

# Protocolos TCP/IP e Endereçamento de Rede

---

## Conteudista

Prof. Esp. Hugo Fernandes

## Revisão Textual

Aline de Fátima Camargo da Silva



# Sumário

---

<b>Objetivos da Unidade .....</b>	<b>3</b>
<b>TCP/IP .....</b>	<b>4</b>
<b>Endereço IPv4 .....</b>	<b>13</b>
Rede Classe A – Prefixo/8 .....	24
Rede Classe B – Prefixo/16 .....	25
Rede Classe C – Prefixo/24 .....	25
<b>Atividades de Fixação .....</b>	<b>27</b>
<b>Material Complementar.....</b>	<b>28</b>
<b>Referências.....</b>	<b>29</b>
<b>Gabarito .....</b>	<b>30</b>

# Objetivos da Unidade

---

- Conhecer a suíte TCP/IP, o modelo de referência OSI e o endereçamento IPv4;
- Entender que endereços IP são necessários para comunicação entre as máquinas;
- Compreender que para definir um endereço IP existem algumas regras as quais devem ser seguidas, pois, do contrário, a comunicação não será possível.

Atenção, estudante! Aqui, reforçamos o acesso ao conteúdo *on-line* para que você assista à videoaula. Será muito importante para o entendimento do conteúdo.

Este arquivo PDF contém o mesmo conteúdo visto *on-line*. Sua disponibilização é para consulta *off-line* e possibilidade de impressão. No entanto, recomendamos que acesse o conteúdo *on-line* para melhor aproveitamento.

## VOCÊ SABE RESPONDER?

Com tantos computadores ligados à rede, como identificá-los?

# TCP/IP

Todos os equipamentos conectados à rede de computadores precisam ser identificados com um endereço lógico ao qual chamamos de endereço IP, o qual, por sua vez, é usado pelas máquinas para se comunicarem umas com as outras. O processo para que uma mensagem ou informação seja enviada de uma máquina para outra passa por vários protocolos de comunicação e, geralmente, todos os protocolos usados pertencem à suíte TCP/IP.



### Trocando Ideias

Você sabia que o protocolo TCP/IP teve sua origem em uma pesquisa realizada no final da década de 1960 e início de 1970 pela *Defense Advanced Research Project Agency* (Darpa), mantida pelo Departamento de Defesa dos Estados Unidos (DOD)? A intenção era construir uma rede para conectar um grande número de instalações militares. Os principais requisitos para a rede foram os seguintes:

- Deveria continuar a funcionar durante uma guerra nuclear – o desenvolvimento ocorreu durante a Guerra Fria;
- Deveria ser completamente descentralizada, sem instalação central, a qual poderia ser destruída e derrubar toda a rede;
- Deveria ser totalmente redundante e capaz de continuar a comunicação entre A e B, mesmo que sites intermediários e links parassem de funcionar durante a conversa;
- A arquitetura deveria ser flexível, uma vez que a gama de aplicações previstas para a rede era ampla – desde transferência de arquivos até dados sensíveis ao tempo, como voz.

O protocolo TCP/IP é constituído por outros protocolos e cada um tem uma função específica dentro da suíte TCP/IP. Foi dividido em camadas para se tornar compatível com o modelo de referência OSI. O TCP/IP foi criado antes da padronização do modelo de referência OSI. Esse modelo foi estabelecido para poder padronizar as funções e características dos protocolos a serem desenvolvidos. Portanto, qualquer protocolo a ser elaborado com o objetivo de se tornar de uso público deve seguir as recomendações estabelecidas no modelo de referência OSI, o qual foi dividido em sete camadas: aplicação, apresentação, sessão, transporte, rede, enlace e física, cada uma com características diferentes.

Aplicação
Apresentação
Sessão
Transporte
Redes
Enlace
Física

**Figura 1** – Modelo de referência OSI

**Fonte:** Acervo do Conteudista

**#ParaTodosVerem:**a figura mostra um quadro retangular dividido em linhas, em cada uma delas, de cima para baixo, há os termos “Aplicação”, “Apresentação”, “Sessão”, “Transporte”, “Redes”, “Enlace”, “Física”. Fim da descrição.

Cada uma das camadas tem uma variedade de protocolos com objetivos diferentes, no entanto, todos se baseiam na função de cada camada. Os dados, no sentido de transmissão, são enviados a partir da camada de aplicação, passando pela camada de apresentação até chegar à camada física. No sentido de recepção, os dados chegam à camada física e passam por todas as outras camadas até chegarem à camada de aplicação.

A **camada de aplicação** tem como função principal prover a comunicação da rede de computadores com os usuários. Nela, ficam as aplicações ou aplicativos usados para comunicação em rede. É a camada em que o usuário pode interagir com os programas desenvolvidos; encapsula a complexidade dos protocolos usados nessa.

A **camada de apresentação** do modelo de referência OSI tem como função preparar os dados para serem enviados para a camada de aplicação, além de realizar modificações para entregar as informações à camada de sessão. Resumindo, é responsável por traduzir dados de um formato para outro, portanto, é nela que se encontram os mecanismos para fazer criptografia, compressão e descompressão.

A **camada de sessão** tem como função principal estabelecer uma sessão entre uma máquina local e outra remota, ou seja, é responsável por controlar o diálogo entre duas máquinas. Nesse diálogo são trocadas informações para estabelecer uma conexão, controlar a troca de dados e, por último, finalizar a conexão. A negociação para transmissão de dados entre as duas máquinas envolve três modos diferentes de transmissão, isto é, antes de começar a transmitir, as duas máquinas devem negociar o modo de transmissão, que pode ser *simplex*, *half duplex* ou *full duplex*, em que:

<b><i>Simplex</i></b>	A transmissão ocorre apenas em um sentido. Analogamente, podemos exemplificar esse tipo de transmissão com a televisão e o rádio, pois o sentido de transmissão acontece somente em uma direção.
<b><i>Half duplex</i></b>	A transmissão ocorre nos dois sentidos, no entanto, não se dá simultaneamente. O modo de transmissão mais conhecido que usa esse tipo de técnica é o walkie-talkie. Nesse tipo de comunicação, apenas uma das partes deve se comunicar a cada vez.
<b><i>Full duplex</i></b>	A transmissão pode se dar nos dois sentidos, simultaneamente. Esse modo de transmissão é o mais usual, atualmente, em equipamentos de comunicação.

Para que duas máquinas possam se comunicar, esses modos de transmissão precisam ser negociados e isso é feito pelos protocolos definidos para essa camada.

A **camada de transporte** tem a função de garantir a transmissão fim a fim. Além disso, ela tem a função de receber os dados da camada de sessão, segmentar e identificar para enviá-los à camada de rede. A segmentação é necessária para que os dados sejam transportados por tecnologias usadas na camada de enlace.

Analogamente é como se tivéssemos um veículo de carga com baú pequeno. Nesse tipo de transporte, poderíamos colocar uma quantidade pequena de objetos para transportar, mas se tivéssemos um caminhão com baú grande, poderíamos colocar mais objetos. É dessa forma que os protocolos da camada de transporte segmentam os dados; se a tecnologia usada para transmitir os dados conseguir encapsular grandes volumes de dados, então serão segmentados no tamanho correto.

O controle de fluxo também é de responsabilidade dessa camada. Esse controle é necessário, pois há uma variedade muito grande de computadores, servidores e equipamentos, em geral, compondo a rede de computadores. Considerando esse aspecto, é fácil chegar à conclusão de que um servidor que tenha alta capacidade de processamento responderá de forma muito mais rápida a uma solicitação de um cliente.

Assim, certas informações poderão ser perdidas, pois o cliente não conseguirá processar na mesma velocidade do servidor. Para evitar que os dados sejam perdidos e tenha que haver solicitação de retransmissão, o que acarretaria maior fluxo de informações na rede e, portanto, pior desempenho, o controle de fluxo é necessário.

Esse mecanismo funciona da seguinte forma: uma vez solicitados dados ao servidor, o cliente informa a quantidade de memória – *buffer* – disponível; o servidor, de posse dessa informação, envia somente a quantidade de dados que o cliente possa receber; esse processo se repetirá enquanto houver dados a serem transmitidos. A cada solicitação enviada pelo cliente, este precisa informar a quantidade de *buffer* disponível naquele momento, dessa feita, a cada solicitação, um tamanho de janela poderá ser informado. Esse tipo de técnica chamamos de janela deslizante.

A camada de transporte mantém um mecanismo que torna a entrega das informações confiáveis. Esse mecanismo é necessário devido à segmentação dos pacotes. Cada um destes pode pegar caminhos diversos para chegar ao mesmo destino e alguns podem se perder por vários motivos. Quando isso ocorre, é solicitada a retransmissão desses pacotes que, por certo motivo, não chegaram.

Na camada de transporte também é definido o conceito de portas, ou seja, para cada aplicação usada, existe uma porta associada a ela. Isso garante que uma determinada informação tenha o destino correto; por exemplo, a porta 80 é usada nas aplicações que acessam páginas web; a porta 110 é usada no protocolo POP; a 25, no SMTP para envio e recebimento de e-mails. Assim, se uma máquina estiver fornecendo serviços diferentes, não haverá problemas, pois uma aplicação será diferenciada da outra pelo número da porta.

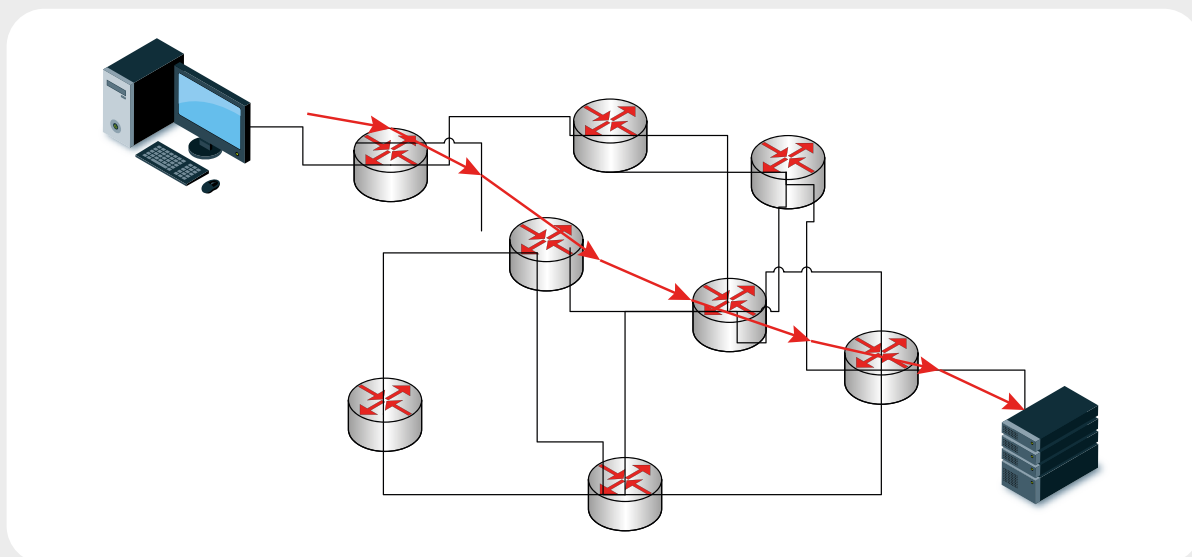
A **camada de rede** tem como principal função encaminhar os pacotes pela rede, ou seja, é nessa camada que os pacotes são abertos pelos roteadores para decidir se serão encaminhados para a rede LAN ou, então, se serão novamente

empacotados para serem retransmitidos pela rede. Essa decisão é tomada tendo como base o endereço lógico, ou endereço IP, contido em um protocolo usado para comunicação de dados.

Toda vez que uma máquina quer acessar uma página web em um servidor, deve conhecer o endereço IP do servidor para que possa alcançá-lo. Esse endereço é inserido em um protocolo que é enviado pela rede. Em cada roteador pelo qual esse protocolo passa, tal endereço é analisado a fim de definir qual o melhor caminho deve ser seguido para chegar ao destino. A Figura 2 exibe, pela seta vermelha, o melhor caminho possível para se chegar ao destino – lembrando que este apontado pela seta vermelha não será necessariamente o percurso seguido por todos os pacotes, pois caso a via apresentada tenha algum ponto de congestionamento, outro poderá ser estabelecido a fim de que os pacotes cheguem ao destino.

Na montagem do protocolo que leva o endereço IP de destino, é inserido também o endereço de origem, pois o servidor apenas saberá para quem deve responder se o endereço de origem for enviado.

Por exemplo, na comunicação demonstrada na Figura 2, o computador cliente enviará uma solicitação para acessar uma página no servidor. Ao descobrir o endereço IP do servidor, ele o inserirá no protocolo e enviará também o seu endereço, ou seja, o endereço IP da máquina cliente. Ao chegar esse pacote para o servidor, este abrirá o pacote, analisará o serviço desejado e o que foi requisitado, montará um pacote com as informações requisitadas e incluirá, nesse pacote, o endereço da máquina cliente.



**Figura 2** – Caminho de um pacote pela rede

**Fonte:** Adaptado de Getty Images

**#ParaTodosVerem:** a imagem mostra um diagrama com formas cilíndricas cinzas dispostas aleatoriamente e conectadas por linhas pretas e vermelhas. Estão conectados nas extremidades um computador de mesa, na extremidade superior esquerda, e um servidor, na extremidade inferior direita. Fim da descrição.



A **camada de enlace** de dados tem como principal função fornecer tecnologias para que os pacotes sejam encapsulados e enviados pela rede. Muitas tecnologias são definidas nessa camada e as informações são transmitidas no formato de quadros. Para cada tecnologia, um tamanho de quadro é definido.

A camada de enlace é responsável, ainda, pelo controle de erros. Usa-se técnicas para verificar se houve erro durante a transmissão. Muitas vezes, as informações transmitidas podem estar corretas, porém, no caminho, algumas alterações podem ocorrer e interferir nos dados que são transmitidos.

O controle de erros consegue detectar se o quadro enviado está com as informações corretas ou não. Isso pode ser feito usando a técnica de paridade, paridade combinada, *check sum* ou, então, a melhor das opções, denominada Verificação de Redundância Cíclica (CRC). Nessa camada são definidos os endereços físicos – endereços MAC – que são usados por equipamentos para direcionar os quadros nas redes LAN para o seu destino.

Os equipamentos que usam o endereço MAC para direcionar os quadros em redes LAN são os *switches* e as *bridges*, os quais são capazes de direcionar um quadro para uma porta específica, de acordo com a tabela montada em sua memória. Nessa tabela há informações para qual lugar um quadro deve seguir. Tal camada é usada, frequentemente, nas redes LAN, pois algumas tecnologias, como ethernet, ATM, X25, ADSL, fazem também, na camada de enlace, o controle de fluxo e o enquadramento dos dados para formar o quadro.

Por último, a **camada física** define as características elétricas dos sinais e mecânicas das interfaces, conectores e outros componentes usados em redes de computadores. Nela, os quadros são enviados bit a bit para o outro lado.

Como se pode perceber, há uma série de mudanças feitas no sinal, desde a camada de aplicação até a camada física e, como foi descrito, cada camada tem uma função e protocolos específicos para auxiliar na transmissão e recepção das informações. Caso uma empresa, instituição ou qualquer organização queira desenvolver uma arquitetura para transmissão de dados e torná-la compatível aos equipamentos usados atualmente, deve seguir o que está definido no modelo de referência OSI. O protocolo TCP/IP se baseia no modelo de referência OSI. Na verdade, como foi descrito, o protocolo TCP/IP já fora definido quando a ISO padronizou o modelo de referência. Para se tornar compatível com o padrão OSI, o TCP/IP foi organizado nas seguintes camadas.



**Figura 3** – Arquitetura TCP/IP

**Fonte:** Acervo do Conteudista

**#ParaTodosVerem:** a figura mostra um quadro retangular dividido em linhas, em cada uma delas, de cima para baixo, há os termos “Aplicação”, “Transporte”, “Redes”, “Enlace”, “Física”. Fim da descrição.

O protocolo TCP/IP foi dividido em cinco camadas. As camadas de aplicação, apresentação e sessão ficaram sob a responsabilidade da camada de aplicação, ou seja, as outras camadas têm as mesmas funções descritas no modelo de referência OSI e são compostas por protocolos específicos para cumprir cada definição.



### Importante

Muitas bibliografias adotam que a suíte TCP/ IP está dividida em quatro camadas, pois consideram as camadas de enlace e física como uma só.

Uma comparação entre os modelos OSI e TCP/IP com os protocolos mais comuns usados em cada camada é apresentada no Quadro 1. Os protocolos mais comuns da camada de aplicação são apresentados no meio do Quadro com a denominação “protocolos incluídos”. Tais protocolos estão divididos em duas partes: uma começando pelo protocolo SNMP e a outra iniciando pelo protocolo FTP.

Isso ocorre porque, na camada de transporte, há dois protocolos principais: TCP e UDP. Os protocolos da camada de aplicação inseridos acima do protocolo TCP, usam-no para enviar as informações. Os protocolos da camada de aplicação inseridos acima do protocolo UDP, usam-no na transmissão de informações. Os protocolos TCP e UDP diferem na forma como são usados para transmitir as informações: enquanto o TCP garante a entrega fim a fim das informações, o protocolo UDP não usa os mesmos mecanismos de garantia de entrega fim a fim.

Portanto, o UDP não é considerado um protocolo confiável para a entrega de informações. Isso não significa que ele não possa ser usado, mesmo porque as aplicações que requerem velocidade na transmissão usam esse tipo de protocolo para tal fim, pois por não ter que se preocupar em saber se a mensagem chegou ou não ao remetente, requer menos campo no cabeçalho, tornando-se, assim, um protocolo mais leve para a transmissão de dados em relação ao TCP.

Ambos os protocolos, TCP e UDP, são encapsulados no protocolo IP da camada de rede, sendo assim, todas as informações advindas da camada de aplicação chegam à camada de rede e são encapsuladas no protocolo IP, o qual reserva campos importantíssimos, sendo que dois, os endereços IP de origem e de destino, são enviados no cabeçalho desse protocolo.

Na camada de enlace são inseridas as tecnologias para inseri-los em quadros para transmissão. Se considerarmos um computador, então, nessa camada, é inserido o *driver* da placa de rede, isto é, nela ainda há componentes de software controlando o fluxo de informações.

**Quadro 1** – Comparação entre modelo OSI e CP/IPTCP/IP

Camadas OSI	Protocolos incluídos		Camadas TCP/IP
Aplicação	SNMP TFTP NFS DND BOOTP	FTP Telnet Finger SMTP POP	Aplicação
Apresentação			
Sessão			
Transporte	UDP	TCP	Transporte de Máquina para Máquina
Rede	IP		Internet
Dados	Cartões de Interface de Rede		Interface de Rede
Física			

**Fonte:** Gallo; Hancock, 2003

Por último, na camada física, é inserido o *hardware* para que seja possível a transmissão de dados. Portanto, o cabo de par trançado, o cabo coaxial, a fibra óptica, a rede *wireless*, a placa de rede e as interfaces fazem parte dessa camada.

A camada de rede em conjunto com o protocolo IP nos fornece um destaque que deve ser estudado com mais detalhes. Tal item se refere ao endereço IPv4 – lê-se, IP versão 4 –; é por esse endereço que as máquinas conseguem se comunicar nas redes LAN, MAN e WAN e precisamos compreender como é constituído e quais são as variações possíveis para identificar todas as máquinas na rede.



## Saiba Mais

Afinal, por que TCP/IP?

Existem inúmeras razões pelas quais o TCP/IP foi escolhido para ser o protocolo da internet, entre as quais:

- Foi aceito como um protocolo-padrão da indústria;
- É fornecido em quase todos os sistemas operacionais de rede e, portanto, permite conectividade entre sistemas diferentes – por exemplo, de um computador *Unix* para um computador *Windows*;
- Os protocolos estão sob domínio público e livremente disponíveis, tornando-o uma escolha popular para as empresas de *software*. Não há restrições quanto ao seu uso e não há *royalties* a pagar;
- É um protocolo bem concebido;
- É um padrão aberto, no qual nenhum fornecedor único tem qualquer controle sobre o protocolo e qualquer pessoa tem permissão para usá-lo e desenvolver aplicativos baseados nele.

## Endereço IPv4

A primeira padronização do endereçamento IP, disponibilizada em setembro de 1981, especificava que qualquer interface interconectada à internet precisaria ser identificada usando os 32 bits disponíveis para endereço IP. Tal especificação descreve que a primeira parte do endereço IP identifica uma rede a qual o *host* pertence, ao passo que a segunda parte identifica um *host* em particular dentro da rede estipulada na primeira parte. Dito de outra forma:

Número da rede    Número do *Host*

Ou

Prefixo da rede    Número do *host*

O endereço IP é composto de 32 bits separados em quatro grupos de oito bits, cada. Conforme pode ser visto a seguir, seu formato é representado sempre do mesmo modo:

xxx.xxx.xxx.xxx

O valor de x para cada grupo pode variar de 0 a 255. A princípio, entenderemos as regras gerais para compor um endereço IP. Depois que elas forem compreendidas, passaremos a citar outras, a fim de que um endereço seja aceito pelos equipamentos configurados em redes de computadores. Seguindo o exposto anteriormente, hipoteticamente, podemos ter endereços que começam com:

0.0.0.0

Até:

255.255.255.255

Temos um total de 32 bits – oito bits vezes quatro grupos – para representar um endereço IP. Assim, temos 256 combinações diferentes para cada grupo que varia de 0 até 255.

Para que uma máquina possa se comunicar com outra máquina em uma rede LAN, ambas devem estar dentro da mesma rede não apenas fisicamente interligadas, mas também logicamente definidas pelo endereço IP. Dessa forma, um endereço IP é composto por um endereço de rede e um endereço de máquina dentro dessa rede.

Por esse motivo é que alguns endereços definidos em uma rede de computadores, interligados fisicamente por um cabo, não permitem que duas máquinas se comuniquem. Para que um endereço IP seja dividido em endereços de rede e de máquina, foram definidos pontos de corte no formato do endereço. O primeiro ponto de corte foi estabelecido da seguinte maneira:



xxx. xxx.xxx.xxx

**Figura 4** – Ponto de corte para identificar endereço de rede e endereço de máquina

**Fonte:** Acervo do Conteudista

**#ParaTodosVerem:** a imagem mostra uma sequência xxx.xxx.xxx.xxx, a primeira sequência é contornada por um retângulo vermelho. Fim da descrição.

O primeiro ponto de corte foi definido no primeiro grupo de oito bits. A Figura 4 mostra o primeiro grupo com um retângulo verde. Essa marcação em verde representa o endereço de rede e os outros três grupos podem representar um endereço de máquina dentro da rede. Por exemplo, o endereço apresentado na Figura 5 está dividido em endereço de rede e endereço de máquina:



101.100.100.150

**Figura 5 – Endereço de rede**

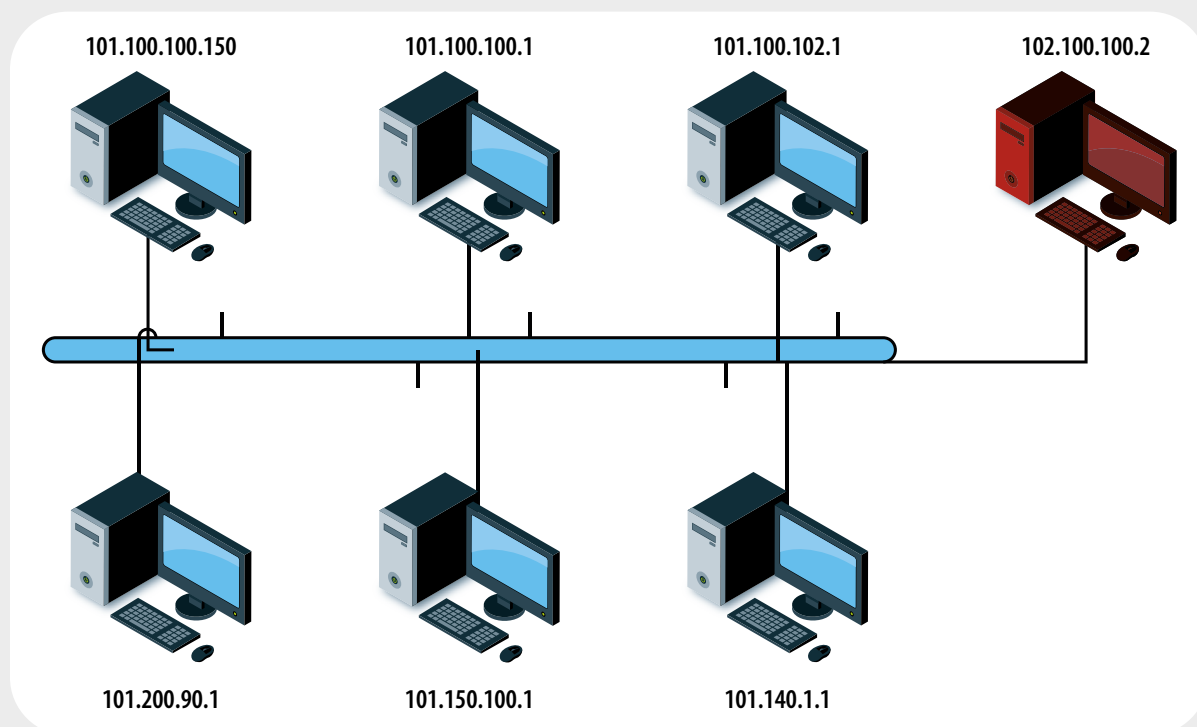
**Fonte:** Acervo do Conteudista

**#ParaTodosVerem:** a imagem mostra uma sequência 101.100.100.150, a primeira sequência é contornada por um retângulo vermelho. Fim da descrição.

O endereço de rede está representado pela parte em verde (101) e o endereço de máquina corresponde aos outros três grupos (100.100.150). Assim, todos os endereços que começam com o valor 101 pertencerão a essa rede e dentro desta deverá ser dado um endereço de máquina diverso para cada máquina.

Caso, dentro de uma rede fisicamente interligada, usássemos um endereço 102.100.100.149 para identificar uma máquina na rede do exemplo da Figura 5, as máquinas não se comunicariam, pois, embora interligadas fisicamente, o endereço de rede 101 é diferente do endereço de rede 102.

No exemplo de endereço de rede e de máquina da Figura 5, podemos ter máquinas com os endereços exibidos na Figura a seguir:



**Figura 6** – Exemplo de rede

**Fonte:** Adaptado de Getty Images

**#ParaTodosVerem:** a imagem mostra um diagrama formado por uma linha azul que se conecta a três computadores de mesa azul na parte de cima, e três na parte de baixo, com seus respectivos endereços de rede. Há um computador vermelho na extremidade direita. Fim da descrição.

Na Figura 6 estão representados sete computadores interligados fisicamente em uma mesma rede; seis desses computadores estão na mesma rede lógica, identificados pelo endereço 101; os outros três grupos representam o endereço da máquina dentro da rede. Observe que cada máquina tem um endereço variado. Caso apareça, nessa rede, um endereço igual ao de outra máquina, esta não conseguirá se comunicar. Uma das máquinas, a que está em vermelho, não conseguirá se comunicar com as outras porque, embora esteja fisicamente interligada, não faz parte da mesma rede lógica – pois está usando o endereço de rede 102.

Como o primeiro grupo de oito bits representa o endereço de rede, então podemos ter 256 endereços de redes disponíveis, pois  $2^8 = 256$  (o número dois, na fórmula, representa a quantidade de símbolos possíveis no sistema de numeração binária e o número oito representa a quantidade de bits do primeiro grupo). Os outros três grupos de oito bits representarão os endereços de máquinas dentro de uma determinada rede, portanto, podemos representar  $2^{24} = 16.777.216$  endereços de máquinas para cada uma das 256 redes disponíveis.



Considerando o exposto anteriormente, com o ponto de corte no primeiro grupo para representar a rede, poderíamos ter um endereço de rede 1.0.0.0 até 1.255.255.255, com todas as combinações possíveis entre o intervalo apresentado. Outra rede poderia ser implementada com os endereços 2.0.0.0 até 2.255.255.255, com todas as combinações possíveis entre o intervalo apresentado.

É importante salientar que algumas regras descritas até aqui são para fins didáticos, isto é, algumas delas foram estabelecidas para que o primeiro e o último endereço não fossem usados, pois já são reservados para usos específicos. O segundo ponto de corte, definido para representar a rede, foi determinado conforme apresentado na Figura 7:



XXX.XXX.XXX.XXX

**Figura 7** – Exemplo de endereço de rede e endereço de máquina

**Fonte:** Acervo do Conteudista

**#ParaTodosVerem:** a imagem mostra uma sequência XXX.XXX.XXX.XXX, as duas primeiras sequências são contornadas por um retângulo vermelho. Fim da descrição.

Nessa característica de ponto de corte, dois grupos de oito bits são considerados para representar um endereço de rede e dois grupos de oito bits são levados em conta para representar um endereço de máquina. Aumentando o ponto de corte, ampliamos também a quantidade de endereços de redes e diminuímos a quantidade de máquinas para cada rede. Um exemplo de rede pode ser visto na Figura a seguir:



101.100.100.150

**Figura 8** – Exemplo de endereço

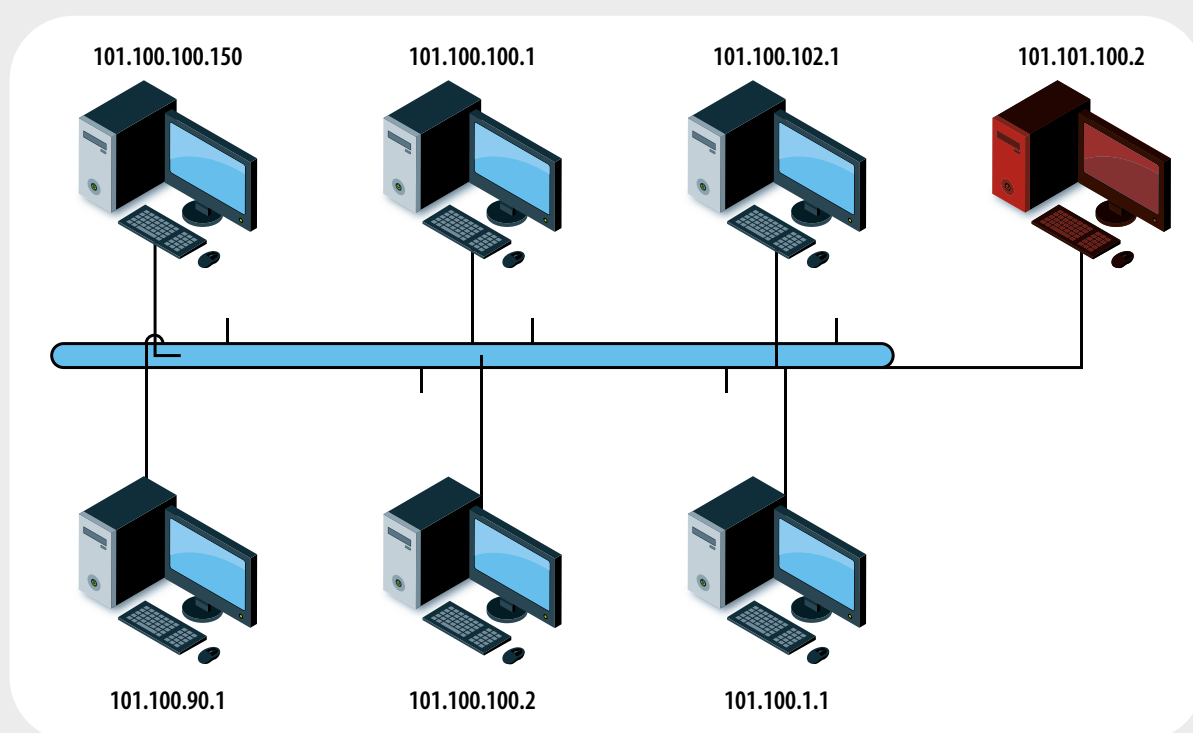
**Fonte:** Acervo do Conteudista

**#ParaTodosVerem:** a imagem mostra uma sequência 101.100.100.150, as primeiras duas sequências são contornadas por um retângulo vermelho. Fim da descrição.

Agora, o endereço de rede é representado pelos dois primeiros grupos de oito bits (101.100) e os outros dois grupos de oito bits poderão identificar as máquinas (100.150) dentro da rede. Caso um computador seja configurado com o endereço diferente de 101.100, será então considerado fora da rede lógica e não conseguirá se comunicar com as máquinas que estão com o endereço de rede 101.100.

Na Figura 9, seis máquinas usam o endereço de rede 100.100, portanto, todas as seis vão conseguir se comunicar. Uma das máquinas, a que está com a cor vermelha, não se comunicará com as outras seis, pois seu endereço de rede (101.101) não é semelhante aos outros endereços de rede.

As características que podemos citar para este ponto de corte a fim de representar o endereço de rede e o endereço da máquina são as seguintes: o endereço de rede, agora, é composto por dois conjuntos de oito bits. Desse modo, para representar o endereço de rede, temos 16 bits disponíveis, isto é,  $2^{16} = 65.536$  (o número dois, na fórmula, representa a quantidade de símbolos possíveis no sistema de numeração binária e o número dezesseis representa a soma da quantidade de bits do primeiro e segundo grupo).



**Figura 9** – Exemplo de endereçamento de rede

**Fonte:** Adaptado de Getty Images

**#ParaTodosVerem:** a imagem mostra um diagrama formado por uma linha azul que se conecta a três computadores de mesa azul na parte de cima, e três na parte de baixo, com seus respectivos endereços de rede. Há um computador vermelho na extremidade direita. Fim da descrição.

Note que a quantidade de redes disponíveis aumentou significativamente, passando de 256 redes, possíveis quando o ponto de corte estava somente no primeiro grupo de oito bits, para 65.536 redes possíveis com o ponto de corte nos dois primeiros grupos de oito bits.

A quantidade de máquinas possíveis em cada rede baixou significativamente: de 16.777.216 para 65.536, pois sobraram os dois grupos de oito bits do lado direito para identificar as máquinas, ou seja,  $2^{16} = 65.536$ . Dessa maneira, considerando a rede apresentada na Figura 8, podemos identificar máquinas que começam em 101.100.0.0 até 101.100.255.255. Outra rede poderia começar com 100.200.0.0 e ir até 100.200.255.255. Por questões didáticas, vamos considerar essa forma, no entanto, algumas regras complementam o exposto anteriormente a fim de garantir certas padronizações para uso específico.

Outro ponto de corte possível para diferenciar endereço de rede e endereço de máquina é feito no terceiro conjunto de oito bits.



XXX.XXX.XXX.XXX

**Figura 10** – Exemplo de endereçamento de rede e endereçamento de máquina

**Fonte:** Acervo do Conteudista

**#ParaTodosVerem:** a imagem mostra uma sequência XXX.XXX.XXX.XXX, as três primeiras sequências são contornadas por um retângulo vermelho. Fim da descrição.

Nesse tipo de endereçamento, os três conjuntos representados pela cor verde são destinados a endereços de rede e o último conjunto de oito bits é usado para identificar as máquinas nessa rede. Nesse formato, dezesseis bits, referentes aos primeiros três grupos de oito bits, são usados para rede, portanto, temos  $2^{16} = 16.777.216$  endereços de redes possíveis e  $2^8 = 256$  endereços possíveis para identificar as máquinas. A Figura 11 apresenta um endereço possível para essa rede:



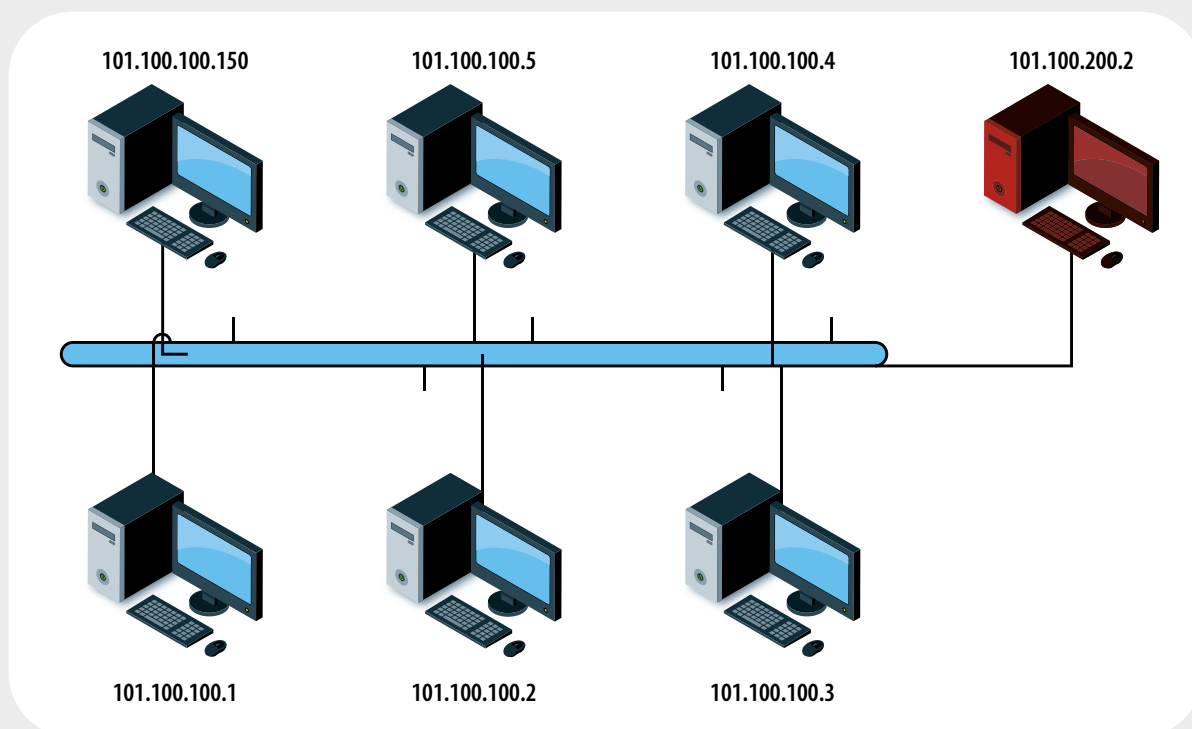
101.100.100.150

**Figura 11** – Exemplo de endereço

**Fonte:** Acervo do Conteudista

**#ParaTodosVerem:** a imagem mostra uma sequência 101.100.100.150, as primeiras três sequências são contornadas por um retângulo vermelho. Fim da descrição.

No exemplo da Figura 11, o endereço 101.100.100 é o que identifica a rede e o número 150, a máquina dentro dessa rede. Com esse tipo de ponto de corte, podemos ter, em cada rede, apenas 256 endereços IP, pois somente os oito bits do último conjunto de bits poderão ser usados para identificar as máquinas. Qualquer endereço de rede diferente do 101.100.100 pertenceria a outra rede e, assim, não se comunicaria com a rede apresentada na Figura 11. A Figura, a seguir, exhibe um exemplo de rede com características semelhantes ao explanado:



**Figura 12** – Exemplo de endereço de rede

**Fonte:** Adaptado de Getty Images

**#ParaTodosVerem:** a imagem mostra um diagrama formado por uma linha azul que se conecta a três computadores de mesa azul na parte de cima, e três na parte de baixo, com seus respectivos endereços de rede. Há um computador vermelho na extremidade direita. Fim da descrição.

Nessa rede há seis máquinas que têm o mesmo endereço e uma sétima, a qual está na cor vermelha, embora esteja interligada fisicamente, não se comunicará com as outras pelo motivo de estar com endereço de rede diferente das demais. Com essas características, essa rede pode ter endereços que variam de 101.100.100.0 até 101.100.100.255.

Os três pontos de corte demonstrados anteriormente são os mais usados para endereçar uma rede e uma máquina dentro de uma rede, entretanto, há outras duas formas disponíveis que não são usuais. Uma das quais é usada para transmitir pacotes em *multicast*, ou seja, transmitir pacotes para um conjunto de máquinas com endereços específicos. Esse tipo de endereçamento foi criado para possibilitar que apenas um conjunto de pessoas habilitadas pudesse receber dados pela internet.

É o caso da transmissão televisiva ou, então, de filmes sob demanda, em que uma quantidade limitada de usuários assinaria esse tipo de serviço e receberia o sinal pela internet. O outro formato foi deixado para uso futuro, isto é, para alguma aplicação na qual, no momento da definição do padrão de endereçamento, não fora pensado.

Para definir os pontos de corte no endereçamento, foi estipulado um método que chamamos de máscara, a qual, por sua vez, também é composta por quatro conjuntos de oito bits, cada, portanto, é semelhante ao formato do endereço IP. Cada conjunto de oito bits da máscara é associado a cada conjunto de oito bits do endereço IP.

XXX.XXX.XXX.XXX

Os valores para cada conjunto, separados por ponto, vão de 0 até 255. Neste primeiro momento, vamos considerar que os valores assumidos por cada conjunto de oito bits separados por pontos podem ser somente os valores 0 ou 255. Assim, nenhum outro valor poderá ser definido para uma máscara. Os pontos de corte que representam os endereços de rede serão representados pelo valor 255 e os endereços de máquinas serão associados ao zero.

Na representação anterior, a máscara 255.0.0.0 define o ponto de corte para ilustrar o que é rede e o que é reservado para o endereço de máquina. O valor 255 define que o primeiro conjunto de oito bits do endereço IP será reservado para identificar a rede e os outros três conjuntos de oito bits serão usados para apontar as máquinas dentro de uma rede específica. O valor zero, na máscara, é associado ao endereço da máquina.

Endereço IP: 101.100.100.150  
Máscara 255. 0. 0. 0

**Figura 13** – Exemplo de máscara de rede

**Fonte:** Acervo do Conteudista

**#ParaTodosVerem:** a imagem mostra os valores: “Endereço IP: 101.100.100.150”, a primeira sequência é contornada por um retângulo vermelho; abaixo, “Máscara: 255.0.0.0”. Fim da descrição.

Seguindo o raciocínio anterior, o outro ponto de corte ficaria da seguinte forma, usando máscara:

Endereço IP: 101.100.100.150  
Máscara 255.255. 0. 0

**Figura 14** – Exemplo de máscara

**Fonte:** Acervo do Conteudista

**#ParaTodosVerem:** a imagem mostra os valores: “Endereço IP: 101.100.100.150”, as duas primeiras sequências são contornadas por um retângulo vermelho; abaixo, “Máscara: 255.255.0.0”. Fim da descrição.

Os valores 255 estão associados ao endereço de rede e os valores zero, aos endereços de máquina. Por último, o ponto de corte ficaria da seguinte forma:

Endereço IP: 101.100.100.150  
Máscara 255.255. 0. 0

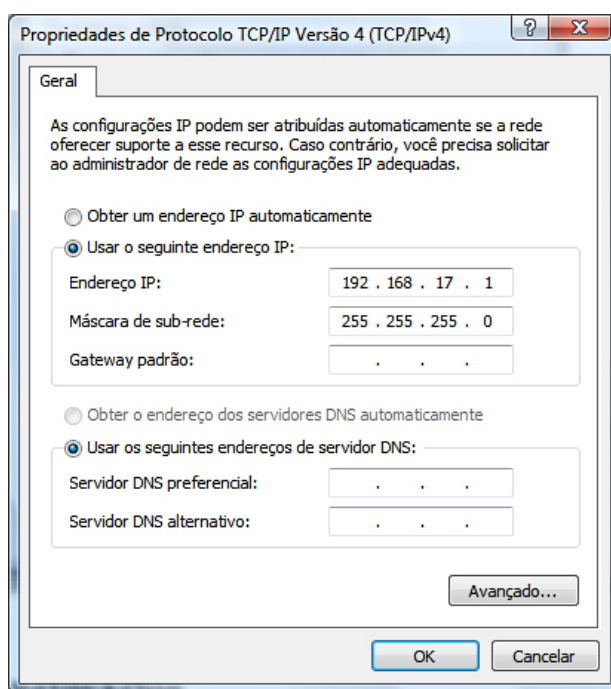
**Figura 15** – Exemplo de máscara de rede

**Fonte:** Acervo do Conteudista

**#ParaTodosVerem:** a imagem mostra os valores: “Endereço IP: 101.100.100.150”, as três primeiras sequências são contornadas por um retângulo vermelho; abaixo, “Máscara: 255.255.255.0”. Fim da descrição.

A máscara define que os três primeiros conjuntos de oito bits serão usados para identificar a rede, pois a máscara tem o valor 255 definido nos três primeiros conjuntos de oito bits.

A Figura, a seguir, mostra um endereço configurado em um computador com sistema operacional *Windows*. Note que, na configuração, é solicitado um endereço IP e a máscara para definir, no endereço, o que é endereço de rede e o que é endereço de máquina. O endereço apresentado na Figura 16 define 192.168.17.1 e a máscara, 255.255.255.0, desse modo, o endereço 192.168.17 identifica a rede, pois a máscara é 255.255.255.0 e o número 1 identifica essa máquina dentro da rede.



**Figura 16** – Exemplo de configuração de endereço de rede

**Fonte:** Acervo do Conteudista

**#ParaTodosVerem:** a imagem mostra um *print* de uma caixa de diálogo do sistema *Windows*. A caixa apresenta opções para configuração de IP. Fim da descrição.

As máscaras são classificadas em classes: classe A, classe B e classe C, de modo que cada uma delas define a quantidade de redes e de máquinas que são possíveis de inserir dentro dessa rede.

## Classes de Endereços Primários



### Importante

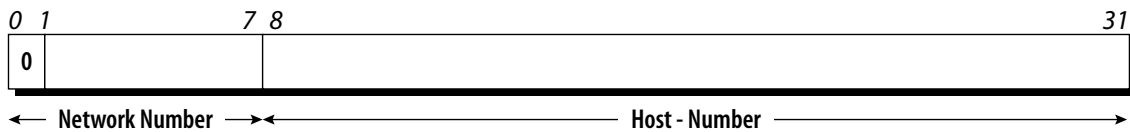
A classe da rede indica a quantidade de redes e hosts possíveis. Definimos a classe por meio da máscara de rede.

Para fornecer certa flexibilidade referente ao tamanho da rede e quantidade de *hosts* inseridos nestas, foi decidido que o espaço de endereço IP deveria ser dividido em três classes de endereços: Classe A, Classe B e Classe C. Essas características são chamadas de classe cheia – *classfull*. Cada classe tem uma quantidade fixa de bits para identificar a rede.

Uma das principais características do endereço IP classe cheia é que há um ponto bem definido o qual identifica o que é reservado para rede e o que é reservado para *hosts*. Por exemplo, se os dois primeiros bits do primeiro conjunto de oito bits forem um e zero (1-0), conforme apresentado na Figura e identificado como classe B, o ponto usado para definir rede e *host* estará entre o 15º e 16º bit. A especificação de endereçamento IP classifica as máscaras pelos primeiros bits do primeiro conjunto de oito bits. A seguir, veremos isso mais detalhadamente para identificar os *hosts*:

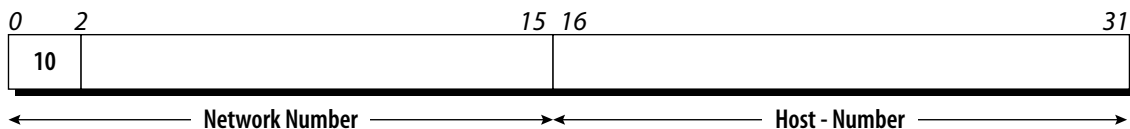
### Class A

bit#



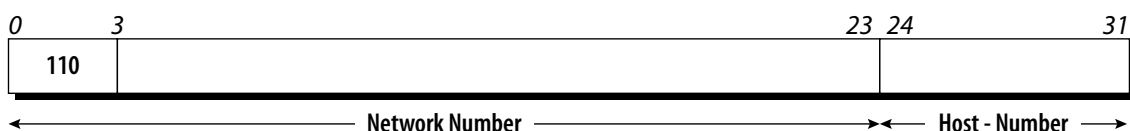
### Class B

bit#



### Class C

bit#



**Figura 17** – Classes de endereços

**Fonte:** Acervo do Conteudista

**#ParaTodosVerem:** a imagem mostra um diagrama que consiste em várias seções com texto rotulado que fornece instruções e informações. No canto superior esquerdo, há uma seção denominada “Classe A” que representa uma determinada classe ou categoria. Abaixo desse rótulo, o texto menciona “bit” e “0 1”, indicando a faixa de valores dentro desta classe. Movendo-se para o lado direito da imagem, há uma seção denominada “7 8” e “31”, representando valores específicos dentro da categoria Classe A. Além disso, o texto “0” é mencionado separadamente, possivelmente indicando um valor dentro deste intervalo. Abaixo da seção Classe A, há outra seção rotulada, “+ Número de rede. há uma seção denominada “Host - Número”, que fornece informações sobre os números de host associados aos números de rede mencionados na seção anterior. No lado inferior direito, há uma seção denominada “Classe C”, indicando outra classe. O texto menciona “bit” e “0”, bem como “3” e “23 24”. Semelhante à seção Classe B, há uma seção “Número de Rede” abaixo da seção Classe C, fornecendo mais informações sobre os números de rede associados à Classe C. Fim da descrição.

## Rede Classe A – Prefixo/8

Cada endereço de rede classe A tem um prefixo de rede com 8 bits, e o bit mais significativo é configurado fixamente com o valor 0. Os outros sete bits do primeiro octeto são usados para identificar a rede. Os 24 bits restantes são utilizados para identificar os *hosts*. Observe, na Figura 17, que o primeiro bit é fixo em zero, portanto, não é usado para identificar a rede, consequentemente, não empregaremos os oito bits, mas teremos disponíveis sete bits para manipular.



Podemos definir, no máximo, 126 redes ( $2^7 - 2$ ). Nesse cálculo são subtraídas duas redes: uma 0.0.0.0, que é usada como rota padrão; e a 127 /8 ou 127.0.0.0, que é usada para *loopback*.

Cada rede com o prefixo /8 suporta 16.777,214 ( $2^{24} - 2$ ) *hosts*. O cálculo subtrai dois endereços: um é o endereço tudo 0, que é usado para identificar a rede; e o outro é o endereço tudo 1, usado para broadcast. Assim, esses dois endereços não podem identificar os *hosts* na rede.

## Rede Classe B – Prefixo/16

Cada endereço de rede classe **B** tem um prefixo de rede com 16 bits, sendo que os dois bits mais significativos são configurados fixamente em 1-0. Observe, na Figura 17, que os dois primeiros bits são fixos em 10 e, dessa maneira, não são usados para identificar a rede.

Os outros 14 bits dos dois octetos mais significativos são usados para determinar as redes. Os outros 16 bits são utilizados para identificar os *hosts* dentro de cada rede. As redes classe **B** são referenciadas como /16, pois têm 16 bits usados como prefixo de redes. Podemos definir, no máximo, 16.384 ( $2^{14}$ ) redes com até 65.534 ( $2^{16} - 2$ ) *hosts* por rede.

## Rede Classe C – Prefixo/24

Cada endereço de rede classe **C** tem um prefixo de rede com 24 bits, sendo que os três bits mais significativos são configurados fixamente em 1-1-0. Os outros 21 bits dos três octetos mais significativos são empregados para determinar as redes. Os outros 8 bits são usados para apontar os *hosts* dentro de cada rede. As redes classe **C** são referenciadas como /24, pois têm 24 bits utilizados como prefixo de redes. Podemos definir, no máximo, 2.097,152 ( $2^{21}$ ) redes com até 254 ( $2^8 - 2$ ) *hosts* por rede.

## Outras Classes

Acrescentando a essas classes, temos, ainda, a classe **D**, em que os quatro bits mais significativos são configurados fixamente em 1-1-1-0 – esses endereços são usados para multicast – e a classe **E**, com os cinco bits mais significativos fixados em 1-1-1-1-0, que foi reservada para uso futuro.

O Quadro mais à frente mostra a faixa dos valores que podem assumir cada uma das principais classes já apresentadas. As letras **xxx** representam o campo do endereço dos hosts, o qual é definido pelo administrador da rede.

A faixa de endereço é fixa devido aos bits mais significativos serem fixos, portanto, acabam restringindo cada classe em uma faixa específica. Por exemplo, na classe **A**, o endereço de rede pode começar em 1 e variar até 126, pois o bit mais significativo é fixo em zero. Dessa forma, sobram sete bits para fazer as combinações de rede, ou seja,  $2^7 - 2 = 126$  redes possíveis, portanto, de 1 até 126. As outras classes seguem o mesmo raciocínio, no entanto, com quantidade de bits fixos diferente para cada uma.

**Quadro 2 – Classes**

Endereço da classe	Faixa na representação decimal
A (prefixo /8)	1.xxx.xxx.xxx até 126.xxx.xxx.xxx
B (prefixo /16)	128.0.xxx.xxx até 191.255.xxx.xxx
C (prefixo /24)	192.0.0.xxx até 223.255.255.xxx

**Fonte:** Acervo do Conteudista

A especificação original do IPv4 foi desenvolvida sem considerar que a quantidade de usuários da internet pudesse aumentar de forma espantosa como se vê atualmente.

O endereço IP é inserido em dois dos campos do protocolo IP: um dos quais é o endereço de origem e o outro é o endereço de destino.

# Atividades de Fixação

---

**1 – Qual é a função principal de um endereço de Internet Protocol (IP) em uma rede de computadores? Assinale a alternativa correta.**

- a. Identificar o modelo do computador.
- b. Determinar a localização física do computador.
- c. Roteamento de dados e identificação única de dispositivos em uma rede.
- d. Proteger o computador contra ataques cibernéticos.
- e. Controlar a velocidade da conexão de internet.

**2 – O que o TCP/IP representa em redes de computadores? Assinale a alternativa correta.**

- a. Um tipo de cabo de rede utilizado para conexões de alta velocidade.
- b. Um protocolo de segurança para proteger dados em redes sem fio.
- c. Um modelo de protocolo de rede e um conjunto de protocolos amplamente usados na comunicação de dados em redes.
- d. Um sistema operacional exclusivo para servidores de rede.
- e. Um tipo de *firewall* usado para proteger redes contra ataques cibernéticos.

Atenção, estudante! Veja o gabarito desta atividade de fixação no fim deste conteúdo.

# Material Complementar

---



## Livro

### **Estendendo os Endereços IP – Endereçamento IP e Sub-redes**

PAQUET, D.; TEARE, C. Estendendo os endereços IP – endereçamento IP e sub-redes. *In*: PAQUET, D.; TEARE, C. **Construindo redes cisco escaláveis**. São Paulo: Pearson, 2002. p. 60.



## Vídeo

### **Cálculo de Sub-Redes**

<https://youtu.be/7tUEHsQR9ak>

# Referências

---

GALLO, M. A.; HANCOCK, W. M. **Comunicação entre computadores e tecnologias de rede**. São Paulo: Thomson Learning, 2003.

KUROSE, J. F. **Redes de computadores e a internet**: uma nova abordagem. São Paulo: Addison-Wesley, 2004.

P. JUNIOR, C. A. C. V.; BRABO, G. S.; AMORAS, R. A. S. **Segurança em redes wireless padrão IEEE 800.11<sup>a</sup>**: protocolos WEP, WAP e análise de desenvolvimento. [20--]. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Universidade da Amazônia, Manaus, AM, [20--].

STALLINGS, W. **Redes e sistemas de comunicação de dados**: teoria e aplicações corporativas. 5. ed. Rio de Janeiro: Elsevier, 2005

TANENBAUM, A. S. **Redes de computadores**. 4. ed. São Paulo: Campus, 2003.

# Gabarito

---

## Questão 1

**c) Roteamento de dados e identificação única de dispositivos em uma rede.**

**Justificativa:** o endereço de IP desempenha um papel crucial em uma rede de computadores, permitindo o roteamento eficiente de dados e identificando exclusivamente dispositivos em uma rede. Ele não está relacionado ao modelo do computador, à localização física ou à velocidade da conexão de internet. Embora a segurança da rede possa envolver o uso de endereços de IP, sua função principal é o roteamento e a identificação de dispositivos na rede.

## Questão 2

**c) Um modelo de protocolo de rede e um conjunto de protocolos amplamente usados na comunicação de dados em redes.**

**Justificativa:** o Protocolo de Controle de Transmissão/Protocolo de Internet (TCP/IP) é um modelo de protocolo de rede e um conjunto de protocolos que são amplamente usados na comunicação de dados em redes de computadores, incluindo a Internet. Ele não se refere a um cabo de rede específico, a um protocolo de segurança sem fio, a um sistema operacional exclusivo ou a um tipo de *firewall*.