

The background features a collection of 3D blocks in various colors (purple, blue, yellow, green, orange, pink, grey) arranged in a scattered, overlapping manner. Some blocks are solid, while others are hollow. Thin, curved lines in blue, red, and green weave through the blocks, adding a sense of movement and connectivity.

# Conceitos básicos 10 de TCP/IP

- ✓ Camadas do protocolo TCP/IP;
- ✓ Análise do endereço IP.

## 10.1. Introdução

Entendemos por protocolo TCP/IP (Transmission Control Protocol/Internet Protocol) um agregado formado por uma série de protocolos utilizados para a comunicação em redes de grandes proporções.

O TCP/IP é dividido em quatro camadas, dentro das quais estão localizados os diferentes protocolos que o compõem. Tal método tende a maximizar a agilidade no que diz respeito à comunicação. Esses protocolos possuem responsabilidades distintas, e as transações na rede somente poderão ser efetuadas com sucesso quando todos cumprirem seu papel de modo satisfatório.

## 10.2.Camadas do protocolo TCP/IP

Como já dissemos, o TCP/IP é composto por quatro camadas, nas quais estão dispostos todos os outros protocolos. Vejamos a tabela a seguir:

Camada	Exemplos de protocolo
Aplicação	HTTP FTP
Transporte	TCP UDP
Internet	IP ARP ICMP IGMP
Interface de Rede	ATM Ethernet Token Ring Frame Relay

Nos subtópicos a seguir, conferiremos uma descrição das camadas TCP/IP e dos seus principais protocolos.

## 10.2.1. Camada de aplicação

Esta camada, que está no nível mais alto, é responsável por alocar utilitários e aplicativos que, por meio dela, comunicam-se com a rede.

Há dois protocolos importantes na camada de aplicação:

- **HTTP**

Por meio do Hyper Text Transfer Protocol, ou protocolo de transferência de hipertexto, é que obtemos acesso aos sites da Internet.

- **FTP**

Por meio deste protocolo, File Transfer Protocol, ou protocolo de transferência de arquivo, como o próprio nome sugere, podemos proceder com a transferência de arquivos por meio da Internet.

## 10.2.2. Camada de transporte

Esta camada possui três funções distintas: a primeira delas é definir, por meio de um identificador, os dados sendo transmitidos; a segunda é agir como intermediária entre as camadas da Internet e de aplicação, no que se refere ao envio de dados; a terceira e última é proceder com o gerenciamento das transmissões de dados, assegurando-se de que elas ocorram de maneira satisfatória. Há dois protocolos na camada de transporte que merecem destaque:

- **TCP**

A função deste protocolo é solicitar que o recebimento dos dados seja confirmado, uma vez que eles tiverem alcançado o seu destino. É um protocolo confiável e orientado à conexão, a qual é estabelecida por dois computadores utilizando o processo handshake de três vias, que envolve as seguintes etapas:

1. Inicialização e transmissão de dados pelo computador de origem;
2. Resposta com informações de conexão pelo computador de destino;
3. Confirmação e aceitação do recebimento pelo computador de origem.

- **UDP**

Este protocolo agiliza o processo de envio dos dados por meio da entrega de pacotes sem conexão. Apesar de ser rápido, não é confiável, pois não existe a confirmação dos pacotes recebidos e nem a retransmissão de dados perdidos. Por isso, este protocolo é utilizado para a transmissão de dados em que a perda de alguns pacotes não será um problema.

### 10.2.3. Camada da Internet

Quando se tornar necessário proceder com o envio de dados por meio de uma rede, eles precisam ser roteados, endereçados e empacotados. Tais ações são realizadas na camada da Internet, cujos protocolos mais importantes serão detalhados a seguir:

- **IP**

Se for necessário o envio de pacotes de dados por meio de uma rede, é preciso proceder com o endereçamento desses dados. Em seguida, é necessário proceder com o roteamento deles. Nesse caso, temos de recorrer ao protocolo denominado Internet Protocol, mais conhecido como IP.

O IP é um protocolo sem conexão e não confiável que, para ser efetivamente utilizado com o intuito de direcionar os pacotes de dados ao seu destino, precisa que todos os pacotes enviados contenham, em seu interior, tanto o endereço IP do computador remetente quanto o do destinatário. Enquanto um pacote de dados estiver sendo enviado pela rede, podemos nos deparar com duas situações distintas: na primeira, remetente e destinatário encontram-se em segmentos de rede distintos. Desse modo, o envio do pacote de dados é realizado com o auxílio de um roteador. A segunda situação é oposta à primeira, ou seja, o remetente e o destinatário encontram-se em um único segmento de rede. Sendo assim, o envio do pacote de dados é realizado de forma mais direta.

Outra responsabilidade do IP é determinar o tempo de vida (TTL) dos pacotes, para que estes não trafeguem na rede indefinidamente.

- **ARP**

Antes que um pacote de dados possa ser enviado por meio de uma rede, é preciso que o protocolo ARP faça um mapeamento dos endereços IP (endereços lógicos) alocados nesse pacote para endereços MAC (endereços físicos). Esse procedimento recebe o nome de resolução de endereços.

Para que o mapeamento citado possa ser realizado, existe uma tabela alocada em uma área de memória, denominada cache ARP, que contém os endereços MAC correspondentes aos endereços IP das máquinas existentes em um mesmo segmento de rede.

Por meio desse mapeamento é que os adaptadores de rede farão a identificação do destino de um pacote, processando as seguintes etapas:

1. No computador de origem, o cache do ARP é verificado;
2. Caso não seja encontrado o endereço MAC no cache, uma solicitação do **ARP** é enviada pelo segmento por meio de uma transmissão por difusão, a fim de encontrar o computador de destino;
3. Identificado o computador de destino, a entrada do **ARP** é adicionada a ele, contendo o seu endereço;
4. O computador de destino envia uma solicitação do **ARP**;
5. A entrada do **ARP** é adicionada ao computador de origem;
6. Feita a verificação, o pacote **IP** é enviado.

- **ICMP (Internet Control Message Protocol)**

A função deste protocolo é enviar mensagens ao computador remetente caso ocorra alguma falha no momento em que um pacote de dados estiver sendo enviado através de uma rede. Por meio de tais mensagens, podemos analisar os erros ocorridos, bem como utilizar as informações retornadas para solucionar eventuais problemas.

- **IGMP (Internet Group Management Protocol)**

Antes de falarmos sobre o protocolo IGMP, é interessante discorrermos sobre o conceito de difusão seletiva IP. Quando é necessário que uma mensagem qualquer seja enviada a mais de um destinatário simultaneamente, utilizamos a difusão seletiva IP. Esses usuários formam um conjunto ou grupo para o qual um pacote de dados é enviado utilizando-se um endereço IP de difusão seletiva.

Os destinatários de diferentes grupos como esse, conhecidos como grupos de difusão seletiva, são alocados em listas. A função do protocolo IGMP é administrar essas listas.

### 10.2.4. Camada de interface de rede

Por meio desta camada, podemos obter acesso físico ao ambiente de rede. Dois protocolos presentes nesta camada são o ATM (modo de transferência assíncrona) e o Ethernet. O adaptador de rede é um exemplo de componente de hardware encontrado na camada de rede.

## 10.3. Analisando o endereço IP

Podemos definir como endereço IP um número de identificação responsável por assegurar a individualidade de identificação de um micro na rede. Esse tipo de endereço deve ser composto por quatro números, entre 0 e 255, dispostos da seguinte maneira: xxx.xxx.xxx.xxx.

Os endereços IP são organizados em classes com o intuito de determinar o local de um host de destino em relação ao computador de origem. Um host remete a qualquer dispositivo em uma rede TCP/IP (como micros, impressoras e roteadores) que utilize o endereçamento IP como meio de transmissão e recepção de informações.

É possível atribuir endereços IP a todos os computadores conectados à rede por meio da sua divisão em sub-redes.

É preciso destacar que alguns endereços IP possuem funções especiais e, por isso, não podem ser utilizados como endereços de host. São eles:

- **Endereço com todos os bits destinados à identificação da máquina iguais a 0:** Representa o endereço da rede. Por exemplo: 192.168.1.0;
- **Endereço com todos os bits destinados à identificação da máquina iguais a 1:** Representa o endereço de broadcast. Por exemplo: 192.168.1.255;
- **Endereços da rede 127.0.0.0:** Usados como alias que faz referência à própria máquina. O endereço 127.0.0.1, associado ao nome do host local, é normalmente utilizado.

### 10.3.1. Classes de endereço

As identificações de rede são atribuídas com a utilização das classes de endereço. Esse processo é feito com o objetivo de permitir que computadores conectados nas diferentes redes de uma empresa possam estabelecer uma comunicação com a Internet.



Uma classe de endereço é determinada de acordo com a estrutura de um endereço IP. Este, como já vimos, possui quatro segmentos numéricos cujos valores variam entre 0 e 255. O valor do byte do endereço IP irá definir a sua classe, conforme o intervalo de valores ao qual se enquadra. Vejamos a tabela a seguir:

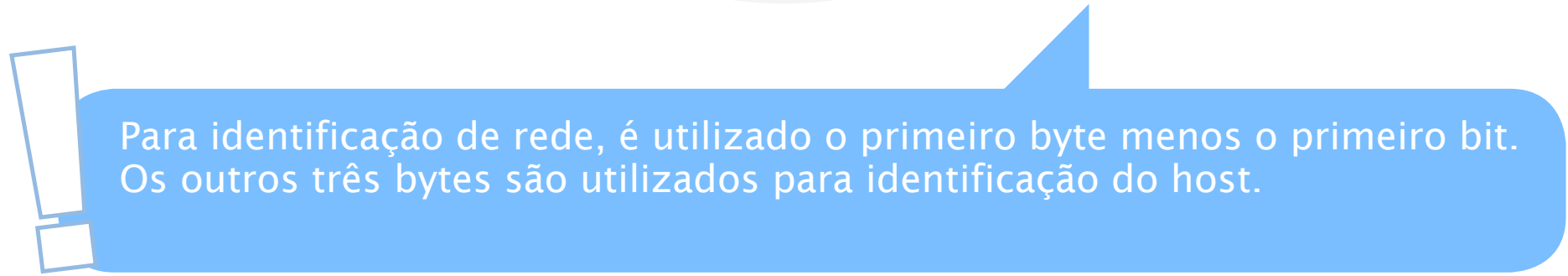
Intervalo	Classe
1 - 126	A
128 - 191	B
192 - 223	C
224 - 239	D
240 - 255	E

Estão descritas, nos subtópicos adiante, as diferentes classes de identificação de rede com as suas respectivas características.

Para calcular a quantidade de redes possível em uma classe e a quantidade de hosts possível em cada rede, aplicamos a fórmula  $2^n - 2$ , em que  $n$  equivale à quantidade de bits que podem ser alterados.

- **Classe A**

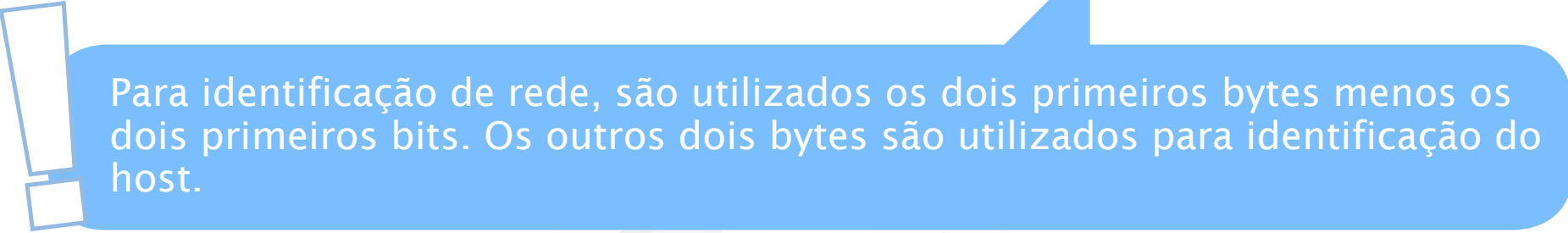
- Em redes que possuem uma grande quantidade de hosts, são atribuídos endereços de Classe A;
- Possibilita a existência de 126 redes;
- Cada rede pode possuir 16.777.214 hosts.



Para identificação de rede, é utilizado o primeiro byte menos o primeiro bit. Os outros três bytes são utilizados para identificação do host.

- **Classe B**

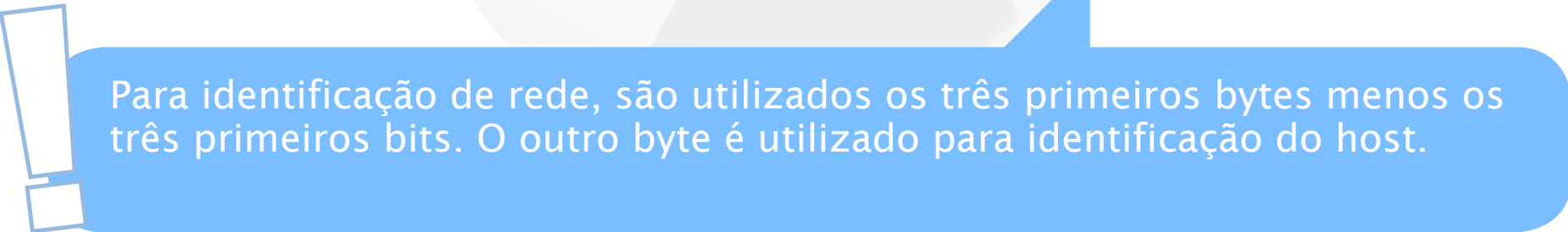
- Em redes médias e pequenas, são atribuídos endereços de Classe B;
- Possibilita a existência de 16.382 redes;
- Cada rede pode possuir 65.534 hosts.



Para identificação de rede, são utilizados os dois primeiros bytes menos os dois primeiros bits. Os outros dois bytes são utilizados para identificação do host.

- **Classe C**

- Em pequenas LANs, são atribuídos endereços de Classe C;
- Possibilita a existência de, aproximadamente, 2.097.150 redes;
- Cada rede pode possuir 254 hosts.



Para identificação de rede, são utilizados os três primeiros bytes menos os três primeiros bits. O outro byte é utilizado para identificação do host.

- **Classes D e E**

- Ambas as classes não se destinam a hosts;
- A classe D tem os seus endereços utilizados para multicast;
- A classe E tem os seus endereços reservados para uma futura utilização.



## 10.3.2.Sub-redes

É possível evitar o aumento da colisão de dados e a redução do desempenho de uma rede baseada na tecnologia Ethernet, em caso de alto número de computadores e grande volume de tráfego. Basta que os computadores dessa rede sejam agrupados em segmentos separados por um dispositivo físico, como um roteador ou uma ponte.

Os segmentos de uma rede TCP/IP são conhecidos como sub-redes e encontram-se separados por roteadores. Em uma sub-rede, todos os endereços IP dos computadores são portadores da mesma identificação de rede. Por outro lado, para que as sub-redes se comuniquem, cada uma deve possuir uma identificação de rede distinta. A identificação de rede permite, então, que as sub-redes especifiquem as divisões lógicas de uma rede.

### 10.3.2.1. Máscaras de sub-rede

Vimos que uma rede única pode ser segmentada em sub-redes, cada qual com uma identificação de rede diferente, ou seja, com uma identificação de sub-rede. Essa divisão de uma única identificação de rede em identificações de rede menores é realizada via máscara de sub-rede.

Definimos como máscara de sub-rede um recurso que distingue, em um endereço IP, a identificação de rede de uma identificação de host. Essa máscara é representada por um conjunto de quatro números, organizados segundo valores máximos contíguos seguidos por valores mínimos contíguos. Nesse sentido, cada um dos quatro números pode considerar um valor máximo de 255 ou mínimo de 0. Os valores máximos remeterão à identificação de rede, enquanto os mínimos, à identificação de host.

Podemos definir dois tipos de máscaras de sub-rede: o padrão e o personalizado. O primeiro tipo é comum às classes de endereços IP. Sua configuração se dá da seguinte maneira:

Classe de endereço IP	Endereço IP	Máscara de sub-rede	Identificação de rede	Identificação de host
A	w.x.y.z	255.0.0.0	w.0.0.0	x.y.z
B	w.x.y.z	255.255.0.0	w.x.0.0	y.z
C	w.x.y.z	255.255.255.0	w.x.y.0	z

Já o segundo tipo, personalizado, é utilizado no caso de precisarmos dividir as redes em sub-redes sem adicionar equipamentos adicionais.

Há três passos que devem ser seguidos para a definição de uma sub-rede:

1. Uma vez determinado o número de segmentos físicos necessários na rede local, é necessário converter esse valor para binário;
2. Conta-se, então, o número de bits necessários para representar o valor binário do número de segmentos físicos. Por exemplo: precisamos de quatro sub-redes. O valor binário de 4 é 100. Assim, para representar o valor 4 no sistema binário, são usados 3 bits;
3. Por fim, converte-se o número necessário de bits para decimal, no sentido da esquerda para a direita.

Por exemplo: em uma rede classe C, se forem necessários 5 bits, é preciso configurar os primeiros 5 bits (à esquerda) do Host ID como 1, passando a fazer parte do Network ID. O valor binário será, então, 1111 1000, o qual, no sistema decimal, equivale a 248. Nesse caso, a máscara de sub-rede será 255.255.225.248.

A seguir, temos as tabelas de conversões possíveis de máscaras de sub-rede para as classes A, B e C:

- **Classe A**

Número de sub-redes	Bits necessários	Máscara de sub-rede	Computadores por sub-rede
2	2	255.192.0.0	4.194.302
6	3	255.224.0.0	2.097.150
14	4	255.240.0.0	1.048.574
30	5	255.248.0.0	524.286
62	6	255.252.0.0	262.142
126	7	255.254.0.0	131.070
254	8	255.255.0.0	65.534

• Classe B

Número de sub-redes	Bits necessários	Máscara de sub-rede	Computadores por sub-rede
2	2	255.255.192.0	16.382
6	3	255.255.224.0	8.190
14	4	255.255.240.0	4.094
30	5	255.255.248.0	2.046
62	6	255.255.252.0	1.022
126	7	255.255.254.0	510
254	8	255.255.255.0	256

• Classe C

Número de sub-redes	Bits necessários	Máscara de sub-rede	Computadores por sub-rede
2	2	255.255.255.192	62
6	3	255.255.255.224	30
14	4	255.255.255.240	14
30	5	255.255.255.248	6
62	6	255.255.255.252	2

10.3.3.Atribuindo identificação de rede e de host

Um endereço IP é dividido em dois segmentos distintos: identificação de rede e identificação de host.

Um micro qualquer que faça parte de uma rede encontra-se alocado em um segmento de rede. Definir em que segmento esse micro está localizado é de responsabilidade da identificação de rede, sendo que esta é comum a todos os micros do segmento.

Além da identificação de rede, todos os micros ou outros componentes presentes em uma rede possuem uma identificação de host diferente. Jamais dois hosts em uma rede possuirão identificação de host igual.

### 10.3.4.Determinando host local ou remoto

Um host local é aquele cuja identificação de rede é similar à de outro host, ou seja, que se encontra na mesma sub-rede que o micro (host) com o qual está trocando informações. Um host remoto é aquele cuja identificação de rede difere da de outro host, ou seja, que se encontra em uma sub-rede diferente da do micro (host) com o qual está trocando informações.

