NÃO PODE FALTAR

REDES E SUB-REDES

Renato Cividini Matthiesen

O QUE É IPV4?

O IPv4 (Protocolo de Internet versão 4) é a quarta versão do Protocolo de Internet (IP) e é utilizado para a configuração de computadores, impressoras e nós de rede com o famoso endereço IP.

Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

CONVITE AO ESTUDO

Caro aluno, seja muito bem-vindo à segunda unidade da disciplina de Redes e Sistemas Distribuídos: **arquitetura e tecnologia de redes**. Esta é uma unidade de ensino que tem por objetivo levá-lo ao estudo sobre endereçamento IP (*Internet Protocol*) de uma rede, compreensão e configuração de endereços e máscaras de rede e de sistemas de nomes de domínio. Adicionalmente, o estudo também abrange conceitos de Ethernet, operação de rede com interoperabilidade de protocolos e gerenciamento de desempenho e configuração de uma rede de computadores. O adequado estudo desta unidade fará com que a construção do

conhecimento em redes possa seguir para abordagens técnicas e práticas embasadas em tecnologias de comunicação de dados e estruturas de redes de computadores e levar o profissional de redes à construção de soluções computacionais distribuídas.

A primeira seção, **Redes e sub-redes**, abordará conceitos sobre endereçamento IP, notação e classes de endereço, atribuição de endereço, configuração de máscaras de rede, segmentação de uma rede local e utilização de um servidor DNS (*Domain Name System*). A compreensão sobre endereços IP e sua utilização é fundamental para o trabalho de um profissional de tecnologia da informação no cenário das redes de computadores.

Em seguida, a segunda seção, **Ethernet e IPv6**, apresentará conceitos de Ethernet e domínios de broadcast e de colisão, operação, velocidade e comutação em redes. Este estudo lhe levará a compreender melhor o funcionamento de uma rede baseada no protocolo IEEE 802.3 e analisar a performance de uma rede em função da operação dentro de um canal compartilhado e com controle de colisão. Conheceremos informações e características do endereço IPv6 (*Internet Protocol version 6*) e veremos também as diferenças entre o IPv4 e o IPv6, explorando os tipos de endereços, coexistência, interoperabilidade e comandos de testes e conectividade. Aqui, você se aprofundará nas atividades de endereçamento e testes de rede, para que tenha conhecimento em planejar redes com as versões adequadas de endereços IP, assim como a coexistência de ambos os endereços em uma rede.

Para finalizar, temos a terceira seção, **Gerência de desempenho, configuração e contabilização**, que trará conceitos e prática para análise e configurações de uma rede de computadores, análise de gargalos, tempo de resposta, latência de rede, QoS (*Quality of Services*) e análise de tráfico. Faremos também uma introdução ao protocolo VLAN *Trunk* e ao serviço de acesso remoto com o SSH (*Secure Shell*). Os conhecimentos adquiridos nesta seção levarão o profissional de tecnologia da informação a gerenciar uma rede de forma técnica e utilizar ferramentas de monitoramento e gerenciamento da rede.

Com os conhecimentos assimilados desta unidade, você será capaz de fazer o planejamento de um esquema de endereçamento de redes utilizando os protocolos IPv4 e IPv6, o planejamento e a definição de máscaras de sub-redes e a configuração de um servidor DNS, além de realizar o gerenciamento de uma rede de computadores com análise de desempenho e contabilização via ferramentas de análise, redes virtuais e acesso remoto.

PRATICAR PARA APRENDER

Caro aluno, esta seção traz para você um conteúdo referente à arquitetura e tecnologia de redes, focando em endereçamento IP de uma rede de computadores local (LAN – *Local Area Network*). O endereçamento de uma rede local deve levar em consideração a análise de volume de endereços para os dispositivos da rede, a topologia da rede e a estrutura organizacional. O endereçamento de uma rede local necessita seguir critérios preestabelecidos referente a classes (ou sem classes) e números de endereços IPs a serem utilizados, assim como sua distribuição e organização em sub-redes, o que é realizado através do uso de máscara de rede.

A atribuição de endereços de rede para hosts de uma rede local irá, em primeiro lugar, levar em consideração o número de dispositivos que poderão fazer parte da rede. Tendo em vista o número de hosts a serem endereçados, o administrador da rede definirá a classe IP para sub-rede, ou fará o seu cálculo da máscara da sub-rede utilizando a técnica de CIDR (*Classless Inter-Domain Routing*).

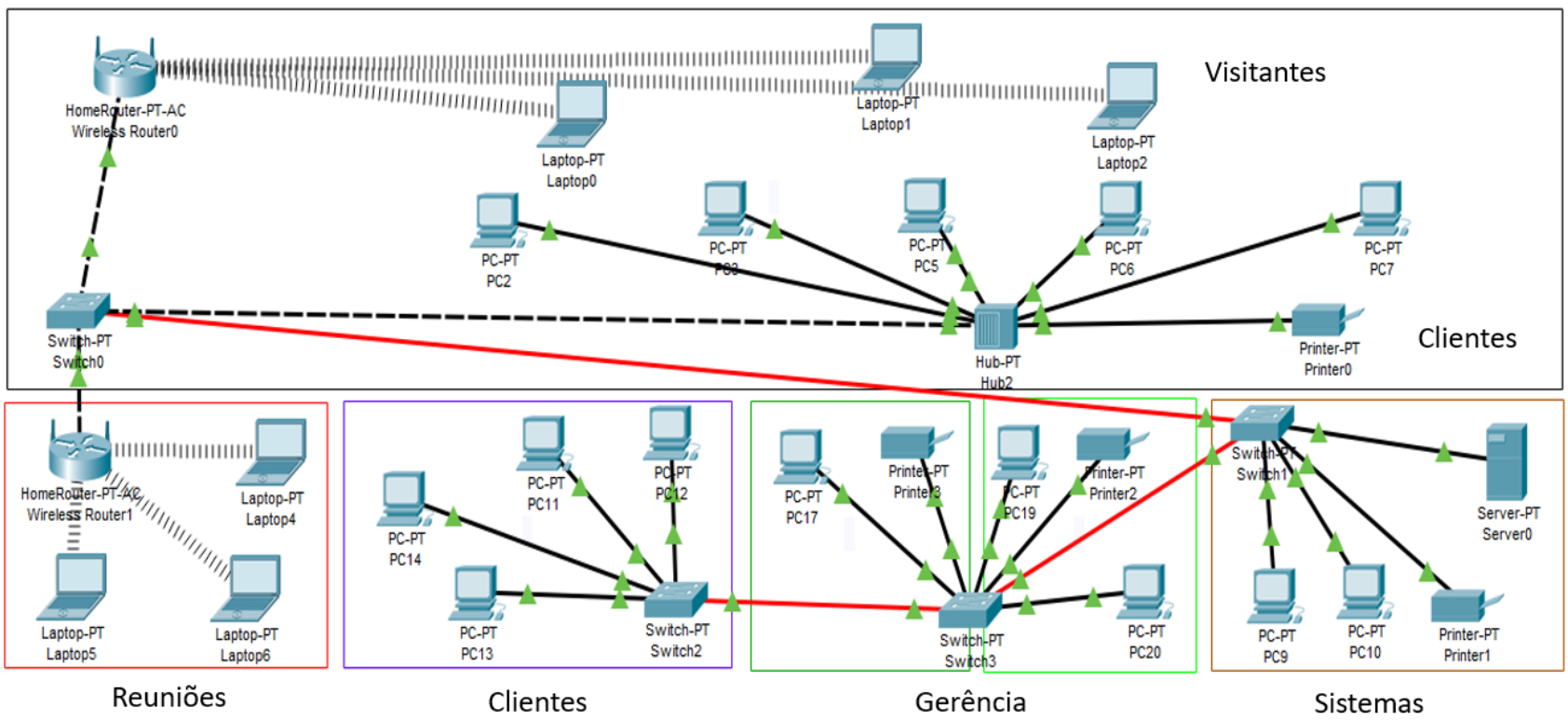
Aprofundaremos nossos estudos sobre redes conhecendo o DNS (*Domain Name System*), ou sistema de nomes de domínio, que estrutura uma rede dentro de um serviço de nomes de domínio para que as pesquisas possam utilizar nomes definidos por URL (*Uniform Resource Locator*) na tradução de endereços IPs para nomes utilizados nos browsers de internet.

Tendo as informações sobre endereços de rede e máscara de rede, podem ser informados manualmente os endereços e as máscaras nos dispositivos, ou fazê-lo de forma automática, utilizando-se de um servidor DHCP (*Dynamic Host Configuration Protocol*), através do serviço de mesmo nome em um sistema operacional de rede.

A empresa de *coworking* que contratou sua consultoria para análise e implantação de um sistema de redes de computadores precisa, nesta segunda fase do projeto, de uma análise mais aprofundada sobre o seu sistema de endereçamento de redes, com um estudo e planejamento de utilização de intervalo de endereços IP a serem atribuídos para os dispositivos que estarão conectados nesta rede. Desta forma, a rede interna precisa ser adequadamente configurada com endereços IPs e máscara de sub-rede, para que todo o sistema computacional possa ser executado sem ocorrer falhas ou lentidões mediante a possibilidade de configurações de endereços repetidos por usuários do ambiente.

Com o objetivo de manter uma configuração profissional dos computadores e dispositivos da rede na empresa, deve ser proposto segmentar a rede em cinco sub-redes (Gerência, Sistemas, Reuniões, Clientes e Visitantes), dentro de uma estrutura de rede em Classe C, com a rede 192.168.10.0 e máscara de rede 255.255.255.0. A topologia da rede é mais uma vez representada na Figura 2.1 a seguir.

Figura 2.1 | Topologia de estudo para configuração de HTTP e DNS



Fonte: elaborada pelo autor.

Seu trabalho consiste em gerar um relatório, chamado de **Relatório do projeto de redes: configuração do endereçamento da rede.**

O endereçamento de rede através da atribuição de números IPs para cada dispositivo é uma tarefa envolvente, que leva o profissional de tecnologia da informação a praticar os conceitos sobre arquitetura de redes de computadores e

atribuir endereços lógicos internos para as redes de computadores definidos pelas classes e pelas sub-redes e desenhados através das máscaras de rede.

CONCEITO-CHAVE

Você já imaginou como toda a internet funciona? Já pensou que cada dispositivo conectado à internet possui um endereço único, dentro do domínio de sua rede, e que ele pode se comunicar com outro dispositivo localizado do outro lado do mundo? Pois bem, este sistema funciona graças ao protocolo IP e aos critérios de endereçamentos público e privado.

A seguir, desenvolveremos o conhecimento para que possamos realizar o endereçamento de nossas máquinas e nossas sub-redes.

ENDEREÇO IP (INTERNET PROTOCOL)

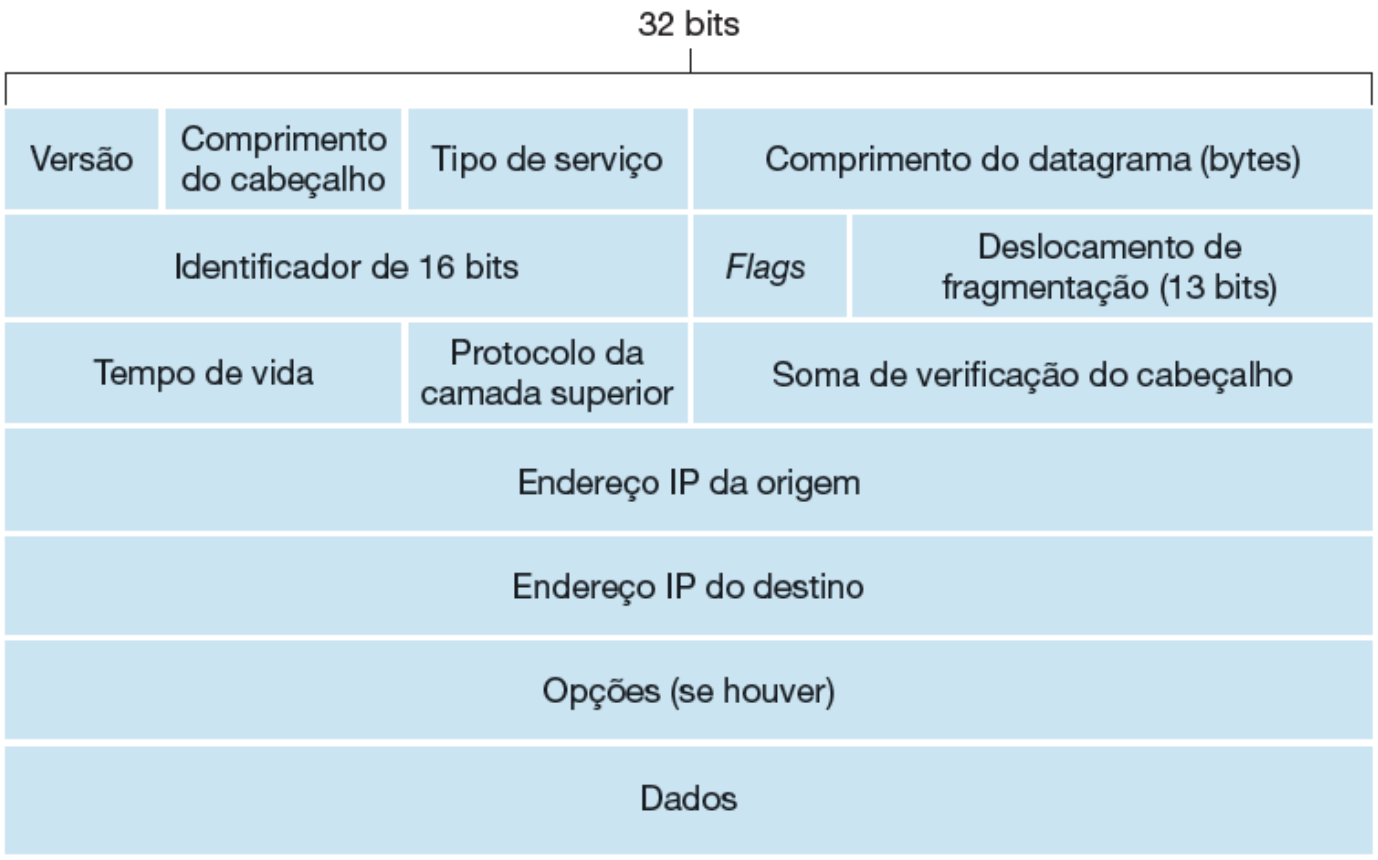
De acordo com Stallings (2016), na maioria dos casos, uma rede local ou uma rede remota não é uma entidade isolada, e necessita de um sistema que possa fazer com que tenha acesso a outras redes.

> Nesta seção, trabalharemos o conceito e a aplicação do protocolo IPv4 (Internet Protocol version 4) para a configuração de computadores, impressoras e nós de rede com o famoso endereço IP. A versão IPv6 (Internet Protocol version 6) também será abordada, porém na Seção 2 desta unidade.

Conforme relata Forouzan (2010), o IPv4 é um protocolo de datagramas sem conexão e não confiável, ou seja, um serviço de entregas chamado de *best-effort*, o que significa que o IPv4 não possui mecanismos de controle de erros ou de fluxo, com exceção da detecção de erros no cabeçalho. Isto nos remete a relembrar que um protocolo adicional de camada de transporte deverá assumir a responsabilidade de realizar a conexão e a entrega confiável dos dados, tarefa realizada pelo protocolo TCP (*Transmission Control Protocol*). As definições técnicas sobre o protocolo IP estão formalizadas na RFC 791 da IETF.

> Observação: IETF (*Internet Engineering Task Force*) e RFC (*Request of Comments*). A RFC 791 define as especificações e questões técnicas a respeito do protocolo IP.

Figura 2.2 | Formato do datagrama IPv4



Fonte: Kurose e Ross (2013, p. 246).

A seguir, é apresentada uma breve descrição dos campos do datagrama IPv4.

Versão: versão do protocolo IP (4 ou 6).

Comprimento do cabeçalho: tamanho do cabeçalho.

Tipo de serviço: prioridade do pacote.

Comprimento do datagrama: tamanho total do pacote (datagrama), com cabeçalho e dados.

Identificador de 16 bits: fragmento do pacote IP original.

Flag: MF, usado para o deslocamento dos datagramas e sua reconstrução; DF, utilização para autorização de fragmentação.

Deslocamento de fragmentação: ordem dos pacotes no processo de remontagem.

Tempo de vida: TLL (*Time to Live*). Indica o "tempo de vida" que o pacote possui a cada salto pelos nós da rede.

Protocolo da camada superior: repassa os dados para os protocolos das camadas superiores.

Soma de verificação do cabeçalho: informa os erros no cabeçalho.

Endereço IP de origem: endereço do remetente.

Endereço IP de destino: endereço do receptor.

Opções: implementações opcionais.

Dados: dados a serem transmitidos.

Observada a composição do fragmento IP na rede, refletiremos sobre como é feito o endereçamento de cada dispositivo conectado em uma rede de computadores.

Por exemplo, no sistema telefônico, a composição de um número local é estruturada em um conjunto de números, em que parte do número identifica o país, outra parte a região, outra ainda a central telefônica e outra o número do assinante.

Exemplo de número telefônico: **55 19 3555 0001**

55: identifica um país.

19: identifica uma região.

3555: identifica a central telefônica.

0001: identifica o número do assinante (número hipotético).

A composição do endereço IP também segue esta estrutura, em que parte do número identifica a rede que o dispositivo pertence e parte determina o endereço do próprio dispositivo.

Exemplo de número IPv4: **192.168.5.114**

192.168.5: identifica a rede ou sub-rede que o dispositivo pertence.

114: identifica o dispositivo dentro da rede em que ele pertence.

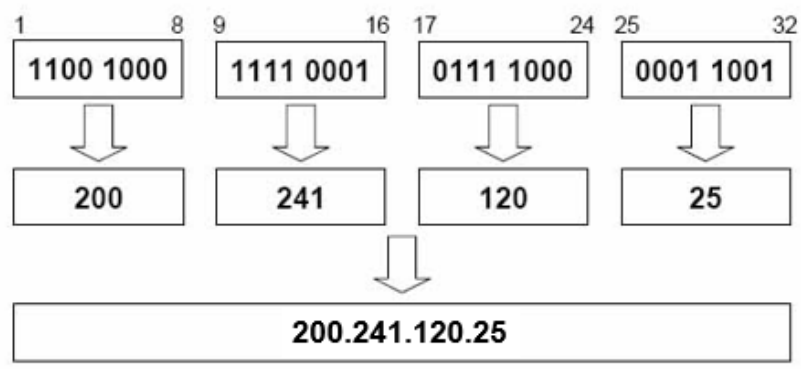
Kurose e Ross (2013) definem o IP como um endereço lógico, criado para que um dispositivo em rede possa se comunicar com outro dispositivo em rede. Trata-se de um endereço formado por 32 bits (ou 4 bytes), o que permite que sejam definidos 232 endereços de rede, ou seja, mais de 4 bilhões de endereços, o que pode parecer o suficiente para endereçar todos os dispositivos em rede, mas não é na verdade.

REFLITA

> O contexto atual de IoT (*Internet of Things*), ou Internet das Coisas, faz com que diversos dispositivos possam ser conectados a uma rede de computadores e à internet. Diamandis e Kotler (2018) sustentam que, no ano de 2020, já deve haver mais de 50 bilhões de dispositivos conectados em rede, e que em dez anos, ou seja, no ano de 2030, o número deverá chegar a 10 trilhões. Todos estes dispositivos precisarão de um endereço IP para seu funcionamento.

Um endereço IPv4 é um número binário, formado por quatro conjunto de números, chamados de octetos, que normalmente são representados por notação decimal. Um exemplo de endereços IP é: 192.168.0.15; outro exemplo é: 172.16.15.108; e outro ainda é: 200.204.0.10. Perceba que, se o endereço é formado por 4 bytes, cada 1 byte corresponde a 8 bits. Por exemplo, o endereço IP 200.241.120.25 tem o número decimal 200, equivalente aos 8 primeiros bits do endereço; 241 é o decimal do segundo conjunto de 8 bits; 120 é o terceiro; e 25, o quarto. Este número IP é a representação do número binário: 11000001.00100000.11011000.00001001. A Figura 2.3 apresenta um exemplo de endereço IPv4 dividido em octetos binários com as devidas representações.

Figura 2.3 | Formato do endereço IPv4



Fonte: elaborada pelo autor.

Um endereço IPv4 é dividido em duas categorias:

- **Pública**, que o identifica como endereço único atribuído e alocado definitivamente e globalmente único para um dispositivo na internet. Para obter um endereço desta categoria, é necessário solicitá-lo a uma instituição de registro de internet.

- **Privada**, na qual um endereço IPv4 deve estar definido dentro de um intervalo de endereços com números limitados a um conjunto de classes e/ou sub-redes que podem ser utilizados livremente em redes privadas, sem acesso direto à internet.

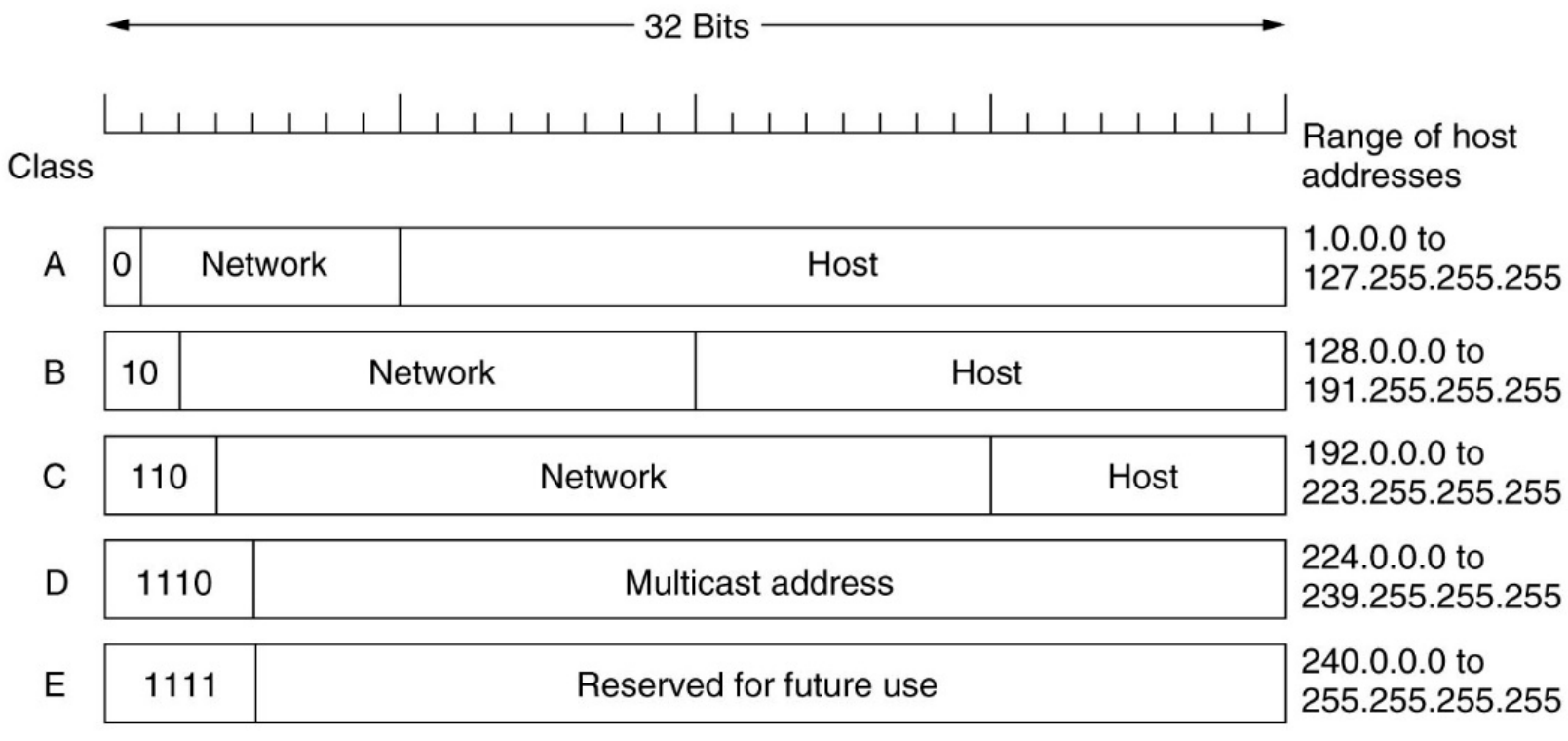
> **SAIBA MAIS**
>
> Os endereços IP dos *hosts* de uma rede de computadores podem ser de natureza pública ou privada. Os endereços de natureza pública são atribuídos e controlados pela IANA (*Internet Assigned Numbers Authority*), organização responsável pela atribuição e pelo controle de endereços IPs no mundo. Já os endereços privados são atribuídos utilizando-se de faixas autorizadas dentro das classes de endereços IPs. Você está convidado a visitar o site da IANA. A entidade brasileira correspondente à IANA é a NIC.BR, que também pode ser visitada na internet.

CLASSES DE ENDEREÇOS IPV4

Um endereço IP privado está condicionado a um intervalo definido, que pode ser utilizado para configuração manual ou automática dentro de uma rede privada. Para melhor aproveitamento e gestão de uma rede, os endereços IPs privados estão divididos em cinco classes: A, B, C, D e E. As classes A, B e C são aquelas úteis e configuráveis dentro de uma rede local.

- Endereços de classe A estão compreendidos dentro do limite de 1.0.0.0 até 127.255.255.255.
- Endereços de classe B, de 128.0.0.0 até 191.255.255.255.
- E endereços de classe C, de 192.0.0.0 até 223.255.255.255.

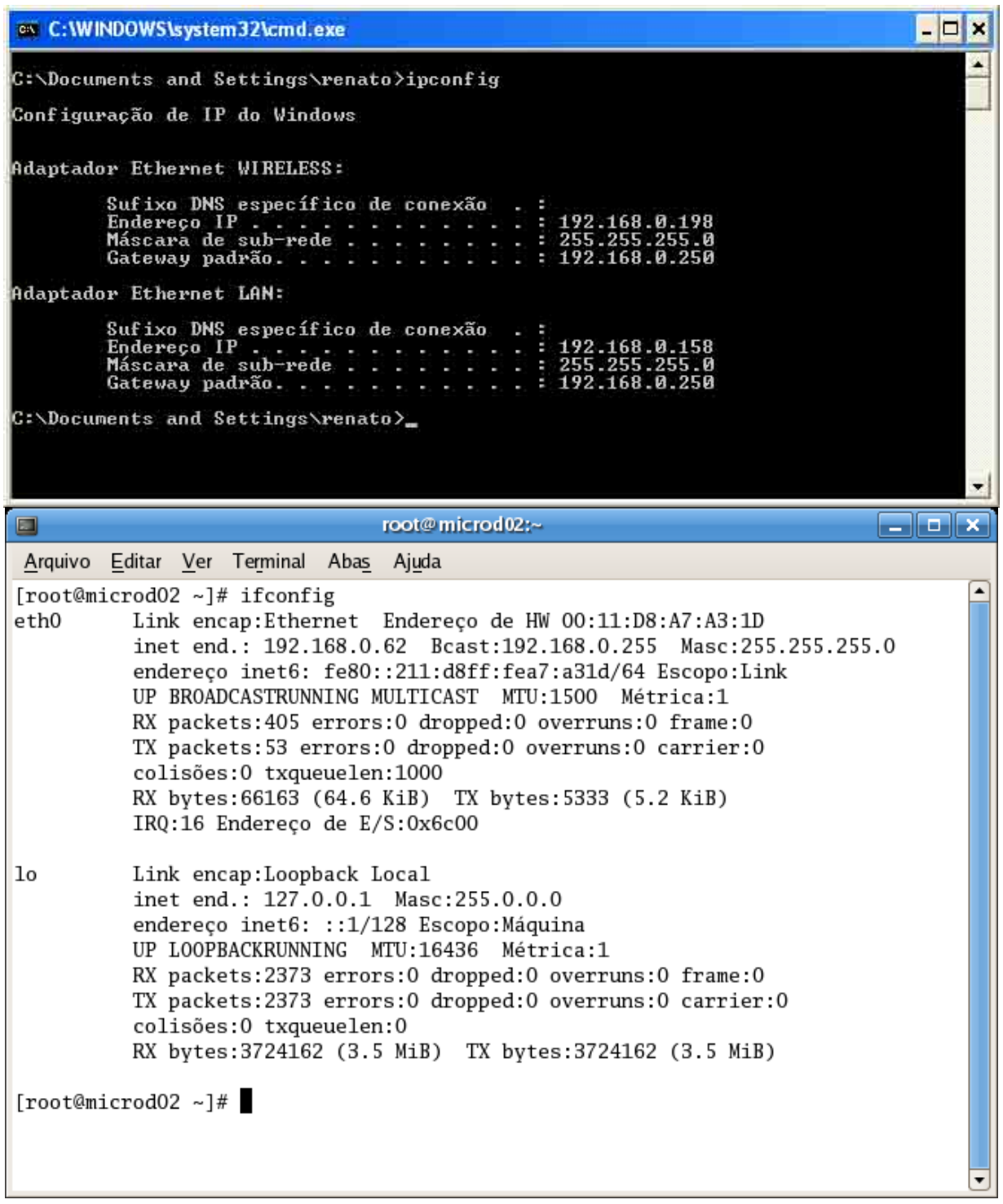
Figura 2.4 | Classes de endereços IPv4



Fonte: Tanenbaum (2011, p. 282).

O endereço IP de um *host* pode ser visualizado através do comando **ipconfig/all**, quando estiver utilizando sistemas operacionais Windows, e **ifconfig** se estiver com um sistema Linux. A Figura 2.5 demonstra um exemplo de informação sobre endereço IP apresentado em console via comando **ipconfig/all** e **ifconfig** .

Figura 2.5 | Visualização (parcial) de endereço IP de um *host*



Fonte: captura de tela do *prompt* de comando do sistema operacional elaborada pelo autor.

Além da utilização de endereços dentro de intervalos definidos pelas classes A, B e C em uma rede local privada, há ainda outras regras de endereçamento que necessitam ser observadas. As regras são:

1. Não pode haver duas ou mais estações com o mesmo endereço IP na mesma rede.
2. A mesma sub-rede deve ser definida em um endereço IP para que dois hosts se comuniquem diretamente.
3. Para determinar qual parte da rede IP significa a rede, é usado o artifício de sub-rede, identificado no próprio endereço IP. De forma complementar, o Quadro 2.1 traz algumas regras sobre a composição de um endereço IP que o invalidam quando utilizados para o endereçamento de um *host* de rede.

Quadro 2.1 | Regras de endereçamento IP reservados

Endereço inválido	Razão
0.xxx.xxx.xxx	Um endereço IP não pode começar com zero quando atribuído a um *host*. O identificador de rede 0 é utilizado para indicar que está na mesma rede.
127.xxx.xxx.xxx	Um endereço IP não pode começar com o número 127. Este número é reservado para testes internos (*loopback*).
255.xxx.xxx.xxx xxx.255.255.255 xxx.xxx.255.255	Nenhum identificador de rede pode ser 255 e nenhum identificador de host pode ser composto apenas de endereços 255. Este número na posição de identificação do *host* é reservado para *broadcast*.
xxx.0.0.0	Nenhum identificador de *host* pode ser composto apenas de zeros.
xxx.xxx.xxx.255	Nenhum endereço de *host* de classe C pode terminar com 0 ou com 255, pois os endereços com o primeiro e o último número do intervalo são reservados.

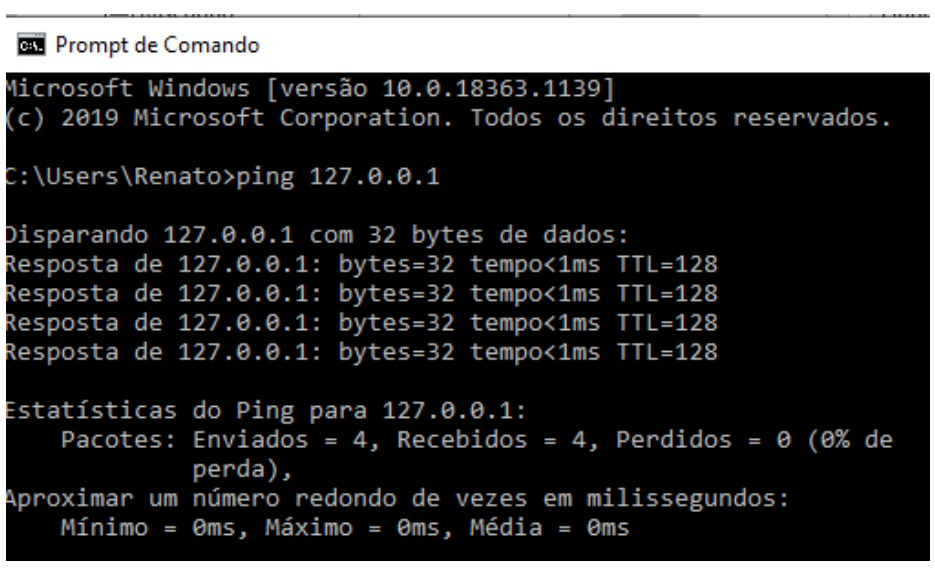
Fonte: elaborado pelo autor.

- **Endereço de *broadcast***: são endereços destinados para comunicação simultânea com todos os hosts da rede. Por exemplo, um servidor de endereços IP, como o DHCP (*Dynamic Host Configuration Protocol*), o utiliza para que as estações possam receber seus endereços IP quando se conectam à rede. Os endereços de broadcast utilizam o 255 na identificação do host de rede, por exemplo: xxx.255.255.255, xxx.xxx.255.255 ou xxx.xxx.xxx.255. Conforme relata Kurose e Ross (2013), quando um host envia um datagrama com o endereço 255.255.255.255, a mensagem é entregue a todos os outros hosts da mesma sub-rede.
- **Endereço de *loopback***: o endereço IPv4 127.0.0.1 é um endereço reservado para realizar testes de comunicação interprocessos da interface da rede pelo

Ver anotações 0

próprio dispositivo. Quando uma aplicação usa o endereço de *loopback* como destino, o software do protocolo TCP/IP devolve os dados sem gerar tráfego na rede. É uma forma simples de fazer com que um cliente local de rede se comunique com o servidor local de forma a testar a própria interface de rede. Este endereço é importante para testar o próprio dispositivo de rede (placa de rede ativa). Você pode testar sua interface digitando **ping 127.0.0.1**. A Figura 2.6 apresenta um exemplo de teste de interface com o comando ping.

Figura 2.6 | Teste de interface de rede com o comando ping e endereço de *loopback*



Fonte: captura de tela do *prompt* de comando do sistema operacional elaborada pelo autor.

Se você **não deseja** conectar diretamente seu dispositivo à internet, você pode utilizar qualquer faixa de endereço, conforme apresentado. Para evitar conflitos, se for conectar seu computador à internet, é necessário que se utilize uma das faixas de endereços reservadas, com as classes A, B ou C em sua rede interna. O Quadro 2.2 apresenta as faixas de endereços reservados mais comuns.

Quadro 2.2 | Faixas de endereços IPs comuns

Classe	Faixa	Redes e *hosts*
A	**10**.x.x.x	**10** é o endereço da **rede**, e x.x.x são os endereços de *hosts*. Composição: **Rede**.*Host.Host.Host*
B	**172.16**.x.x	**172.16** é o endereço da **rede**, e x.x é o endereço de hosts. Composição: **Rede**.**Rede**.*Host*.*Host*

Classe	Faixa	Redes e *hosts*
C	**192.168.1**.x	**192.168.1** é o endereço da **rede**, e x é o endereço de hosts. Composição: **Rede**.**Rede**.**Rede**.*Host*

Fonte: elaborado pelo autor.

EXEMPLIFICANDO

Para ilustrar a utilização destes endereços, vamos observar alguns exemplos:

- O endereço de classe A: endereço 10.0.0.85 informa que 10 é o endereço da rede, e 0.0.85 é o endereço do *host*.
- O endereço de classe B: endereço 172.16.25.85 informa que 172.16 é o endereço da rede, e 25.85 é o endereço do *host*.
- O endereço de classe C: endereço 192.168.0.85 informa que 192.168.0 é o endereço da rede, e 85 é o endereço do *host*.

Em uma rede privada, os endereços devem seguir:

- Classe A: 10.0.0.0 a 10.255.255.255.
- Classe B: 172.16.0.0 a 172.31.255.255.
- Classe C: 192.168.0.0 a 192.168.255.255.

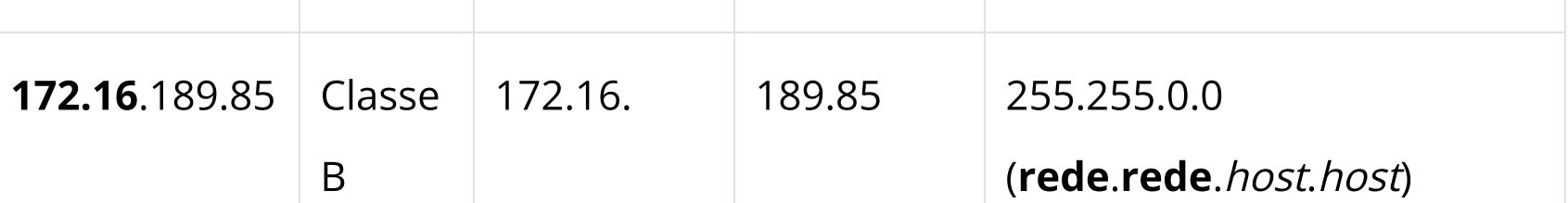
Em redes públicas, os endereços IP precisam ser atribuídos pelo órgão regulamentador e serão utilizados por servidores, como o 201.55.233.117, que identifica o servidor do Google.

MÁSCARA DA SUB-REDE

Uma máscara de rede é uma técnica utilizada para definir a porção do número IP que está designada para identificar a rede e a porção utilizada para identificar o host. A Figura 2.7, apresentada a seguir, demonstra que o endereço IPv4 da rede é 192.168.0.12, e sua máscara da rede é 255.255.255.0, de forma que os três primeiros octetos (255.255.255) representam a rede, e o quarto octeto (0) representa o host. Podemos perceber também que há um endereço que identifica

o Gateway Padrão (192.168.0.1), que representa o caminho de saída das mensagens da sub-rede. Este endereço é normalmente identificado do IP de um dispositivo concentrador/controlador de rede, representado por um *switch* ou roteador.

Figura 2.7 | Exemplo de configuração de número IP, máscara de sub-rede e *gateway*



Fonte: captura de tela do *prompt* de comando do sistema operacional elaborada pelo autor.

O Quadro 2.3 busca complementar as informações anteriores com a distribuição dos octetos do endereço IP em conformidade com as classes de rede.

Quadro 2.3 | Máscaras de sub-rede

Endereço IP	**Classe**	**Rede**	***Host***	**Máscara**
10.158.201.85	Classe A	10.	158.201.85	**255**.0.0.0 (rede.*host*.*host*.*host*)
172.16.189.85	Classe B	172.16.	189.85	255.255.0.0 (**rede**.**rede**.*host*.*host*)
192.168.12.85	Classe C	192.168.12.	85	**255.255.255**.0 (**rede**.**rede**.**rede**.*host*)

Fonte: elaborado pelo autor.

Observamos que o endereço IP permite que uma rede seja dividida em redes diferentes. A composição de um endereço IP define, conforme vimos, que um host tem sua identidade única e pertence a uma rede. Considerando que uma rede pode ser segmentada, ou seja, dividida em sub-redes, o endereçamento também precisa ser utilizado para formalizar esta identificação. Imagine que uma empresa precise isolar os departamentos X, Y e Z dentro de uma rede interna. Isso é possível por meio da manipulação da máscara de redes. Conforme apresentam Kurose e Ross (2013), para determinar as sub-redes, cada interface deve ser

destacada de seu hospedeiro ou roteador, criando ilhas de redes isoladas com interfaces fechando as terminações das redes isoladas. As sub-redes são o termo técnico destas ilhas isoladas. Além da atribuição de mais endereços dentro das classes A, B e C, que permitem a configuração de sub-redes, outro método também foi criado com o objetivo de melhor aproveitar os endereços IPs dentro das redes, chamado pelos autores de CIDR (*Classless Inter-Domain Routing*). Esta é uma estratégia de atribuição de endereços conhecida como roteamento interdomínio sem classes, a qual generaliza a noção de endereçamento de sub-rede.

Da mesma forma que ocorre com o endereçamento de sub-rede utilizando as classes mencionadas, no CIDR o IP de 32 bits é dividido em duas partes, conservando a notação decimal com quatro grupos de números (octetos) separados por ponto, mas adicionado de um novo número separado pela barra. Como exemplo, um endereço na notação CIDR segue o seguinte formato: x.x.x.x/y, onde o y identifica o número de bits da primeira parte do endereço que identifica a rede. O restante dos bits identificará os *hosts*.

Em uma rede classe C, por exemplo, temos os três primeiros octetos (formados cada um por 8 bits) definindo a rede, o que daria uma máscara em notação CIDR da seguinte forma: 192.168.15.85/**24**, onde 24 representa a soma dos bits dos três octetos que identificam a rede. Em uma rede classe B, temos os dois primeiros octetos definindo a rede, o que daria uma máscara de notação CIDR: 172.16.189,85/**16**, onde 16 representa a soma dos bits dos dois octetos que identificam a rede. Estas máscaras fazem com que muitos endereços IP dentro das classes não sejam utilizados, o que representa um desperdício de endereços.

O CIDR permite que a notação que define a máscara de rede (/24 ou /16, por exemplo) tenha números diferentes, utilizando um volume maior de bits nos octetos que definem a rede, o que divide o número de hosts para sub-redes e, desta forma, aproveita-se o número de endereços para *hosts* dentro de uma rede segmentada em sub-redes.

DIVISÃO DE UMA REDE EM SUB-REDES

Uma rede A, B o C pode ser dividida em sub-redes para que uma rede com um número determinado de dispositivos possa ser configurada de forma otimizada. De acordo com Tanenbaum (2011), a segmentação de uma rede, ou divisão em sub-redes, oferece alguns benefícios, como:

1. Reduzir o tráfego da rede, considerando que os hosts de uma sub-rede fazem domínio de *broadcast*.
2. Simplificar o gerenciamento da rede com identificação de falhas através do mapeamento de endereços.
3. Controlar os recursos da rede através de sua segmentação.

Vamos tomar como exemplo uma rede classe C definida como 192.168.123.x. Conforme exemplo apresentado pela Microsoft (2020), se houver uma rede com 150 *hosts* em uma única rede, podemos apenas atribuir os endereços dentro do intervalo de rede definição (classe C com intervalo de endereços de 192.168.123.1 até 192.168.123.152). Porém, ser tivermos redes separadas fisicamente, divididas em três redes de 50 hosts cada, pode-se utilizar a classe C e um endereço 192.168.123.0, utilizando os endereços úteis de 192.168.123.1 até 192.168.123.254 que comportam os 150 *hosts*, mas precisaremos dividi-la em sub-redes.

> Lembre-se das regras de endereçamento que excluem os endereços 192.168.123.0 (primeiro endereço da sub-rede) e 192.168.123.255 (último endereço da sub-rede). Este é o exemplo de endereços que precisam ser desconsiderados para atribuição aos *hosts* no exemplo da rede 192.168.123.0, pois, como temos três sub-redes, teremos três endereços de rede e três endereços de broadcast.

Para dividir uma rede em quatro sub-redes, por exemplo, utiliza-se uma máscara de sub-rede, que torna o endereço de rede maior (utilizando mais bits emprestados dos bits do endereço da rede) e o número de endereços de hosts menor (pois empresta bits do octeto do host), ou seja, utiliza-se de alguns dos bits utilizados para identificar os hosts para identificar parte da rede. Por exemplo, a máscara de sub-rede 255.255.255.192 (11111111.11111111.11111111.11000000 binário) oferece quatro redes de 62 hosts cada. Os dois primeiros bits do último

octeto se tornam endereços de rede e possibilitam que se tenha redes adicionais. Usando uma máscara de rede 255.255.255.192, a rede 192.168.123.0 dispõe de quatro redes, sendo a primeira sub-rede 192.168.123.0, a segunda 192.168.123.64, a terceira 192.168.126.128 e a quarta 192.168.123.192, com 62 hosts endereçáveis em cada uma delas.

Para calcular as sub-redes através de um exemplo adaptado de Nunes (2017) e poder melhor entender a divisão da rede apresentada anteriormente, seguiremos estes passos:

Passo 1: fazer a conversão da máscara de rede de 255.255.255.0 para binário, que resulta em 1111111.11111111.11111111.00000000.

EXEMPLIFICANDO

Na conversão de número binário para decimal, devemos somar os valores numéricos representados pela posição do número binário 1 na posição em seu octeto. Veja a tabela a seguir.

1	1	1	1	1	1	1	1	8 *Bits*
128	64	32	16	8	4	2	1	Valor Binário
128+	64+	32+	16+	8+	4+	2+	1+	=255

Exemplo de conversão:

Binário	0	1	0	0	1	0	0	1
Decimal	0+	**64+**	0+	0+	8+	0+	0+	1+ =73

Na conversão de números decimais para binário, devemos dividir o número decimal por 2 até que o resultado seja 0 ou 1. O número final e os restos da divisão são posicionados no octeto do byte de forma invertida.

Exemplo de conversão do número 73 decimal para binário:

Decimal			73/2=36	36/2=18	18/2=9	9/2=4	4/2=2	2/2=1
Binário	73=		1	0	0	1	0	0

Ver anotações

> O número 73 em decimal = 1001 0010 em binário (o oitavo bit é naturalmente 0).

Passo 2: fazer o cálculo da quantidade de hosts para cada uma das sub-redes, considerando o número (n) de bits necessários para:

- **A rede**: $2^n = 2^2 = 4$, ou seja, para fazer quatro sub-redes será necessário alocar dois bits da máscara de rede. Note que podemos ter dois ou quatro (ou mais, desde que sejam números pares), assim como precisamos dividir nossa rede em três sub-redes, utilizaremos o cálculo com quatro sub-redes.
- ***Hosts* de sub-rede**: $2^n = 2^6 = 64$, com possibilidade de até 64 *hosts* em cada sub-rede. Considere que, para converter os octetos, são utilizados: 1, 2, 4, 8, 16, 32, 64 e 128. Como foram utilizados dois bits para a definição das redes, sobraram outros seis bits para os *hosts*.

Passo 3: elaborar a tabela ou o racional com os endereços da sub-rede. Novamente, lembre-se das regras de endereçamento, que excluem todos os endereços de rede e de *broadcast*, por exemplo, os endereços 192.168.123.0 e 192.168.123.255.

- **Sub-rede 1**: 192.168.123.0: *hosts* que variam de 192.168.123.1 até 192.168.123.62, e *broadcast* 192.168.123.63.
- **Sub-rede 2:** 192.168.123.64: *hosts* que variam de 192.168.123.65 até 192.168.123.126, e *broadcast* 192.168.123.127.
- **Sub-rede 3**: 192.168.123.128: *hosts* que variam de 192.168.123.129 até 192.168.123.190, e *broadcast* 192.168.123.191.
- **Sub-rede 4**: 192.168.123.192: *hosts* que variam de 192.168.123.193 até 192.168.123.254, e *broadcast* 192.168.123.255.

Passo 4: identificar a máscara da rede. Considere que a máscara de rede 11111111.11111111.11111111.00000000 binário (255.255.255.0 decimal) utilizou dois bits do octeto do host para adicionar nos octetos da rede (sub-rede), O primeiro bit da máscara representa o número decimal 128, e o segundo bit, 64;

desta forma, temos 128 + 64 = 192, ficando a máscara da rede como 11111111.11111111.1111111.11000000 binário (255.255.255.192 decimal). Em notação CIDR, temos a máscara binária 11111111.11111111.11111111.11000000 com 26 bits definindo a máscara da rede, o que resulta em uma notação decimal de um endereço IP como 192.168.123.1/26, onde 192.168.123.1 é um dos endereços da rede e /26 identifica a sub-rede, formada pela somatória dos bits que identificam a rede. A notação para a nova máscara de sub-rede é: **255.255.255.192, ou /26.**

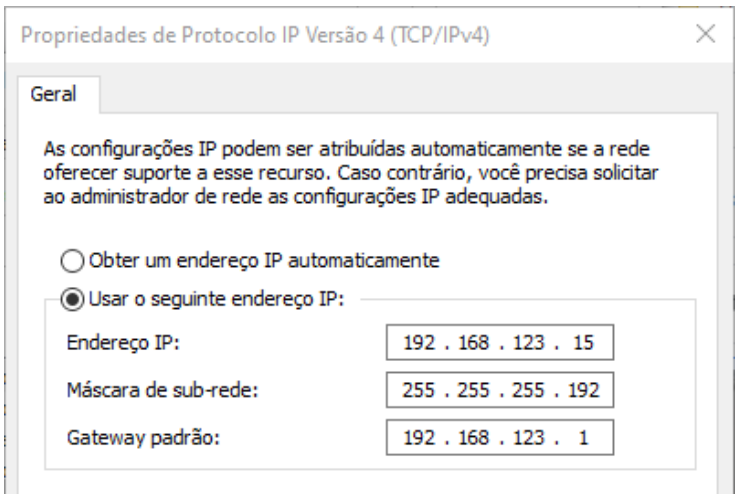
ASSIMILE

Um número binário pode tomar os valores de 0 e 1, ou seja, dois valores numéricos. Um número binário de dois dígitos pode tomar as posições 00, 01, 10, 11, ou seja, quatro valores numéricos. Esta sequência se dará exponencialmente até 256 valores numéricos em um octeto, ou seja, em um número binário de oito dígitos, como um octeto de um endereço IP. Como pode ser visto na representação a seguir, dois bits do octeto que forma o endereço de host de um endereço de classe C foram adicionados aos outros três bits que identificam a rede para a formatação do número a ser utilizado para representar a sub-rede, no quarto octeto da máscara. Perceba que, quando temos o bit 0, o valor decimal representado no octeto é desconsiderado na soma da máscara da rede; quando temos o bit 1, somamos os valores decimais para a composição da máscara da sub-rede.

Bits da rede		**Bits do *host***					
128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Os endereços IPs e as máscaras (e sub-rede, se desejado) precisam ser informados em cada *host* da rede. Segue, na Figura 2.8, um exemplo de configuração de endereço IP e máscara de rede em um sistema Windows.

Figura 2.8 | Exemplo de configuração de endereço IP



Fonte: captura de tela elaborada pelo autor.

DNS (*DOMAIN NAME SYSTEM*)

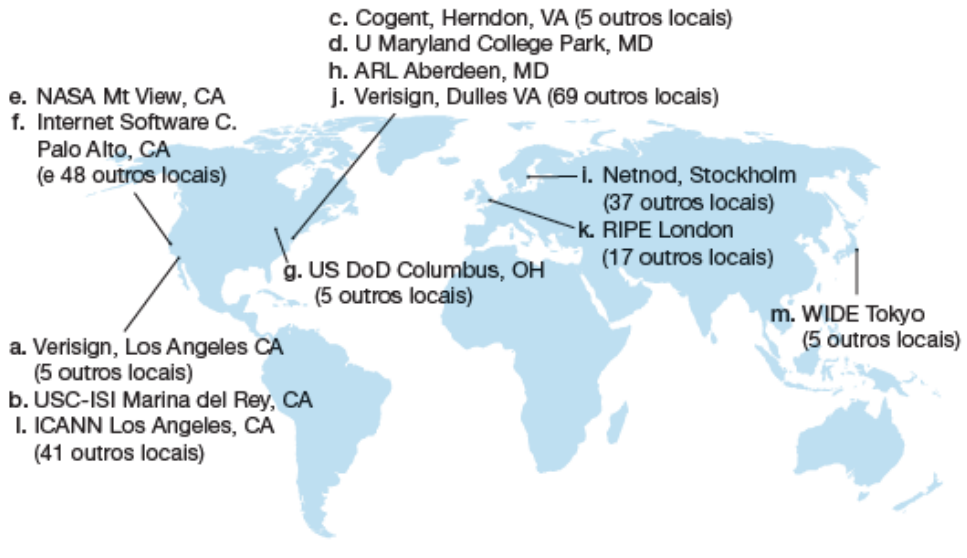
O DNS é um protocolo utilizado para um sistema de domínio que faz a interconexão de URL (*Uniform Resource Locator*), ou seja, nomes de endereços de sites da internet com endereços IP. Este protocolo implementa um serviço importante de resolução de nomes mediante endereços IPs externos, localizados dentro de uma estrutura hierárquica na internet. As empresas também utilizam servidores de DNS para que suas redes locais possam encontrar informações mediante a utilização de nomes, inseridas como URL no lugar de endereços IPs, utilizando-se de um servidor de DNS.

De acordo com Kurose e Ross (2013), o DNS costuma ser empregado por outras entidades da camada de aplicação, como o HTTP, SMTP e FTP, para traduzir nomes de hosts fornecidos por usuários para endereço IP. De forma sintética, para que uma URL informada em um navegador possa retornar o conteúdo do site, é necessário que ele busque o seu endereço IP correspondente através de alguns passos:

1. O *host* do usuário executa o lado cliente da aplicação DNS.
2. O navegador extrai o nome do host do URL e passa o nome para o lado do cliente da aplicação DNS.
3. O cliente DNS envia uma consulta com o nome do *host* para um servidor DNS.
4. O cliente DNS recebe uma resposta com o endereço IP do nome do *host* pesquisado.
5. O navegador recebe o endereço do DNS e abre uma conexão TCP com o processo servidor do HTTP via porta 80 naquele endereço IP.

O DNS é um protocolo que implementa um serviço de resolução (tradução) de nomes, endereços de páginas definidas por suas URL (*Uniform Resource Locator*) em endereços IPs dentro de uma estrutura hierárquica de servidores espalhados pelo mundo todo. Na internet, existem servidores DNS raiz que se interligam a servidores de domínio de alto nível, chamados de TLD (*Top Level Domain*), responsáveis por domínios, como .com, .org, .net, .edu e .gov, e por domínios de alto nível de países, como .uk, .fr., .br. Abaixo destes servidores, estão os servidores DNS autorizativos (de autoridade, ou locais), disponibilizados por organizações que desejam oferecer hosts servidores para acesso público na internet, e finalmente os servidores de nomes locais, que necessariamente não pertencem a uma hierarquia e são chamados de servidores de nomes *default*. A Figura 2.9 apresenta os servidores raiz do mundo em 2012.

Figura 2.9 | Servidores raiz no mundo em 2012



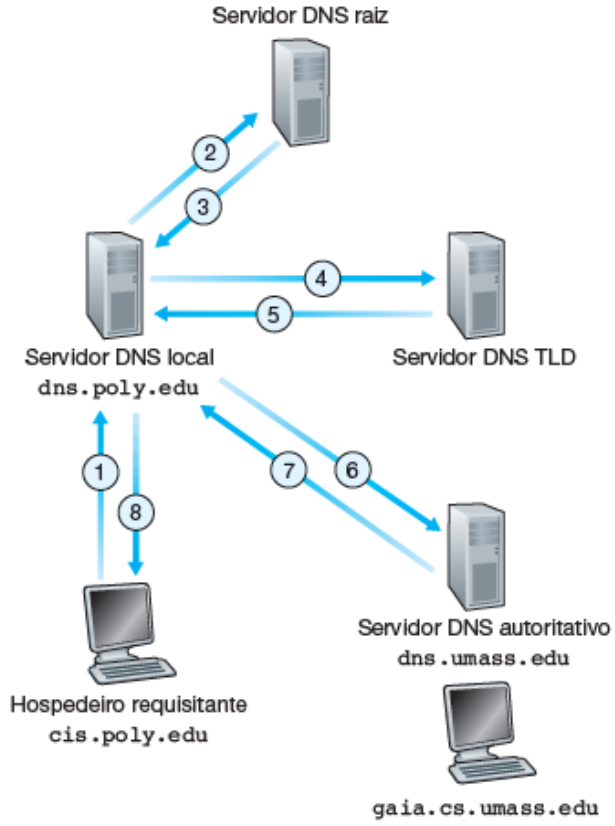
Fonte: Kurose e Ross (2013, p. 99).

Em sua funcionalidade básica, quando um resolvedor tem uma consulta sobre um nome de domínio, ele a envia a um dos servidores de nomes local. Se o domínio que estiver sendo buscado estiver sob a jurisdição do servidor de nomes, serão retornados os registros com as informações de acesso. Caso o domínio for remoto e não houver informações sobre o domínio solicitado no local, o servidor de nomes (DNS) enviará uma mensagem de consulta para o servidor DNS de nível superior, buscando o domínio solicitado. Dois protocolos agem neste processo: o próprio DNS que traduz nomes simbólicos em endereços IP e o LDAP (*Ligh-weith Directory Access Protocol*), que organiza as informações como uma árvore e permite

pesquisas em diferentes componentes e realiza a busca pelas informações solicitadas. A Figura 2.10 ilustra a relação hierárquica e distribuída entre servidores de controle de DNS espalhados pelo mundo com servidores locais.

Conforme exemplificam Kurose e Ross (2013): um hospedeiro **cis.poly.edu** deseja o endereço IP de **gaia.cs.umass.edu**. Considere que o servidor DNS local é **dns.poly.edu** e que um servidor DNS autorizativo para **gaia.cs.umass.edu** seja denominado **dns.umass.edu**. Como mostra a Figura 2.10, o hospedeiro **cis.poly.edu** primeiro envia uma mensagem de consulta DNS ao seu servidor DNS local dns.poly.edu. A mensagem de consulta contém o nome de hospedeiro a ser traduzido, isto é, **gaia.cs.umass.edu.** O servidor DNS local transmite uma mensagem de consulta a um servidor DNS raiz, que verifica o sufixo **edu** e retorna ao servidor DNS local uma lista de endereços IP de servidores TLD responsáveis por **edu**. O servidor DNS local retransmite a mensagem de consulta a um desses servidores TLD, o qual, por sua vez, percebe o sufixo **umass.edu** e responde com o endereço IP do servidor DNS autorizado para a instituição com dns.umass.edu. O servidor DNS local reenvia a mensagem de consulta para **dns.umass.edu**, que responde com o endereço IP de **gaia.cs.umass.edu**. Para poder obter o mapeamento para um único nome de hospedeiro, foram enviadas oito mensagens DNS: quatro mensagens de consulta e quatro de resposta.

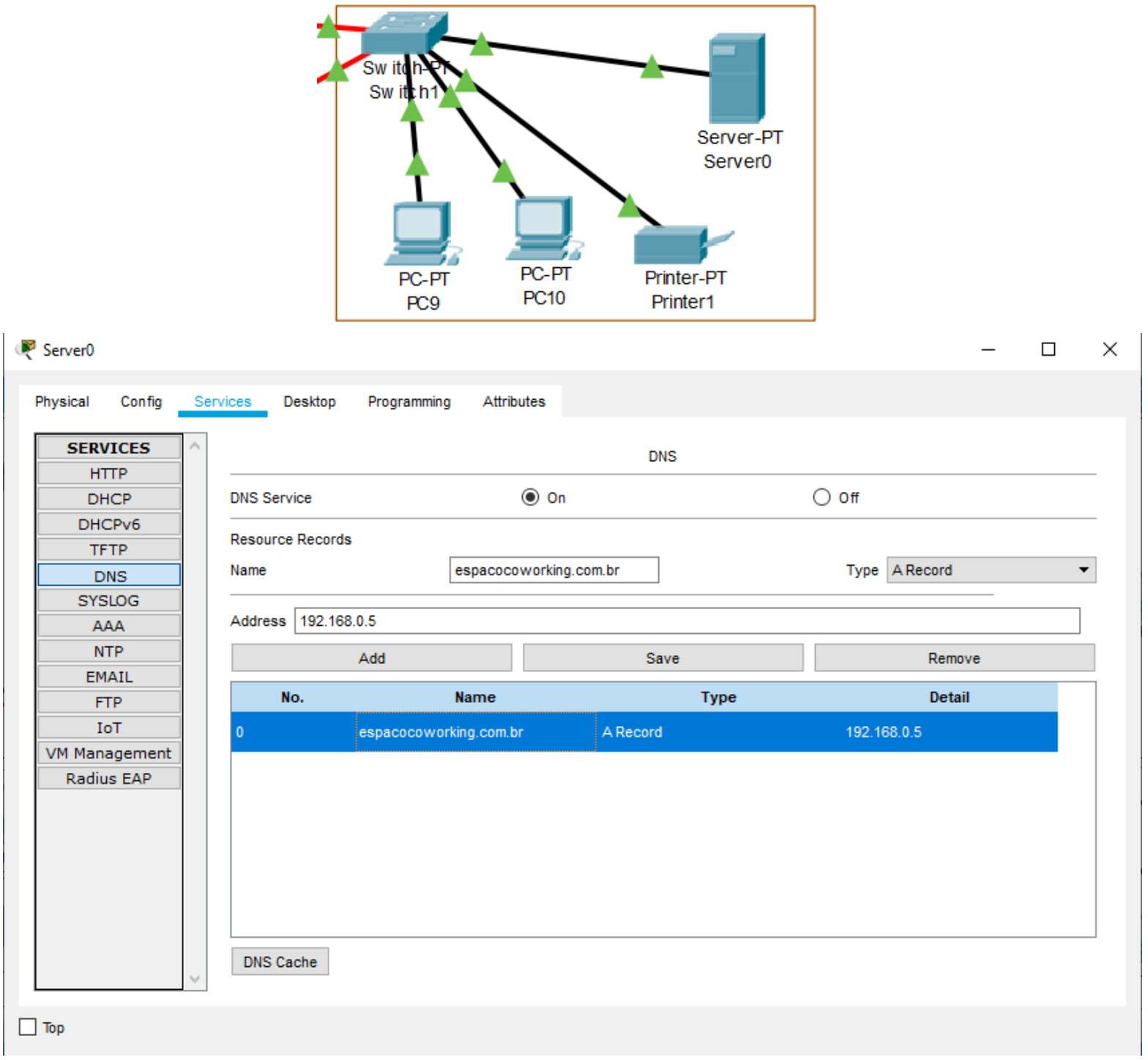
Figura 2.10 | Interação entre servidores de DNS



Fonte: Kurose e Ross (2013, p. 100).

Dentro de uma organização, é possível implementar um servidor de DNS para que informações possam ser compartilhadas dentro da estrutura da rede. De acordo com Northrup e Mackin (2009), a implantação de um servidor DNS é um procedimento razoavelmente simples, especialmente em um controlador de domínio. Kurose e Ross (2013) identificam um DNS como um servidor organizado de maneira hierárquica e distribuída. A seguir, temos um exemplo de topologia de rede com um servidor DNS instalado e configurado através da ferramenta *Packet Tracer*, demonstrada na Figura 2.11.

Figura 2.11 | Servidor DNS em uma rede



Fonte: elaborada pelo autor.

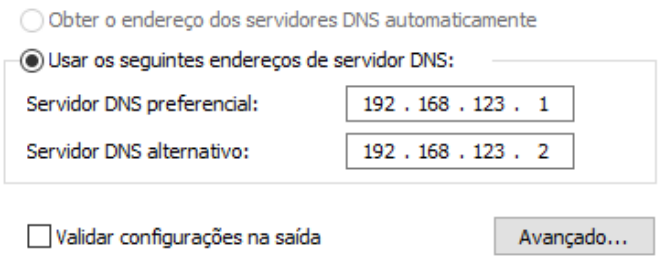
Em um sistema Windows Server, a ativação do servidor DNS se dá primeiramente pela criação de uma zona DNS, que é um banco de dados com registros que associam nomes a endereços para uma parte definida de um espaço de nomes DNS. Depois, o servidor DNS precisa ser configurado para registros de DNS e, por último, configurar a replicação e transferência de zona. Já em distribuições Linux,

as configurações podem ser feitas em menus do ambiente gráfico ou via configuração textual no arquivo **/etc/named.conf**. O arquivo ***localhost*** define todas as configurações de domínio local para informar o endereço de consulta ao *hostname localhost*. O banco de dados do domínio é definido pelos arquivos zona e zona reversa.

> **ASSIMILE**
>
> De forma geral, o DNS trata da busca de endereços IPs para que você possa fazer suas buscas e operações via sistemas em rede, dentro da WWW (*World Wide Web*), por exemplo. Na prática, um conjunto de páginas web em formato HTTP, chamado de site, é acessado através de um endereço URL informado em um *browser*, que carrega a sua página principal, chamada de *home page*, dentro de um ambiente WWW. Sites de busca auxiliam na localização de URLs dentro desta estrutura hierárquica, como Google, Yahoo, Bing, Baidu, entre outros. O Google representa, conforme Laudon e Laudon (2014), mais de 83% das buscas realizadas na internet.

Junto à configuração do endereço IP do *host* e às informações de máscara de rede, deve também ser informado o endereço de DNS na rede. Segue, na Figura 2.12, um exemplo de configuração de endereço de DNS em um sistema Windows.

Figura 2.12 | Exemplo de configuração de DNS



Fonte: captura de tela elaborada pelo autor.

DHCP (*DYNAMIC HOST CONFIGURATION PROTOCOL*)

O DHCP permite atribuir endereços IP, máscaras de sub-rede e outras informações de configuração a computadores clientes em uma rede local. Uma rede que possui um servidor DHCP disponível permite aos seus computadores obterem um endereço IP através de solicitação e atribuição automática pelo servidor, conforme defendem Northrup e Mackin (2009).

Um administrador de rede pode configurar um serviço de DHCP para que determinado host receba o mesmo endereço IP toda vez que se conectar, ou um endereço IP temporário, diferente a cada conexão. Kurose e Ross (2013) classificam o DHCP como um protocolo *plug and play*, considerando sua capacidade de automatizar os aspectos relativos à rede da conexão de um host. Ademais, o DHCP é um protocolo cliente-servidor, no qual, em geral, um *host* representa o cliente. A Figura 2.13 ilustra um servidor DHCP conectado à rede 223.1.2.0/24, servindo o roteador de agente de repasse para clientes conectados às sub-redes 223.1.1.0/24 e 223.1.3.0/24. Para um hospedeiro recém-chegado, o protocolo DHCP e um processo de quatro etapas:

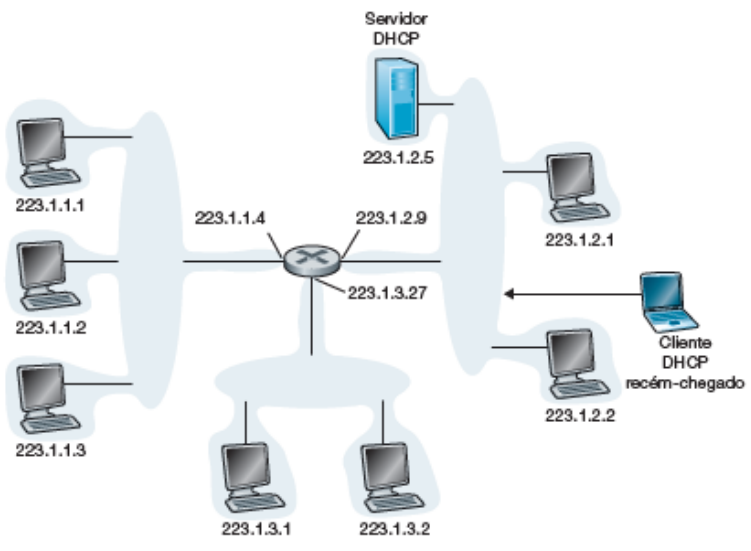
1. Descoberta do servidor DCHP.

2. Oferta dos servidores DHCP.

3. Solicitação DHCP.

4. Configuração de requisição DHCP.

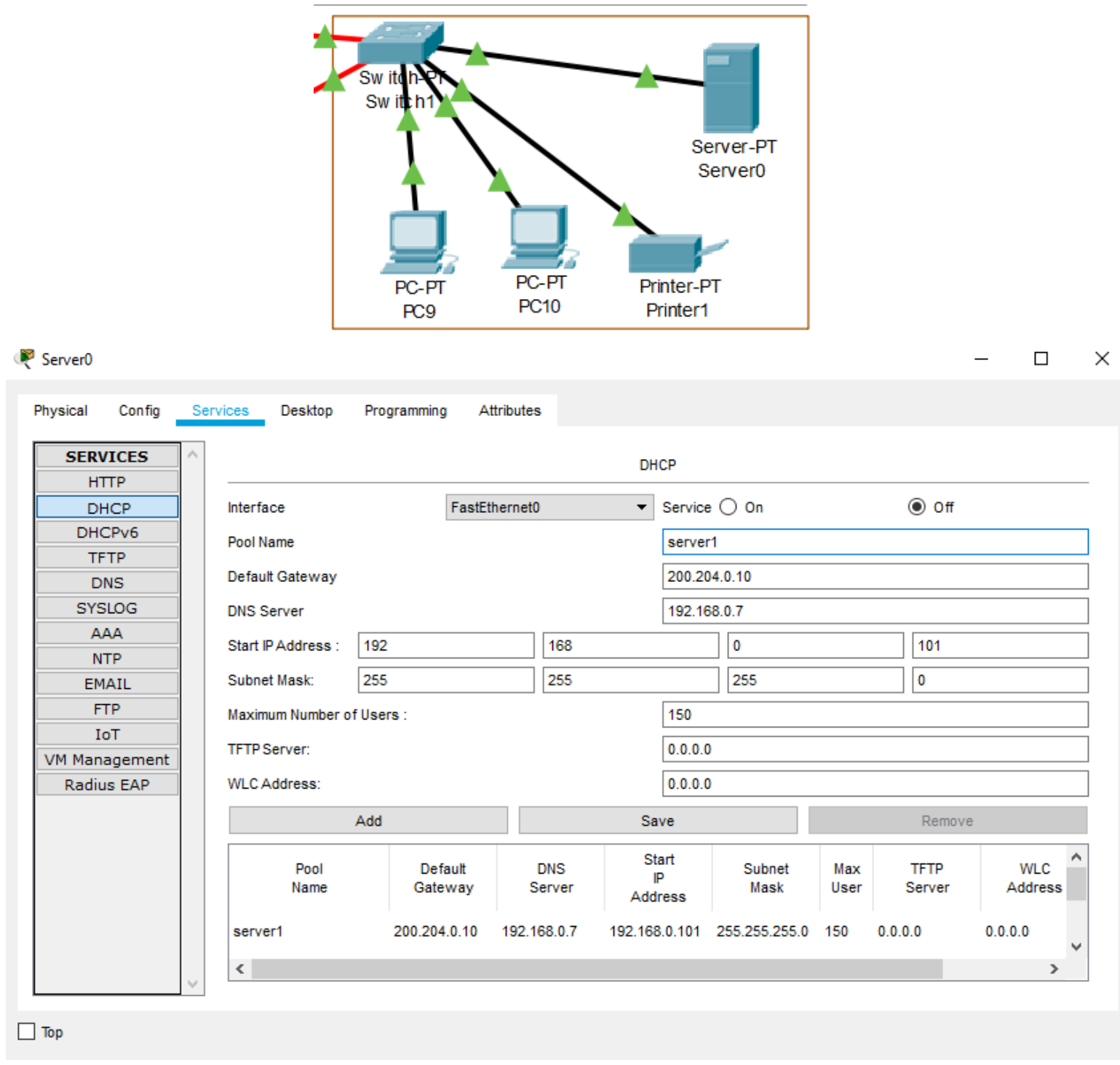
Figura 2.13 | Servidor DHCP em uma rede



Fonte: Kurose e Ross (2013, p. 256).

A seguir, temos um exemplo de topologia de rede com um servidor DHCP instalado e configurado através da ferramenta *Packet Tracer*, demonstrada na Figura 2.14. A imagem refere-se ao departamento Servidor, no qual existe um servidor de rede que suporta serviços de DNS, DHCP, HTTP, FTP, entre outros, ligados a um Switch que interliga e serve toda uma rede de um departamento. A parte inferior da figura a seguir mostra a configuração do serviço de DHCP no *Packet Tracer.*

Figura 2.14 | Exemplo de configuração de servidor DHCP na ferramenta *Packet Tracer*

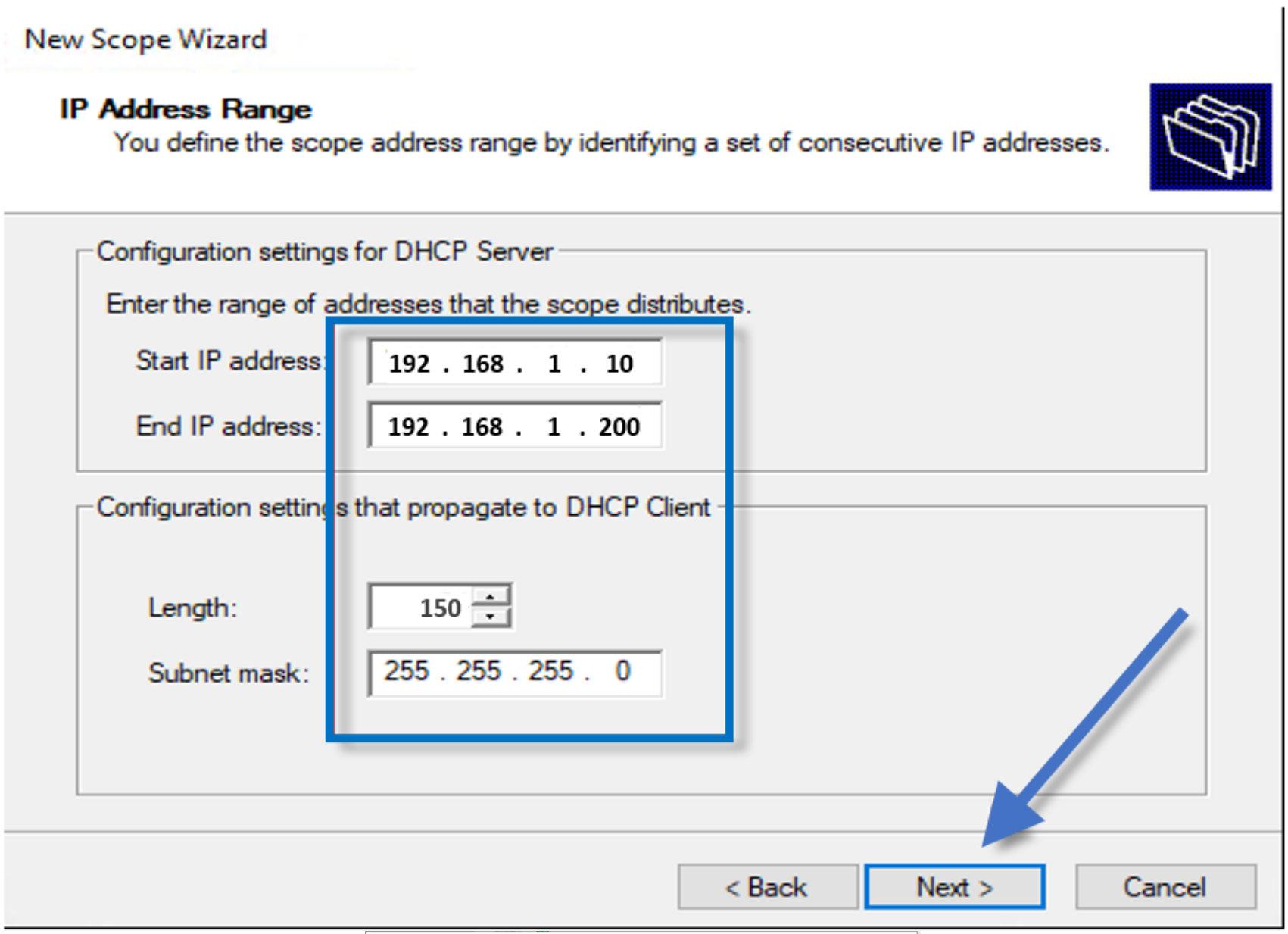


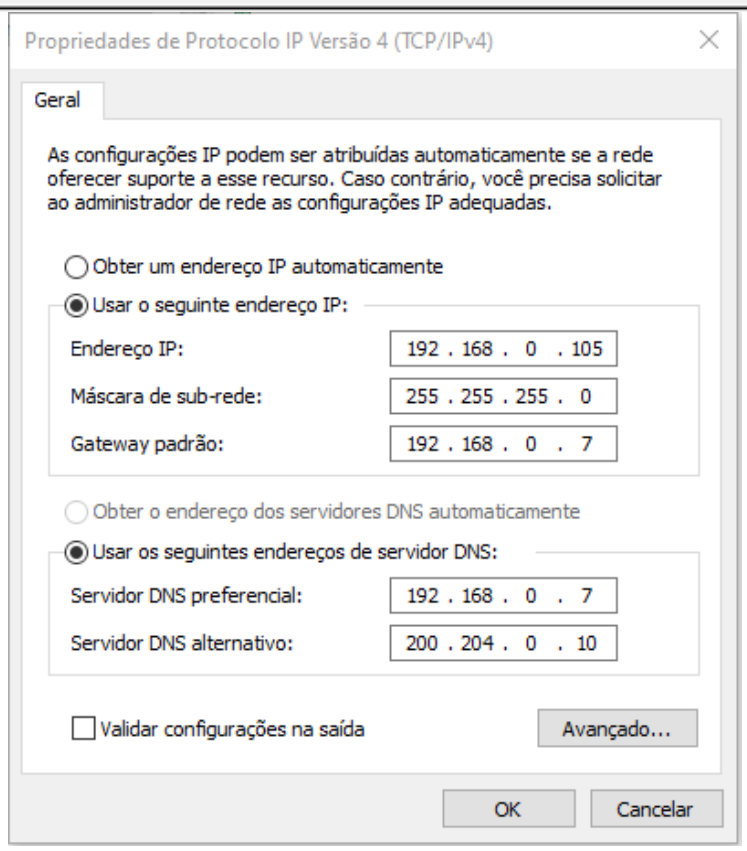
Fonte: elaborada pelo autor.

Em distribuições Linux, as configurações podem ser feitas em menus do ambiente gráfico ou via configuração textual no arquivo **/etc/dhcpd.conf.** A sua ativação se dá pela execução do programa **ntsysv** com a seleção da opção dhcpd. Ainda em Linux, o servidor DHCP pode ser executado através do comando **# service dhcpd start.**

Em um ambiente Windows Server, a configuração do intervalo de endereços a serem automaticamente atribuídos aos *hosts* se dá por meio do menu Iniciar > Programas > Ferramentas Administrativas > DHCP. A Figura 2.15 apresenta as telas de configuração de um servidor DHCP em plataforma Windows Server e cliente em plataforma Windows.

Figura 2.15 | Configuração de intervalos de endereços IPv4





Fonte: captura de tela elaborada pelo autor.

REFLITA

A configuração manual de endereços IP em redes de computadores locais pode ser uma estratégia mais assertiva quando se pensa em maior segurança, porém adequa-se a ambientes com poucos dispositivos na rede, devido à dificuldade de configuração individual e manual de cada dispositivo. Em redes maiores, a utilização de um servidor DHCP traz maior comodidade à gestão da rede, no entanto pode oferecer maiores riscos à segurança da rede.

Assim, um servidor DHCP mantém um banco de dados dos endereços que o servidor pode atribuir a *hosts* da rede. Quando um servidor DHCP atribui um endereço a um computador na rede, este se torna um host ativo com o endereço atribuído por seis ou oito dias por padrão.

PESQUISE MAIS

O site de suporte da Microsoft traz uma seção interessante, chamada Noções básicas sobre endereçamento *TCP/IP e sub-rede*, que explica o endereçamento IP de uma rede.

Configurar uma rede com o IPv4 e sub-redes leva à utilização dos endereços IPs em redes de classes A, B ou C, alocados em sub-redes. Esta configuração deve seguir uma política de atribuição de endereços, utilizando-se de máscaras de rede para a realização da divisão das redes. O padrão CIDR (*Classless Inter-Domain Routing*) também é utilizado para configuração de sub-redes. Adicionalmente, existe o VLSM (*Variable Length Subnet Masking*), também utilizado para planejamento e configuração de endereços IPs e máscaras em sub-redes. O site *Hardware* pode ser visitado para um estudo complementar sobre este assunto junto ao conteúdo: *Faixas de endereços IP CIDR e máscaras de tamanho variável* (MONQUEIRO, 2007).

Caro aluno, esta seção trouxe para você informações importantes para a configuração de endereços IPv4 em hosts em uma rede. Os endereços podem ser atribuídos de forma manual ou de forma automática por um servidor DHCP. Também houve o aprendizado sobre máscaras de rede e a configuração de uma sub-rede através de seus endereços e máscaras. Estas informações são fundamentais para que você possa configurar dispositivos adequadamente, em conformidade com regras e técnicas de endereçamento IP, de forma a deixar sua rede com performance superior a uma rede sem planejamento de endereçamento IP.

FAÇA VALER A PENA

Questão 1

Um endereço IP privado está condicionado a um intervalo definido, que pode ser utilizado para configuração manual ou automática dentro de uma rede privada. Para melhor aproveitamento e gestão de uma rede, os endereços IPs privados estão divididos em cinco classes: A, B, C, D e E. A classe A permite até 128 redes com 16.777.214 milhões de endereços cada uma; a classe B permite 16.384 redes com até 65.536 *hosts*; e a classe C permite, aproximadamente, 2 milhões de redes com até 254 endereços cada uma delas (considerando que são reservados o endereço 0 e 255 para broadcast). Conforme ressalta Tanenbaum (2011), esse é um projeto hierárquico, no qual os tamanhos dos blocos de endereços são fixos.

Assinale a alternativa que representa um endereço IPv4 de classe B válido para atribuir a um host dentro de uma rede local:

a. 10.0.12.1.

b. 172.16.10.100.

c. 192.168.15.111.

d. 127.0.0.1.

e. 200.204.0.10.

Questão 2

O protocolo IP (*Internet Protocol*) possui duas versões ativas que podem ser utilizadas para o endereçamento de hosts em uma rede de computadores. Trata-se de um protocolo de camada de inter-rede do modelo TCP/IP (*Transmission Control Protocol/Internet Protocol*) utilizado para endereçamento e roteamento das redes de computadores internas e conectadas à internet.

Sobre o protocolo IP em sua versão IPv4, analise as afirmativas a seguir:

I. É um protocolo de datagramas sem conexão e não confiável.

II. IPv4 não possui mecanismos de controle de erros ou de fluxo, com exceção da detecção de erros no cabeçalho.

III. Ele é formado por um conjunto de quatro números binários de oito bits cada um, constituindo-se desta forma de um endereço de 32 bits.

IV. Um exemplo de endereço IPv4 é: 192.356.4.299.

Considerando o contexto apresentado, é correto o que se afirma em:

a. I e II, apenas.

b. I e III, apenas

c. II e III, apenas.

d. I, II e III, apenas.

e. I, II, III e IV.

Questão 3

A máscara de sub-rede é uma técnica de definição de endereço de rede utilizado para alocar a parte do endereço IP (*Internet Protocol*) que define o endereço da rede e a parte que aloca o endereço e um host que faz parte da rede. As máscaras podem ser definidas junto aos endereços de classes definidas, como as classes A, B e C, chamado de endereçamento com classes, assim como pela distribuição dos bits dos octetos que forma os quatro números de um endereço IP, de forma que parte dos bits do host definem a sub-rede no endereçamento sem classe.

Assinale a alternativa que apresenta uma máscara de sub-rede de classe C dividida em duas sub-redes:

a. 255.255.255.0.

b. 255.255.255.240.

c. 255.255.255.192.

d. 255.255.255.224.

e. 255.255.255.128.

REFERÊNCIAS

DIAMANDIS, P. H.; KOTLER, S. **Oportunidades Exponenciais**: um manual prático para transformar os maiores problemas do mundo nas maiores oportunidades de negócio. Rio de Janeiro: Alta Books, 2018.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 4. ed. Porto Alegre: AMGH, 2010.

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.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de Informações Gerenciais**. 11. ed. São Paulo: Pearson Prentice Hall, 2014.

MICROSOFT. **Noções básicas sobre endereçamento TCP/IP e sub-rede**. 2020. Disponível em: https://support.microsoft.com/pt-br/help/164015/understanding-tcp-ip-addressing-and-subnetting-basics. Acesso em: 28 out. 2020.

MICROSOFT. **Configurando o serviço do servidor DNS**. 2018. Disponível em: https://docs.microsoft.com/pt-br/windows-server/identity/ad-ds/manage/ad-forest-recovery-configure-dns. Acesso em: 29 out. 2020.

MONQUEIRO, J. C. B. Faixas de endereços IP, CIDR e máscaras de tamanho variável. **Hardware**, 2007. Disponível em: https://www.hardware.com.br/tutoriais/endereco-ip-cidr/pagina2.html. Acesso em: 28 out. 2020.

NORTHRUP, T.; MACKIN, J. C. **Configuração do Windows Server**: infraestrutura de rede. Porto Alegre: Bookman, 2009.

NUNES, S. E. **Redes de Computadores**. Londrina, PR: Editora e Distribuidora Educacional S. A., 2017.

STALLINGS, W. **Redes e Sistemas de Comunicação de Dados**. Rio de Janeiro: Elsevier, 2016. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595156708/. Acesso em: 21 out. 2020.

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