 22 bits



Fonte: Elaboração própria (2022).

Arte/Diagramação: DME/FURB (2023).

Para operar com endereços de rede compostos por sub-redes, o router precisa conhecer qual o tamanho total do endereço de rede e de sub-rede que compõe o endereço IPv4: isto é feito através do uso da máscara de sub-rede. No exemplo da Figura 7, o valor da **máscara de sub-rede** é 255.255.252.0.

Os protocolos de roteamento geralmente se referem ao tamanho do prefixo de rede estendido em vez da máscara de sub-rede, que equivale ao número de bits 1 utilizados na máscara de sub-rede. A notação compacta utilizada ao escrever os endereços IPv6 para definir o tamanho do prefixo de rede de um endereço IP, por ser mais fácil de interpretar do que escrever a máscara de sub-rede no formato decimal, também pode ser utilizada para escrever os endereços IPv4.

Figura 7 - Exemplo de Endereço IPv4 com Máscara de Sub-rede

	1° byte	2° byte	3° byte	4° byte
130.10.150.205 endereço	10000010	00001010	100101	10. 11001101
255.255.252.0 máscara	11111111	11111111	111111	00. 00000000
130.10.148.0 sub-rede	10000010	00001010	100101	00. 00000000
130.10.151.255 broadcast	10000010	00001010	100101	11. 11111111

Fonte: Elaboração própria (2022).

Arte/Diagramação: DME/FURB (2023).

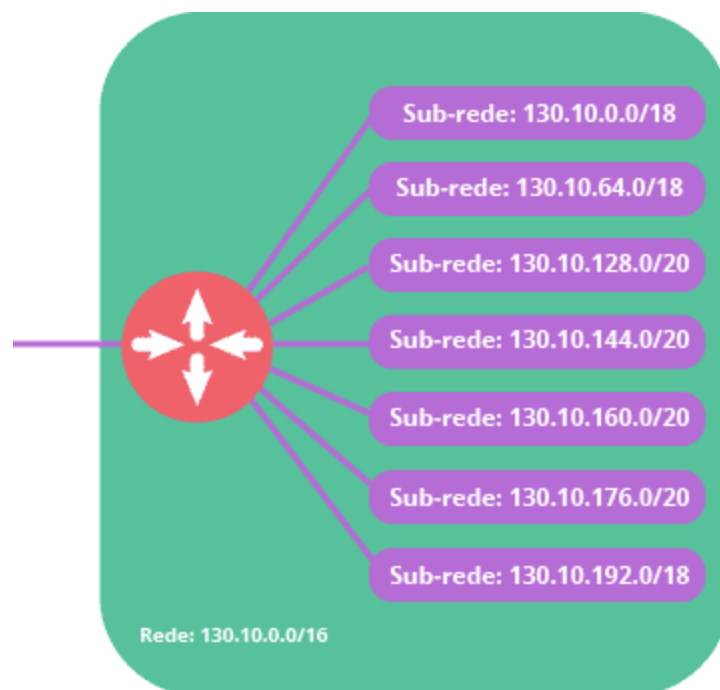
Por exemplo, o endereço IPv4 130.10.150.205 (Figura 7) para o equipamento de rede com uma máscara de sub-rede 255.255.252.0 (o que significa 22 bits para o número de rede) pode ser escrito como 130.10.150.205/22. Neste exemplo, o endereço IPv4 130.10.151.255 refere-se a todos os equipamentos da sub-rede 130.10.148.0 onde o equipamento de rede 130.10.150.205/22 está instalado.

i Dica

Para facilitar o cálculo da máscara de sub-rede e dos endereços de sub-rede e de broadcast de sub-rede, pode-se utilizar uma [calculadora CIDR on-line](#).

A sub-rede reduz o espaço de tabela do *router* ao criar uma hierarquia. Dessa forma, o *router* precisa apenas buscar a rede de destino fazendo uma operação binária E do endereço com a máscara de sub-rede mais genérica e assim rotear o pacote sem precisar ter conhecimento de todas as eventuais sub-redes de uma rede e de todos os equipamentos de cada uma das sub-redes. A Figura 8 apresenta um exemplo de uma rede que é vista pelos routers externos como sendo uma única rede com número de rede de 16 bits, mas que internamente é organizada em 3 sub-redes com números de rede de 18 bits (para comportar $2^{14} - 2 = 16382$ endereços de equipamentos cada uma) e em 4 sub-redes com números de rede de 20 bits (para comportar $2^{12} - 2 = 4094$ endereços de equipamentos cada uma).

Figura 8 - Exemplo de Hierarquia na Definição de Redes e Sub-redes



Fonte: Elaboração própria (2022).

Para os endereços IPv6, de 16 bytes (128 bits), foi criada uma notação própria: eles são escritos como 8 grupos de 4 dígitos hexadecimais (2 bytes), cada grupo separado por dois pontos, como no seguinte exemplo:

FE80:0000:0000:0001:0123:0067:AB80:1001

Como muitos endereços IPv6 contêm muitos zeros, foram permitidas duas otimizações. Em primeiro lugar, os zeros à esquerda de um grupo poderão ser omitidos. Em segundo lugar, um ou mais grupos de quatro zeros poderão ser substituídos por um único par de dois pontos. Consequentemente, o endereço IPv6 anterior pode ser escrito da seguinte maneira (FLORENTINO, 2012):

FE80::1:123:67:AB80:1001

O endereçamento IPv6 permite três tipos de endereços:

(Clique nos cartões para acessar os conteúdos)

Ponto a ponto

: corresponde a uma interface de um equipamento;

Multidifusão

Corresponde a múltiplas interfaces de um grupo de equipamentos;

Seletiva

Cpara apenas um dos equipamentos.

Nas redes IPv6 não existem mais os endereços de difusão, sendo que estes agora são realizados por grupos de multidifusão específicos.



Saiba Mais

Veja [aqui](#) quais foram os endereços IPv6 entregues para cada um dos 5 RIRs.

Para os endereços IPv6, a informação que determina quantos/quais bits do endereço representam o número de rede e quantos/quais bits do endereço representam o número de equipamento é disponibilizada aos equipamentos de rede através de um número que indica o tamanho do prefixo de rede. Por exemplo, o endereço IPv6 FE80::1:123:67:AB80:1001/64 significa que os primeiros 64 bits do endereço definem o número de rede e os últimos 64 bits definem o número de equipamento.

Com o IPv6 todas as redes locais devem ter prefixos 64 bits. Usuários receberão dos provedores de acesso redes com prefixos de 48 bits e com isso terão a seu dispor uma quantidade suficiente de endereços IP para configurar aproximadamente 65 mil redes locais, cada uma com 2^{64} endereços (Figura 9).

Figura 9 - Formato do Endereço IPv6



Fonte: Elaboração própria (2022).

Arte/Diagramação: DME/FURB (2023).

Portanto, para o endereço IPv6 exemplo da Figura 45 FE80::1:123:67:AB80:1001/64 de um equipamento de rede significa que ele está instalado na sub-rede FE80:0:0:1::/64.

Figura 10 - Exemplo de Endereço IPv6

	6 bytes	2 bytes	8 bytes
FE80::1:123:67:AB80:1001/64 endereço	FE80 : 0000 : 0000	0001	0123 : 0067 : AB80 : 1001
FE80::/48 rede	FE80 : 0000 : 0000	0000	0000 : 0000 : 0000 : 0000
FE80:0:0:1::/64 sub-rede	FE80 : 0000 : 0000	00011	0000 : 0000 : 0000 : 0000

Fonte: Elaboração própria (2022).

Arte/Diagramação: DME/FURB (2023).

Os endereços IPv6 foram divididos em faixas de endereços de acordo com a Tabela 2.

Tabela 2 - Distribuição dos Endereços IPv6

Endereços	Equipamento
::1/128	Endereço reservado de <i>loopback</i> (representa o próprio equipamento de rede – <i>localhost</i>)
2000::/3	Endereços disponíveis para provedores de internet (ISP) atribuírem a seus usuários
FE80::/10	Endereços para um mesmo segmento de rede (<i>local link</i>)
FF00::/8	Endereços utilizados para multidifusão

Métodos de Atribuição de Endereços IP

Como é atribuído um endereço IP para um equipamento de rede? Pois existem dois métodos para atribuir endereços IP a um equipamento: **endereçamento estático e endereçamento dinâmico**. Independentemente do esquema de endereçamento usado, dois equipamentos não podem ter um mesmo endereço IP (KUROSE; ROSS, 2013).

A atribuição de endereços IP estaticamente implica na configuração de cada dispositivo com um endereço IP fixo. Esse método exige que se mantenha um registro detalhado do endereçamento efetuado para evitar que se configurem endereços IP duplicados. Existem alguns métodos para atribuir endereços IP dinamicamente. Os principais exemplos são:

(Clique no + e acesse os conteúdos)

DHCP (Dynamic Host Configuration Protocol) ou DHCPv6 (Dynamic Host Configuration Protocol version 6):

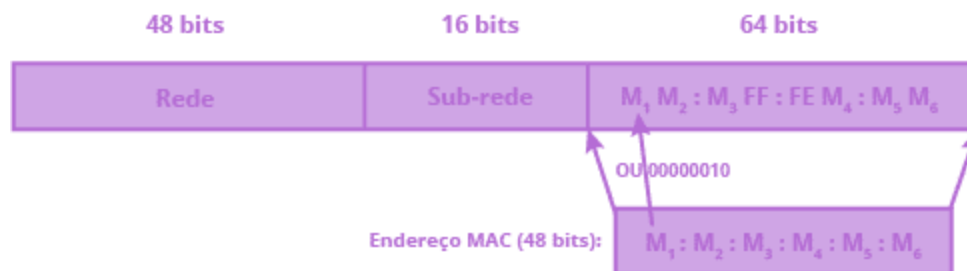
Permite que um equipamento obtenha um endereço IP de forma rápida e dinâmica. Tudo o que é necessário ao se usar o DHCP é um intervalo pré-definido de endereços IP em um servidor DHCP. À medida que se conectam à rede, os equipamentos entram em contato com o servidor DHCP e solicitam um endereço IP com a correspondente máscara/comprimento de sub-rede e o endereço IP do gateway padrão da rede. O servidor DHCP escolhe um endereço livre e o atribui a esse equipamento;

Configuração automática

Trata-se de uma inovação do IPv6 para redes que não necessitam conhecer seus endereços IP. Para tal são utilizados os endereços MAC dos adaptadores de rede associados às informações de rede fornecidas pelos roteadores (Router Solicitation e Router Advertisement do ICMPv6) (FLORENTINO, 2012). Para adaptar o endereço MAC de 48 bits num endereço de 64 bits da interface de rede, o endereço é expandido através da repartida do endereço ao meio (24 bits + 24 bits) e da inserção dos

bytes “FFFE”, mudando o sétimo bit do primeiro byte do endereço MAC para 1, completando assim o endereço IPv6 (Figura 46).

Figura 11 - Formação Automática de um Endereço IPv6



Fonte: Elaboração própria (2022).

Arte/Diagramação: DME/FURB (2023).

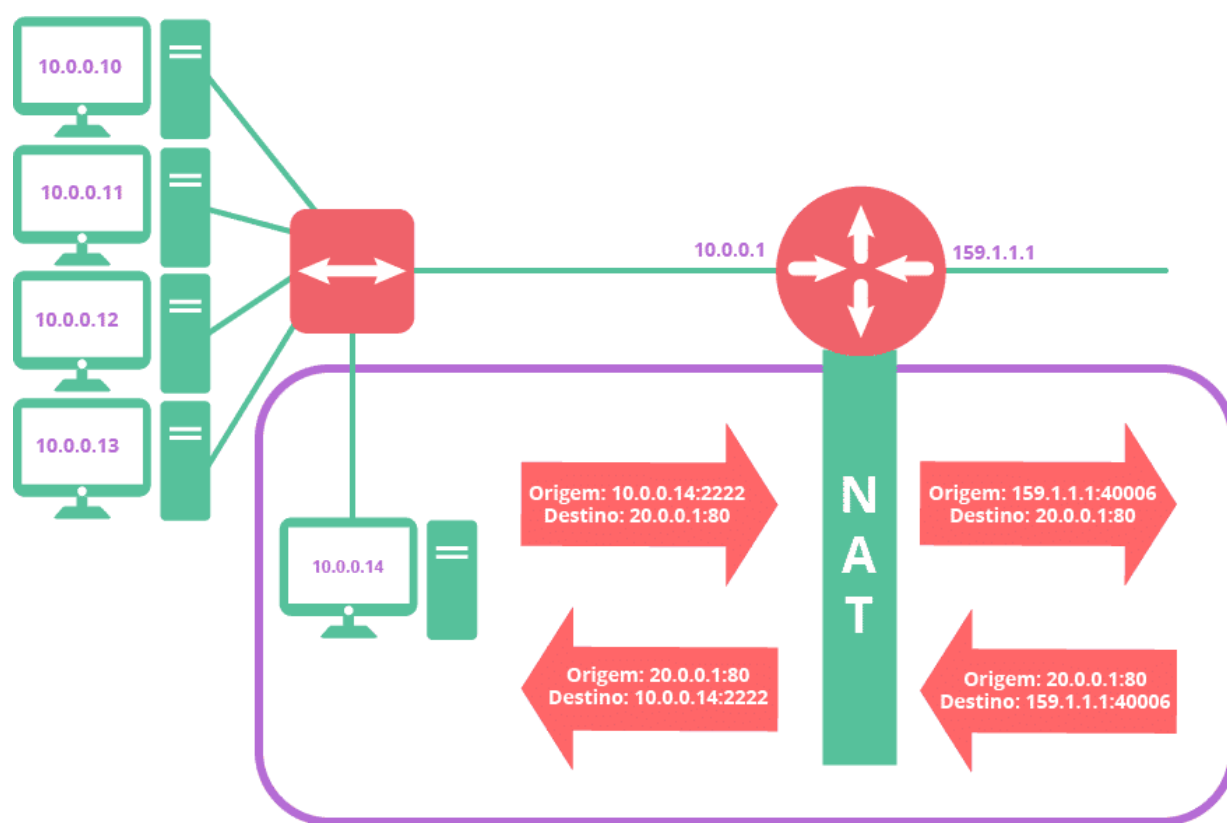
Conversão de Endereços Privados em Globais

Uma forma de contornar a explosão de endereços IP requeridos pela inclusão de cada vez mais equipamentos nas redes é utilizar um algoritmo de mapeamento dos endereços IPv4 privados de intranets em endereços globais da internet. Desta forma, todos os recursos de uma rede privada de computadores passam a ser utilizados sem que se gastem endereços IP globais, disponibilizando-se o acesso à internet a vários equipamentos com apenas um endereço IP global para vários endereços IP privados.

Para permitir esta conversão de endereços IPv4 privados em endereços IPv4 globais utiliza-se um mecanismo de tradução de endereços que interliga a rede privada à internet. Este tradutor denomina-se **NAT** (*Network Address Translation*), definido na RFC 3022, cujo mecanismo é conhecido como **IP masquerading**, onde toda a rede privada é mapeada em um único IPv4 global (KUROSE; ROSS, 2013).

Neste processo, um número muito grande de conexões é possível através da multiplexação que utiliza as informações de portas (endereços de 16 bits da camada de transporte, utilizados para identificar os processos de origem e de destino de uma comunicação entre aplicativos de rede). A Figura 12 apresenta um exemplo de uma topologia de rede com endereçamento privado conectada à internet através de um NAT, onde o equipamento 10.0.0.14 está requisitando um dado da internet.

Figura 12 - Exemplo de Rede Privada com Utilização de NAT



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

Para o funcionamento do NAT, é preciso que o *router* mantenha uma tabela com a informação de tradução (exemplificada na Tabela 3) a fim de permitir que as respostas ao acesso à internet possam ser dirigidas ao respectivo equipamento que a tenha requerido.

Tabela 3 - Exemplo de Tabela NAT de um *Router*

Tabela NAT do Router			
Endereço privado de origem		Endereço global de origem	
IP	Porta	IP	Porta
10.0.0.10	30030	159.1.1.1	40001
10.0.0.11	12034		40002
10.0.0.12	45045		40003
10.0.0.12	23023		40004
10.0.0.12	32032		40005
10.0.0.14	22222		40006

Fonte: Elaboração própria (2022). Arte/Diagramação: DME/FURB (2023).

Para melhor visualizar este procedimento de mapeamento de endereços IPv4 privados em um endereço IPv4 global, observe como ocorre neste NAT exemplo:





Fluxo de uma mensagem através de um NAT

Uploaded by FURBTUBE on 2022-12-14.

VISUALIZAR NO YOUTUBE >

Quando uma rede privada estiver conectada à internet através de um NAT sem configurações estáticas específicas de mapeamento de portas, não é possível conectar-se a um computador local a partir de um equipamento da internet, pois a entrada na tabela NAT é válida somente enquanto uma conexão iniciada desde a rede privada estiver ativa e seria necessário saber qual porta está servindo determinado equipamento naquele instante (FRANÇA, 2010).

Esta restrição inviabiliza o uso de aplicações P2P puras desde redes que utilizam NAT, a menos que se utilize um servidor P2P intermediário disponibilizado especificamente para este fim na internet.

Por outro lado, como o NAT não permite o acesso a equipamentos de uma rede privada originado a partir de uma rede pública como a internet, este mecanismo é uma forma de aumentar a segurança de uma rede local.

CONTINUE

Atividade de Passagem

(ENADE) Uma empresa, no Brasil, recebeu o número IP 204.145.121.0 para endereçar sua rede, respeitando a RFC 1812. Nessa configuração de endereço base:

- ☐ o endereço de broadcast é 204.145.121.1
- ☐ o endereço recebido pertence à classe B
- ☐ o número máximo de hosts endereçáveis é 256
- ☐ se for necessário dividir a rede em quatro sub-redes, então o número máximo de hosts endereçáveis é 254
- ☐ se for necessário dividir a rede em oito sub-redes, então a máscara de rede será 255.255.255.224

SUBMIT

(ENADE) Considerando o mecanismo de tradução de endereços e portas (Network Address Port Translation – NAPT), para redes que utilizam os endereços IP privados (10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16), analise as asserções:

“ao passar por um roteador com NAPT, os endereços de origem nos pacotes originados pelas estações da rede privada são substituídos pelo endereço externo desse roteador”

PORQUE

“não há rotas na Internet para o encaminhamento de pacotes destinados a endereços IP privados, de forma que pacotes destinados a esses endereços são descartados ou rejeitados”.

Em relação às asserções, assinale a opção correta.

☐

As duas asserções são proposições verdadeiras, e a segunda é uma justificativa correta da primeira

☐

As duas asserções são proposições verdadeiras, e a segunda não é uma justificativa correta da primeira

☐

A primeira asserção é uma proposição verdadeira, e a

segunda é uma proposição falsa

☐

A primeira asserção é uma proposição falsa, e a segunda é uma proposição verdadeira

☐

As duas asserções são proposições falsas

SUBMIT

(ENADE) Considere um cenário de NAT em uma empresa cujos equipamentos de rede interna (LAN) usam endereços IP privados. Considere, ainda, que haja apenas um endereço IP válido nas redes dessa empresa, 138.76.28.4, que é atribuído à interface externa do roteador, e à cuja interface interna é atribuído o endereço 10.0.0.254. Considerando que dois computadores A (10.0.0.1) e B (10.0.0.2) da rede da empresa façam acessos simultâneos a um servidor WWW externo, quais deverão ser os endereços IP de origem contidos nos pacotes de A e B, respectivamente, que chegarão a esse servidor?

☐

10.0.0.1 e 10.0.0.2

- ☐ 10.0.0.254 e 10.0.0.254
- ☐ 138.76.28.4 e 138.76.28.4
- ☐ 138.76.28.1 e 138.76.28.2
- ☐ 169.254.1.1 e 169.254.1.2

SUBMIT

(ENADE) Uma empresa deseja expandir sua infraestrutura de Tecnologia da Informação e Comunicação (TIC) para o ambiente de nuvem computacional. A arquitetura a ser implantada deverá ser composta pelo site principal atual, no qual constam servidores locais e as estações móveis dos usuários, e 4 nuvens independentes, que abrigarão servidores dedicados às linhas de negócios específicos. Para o projeto foi contratado um tecnólogo em redes, que recebeu juntamente às especificações anteriores, a faixa de endereçamento IP 10.1.0.0/22 para uso no projeto. Considere que o tecnólogo apresentou o projeto de uma topologia em rede e a proposta para endereçamento dos componentes, representados a seguir.

Site Principal: 100 Servidores: 10.1.0.0/24

Site Principal: 400 Estações móveis: 10.1.1.0/24

Nuvem 1: 150 Servidores: 10.1.2.0/24

Nuvem 2: 80 Servidores: 10.1.3.0/25

Nuvem 3: 40 Servidores: 10.1.3.128/26

Nuvem 4: 10 Servidores: 10.1.3.192/26

Com base nas informações apresentadas, avalie as afirmações a seguir.

I. O endereço 10.1.3.191 é um endereço válido a ser usado por equipamento na Nuvem 3.

II. A quantidade de endereços válidos nas Nuvens 2 e 3 são, respectivamente, 254 e 62.

III. As sub-redes propostas para as Nuvens 1 e 4 atendem às demandas de equipamentos destas localidades.

IV. O plano de endereçamento proposto de acordo com a tabela não é suficiente para o atendimento da quantidade de equipamentos propostos no projeto.

V. No site principal existe um erro de alocação das faixas, que pode ser corrigido utilizando uma faixa única 10.1.0.0/23.

É correto apenas o que se afirma em:

☐

II e IV.

☐

I, II e III.

☐

I, III e V.



III, IV e V.



I, II, IV e V.

SUBMIT

CONTINUE

Resumo da Webaula 6

Nessa aula vimos como são os protocolos utilizados pela camada de rede que levam os dados desde uma origem até o seu destino. Além disso, analisamos como são constituídos os endereços que identificam as redes constituintes da internet assim como os que identificam cada um dos equipamentos conectados a elas.

Mas como é que a internet sabe qual caminho deve ser seguido para que esses protocolos cheguem ao destino? Pois é isso que estudaremos na próxima aula.

CONTINUE

Referências

O estudo das camadas do modelo de referência TCP/IP abordadas nesta parte do livro pode ser encontrado em:

FLORENTINO, Adilson Aparecido. **IPv6 na prática**. São Paulo: Linux New Media, 2012.

FRANÇA, Milena Cristina. **Redes de computadores**. Santa Catarina: Publicações do IF-SC, 2010.

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

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

As normas referenciadas nessa unidade podem ser obtidas diretamente da página da internet dos respectivos organismos de padronização:

- **IANA:** www.iana.org
- **ICANN:** www.icann.org
- **IEEE:** ieeexplore.ieee.org/Xplore/guesthome.jsp
- **IETF:** www.rfc-editor.org/rfc-index.html

- **ISO:** www.iso.org/standards-catalogue/browse-by-ics.html
- **ITU-T:** www.itu.int/pub/T-REC

CONTINUE

Créditos

Reitora

Profª. Ma. Marcia Cristina Sardá Espindola

Vice-Reitor

Prof. Dr. Marcus Vinicius Marques de Moraes

Pró-Reitor de Ensino de Graduação, Ensino Médio e Profissionalizante

Prof. Dr. Romeu Hausmann

Pró-Reitor de Administração

Prof. Me. Jamis Antônio Piazza

Pró-Reitora de Pesquisa, Pós-Graduação, Extensão e Cultura

Profª. Drª. Michele Debiasi Alberton

Divisão de Modalidades de Ensino Chefia da Divisão

Profª. Drª. Clarissa Josgrilberg Pereira

Professores Autores

Prof. Me. Francisco Adell Péricas

Design Instrucional

Profª. Drª. Clarissa Josgrilberg Pereira

Prof. Dr. Maiko Rafael Spiess

Prof. Me. Francisco Adell Péricas

Marcia Luci da Costa

Me. Wilson Guilherme Lobe Junior

Revisão Textual

Me. Wilson Guilherme Lobe Junior

Laura Cristina Zorzo

Roteirização

Laura Cristina Zorzo

Produção de Mídia

Gerson Luís de Souza

Gustavo Bruch Féo

Equipe de Design Gráfico

Amanda Kannenberg

Camylle Sophia Teske

Laura Cristina Zorzo

Nicolle Sassella

Renan Diogo Depiné Fiamoncini

Diagramado por Amanda Kannenberg em 08
de Fevereiro de 2023

CONTINUE