# 1. Características da camada de rede

A camada de rede do modelo OSI, assim como a camada de Internet do modelo TCP/IP, fornece serviços para permitir que dispositivos finais (ETDs) troquem dados a partir de redes diferentes.Os principais serviços prestados por essa camada a fim de possibilitar a comunicação fim a fim entre dois Hosts incluem:

## 1.1. **Endereçamento lógico de dispositivos finais**

Os dispositivos finais, que aqui chamaremos hosts, devem ser configurados com um endereço exclusivo na rede, isto é deve ser possível saber a que rede esse dispositivo pertence e identificá-lo dentro da própria rede. Este endereço deve ser independente do endereço físico da interface de rede. A figura 1 apresenta o endereçamento IP, independente da camada física.

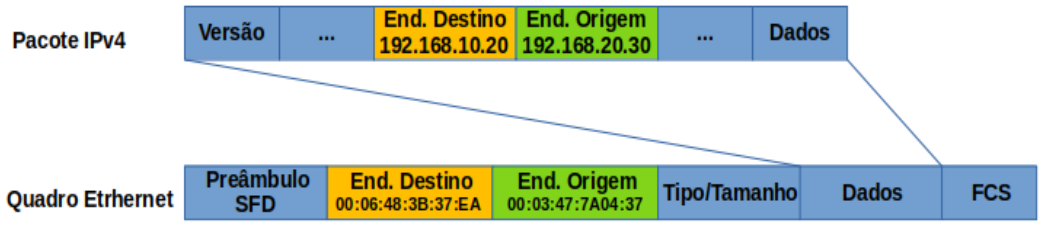



Fig. 1 - Endereçamento lógico da camada 3 Fonte: o autor

O pacote IP recebe um endereço de destino e de origem independente do endereço MAC dos dispositivos, este pacote é tratado pelos dispositivos de Camada 3, ou seja, roteadores e switches de Camada 3 à medida que viaja pela rede até seu destino.

**Destaque**: Os endereços IP de origem e destino permanecem os mesmos desde o momento em que o pacote sai do host de origem até chegar ao host de destino, exceto quando traduzidos pelo dispositivo que executa a Tradução de Endereços de Rede - NAT.

## 1.2. Encapsulamento

A camada de rede do transmissor encapsula a unidade de dados (PDU) da camada de transporte (segmentos) em um pacote adicionando informações de cabeçalho, como os

endereços dos hosts origem (emissor) e destino (receptor). A figura 2 mostra o encapsulamento de um segmento da camada de transporte um um pacote do protocolo IPv4.

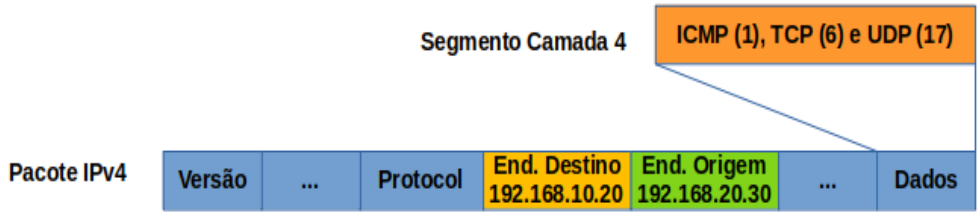



Fig. 2 Encapsulamento da PDU da camada de transporte Fonte: o autor

O protocolo IP encapsula o segmento da camada de transporte (camada imediatamente acima da camada de rede), adicionando um cabeçalho IP. O cabeçalho IP é usado para entregar o pacote ao host de destino.

### 1.3. Desencapsulamento

Quando o pacote chega ao destino, a camada de rede do host receptor verifica o cabeçalho do pacote, remove o pacote, e a PDU resultante da Camada 4 é transferida para o protocolo apropriado na camada de transporte.

### 1.4. **Comutação de pacotes**

Para ser encaminhada a mensagem é dividida em pacotes menores, cada pacote possui informações de endereço de origem e destino, assim cada um pode ser encaminhado individualmente através da rede. Cada nó toma a decisão de qual rota deverá ser usada para encaminhar cada pacote para o próximo nó da rede, conforme apresentado na figura 3

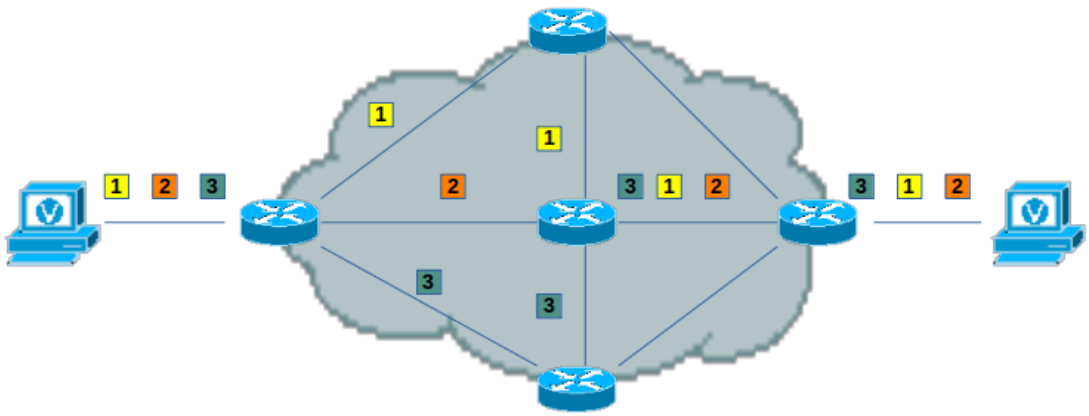



Fig. 3 Comutação de pacotes Fonte: o autor

Esta técnica possibilita melhor aproveitamento do meio físico, uma vez que não há necessidade do estabelecimento de um canal exclusivo entre a origem e o destino, e aumento da disponibilidade pois é possível contornar problemas de congestionamento ou falhas de link, encaminhando os pacotes por rotas alternativas. Porém os pacotes podem chegar fora de ordem, necessitando ser reordenados, função essa sob responsabilidade dos protocolos da camada de transporte.

### 1.4. Roteamento

A camada de rede fornece serviços para direcionar os pacotes para um host de destino em outra rede. Para trafegar para outras redes, o pacote deve ser processado por um roteador. A função do roteador é escolher o melhor caminho e encaminhar os pacotes para o host de destino em um processo conhecido como roteamento. O roteamento é feito a partir de tabelas que podem ser construídas de forma estática ou dinâmica, todo dispositivo que opera utilizando o protocolo TCP/IP possui uma tabela de rotas. Os roteadores, porém, utilizam protocolos de roteamento que constroem essas tabelas.

#### 1.4.1. Protocolos de descoberta de rota

As tabelas podem ser montadas de forma estática, isto é, manualmente pelo administrador ou de forma automática através dos protocolos de roteamento que operam segundo um determinado algoritmo de descoberta de rotas.

- **Algoritmo do Vetor da Distância -** Roteadores que operam segundo este algoritmo, anunciam-se aos outros roteadores da rede, enviando periodicamente mensagens de broadcast divulgando sua tabela de rotas, esta informação será utilizada por outros roteadores para atualizar suas próprias tabelas de rotas.

Quando uma alteração ocorre na rede, por exemplo, uma nova rede é adicionada, esta informação é passada de roteador a roteador. Dependendo do tamanho da rede e do número de rotas existentes o tempo para que esta rota seja conhecida pode ser razoavelmente grande, chamamos a este fenômeno de convergência (neste caso baixa convergência). Por outro lado, como a informação é divulgada por meio de broadcast este algoritmo provoca grande overhead na rede. O principal protocolo que opera segundo este algoritmo é o protocolo RIP.

- **Algoritmo do Estado do Link -** O algoritmo de roteamento pelo estado do link, procura reduzir o tráfego de atualização de rotas na rede. Nesse algoritmo, quando um roteador é adicionado à rede ele solicita as informações de rota aos seus roteadores vizinhos. Uma vez que os roteadores tenham construído suas tabelas de rota, só enviarão mensagens de atualização se houver mudança nos links a ele associados. Os roteadores que operam sob este protocolo mantém além das informações de rotas, informações sobre o estado de cada link que possui com outros roteadores. Os principais protocolos que operam segundo este algoritmo são o protocolo OSPF, BGP, e o ISIS da ISO.

## 1.5. Protocolos da camada de rede (Internet) do Modelo TCP/IP

Os protocolos IP versão 4 (IPv4) e IP versão 6 (IPv6) são os principais protocolos de comunicação desta camada. Outros protocolos como o RIP (Routing Information Protocol), o OSPF (Open Shortest Path First) e o BGP (Border Gateway Protocol) para roteamento ICMP (Internet Control Message Protocol) para troca de mensagens também são muito importantes. A figura 4 mostra os principais protocolos da camada de rede do modelo TCP/IP.

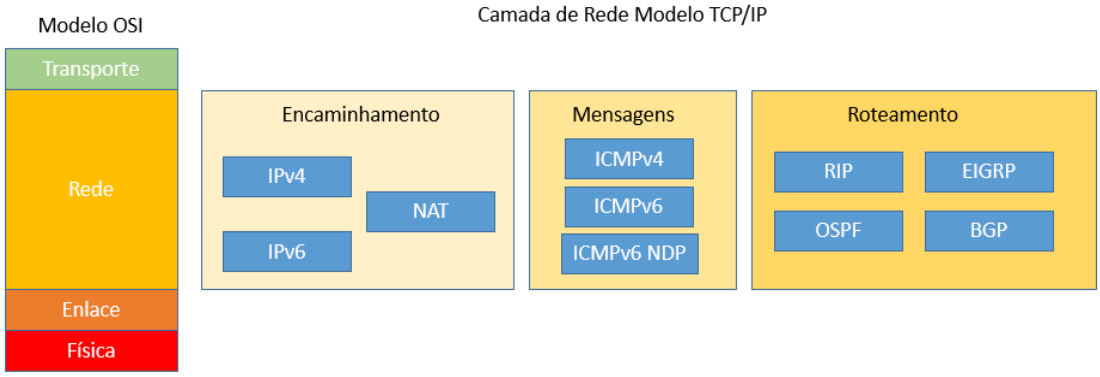



Fig. 4 - Protocolos da camada de rede do modelo TCP/IP Fonte: o autor

### Encaminhamento de pacotes - Protocolo IP (Internet Protocol)

- **IPv4 - Internet Protocol versão 4**. Recebe segmentos de mensagem da camada de transporte, empacota mensagens em pacotes e endereça pacotes para entrega de ponta a ponta através de uma rede. O IPv4 usa um endereço de 32 bits.
- **IPv6 - Internet Protocol versão 6**. Mesma função do IPv4, porém utiliza um endereço de 128 bits e traz melhorias ligadas a qualidade de serviço (QoS).
- **NAT - Network Address Translation**. Converte endereços IPv4 de uma rede privada em endereços IPv4 públicos.

**Protocolos de troca de mensagens de controle - ICMP (Internet Control Message Protocol)**

- **ICMPv4** -. Fornece feedback de um host de destino para um host de origem sobre erros na entrega de pacotes.
- **ICMPv6** - Funcionalidade semelhante ao ICMPv4, porém usado para pacotes IPv6.
- **ICMPv6 NDP - Neighbor Discovery Protocol** - Utilizado para resolução de endereços e detecção de endereço duplicado.

**Protocolos de roteamento**

- **RIP - Routing Information Protocol** - Protocolo de roteamento baseado no algoritmo do vetor da distância (Bellman-Ford)
- **OSPF - Open Short Path First.** Protocolo de roteamento pelo estado de link, definido, que utiliza uma estrutura de dados baseada em áreas
- **EIGRP -** Enhanced Interior Gateway Routing Protocol. Protocolo de roteamento de padrão aberto desenvolvido pela Cisco que usa uma métrica composta com base na largura de banda, atraso, carga e confiabilidade.
- **BGP - Border Gateway Protocol**. Protocolo de roteamento de padrão aberto usado entre os Internet Service Providers (ISPs) e entre estes e seus grandes clientes particulares.

O *Internet Protocol* versão 4 (IPv4) é talvez o protocolo mais importante do modelo TCP/IP, sua primeira versão foi usada na a ativação da ARPANET , em 1983, e ainda é responsável pela maior parte do tráfego da Internet, apesar do rápido crescimento do seu sucessor, o protocolo, o IPv6. O IPv4 é padronizado pelo IETF na RFC 791 (setembro de 1981), que substituiu a RFC 760, de janeiro de 1980).

Suas principais características são:

- Comutação de pacotes
- Não orientado a conexão (sem estado)
- Melhor esforço

## 2. IPv4

### 2.1. Pacote IPv4

O cabeçalho do pacote IPv4 permite que o transmissor e o receptor conversem entre si através das informações de cabeçalho organizado em campos, conforme apresentado na figura 1.

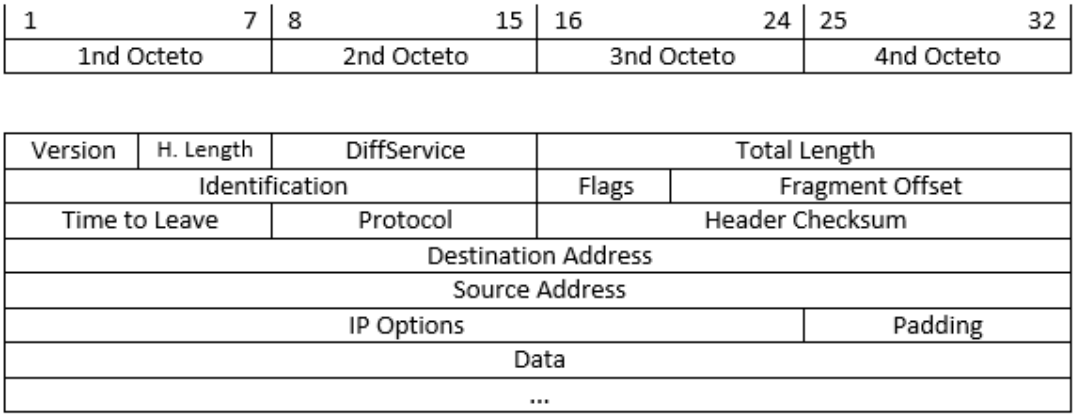



Fig. 1 - Cabeçalho do pacote IPv4 Fonte: o autor

Os principais campos do cabeçalho do pacote IPv4 são:

- **Version (4 bits)** – Identifica a versão do protocolo IP, a sequência 0100, identifica que este é um pacote IP versão 4.
- **H. Length (4 bits)** - Informa o tamanho do cabeçalho do protocolo IP.
- **DiffServ ou Serviços diferenciados ( 8 bits)** - inicialmente chamado ToS - Type of Service, define a prioridade de cada pacote. Os seis bits mais significativos do campo são o DSCP - Differentiated Services Code Point, conjunto de de valores *de QoS* (Qualidade de Serviço) que podem ser utilizados para priorizar o tráfego e os dois últimos são os bits de notificação de congestionamento explícito ECN - Explicit Congestion Notification.
- **Header Checksum (16 bits)** - Usado para detecção de erro no cabeçalho do pacote IPv4.
- **Time to Live - TTL (8 bits)** – Usado para determinar a vida útil de um pacote. O

dispositivo de origem do pacote IPv4 define o valor TTL inicial, que é decrementado cada vez que o pacote é processado por um roteador, se o valor campo TTL chegar a zero, o roteador descarta o pacote enviando uma mensagem ICMP de tempo excedido para o endereço IP de origem. Como o valor deste campo é alterado, o roteador também deve recalcular a soma de verificação do cabeçalho.

- **Protocol** - Este campo é usado para identificar o protocolo da camada de transporte (segmento ou datagrama) que está sendo transmitido no pacote IPI. Valores comuns são ICMP (1), TCP (6) e UDP (17).
- **Source Address (32 bits)** – Contém o endereço IP do remetente. O endereço de origem IPv4 é sempre um endereço unicast.
- **Destination Address** – Contém o endereço IP do destinatário. O endereço IPv4 destino pode ser um endereço unicast, multicast, ou broadcast.

## 2.2. Endereçamento IPv4

O endereço IPv4 é um número de 32 bits, ele identifica exclusivamente um host em uma inter-rede. Apesar de seu esgotamento e substituição pelo IPv6 o endereçamento IPv4 ainda é muito utilizado principalmente dentro das organizações, por isso é muito importante que você conheça suas características e como utilizá-lo para segmentar uma rede em sub-redes e como criar uma máscara de sub-rede de comprimento variável (VLSM) como parte de um esquema de endereçamento IPv4..

Um endereço IPv4, é um número binário de 32 bits representados na forma de 4 octetos mostrados em decimal separados por um ponto. A figura 2 apresenta um endereço IPv4 representado na sua notação decimal (usual) e na sua notação binária (real).

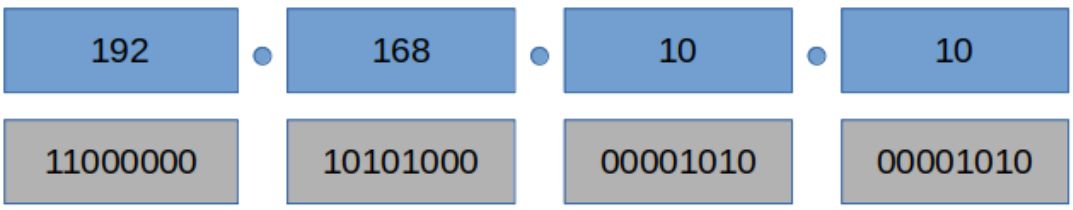



Fig. 2 Endereço IPv4 na representação decimal Fonte: o autor

Aqui o endereço 192.168.10.10 é a representação da notação decimal do binário 11000000101010000000101000001010.

Para representar o endereço IP **$11000000101010000000000000000001_2$** primeiro separamos o binário em quatro octetos como a seguir **11000000.10101000.00000000.00000001**, depois convertemos cada um dos octetos em decimal **$11000000_2 = 192_{10}$** ; **$10101000_2 = 168_{10}$**; **$00000000_2 = 0_{10}$**; **$00000001_2 = 1_{10}$** , agora é só escrever o endereço em sua notação decimal, isto é **192.168.0.1**. Para a partir da representação decimal do endereço IPv4 achar o binário correspondente, é só fazer de maneira inversa.

### 2.2.1. Máscara de subrede

Um endereço IPv4 além de identificar o host indica em qual rede o host se encontra. Isto é feito porque parte do endereço IP representa a rede e parte representa o host e quem determina isso é a máscara de subrede, em outras palavras ela é usada para diferenciar a parte da rede da parte do host de um endereço IPv4. Na figura 3 mostramos a configuração de um endereço IPv4 em um host Windows.

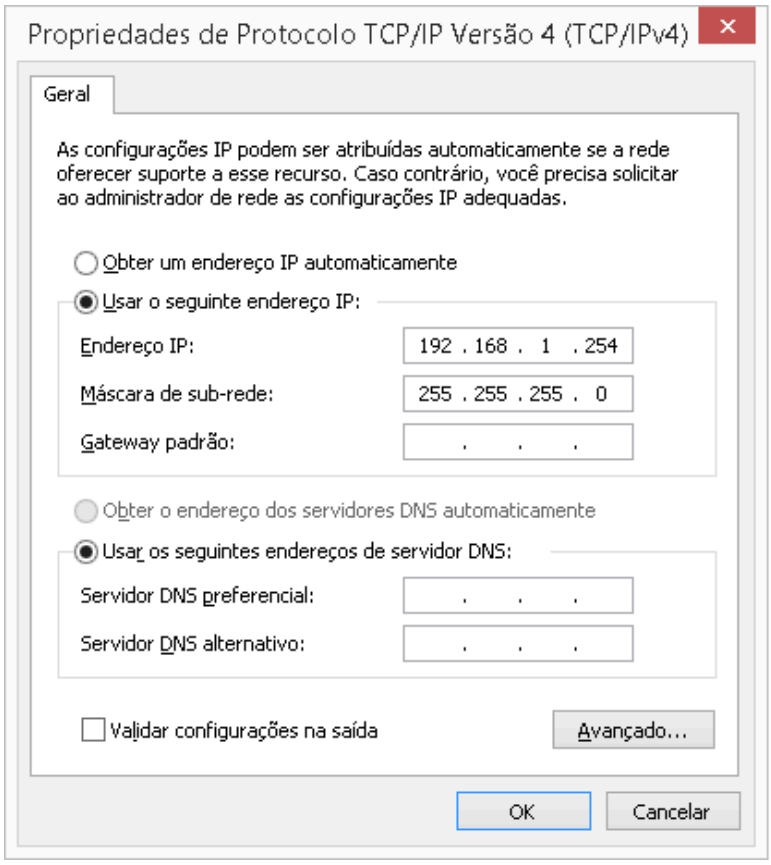


Fig. 3 Configuração de um endereço IPv4 em um host Windows Fonte: o autor

Assim, quando configuramos o endereço IPv4 do host também precisamos configurar a máscara de subrede para este endereço. A figura 4 apresenta uma máscara de

subrede.

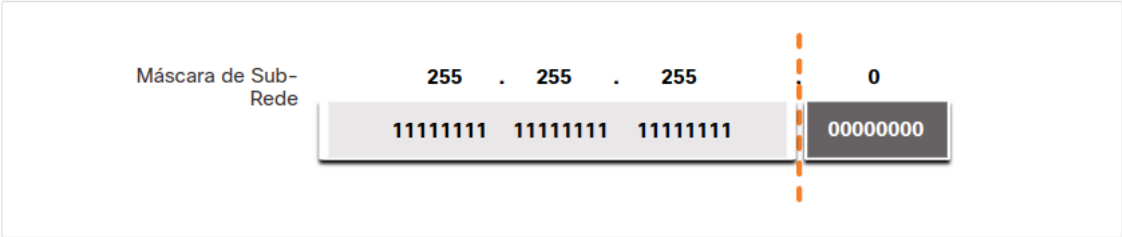



Fig.4 Máscara de subrede Fonte: o autor

Veja que a máscara de sub-rede 255.255.255.0 é uma sequência de 1 bits, seguida por uma sequência de 0 bits. A máscara de sub-rede não contém a parte da rede ou host de um endereço IPv4, apenas diz ao computador fazer isso

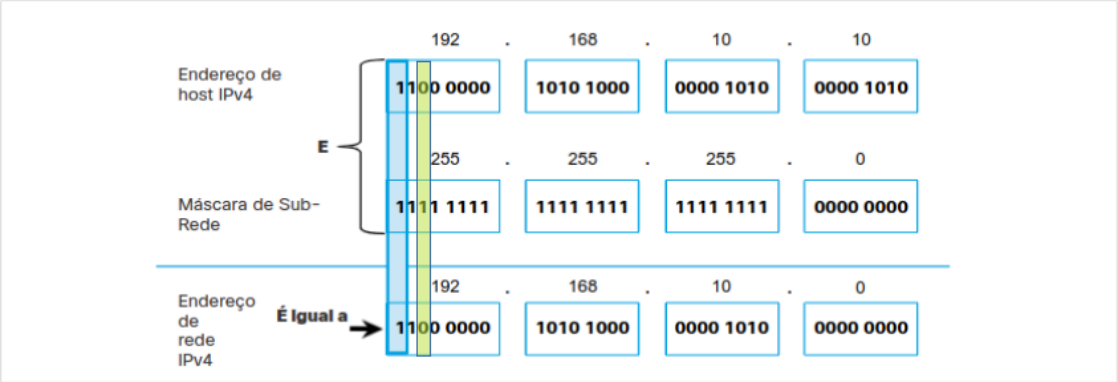



Fig. 5 Operação AND entre a máscara e o endereço IPv4 do hosts Fonte: o autor modificado de CCNA1 - Introduction to Network v7.02 item 11.1.4

Para identificar o endereço de rede de um host IPv4, é feito um AND lógico, bit a bit, entre o endereço IPv4 e a máscara de sub-rede, veja que a operação AND é executada no primeiro bit do endereço do host com o primeiro bit da máscara de sub-rede. Isso resulta em um bit 1 para o endereço de rede. 1 AND 1 = 1. Já no terceiro bit temos 0 AND 1 = 0, que resulta no endereço de rede IPv4 para este host. Neste exemplo, a operação AND entre o endereço de host 192.168.10.10 e a máscara de sub-rede 255.255.255.0 (/24) resulta no endereço de rede IPv4 192.168.10.0/24. Esta é uma operação IPv4 importante, pois informa a que rede um host pertence.

### 2.2.2. Endereço de rede

Um endereço de rede é um endereço que representa uma rede específica, é aquele

que tem todos os bits da porção host iguais a zero (0). Por exemplo para o endereço 192.168.10.11 com máscara 255.255.255.0, isto é, /24 seu endereço de rede será conforme apresentado na tabela 1.

| **Tabela 1 - Endereço de rede para o End. IP de Host 192.168.10.10** | | | | |
|---|---|---|---|---|
| | **1nd Octeto** | **2nd Octeto** | **3nd Octeto** | **4nd Octeto** |
| **End. IP do Host** | 192 | 168 | 10 | 11 |
| | 11000000 | 10100000 | 00001010 | 00001011 |
| **Máscara sub-rede** | 255 | 255 | 255 | 0 |
| | 11111111 | 11111111 | 11111111 | 00000000 |
| **End. Rede (AND Lógico entre o End. IP e a Máscara)** | **Todos os bits de host em "0"** | | | |
| | 192 | 168 | 10 | 0 |
| | 11000000 | 10100000 | 00001010 | 00000000 |

Conforme mostrado na tabela, o endereço de rede tem todos os 0 bits na parte do host, conforme determinado pela máscara de sub-rede. Neste exemplo, o endereço de rede é 192.168.11.0/24. Um endereço de rede não pode ser atribuído a nenhum dispositivo.

### 2.2.3. Endereço de broadcast ou difusão

Um endereço de difusão é um endereço que é usado quando é necessário acessar todos os dispositivos em rede IPv4. Conforme mostrado na tabela 2, o endereço de difusão de rede tem todos os 1 bits na parte do host, conforme determinado pela máscara de sub-rede.

| **Tabela 2 - Endereço de broadcast da rede 192.168.10.0 com máscara 255.255.255.0** | | | | |
|---|---|---|---|---|
| | **1nd Octeto** | **2nd Octeto** | **3nd Octeto** | **4nd Octeto** |
| **End. IP do Host** | 192 | 168 | 10 | 11 |
| | 11000000 | 10100000 | 00001010 | 00001011 |
| **Máscara sub-rede** | 255 | 255 | 255 | 0 |
| | 11111111 | 11111111 | 11111111 | 00000000 |

| | | | | |
|---|---|---|---|---|
| **End. Rede (AND Lógico entre o End. IP e a Máscara)** | **Todos os bits de host em “0”** | | | |
| | 192 | 168 | 10 | 0 |
| | 11000000 | 10100000 | 00001010 | 00000000 |
| **End. Broadcast** | **Todos os bits de host em “1”** | | | |
| | 192 | 168 | 10 | 255 |
| | 11000000 | 10100000 | 00001010 | 11111111 |

Neste exemplo, o endereço de rede é 192.168.11.255/24. Um endereço de difusão também não pode ser atribuído a nenhum dispositivo da rede.

### 2.2.4. Endereços de host

Endereços de host são aqueles que podem ser atribuídos a um dispositivo, da rede como um computador, laptop, smartphone, câmera web, impressora, roteador, etc. A porção host do endereço é indicada pelos bits “0” da máscara de sub-rede, e podem assumir qualquer combinação de bits na parte do host, exceto para todos os bits 0 (endereço de rede) ou todos os bits 1 (endereço de difusão), nesse caso quailquer endereço entre 192.168.10.1/24 a 192.168.10.254/24, inclusive, pode ser um endereço de host.

### 2.2.5. Default Gateway

O Default Gateway é o dispositivo de rede (ECD) que pode encaminhar o tráfego para outras redes. Este endereço deve ser configurado juntamente com o endereço de host e a máscara de subrede de um dispositivo conforme mostrado na figura 6.

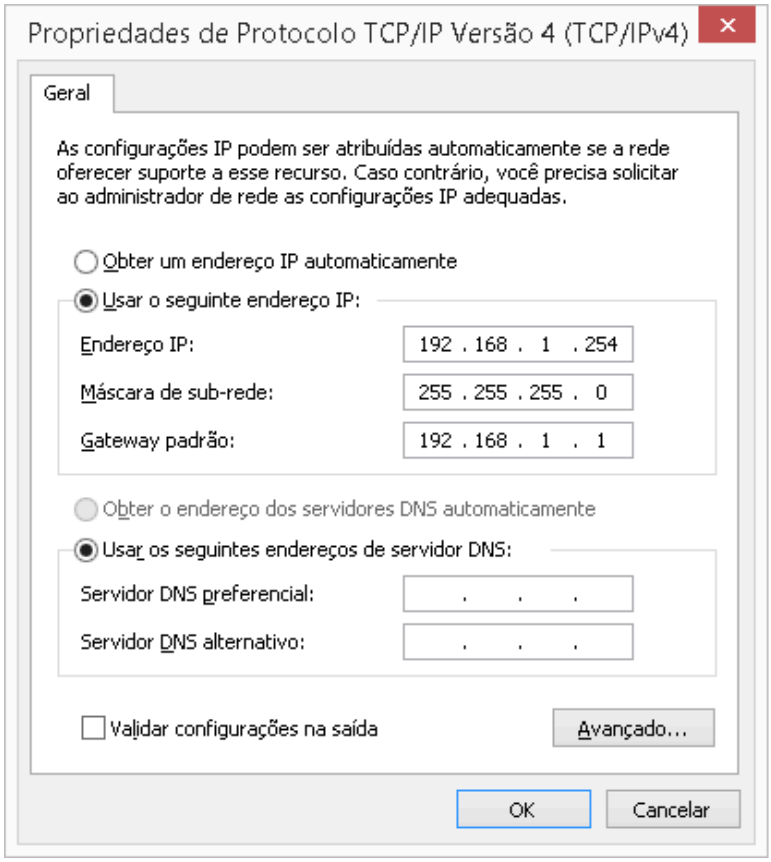


Fig. 6 Configuração do Gateway padrão em um Host Windows

**Destaque:** O Default Gateway é sempre um dispositivo existente na mesma rede do host que está sendo configurado.

### 2.2.6. Endereço automático

Um host utilizando o protocolo IPv4 pode obter automaticamente seu endereço a partir de um servidor DHCP para isso basta ser configurado para obter automaticamente seu endereço IPv4, conforme mostra a figura 7

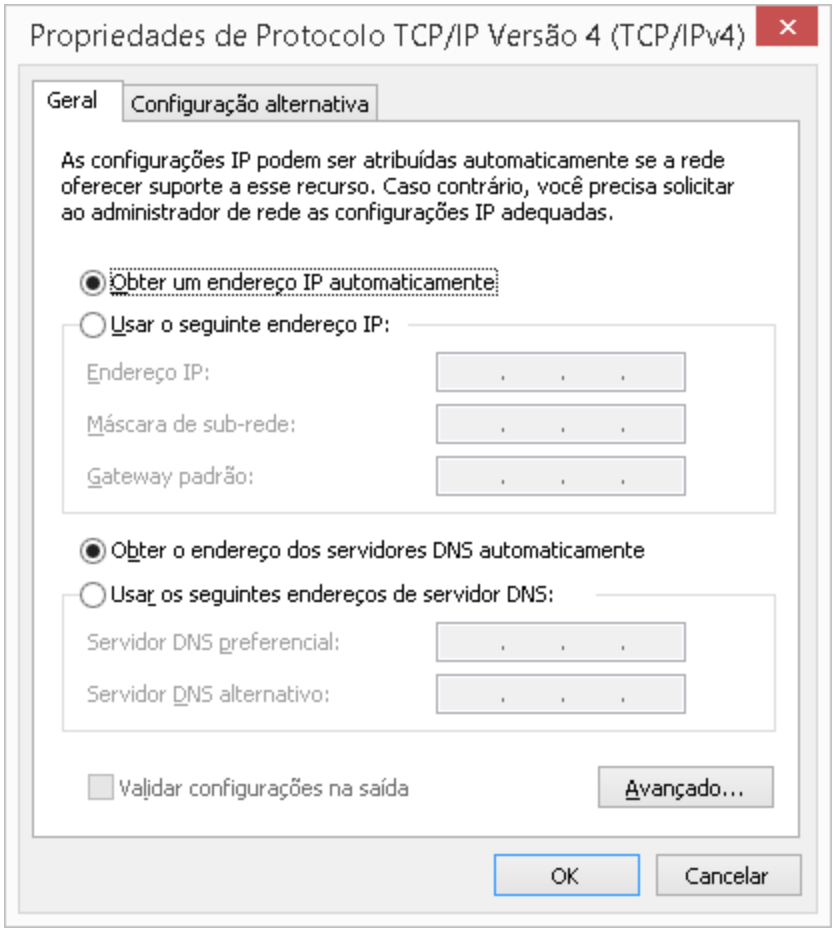


Fig. 7 Configuração de endereçamento automático em um host Windows

O servidor DHCP fornecerá o endereço IPv4, a máscara de sub-rede e gateway padrão. Além disso, pode fornecer outras informações como o servidor DNS e rotas estáticas.

## 2.3. Endereços IPv4 especiais

Os endereços IPv4 são utilizados para referenciar um host na rede global, a Internet, e são roteados globalmente entre provedores de serviços de Internet (ISP). Além dos endereços de rede e de broadcast existem outros tipos de endereços IPv4 reservados para finalidades específicas, que são:

- **Endereços IPv4 Privados** - Esses endereços são atribuídos pelo IANA, para as organizações, na RFC 1918 foi estabelecido um espaço de endereçamento privado, apresentado na tabela 3.

| Tabela 3 - Endereços IPv4 privados | | |
|---|---|---|
| **Classe** | **Endereço de rede e prefixo** | **RFC 1918 Intervalo de endereços privados** |
| A | 10.0.0.0/8 | 10.0.0.0 - 10.255.255.255 |
| B | 172.16.0.0/12 | 172.16.0.0 - 172.31.255.255 |
| C | 192.168.0.0/16 | 192.168.0.0 - 192.168.255.255 |

Estes blocos de endereços podem ser usados pelas organizações para endereçar hosts internos, eles não são exclusivos e podem ser usados internamente em qualquer rede, uma vez que não são roteados na Internet.

- **Endereços de loopback** - São endereços reservados para o host direcionar o tráfego IP para si próprio, utilizam a faixa 127.0.0.0/8 - 127.0.0.1 a 127.255.255.254, mas são normalmente identificados apenas pelo IP 127.0.0.1, possibilitando a comunicação inter-processos (entre aplicações na mesma máquina). Ele também pode ser utilizado para verificar o funcionamento do protocolo IP na máquina, já que ele responde ao comando ping.

- **Endereços link local** - Utilizam a faixa 169.254.0.0/16, isto é, de 169.254.0.1 até 169.254.255.254, e são mais conhecidos como endereço IP privado automático (APIPA) ou endereço auto-atribuído. São atribuídos a um cliente DHCP, para se auto-configurar, sempre que não consegue receber seu endereço IP de servidores DHCP da rede.

- **Endereço de Broadcast restrito ou Limitado**: Identifica um broadcast na própria rede. Representado por todos os bits do endereço iguais a 1. Em notação decimal 255.255.255.255.

Pratique: Utilize o comando ***ipconfig*** para obter informações sobre seus adaptadores de rede e endereçamento IPv4. Digite o comando ipconfig /all no prompt de comando do computador com sistema operacional Windows para obter as informações de todos os seus adaptadores de rede com seus respectivos endereços. Você deve obter uma resposta como a apresentada na figura 8.


Observe o endereço MAC do adaptador, além do endereço IPv4 e sua máscara. Observe também o endereço do default gateway.

## 3. Segmentação de Redes IPv4

A segmentação de redes baseadas em IPv4 é um conceito fundamental em redes de computadores para melhorar a eficiência, segurança e gerenciamento das comunicações entre dispositivos, algumas razões pelas quais a segmentação de redes IPv4 é importante:

- **Eficiência de Tráfego**: Reduz o tráfego de broadcast, que é enviado a todos os dispositivos na rede. Isso melhora a eficiência do tráfego de rede, uma vez que o tráfego desnecessário é minimizado.

- **Desempenho**: O tráfego é direcionado apenas para os dispositivos relevantes na mesma sub-rede. Isso reduz a carga nas redes e dispositivos individuais.

- **Isolamento e Segurança**: Isola diferentes partes da rede. Se um problema de segurança ocorrer em uma sub-rede, a propagação para outras partes da rede pode ser limitada. Isso é especialmente importante em ambientes corporativos onde a segurança é uma preocupação.

- **Gerenciamento de Tráfego:** Com a segmentação, é possível priorizar e controlar o tráfego de maneira mais eficaz.

- **Escalabilidade**: À medida que uma rede cresce, é mais fácil adicionar sub-redes do que expandir uma única rede monolítica.

Em resumo, a segmentação de redes baseadas em IPv4 é uma prática recomendada para melhorar a eficiência, segurança, escalabilidade e gerenciamento das redes de computadores, seja em ambientes corporativos, industriais ou residenciais.

## 3.1. Endereçamento Classful Legado

No seu lançamento, os endereços IPv4 foram divididos em classes (endereçamento classful), conforme definido na RFC 790 substituída pela RFC 820. Os endereços IPv4 eram atribuídos com base em classes conforme mostrado na figura 1.


Fig. 1 Endereçamento IPv4 Classful fonte: Werner, J.A.V. pág. 16

- Classe A (0.0.0.0/8 a 127.0.0.0/8) - Suporta redes extremamente grandes com mais de 16 milhões de endereços de host e apenas 128 redes. Usa o prefixo /8 com o primeiro octeto para indicar o endereço de rede e os três octetos restantes para endereços de host.

- Classe B (128.0.0.0/16 a 191.255.0.0 /16) - Projetada para suportar redes de tamanho médio a grande, com até aproximadamente 65.536 endereços de host e 65.536 endereços de rede. Usa um prefixo fixo /16 com os dois primeiros octetos para indicar o endereço de rede e os dois octetos restantes para endereços de host

- Classe C (192.0.0.0/24 a 223.255.255.0/24) - Com um máximo de 254 hosts por redes, mas com cerca de para 2 milhões de redes, a Classe C foi projetada para suportar redes pequenas. Ela utiliza um prefixo fixo /24 com os três primeiros octetos para indicar a rede e o octeto restante para os endereços de host.

**Destaque**: Há também um bloco multicast de Classe D que consiste nos endereços de 224.0.0.0 a 239.255.255.255 e um bloco de endereços reservados de Classe E que consiste em 240.0.0.0 - 255.255.255.255.

Neste esquema nem todos os requisitos das organizações e da Internet eram atendidos. A classe A e até mesmo a B desperdiçaram muitos endereços, o que acabava com a disponibilidade de endereços IPv4, uma companhia com uma rede de 260 hosts, por exemplo, precisava receber um endereço classe B com mais de 65.000 endereços.

## 3.2. Endereçamento Classless

Como a alocação classful dos endereços IPv4 era muito ineficiente, em 1993, a IETF criou um novo conjunto de padrões que permitia aos provedores de serviços atribuírem endereços IPv4 em qualquer fronteira do bit do endereço (comprimento do prefixo) em vez de apenas um endereço de classe A, B ou C. Este sistema é conhecido como endereçamento Classless Inter-Domain Routing (CIDR), e apesar de estar longe de resolver o problema do esgotamento dos endereços IPv4, traria uma solução temporária até que um novo protocolo IP fosse desenvolvido para acomodar o rápido crescimento no número de usuários da Internet. Em 1994, a IETF começou o trabalho para localizar um sucessor para o IPv4, que resultou na criação do protocolo IPv6, o qual abordaremos mais adiante..

### 3.2.1. Notação por prefixos

Representar os IPv4 seguido da máscara de sub-rede em decimal com pontos pode ser desgastante. Porém, existe um método alternativo chamado comprimento do prefixo, que corresponde ao número de bits 1 da máscara de sub-rede, e é escrito após o endereço IPv4 separado por uma (/), por exemplo o endereço IPv4 192.168.10.1 com máscara 255.255.255.0 pode ser representado como 192.168.10.11/24. A tabela 4 apresenta os prefixos e a correspondência com a notação decimal da máscara.

**Tabela 1 – Prefixos das máscaras de subrede**

| Máscara de Sub-Rede | Binário – 32 bits | Prefixo |
|---|---|---|
| 255.0.0.0 | `11111111.00000000.00000000.00000000` | /8 |
| 255.255.0.0 | `11111111.11111111.00000000.00000000` | /16 |

| | | |
|---|---|---|
| 255.255.255.0 | 11111111.11111111.11111111.00000000 | /24 |
| 255.255.255.128 | 11111111.11111111.11111111.10000000 | /25 |
| 255.255.255.192 | 11111111.11111111.11111111.11000000 | /26 |
| 255.255.255.224 | 11111111.11111111.11111111.11100000 | /27 |
| 255.255.255.240 | 11111111.11111111.11111111.11110000 | /28 |
| 255.255.255.248 | 11111111.11111111.11111111.11111000 | /29 |
| 255.255.255.252 | 11111111.11111111.11111111.11111100 | /30 |

## 3.3. Domínio de broadcast

Em uma rede baseada no protocolo IPv4, transmissões em broadcast são muito comuns, seja para obtenção de um endereço IP de um servidor DHCP (Dynamic Host Configuration Protocol) ou na resolução de endereços do MAC pelo protocolo ARP (Address Resolution Protocol). Podemos definir um domínio de broadcast como a fronteira da rede onde um transmissão em broadcast pode chegar. Os switches propagam broadcasts por todas as interfaces, exceto a interface em que foram recebidos, roteadores por sua vez não propagam broadcasts. A figura 2 apresenta um exemplo de domínios de broadcast.

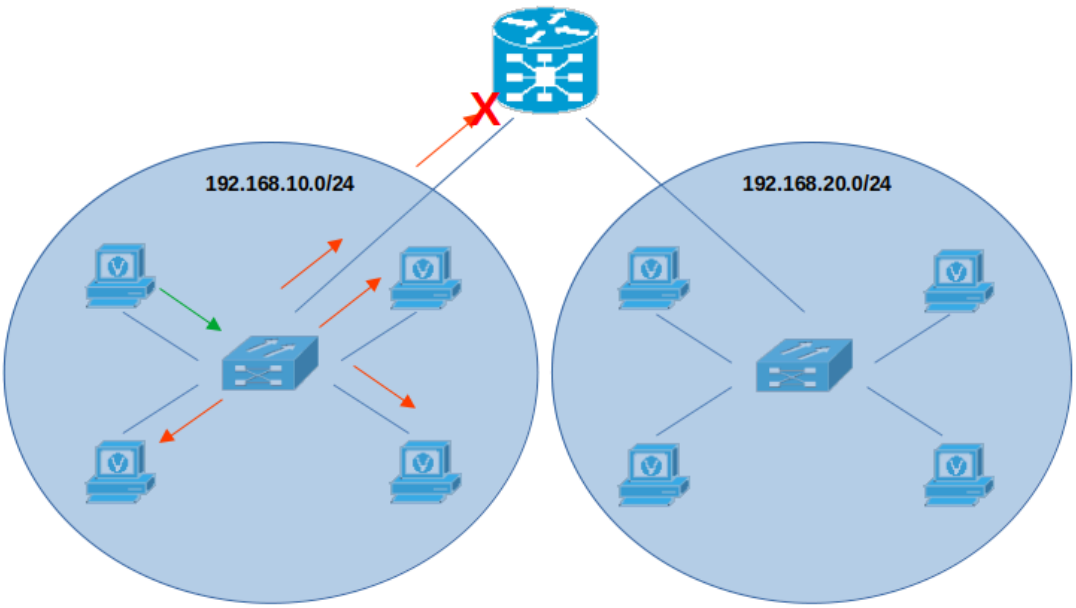



Fig. 2 - Domínios de Broadcast Fonte: o autor

Quando um domínio de broadcast é muito grande, isto é, com muitos hosts, estes podem gerar broadcasts em excesso e afetar a performance. A divisão da rede em sub-redes reduz o tráfego total da rede e melhora seu desempenho. Além disso, permite implantar políticas de controle de acesso, por exemplo, estabelecendo quais sub-redes podem ou não se comunicar e quais não.

## 3.4. Sub-redes IPv4

As sub-redes IPv4 são definidas pelo uso de um ou mais bits de host como bits de rede, com isso estende-se a máscara de sub-rede para pegar emprestado alguns dos bits da porção de host do endereço e criar bits de rede adicionais. Quanto mais bits de host forem emprestados, mais sub-redes poderão ser definidas e por consequência menor o número de hosts por sub-rede.

Podemos dividir uma rede em subredes de várias maneiras: a primeira é a divisão nos limites das classes, isto é, dos octetos: /8, /16 e /24. Por exemplo, utilizando uma máscara de classe B em uma rede de classe A, conforme mostrado na tabela 2.

**Tabela 2 - Divisão de uma rede classe A (/8) em sub-redes classe B (/16).**

| Endereço da Sub-Rede<br>(256 possíveis sub-redes) | Intervalo de host<br>(65,534 possíveis hosts por sub-rede) | Broadcast |
|---|---|---|
| 10.0.0.0/16 | 10.0.0.1 - 10.0.255.254 | 10.0.255.255 |
| 10.1.0.0/16 | 10.1.0.1 - 10.1.255.254 | 10.1.255.255 |
| 10.2.0.0/16 | 10.2.0.1 - 10.2.255.254 | 10.2.255.255 |
| ... | ... | ... |
| 10.255.0.0/16 | 10.255.0.1 - 10.255.255.254 | 10.255.255.255 |

Nesse caso na rede 10.0.0.0/8 foi aplicada a máscara de classe B (/16) ficando 10.0.0.0/16. Assim onde havia 1 rede com 16.777.214 hosts passamos a ter 256 sub-redes redes com 65.534 hosts. Se fosse aplicada uma máscara de classe C (/24), teríamos 65.536 subredes com 254 hosts por rede, conforme mostrado na tabela 2.

**Tabela 3 - Divisão de uma rede classe A (/8) em sub-redes classe C (/24).**

| Endereço da Sub-Rede<br>(65,536 possíveis sub-redes) | Intervalo de host<br>(254 possíveis hosts por sub-rede) | Broadcast |
|---|---|---|
| 10.0.0.0/24 | 10.0.0.1 - 10.0.0.254 | 10.0.0.255 |
| 10.0.1.0/24 | 10.0.1.1 - 10.0.1.254 | 10.0.1.255 |
| … | … | … |
| 10.0.255.0/24 | 10.0.255.1 - 10.0.255.254 | 10.0.255.255 |
| 10.1.0.0/24 | 10.1.0.1 - 10.1.0.254 | 10.1.0.255 |
| 10.1.1.0/24 | 10.1.1.1 - 10.1.1.254 | 10.1.1.255 |
| … | … | … |
| 10.100.0.0/24 | 10.100.0.1 - 10.100.0.254 | 10.100.0.255 |
| ... | ... | ... |
| 10.255.255.0/24 | 10.255.255.1 - 10.2255.255.254 | 10.255.255.255 |

A segunda maneira é a divisão dentro do limite do octeto. Por exemplo, se dividirmos uma rede classe C em sub-redes teremos as seguintes sub-redes apresentadas na tabela 4.

**Tabela 4 - Divisão de uma rede no limite do octeto**

| Prefixo | Máscara de sub-rede | Máscara de sub-rede em binário | sub-redes | hosts |
|---|---|---|---|---|
| /25 | 255.255.255.128 | 11111111.11111111.11111111.**1**0000000 | $2^1$=2 | $2^7$- 2 = 126 |
| /26 | 255.255.255.192 | 11111111.11111111.11111111.**11**000000 | $2^2$=4 | $2^6$- 2 = 62 |
| /27 | 255.255.255.224 | 11111111.11111111.11111111.**111**00000 | $2^3$=8 | $2^5$- 2 = 30 |
| /28 | 255.255.255.240 | 11111111.11111111.11111111.**1111**0000 | $2^4$=16 | $2^4$- 2 = 14 |
| /29 | 255.255.255.248 | 11111111.11111111.11111111.**11111**000 | $2^5$=32 | $2^3$- 2 = 6 |
| /30 | 255.255.255.252 | 11111111.11111111.11111111.**111111**00 | $2^6$=64 | $2^2$- 2 = 2 |

**Destaque**: Sempre que dividimos uma rede em sub-redes perdemos dois endereços por sub-rede: o endereço de rede e o endereço de broadcast da subrede. Por isso a maior máscara possível em um octeto é /30, pois com a  máscara /32 haveriam apenas dois endereços, um para a rede e outro para broadcast não sobrando nenhum IP para hosts.

## 3.5. Redes com máscara variável - VLSM

Quando projetamos o endereçamento de uma rede, muitas vezes nos deparamos com uma distribuição irregular de hosts por sub-rede, de forma que se utilizarmos uma máscara única para divisão, não faremos bom uso dos endereços disponíveis. Uma alternativa é a utilização das subredes com máscaras variáveis - VLSM. Imagine o seguinte cenário descrito na figura 3.

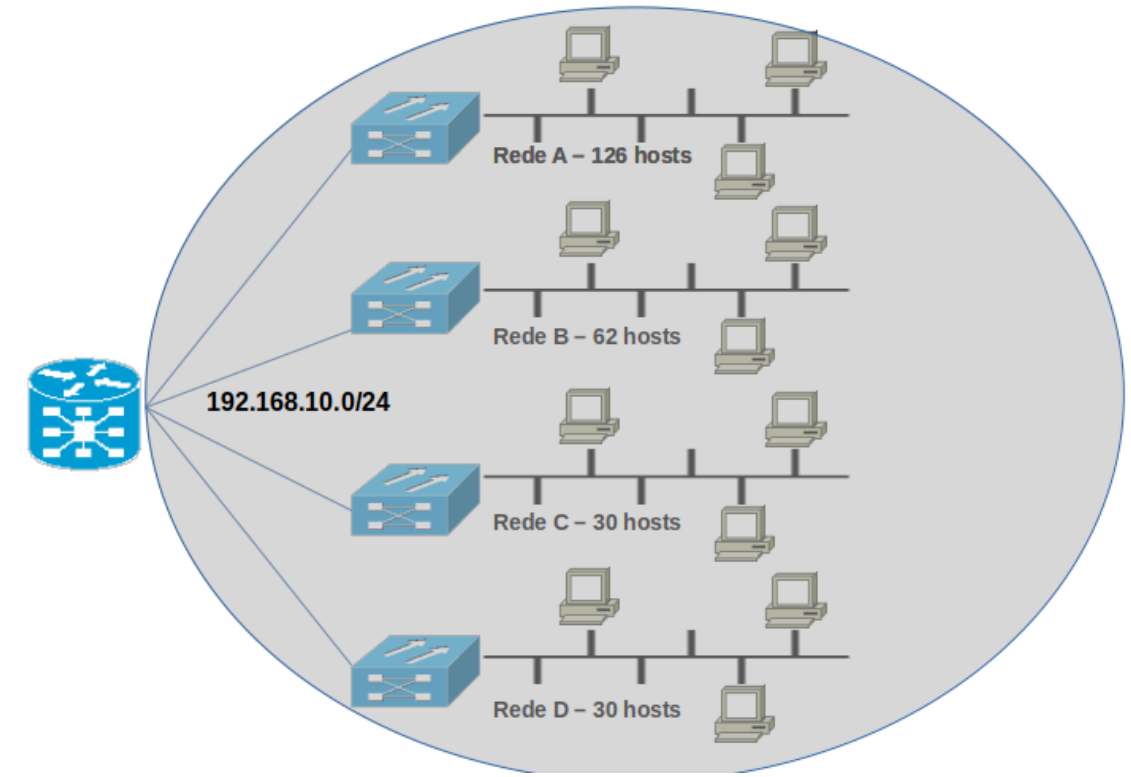



Figura 3 - Cenário para segmentação VLSM fonte: o autor

Temos que estabelecer o endereçamento IPv4 para suprir as redes com as seguintes características apresentadas na tabela 5.

| **Tabela 5 - Distribuição de Hosts por Rede** | |
|---|---|
| Redes | Número de hosts |
| Rede A | 126 |
| Rede B | 62 |
| Rede C | 30 |
| Rede D | 30 |
| Num. Total de hosts | 248 |

A primeira opção seria utilizar redes com máscaras de classe C ou B - Neste caso atendemos todas as redes, mas com um grande desperdício de endereços.

Uma outra alternativa uma vez que a quantidade total de hosts (248) pode ser atendida por uma rede de classe C seria utilizar subredes com  máscara variável - VLSM. Assim com base na tabela 7 a seguinte segmentação, por exemplo, da rede 192.168.10.0/24 apresentada na tabela 6 pode ser efetuada.

| **Tabela 6 - Segmentação com máscara variável** | | | | |
|---|---|---|---|---|
| Rede | Prefixo | Máscara | End. Rede / End. Broadcast | Hosts |
| A | /25 | 255.255.255.128 | End. Rede: 192.168.10.0<br>End. broadcast: 192.168.10.127 | 126 |
| B | /26 | 255.255.255.192 | End. Rede: 192.168.10.128<br>End. broadcast: 192.168.10.191 | 62 |
| C | /27 | 255.255.255.224 | End. Rede: 192.168.10.192<br>End. broadcast: 192.168.10.223 | 32 |
| D | /27 | 255.255.255.224 | End. Rede: 192.168.10.224<br>End. broadcast: 192.168.10.255 | 32 |

## 4. IPv6

O IPv6 foi desenvolvido com o objetivo de superar as limitações do IPv4 e apresentar novos recursos que atendem às demandas atuais e futuras da rede. As principais

melhorias que o IPv6 traz incluem:

- **Espaço de endereçamento** - os endereços IPv6 são baseados no endereçamento hierárquico de 128 bits, em oposição ao IPv4 com 32 bits.
- **Melhora a o tratamento de pacotes** - O cabeçalho IPv6 é mais simples e com menos campos.
- **Melhora a conectividade ponta a ponta e elimina a necessidade de NAT** - Por permitir um grande número de endereços IPv6 públicos, o NAT entre um endereço IPv6 privado e um IPv6 público não é necessário. Isso evita alguns dos problemas introduzidos pelo NAT enfrentados por aplicativos que exigem conectividade de ponta a ponta.

Um endereço IPv4 é composto de 32 bits e fornece aproximadamente 4.294.967.296 endereços exclusivos, o endereço IPv6 é composto de 128 bits e fornece 340.282.366.920.938.463.463.374.607.431.768.211.456, ou 340 undecilhões de endereços. Isto equivale a quantidade de grãos de areia na Terra. Além disso outras melhorias foram acrescentadas como por exemplo o ICMPv6 (Internet Control Message Protocol versão 6), que inclui a resolução de endereços e a configuração automática de endereços, não encontradas no ICMP para IPv4 (ICMPv4).

### 4.1. Pacote IPv6

Uma das principais melhorias do IPv6 em relação ao IPv4 é o cabeçalho IPv6 simplificado, com comprimento fixo de 40 bytes (octetos) sendo a maior parte em função dos endereços IPv6 de origem e de destino, conforme mostrado na figura 1. Este cabeçalho permite um processamento mais eficiente dos pacotes IPv6.

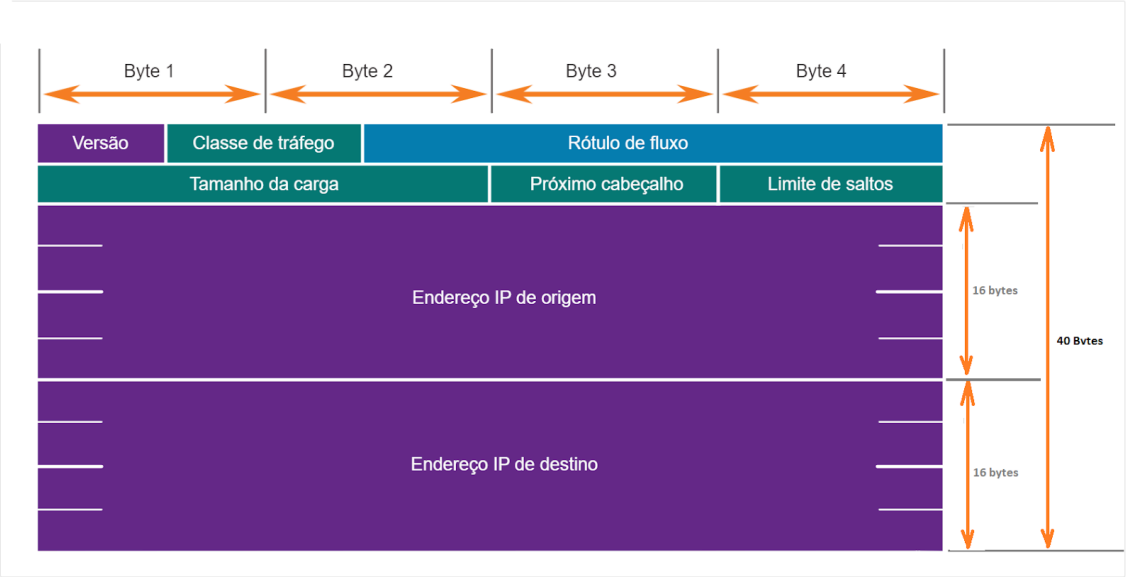



Fig. 1 Operação AND entre a máscara e o endereço IPv4 do hosts Fonte: o autor modificado de CCNA1 - Introduction to Network v7.02 item 11.1.4

Os principais campos no cabeçalho do pacote IPv6 incluem o seguinte:

- **Versão (4 bits)** - Indica a versão do protocolo. 0110 para IP versão 6.
- **Classe de tráfego (8 bits)** - É equivalente ao campo DSv (Serviços diferenciados de IPv4).
- **Etiqueta de fluxo (20 bits)** - Determina que todos os pacotes com a mesma etiqueta de fluxo recebam o mesmo tipo de manipulação pelos roteadores.
- **Comprimento do Payload - carga útil (16 bits)** - Define o comprimento da parte de dados, isto é, da carga útil do pacote IPv6. Não inclui o comprimento do cabeçalho IPv6, que é fixo de 40 bytes.
- **Próximo cabeçalho (8 bits)** - Equivalente ao campo Protocolo do IPv4. Define protocolo da camada de enlace que o pacote está carregando, permitindo que a camada de rede transfira os dados para o protocolo apropriado das camadas superiores.
- **Limite de salto (8 bits)** - Substitui o campo TTL do IPv4, seu valor é subtraído de um cada vez que um roteador encaminha o pacote. Quando atinge o valor 0, o pacote é descartado e uma mensagem de ICMPv6 com tempo excedido é encaminhada para o host de envio, indicando que o pacote não chegou ao destino porque o limite de salto foi excedido
- **Endereço IPv6 de origem (128 bits)** - Identifica o endereço IPv6 do host de envio.
- **Endereço IPv6 de destino (128 bits)** - Identifica o endereço IPv6 do host de destino.

Um pacote IPv6 pode conter também cabeçalhos de extensão (EH), que fornecem informações de camada de rede opcionais. Os cabeçalhos de extensão ficam posicionados entre o cabeçalho IPv6 e a carga. Eles são usados para fragmentação, segurança, suporte à mobilidade e dentre outros.

**Destaque**: Diferente do IPv4, o IPv6 não inclui um campo de verificação erro do cabeçalho, já que esta função é executada nas camadas de Enlace e Transporte. Isso melhora o desempenho da rede, porque os roteadores não precisam calcular a soma de verificação quando diminui o campo Limite de Saltos em cada roteamento. Além disso, os roteadores não fragmentam os pacotes IPv6 roteados.

### 4.2. Endereçamento IPv6

O Endereço IPv6 é um número binário de 128 bits representado como uma sequência de 8 números de 4 dígitos hexadecimais (hextetos), assim 8 “hextetos” x 16 bits = 128 bits, como apresentado na figura 2.

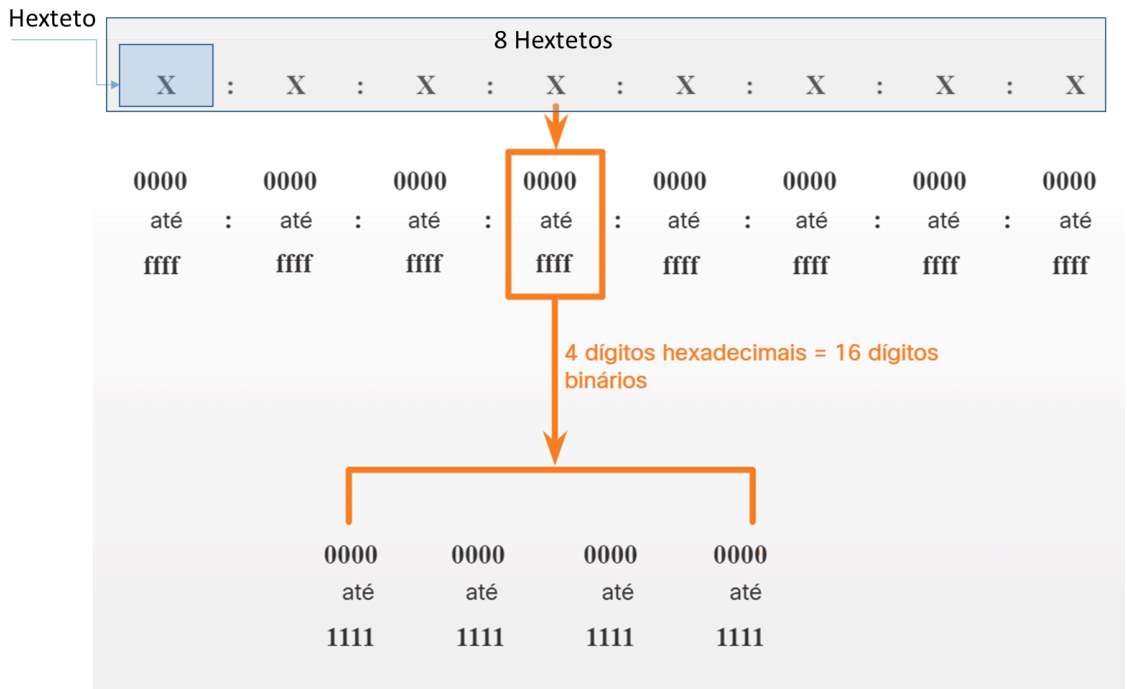



Fig. 2 Representação do Endereço IPv6  Fonte: o autor modificado de CCNA1 - Introduction to Network v7.02 item 12.2.1

Assim como o termo octeto refere-se aos oito bits de um endereço IPv4, no IPv6, um “hexteto” é o termo não oficial (um neologismo) usado definir um segmento de 16 bits ou quatro valores hexadecimais. Cada “**X**”  na figura equivale a um único “hexteto”.

Dessa forma o formato mais utilizado para se escrever um endereço IPv6 é  X:X X:X X:X X:X como mostrado na figura 3

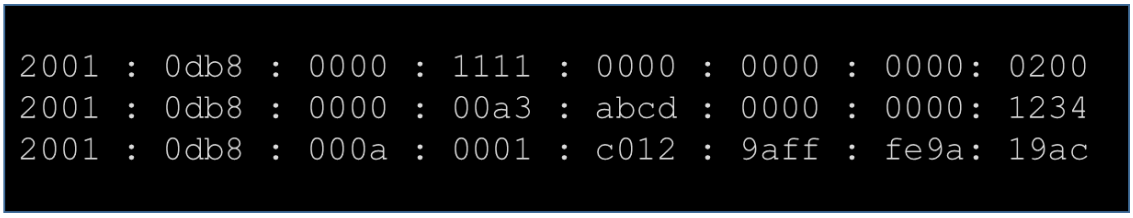



Fig. 3 - Endereços IPv6 fonte: o autor

### 4.2.1 Formato compactado

Existem duas regras que melhoram a representação, reduzindo o número de dígitos necessários para representar um endereço IPv6. Quando associamos essas duas técnicas a notação de endereço IPv6 pode ser bastante reduzida.

- **Regra 1 - Omitir zeros à esquerda**

  É possível omitir os 0s (zeros) à esquerda de qualquer sessão de 16 bits ou “hexteto”. Veja aqui quatro exemplos de como omitir zeros à esquerda:

  **0db8** pode ser representado como **db8**
  **000a** pode ser representado como **a**
  **00a3** pode ser representado como **a3**
  **0200** pode ser representado como **200**
  **0000** pode ser representado como **0**

  Veja na figura 4 como são representados alguns endereços IPv6 após a aplicação desta regra.

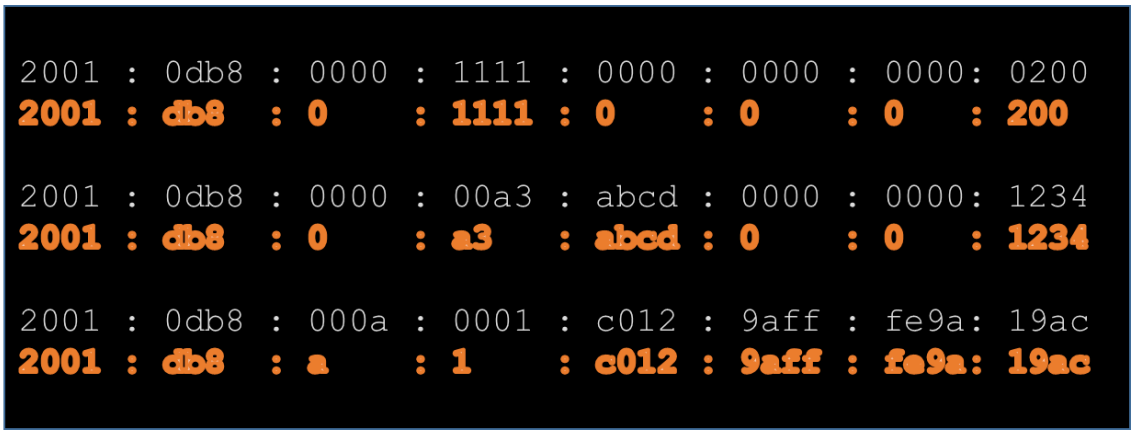


Fig.4 - Endereços IPv6 após aplicação da regra de omitir zeros a esquerda fonte: o autor

**Destaque**: Essa regra só se aplica aos 0s à esquerda, e não aos 0s à direita. Se isso for feito a representação do endereço será ambígua. Por exemplo, o hexteto “abc” poderia ser “0abc” ou “abc0”, porém esses dois hextetos não representam o mesmo valor.

- **Regra 2 - Dois pontos duplos**

Dois-pontos duplos (::) podem substituir uma única sequência contígua de um ou mais segmentos de 16 bits (hextetos) formados apenas por 0s. Veja na figura 5 a aplicação da regra dos dois pontos duplos sobre a regra de omitir os zeros.

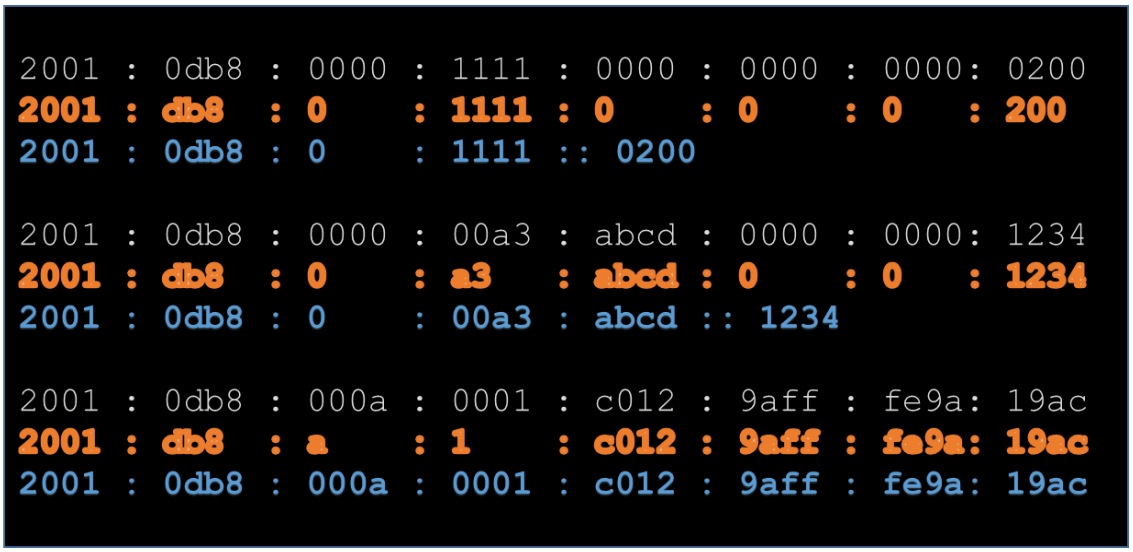


Fig.5 - Endereços IPv6 após aplicação da regra de omitir zeros a esquerda e dois pontos duplos fonte: o autor

**Destaque**: Esta regra só pode ser usada uma vez em um endereço, caso contrário, haveria mais de um endereço resultante possível.

### 4.2.2. Máscara de sub-rede

O IPv6 usa apenas a notação do comprimento do prefixo para indicar a parte da rede do endereço. O comprimento do prefixo pode variar de 0 a 128, porém o comprimento do prefixo IPv6 recomendado para LANs e a maioria dos outros tipos de redes é /64, conforme mostrado na figura 6.

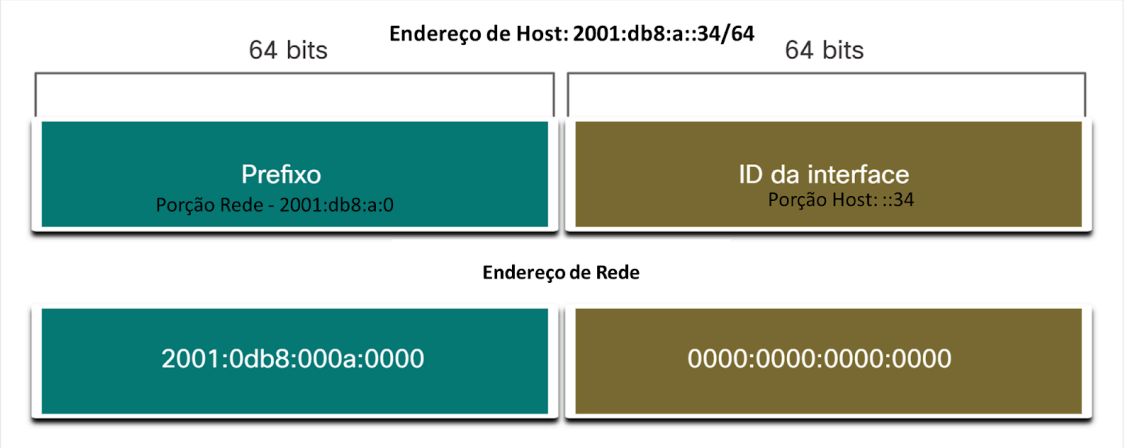



Fig. 6 - Prefixo do endereço IPv6 utilizado em LANs Fonte: o autor modificado de CCNA1 - Introduction to Network v7.02 item 12.3.2

Nesse caso são utilizados 64 bits para definir a rede e 64 para definir os hosts em cada uma das redes. Isso é recomendado para a maioria das redes, porque a configuração automática de endereço sem estado (SLAAC) usa 64 bits para o ID de interface, além de facilitar a criação e o gerenciamento de sub-redes.

### 3. Tipos de endereços IPv6

O IPv6 possui os seguintes tipos de endereço:

- **Unicast** – Identifica univocamente uma interface em um dispositivo habilitado para IPv6.
- **Multicast** – Usado para enviar um único pacote IPv6 para vários destinos.

**Destaque**: O IPv6 não possui um endereço de broadcast, porém há um endereço multicast para todos os nós IPv6 que fornece basicamente a mesma funcionalidade.

#### 4.3.1. Endereços Unicast

- **Endereço unicast global (GUA - Global Unicast Address)** - Corresponde no IPv6 ao endereço IPv4 público. São endereços roteáveis na Internet e globalmente exclusivos. Podem ser configurados de forma estática ou dinâmica.

- **Endereços locais exclusivos (ULA - Unique Local Address)** - Definidos no intervalo **fc00::/7 a fdff::/7**, similares aos endereços privados do IPv4, porém ainda pouco utilizados. Sua estrutura segue a dos endereços GUA.

- **Endereço de Link local (LLA - Link-Local Address)** - Todo dispositivo IPv6 deve ter um endereço LLA, que utiliza a faixa **fe80::/10,** usado para comunicação com outros dispositivos no mesmo link local, isto é na mesma rede ou sub-rede. Estes endereços só precisam ser únicos para a rede em que se encontram, pois não são roteáveis, isto é, os roteadores não encaminham pacotes com um endereço de link local de origem ou destino.

- **Endereço de Loopback** - Assim como no IPv4 o endereço de loopback endereça o próprio host. No IPv6 é defino por **::1/128**

  **Destaque:** O espaço de endereço 2001:db8::/32 é reservado para documentação, incluindo o uso em exemplos.

### 4.3.1.2. Estrutura de um Endereço unicast global (GUA - Global Unicast Address)

Os endereços IPv6 unicast globais (GUA) são endereços globalmente exclusivos e roteáveis na Internet, equivalem aos endereços IPv4 públicos. São atribuídos pelo Internet Committee for Assigned Names and Numbers (ICANN), operador da Internet Assigned Numbers Authority (IANA), que aloca blocos de endereço IPv6 para os cinco Operadores Regionais (RIRs) nos respectivos continentes e estes para os operadores nos países e paras os Operadores de serviço Internet (ISP) . No momento, somente endereços unicast globais com os primeiros três bits de 001, isto é, 2000::/3 até 3fff::/3 estão sendo atribuídos. A figura 7 mostra a estrutura do GUA.

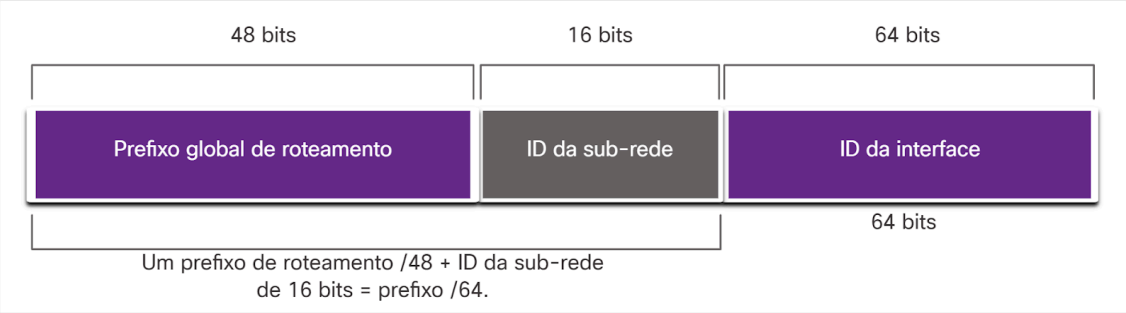



Fig. 7 - Estrutura do GUA Fonte: o autor modificado de CCNA1 - Introduction to Network v7.02 item 12.5.5

O prefixo de 64 bits que define a rede é composto de um prefixo de roteamento global de 48 bits e um complemento de 16 bits que define a sub-rede dentro da rede definido no prefixo de 48 bits. Por exemplo o endereço de rede Por exemplo, o endereço IPv6 2001:db8:abdc:1::/ 64, corresponde a sub-rede ::1/64, da rede 2001:db8:abcd::/48.

### 4.3.2. Endereços Multicast

Os endereços IPv6 multicast, para enviar um único pacote a um ou mais destinos (grupo multicast). Os endereços multicast IPv6 têm o prefixo ff00::/8.

**Destaque**: Os endereços multicast só podem ser utilizados como endereços de destino e nunca como endereços de origem, que devem ser sempre endereços Unicast

**Endereços multicast atribuídos**

São endereços multicast reservados para grupos predefinidos de dispositivos, usados para acessar um grupo de dispositivos que executam um serviço ou um protocolo comum, como por exemplo o DHCPv6. Os dois grupos multicast atribuídos ao IPv6 mais comuns são:

- **Grupo multicast de todos os nós - ff02::1 -** Grupo multicast ao qual todos os dispositivos habilitados para IPv6 se juntam. Um pacote enviado para esse grupo é recebido e processado por todas as interfaces IPv6 no link ou rede. Tem a mesma função que um endereço de broadcast em IPv4

- **Grupo multicast de todos os roteadores - ff02::2** - Este é um grupo multicast ao qual todos os roteadores IPv6 se unem. Um pacote enviado para esse grupo é recebido e processado por todos os roteadores IPv6 no link ou rede.

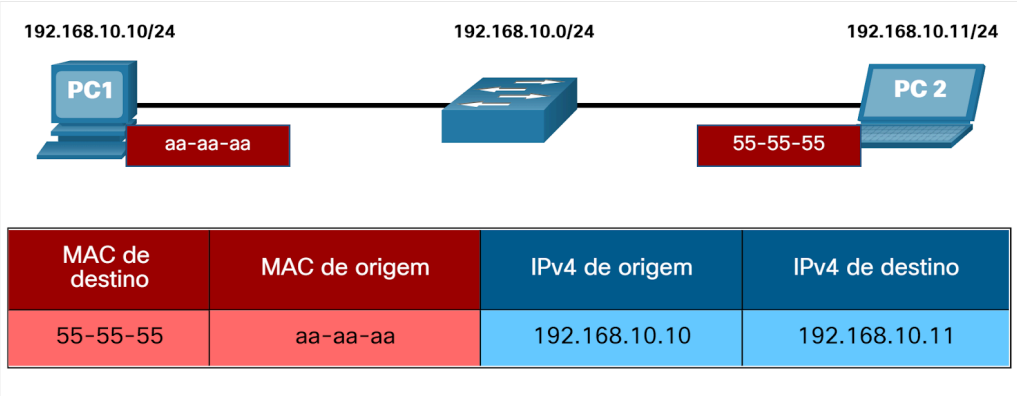
## 5. Roteamento

Roteamento é o processo de definir uma rota e encaminhar pacotes entre redes distintas com base no endereço da camada de rede, normalmente utilizando o protocolo IPv4 ou IPv6. Os pacotes são sempre criados no host de origem, que deve ser capaz de direcionar o pacote para o host de destino com base em uma tabela de roteamento. Tanto os dispositivos finais (ETD) como os dispositivos de rede (ECD) que operam na camada de rede têm suas próprias tabelas de roteamento. Um host pode enviar um pacote para si mesmo através do endereço de loopback, para um outro dispositivo na mesma rede ou para um host remoto em outra rede.

### 5.1.1. Encaminhando pacotes na mesma rede

Quando um host envia um pacote para outro host na mesma rede ele encapsula o pacote em um frame ethernet com o endereço MAC correspondente ao IP do host de destino, determinado através o protocolo ARP no caso do IPv4 ou através de uma solicitação de vizinhança ND ou NDP (Neighbor Discovery) no IPv6. A figura 1 apresenta a comunicação entre dois hosts em uma mesma rede Ethernet utilizando o

protocolo IPv4.




| MAC de destino | MAC de origem | IPv4 de origem | IPv4 de destino |
|---|---|---|---|
| 55-55-55 | aa-aa-aa | 192.168.10.10 | 192.168.10.11 |

Fig. 1 Comunicação de hosts na mesma rede  Fonte: o autor modificado de CCNA1 - Introduction to Network  v7.02 item 9.1.1

Veja que quando o PC1 envia um pacote para o PC2. O quadro Ethernet da camada 2 contém os seguintes dados nos campos de endereço:

- Endereço MAC de destino — Este é o endereço MAC simplificado de PC2, 55-55-55.
- Endereço MAC de origem — Este é o endereço MAC simplificado da NIC Ethernet em PC1, aa-aa-aa .

Mas para o pacote IP da camada 3 os dados de endereço IPV4 são os  seguintes:

- Endereço IPv4 de origem — Este é o endereço IPv4 de PC1, 192.168.10.10 .
- Endereço IPv4 de destino — Este é o endereço IPv4 de PC2, 192.168.10.11.

### 5.1.2. Encaminhando pacotes para a rede remota

Quando o endereço IP de destino (IPv4 ou IPv6) estiver em uma rede remota, o endereço MAC de destino será o endereço do gateway padrão do host ou aquele que estiver indicado na tabela  de rotas do host. Considere o exemplo apresentado na figura 2.

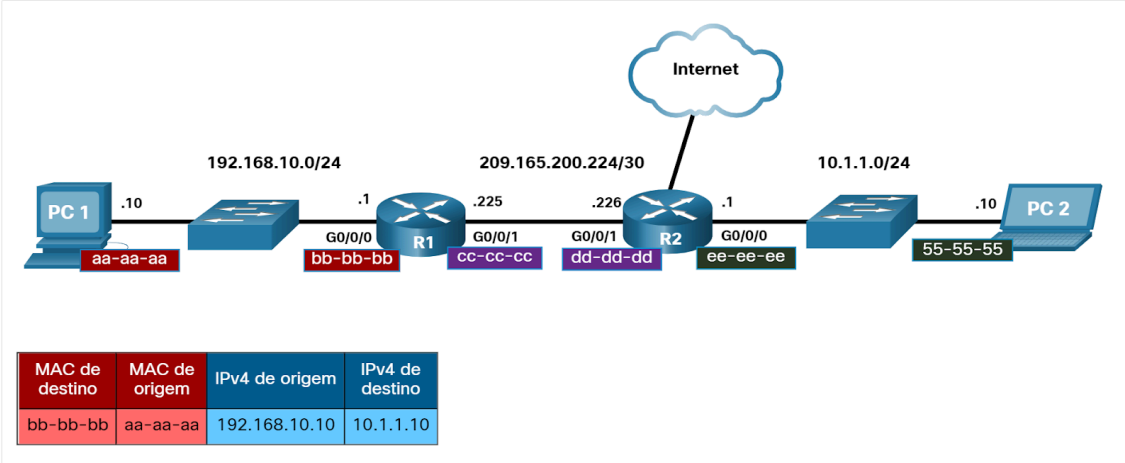



Fig. 2 Comunicação de hosts em redes diferentes Fonte: o autor modificado de CCNA1 - Introduction to Network v7.02 item 9.1.2

Veja que quando o PC1 envia um pacote para o PC2 que está em uma rede remota. O quadro Ethernet da camada 2 contém o seguinte:

- Endereço MAC de destino — Este é o endereço MAC simplificado da interface do roteador R1 conectada a rede 192.168.10.0/24, bb-bb-bb.
- Endereço MAC de origem — Este é o endereço MAC simplificado da NIC Ethernet em PC1, aa-aa-aa .

E o pacote IP da camada 3 contém os endereços IPv4 da seguinte maneira:

- Endereço IPv4 de origem — Este é o endereço IPv4 de PC1, 192.168.10.10 .
- Endereço IPv4 de destino — Este é o endereço IPv4 de PC2,10.1.1.10

.

### 5.1.3. Tabela de rota de um Host

No Windows, o comando **route print** ou **netstat -r** pode ser usado para exibir a tabela de roteamento do host, gerando a mesma saída. A figura 3 apresenta uma tabela de rotas de um host Windows.

Tabela de rotas IPv4

```
===========================================================================
Rotas ativas:
Endereço de rede            Máscara          Ender. gateway Interface       Custo
0.0.0.0                     0.0.0.0          192.168.1.1    192.168.1.223   10
127.0.0.0                   255.0.0.0        No vínculo     127.0.0.1       306
127.0.0.1                   255.255.255.255  No vínculo     127.0.0.1       306
127.255.255.255             255.255.255.255  No vínculo     127.0.0.1       306
192.168.1.0                 255.255.255.0    No vínculo     192.168.1.223   266
192.168.1.223   255.255.255.255  No vínculo     192.168.1.223   266
192.168.1.255   255.255.255.255  No vínculo     192.168.1.223   266
192.168.56.0    255.255.255.0    No vínculo     192.168.56.1    266
192.168.56.1                255.255.255.255  No vínculo     192.168.56.1    266
192.168.56.255  255.255.255.255  No vínculo     192.168.56.1    266
224.0.0.0                   240.0.0.0        No vínculo     127.0.0.1       306
224.0.0.0                   240.0.0.0        No vínculo     192.168.56.1    266
224.0.0.0                   240.0.0.0        No vínculo     192.168.1.223   266
255.255.255.255             255.255.255.255  No vínculo     127.0.0.1       306
255.255.255.255 255.255.255.255  No vínculo     192.168.56.1    266
255.255.255.255 255.255.255.255  No vínculo     192.168.1.223   266
===========================================================================
Rotas persistentes:   Nenhuma
```

Tabela de rotas IPv6

```
===========================================================================
Rotas ativas:
 Se      destino de rede de métrica           Gateway
  1      306 ::1/128                          No vínculo
  5      266 fe80::/64                        No vínculo
  3      266 fe80::/64                        No vínculo
  3      266 fe80::4c37:df1f:9fc9:97f2/128    No vínculo
  3      266 fe80::6502:5c13:8e19:4694/128    No vínculo
  5      266 fe80::b90a:74d4:ab5b:37e9/128    No vínculo
  1      306 ff00::/8                         No vínculo
  5      266 ff00::/8                         No vínculo
  3      266 ff00::/8                         No vínculo
===========================================================================
Rotas persistentes:
Se      destino de rede de métrica           Gateway
0       4294967295 ::/0                      fe80::da7d:7fff:fe7d:4d0b
===========================================================================
```

Fig. 3 Tabela de rotas de um host Windows fonte: o autor

A tabela de roteamento do roteador contém entradas de rota de rede, listando todos os possíveis destinos de rede conhecidos.

Uma  tabela de roteamento armazena três tipos de entradas de rota:

- **Redes conectadas diretamente** - Essas entradas de rota estão associadas às interfaces locais do dispositivo, uma rota diretamente conectada é adicionada sempre que uma interface estiver configurada com um endereço IP, e ativa. Em um roteador cada interface está conectada a um segmento de rede diferente, e sempre possui uma rota diretamente conectada para cada uma delas.

- **Redes remotas** - Essas entradas indicam as rotas cujos acesso está associado a um roteador. Essas rotas são configuradas de forma estática por um administrador ou através de um protocolo de roteamento dinâmico.

- **Rota padrão** — A rota padrão é usada sempre que nenhuma outra correspondência na tabela de roteamento IP for encontrada. Nomalmente é representada pelo endereço 0.0.0.0/0 na tabela de IPv4

**Destaque:** Quando existirem mais de uma rota para a mesma rede o pacote será encaminhado pela rota de menor custo. O custo de uma rota é uma métrica que leva em consideração o números de saltos (roteadores) da origem até o destino e outros aspectos como por exemplo a velocidade do link, dependendo do protocolo de roteamento utilizado.

## 5.2. Resolução de endereços IPv4 - Protocolo ARP

Um dispositivo utilizando o protocolo IPv4 na camada de rede, precisa do protocolo ARP (Address Resolution Protocol) para determinar o endereço MAC de destino de um dispositivo local quando conhece o endereço IPv4. O ARP fornece duas funções básicas:

- Resolução de endereços IPv4 em endereços MAC
- Manutenção da tabela de mapeamentos IPv4 para MAC

Quando um dispositivo precisa enviar dados pela rede seus pacotes IPv4 são enviados à camada de enlace de dados para serem encapsulados nos quadros Ethernet, ele então consulta uma tabela em sua memória, chamada tabela ARP, para encontrar o endereço MAC que é correspondente ao endereço IPv4 do destinatário. Se o endereço IPv4 destino do pacote estiver na mesma rede que o endereço IPv4 origem, o dispositivo pesquisará o endereço IPv4 destino na tabela ARP, mas se o endereço IPv4 destino do pacote estiver em uma rede diferente do endereço IPv4 origem, o dispositivo pesquisará o endereço IPv4 do gateway padrão na tabela ARP. Se nenhuma entrada for encontrada, o dispositivo enviará uma requisição ARP.  A figura 4 mostra uma mensagem encapsulada em um quadro Ethernet II ou Ethernet 802.3.

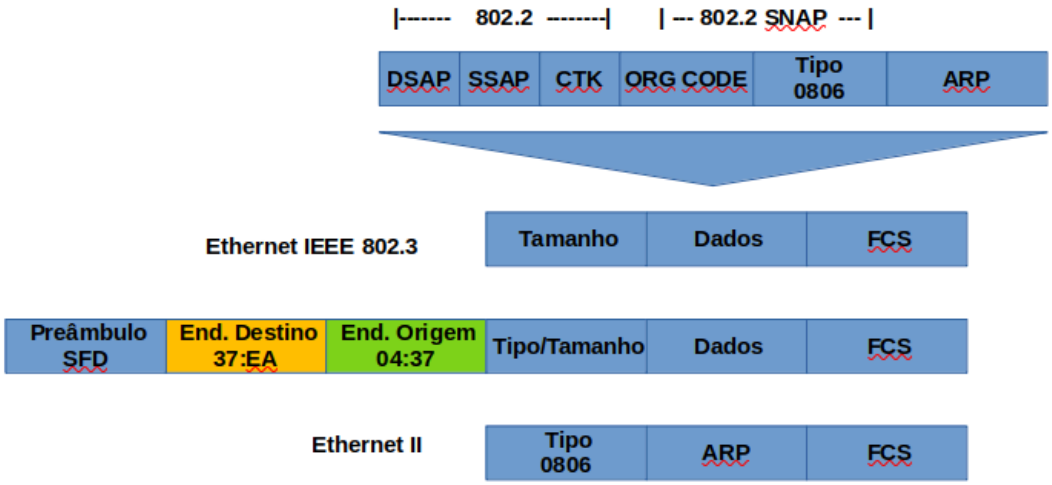



Fig. 4 - Encapsulamento do protocolo ARP Fonte: o autor

Imagine a seguinte situação mostrada na figura 5. O PC1 deseja enviar dados para o PC2, mas não possui o MAC do PC2 na sua tabela ARP.

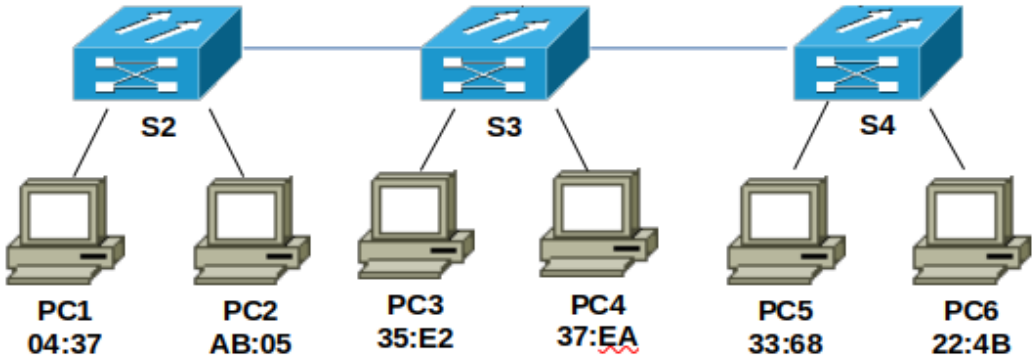



Fig. 5 - Computadores em um rede local Fonte: o autor

### 5.2.1. Requisições ARP

As requisições do ARP são mensagens de broadcast, encapsuladas diretamente em um quadro Ethernet, contendo as seguintes informações de cabeçalho como apresentado na figura 6 utilizando o frame Ethernet II.

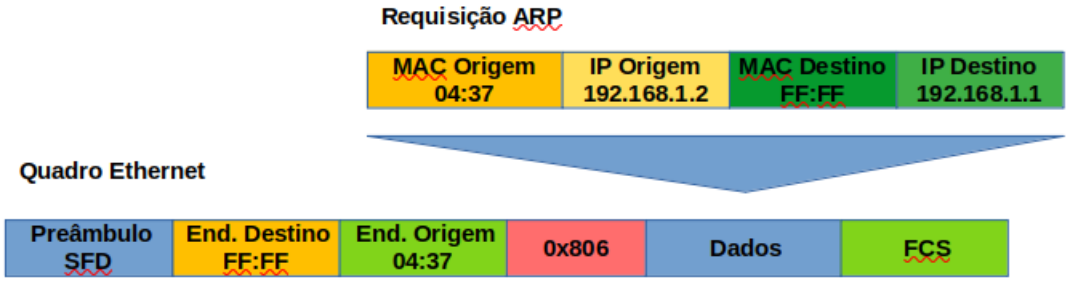



Fig. 6 - Requisição ARP

No Quadro Ethernet podemos observar os seguintes dados:

- Endereço MAC de destino - Como é uma mensagem de broadcast o endereço MAC de destino é sempre **FF:FF:FF:FF:FF:FF**, exigindo que todas as NICs Ethernet na rede, aceitem e processem a requisição..
- Endereço MAC de origem - Este é o endereço MAC do remetente da solicitação ARP.
- Tipo - As mensagens ARP têm um campo de tipo 0x806. Ele informa à NIC de recebimento que a parte de dados do quadro precisa ser transferida para o processo ARP.

No pacote ARP temos as seguintes informações:

- O Mac de origem da mensagem(o mesmo do quadro Ethernet).
- O IP do host de origem.
- O MAC de destino vazio(Preenchido com zeros).
- O IP do host de destino.

### 5.2.2. Resposta ARP

Apenas o dispositivo com o endereço IPv4 de destino igual ao da requisição ARP poderá responder à Requisição ARP. A resposta ARP é encapsulada em um quadro Ethernet usando conforme mostrado na figura 7 utilizando o frame Ethernet II.

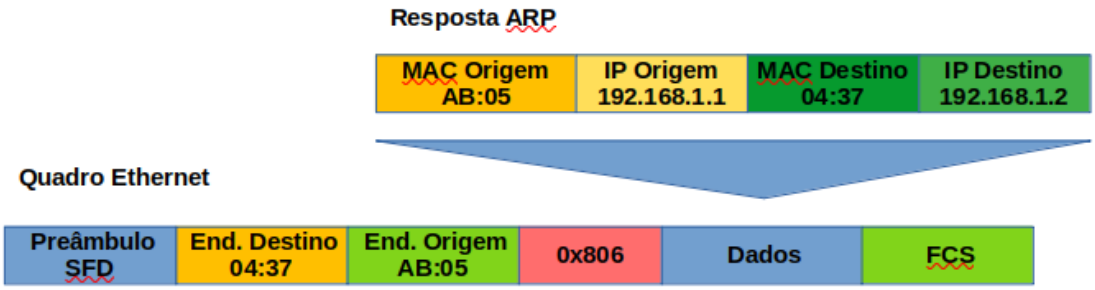



Fig. 7 - Resposta ARP

No Quadro Ethernet podemos observar os seguintes dados:

- Endereço MAC de destino - Este é o endereço MAC do remetente da solicitação ARP.
- Endereço MAC de origem - Este é o endereço MAC do remetente da resposta ARP.
- Tipo - As respostas ARP têm o mesmo campo de tipo 0x806 das requisições.

Na mensagem ARP de resposta temos

- Mac de origem - MAC do remetente da resposta ARP. (idêntico ao quadro Ethernet)
- IP de origem - IP do host do remetente da resposta ARP.
- MAC de destino - MAC do host que enviou a requisição ARP.
- IP de destino - IP do host que enviou a requisição ARP.

Apenas o dispositivo que enviou originalmente uma requisição ARP receberá a resposta ARP unicast, adicionando o endereço IPv4 e o endereço MAC correspondente na sua tabela ARP.

**Destaque**: As entradas na tabela ARP têm carimbo de data/hora (timestamp). Se um dispositivo não receber um quadro de um dispositivo específico antes que o carimbo de data / hora expire, a entrada desse dispositivo será removida da tabela ARP. Além disso, entradas estáticas podem ser inseridas na tabela ARP, estas entradas estáticas não expiram com o tempo e devem ser removidas manualmente.

**Pratique**: Abra o prompt de comando do seu PC e digite arp -a para mostrar a tabela tabela arp do seu PC. A saída deverá parecer com a mostrada na figura 8.

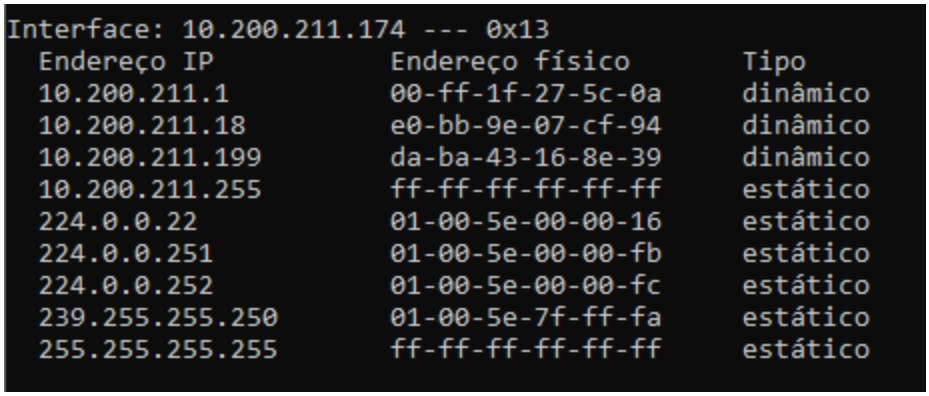


Fig. 8 - Saída do comando arp -a

Para adicionar uma entrada estática na tabela digite arp -s <ip do host> <MAC do host>, e para deletar uma entrada utilize arp -d. Para maiores informações utilize arp /help.

## 5.3. Protocolo ICMP

Você sabe que o protocolo IP é responsável pelo encaminhamento das mensagens da do host de origem até o destino, mas sabe também que a camada de rede tem como uma de suas funções o controle de congestionamento e a construção e manutenção das tabelas de rota. Para que isso seja feito existe o protocolo ICMP, responsável pela troca de mensagens entre hosts e dispositivos de rede. O ICMP está disponível tanto para IPv4 como para IPv6, mas para este inclui funcionalidades adicionais.

### 5.3.1. Mensagens comuns ICMPv4 e ICMPv6

As principais mensagens ICMP comuns ao ICMPv4 e ICMPv6 estão associadas a conectividade entre hosts, destino ou serviço inalcançável ou tempo de pacote excedido.

#### 5.3.1.1. Conectividade de host

Uma mensagem eco ICMP pode ser usada para testar a conectividade entre hosts em uma rede IP. O host local envia uma solicitação de eco ICMP (ICMP Echo Request) para um host e se o host estiver disponível, enviará uma resposta de eco (Echo Reply).

**Pratique**: Utilize o utilitário ping para testar a conectividade para o seu gateway padrão. Em primeiro lugar utilize o utilitário ***ipconfig*** para saber qual o endereço IP do seu gateway padrão, em seguida digite o comando ***ping*** <end. IP do gateway>. A saída deve parecer com a da figura 9.

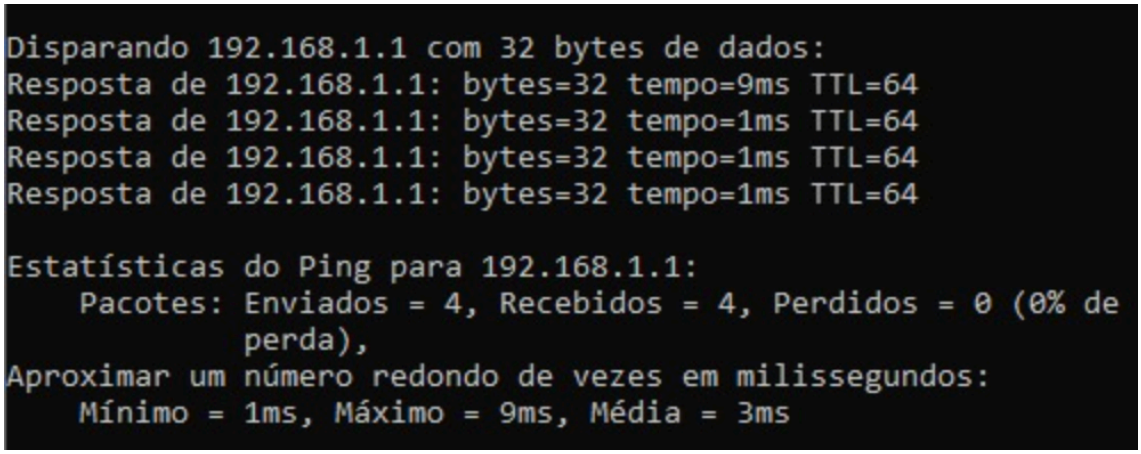


Fig. 9 - Saída do comando ping Fonte: o autor

#### 5.3.1.2. Destino inalcançável

Quando um host ou um roteador não pode entregar um pacote IP, usa uma mensagem ICMP de destino inalcançável para notificar a origem. A mensagem conterá um código que indica por que não foi possível entregar o pacote.

Os principais códigos para o ICMPv4 são:

- 0 = rede inalcançável
- 1 = host inalcançável
- 2 = protocolo inalcançável
- 3 = porta inalcançável

Já para o ICMPv6 os principais códigos são:

- 0 - Nenhuma rota para o destino
- 1 - A comunicação com o destino é proibida (por exemplo,bloqueada por um firewall)
- 2 - Além do escopo do endereço de origem
- 3 - Endereço inacessível
- 4 - porta inalcançável

#### 5.3.1.3. Tempo excedido

Quando um pacote IP é enviado da sua origem nele é configurado um campo (TTL para o IPv4 e Limite de saltos para o IPv6) que indica seu tempo de vida em número de saltos. Sempre que um roteador encaminha o pacote IP, decrementa de 1 esse valor. Se este valor chega a zero o roteador descarta o pacote e envia uma mensagem de tempo excedido para o host de origem.

**Pratique**: Utilize o utilitário ***tracert*** para obter o caminho e os tempos entre os saltos (roteadores) entre dois pontos. Gite o comando ***tracert*** www.grancursosonline.com.br a saída deverá parecer com a figura 10.

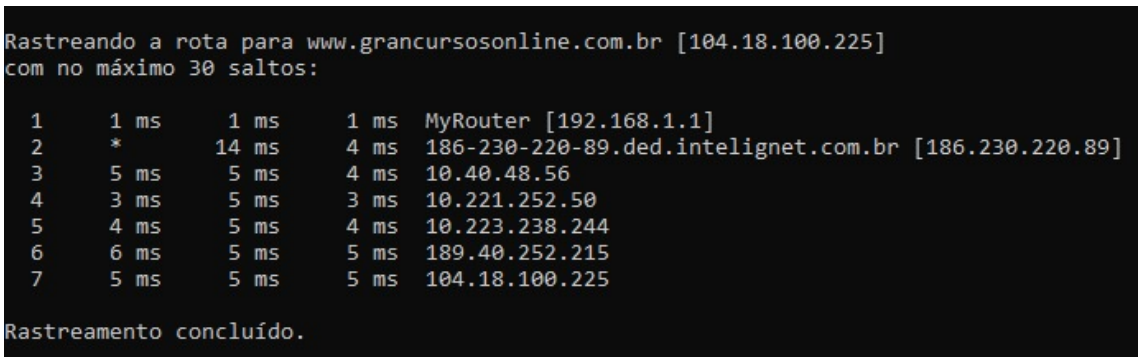


Fig. 10 - Saída do comando tracert Fonte: o autor

### 5.3.2. Mensagens ICMPv6

O ICMPv6 traz novas funcionalidades e novos recursos que não são encontrados no ICMPv4. Isso inclui mensagens relacionadas ao protocolo ND ou NDP (Neighbor Discovery Protocol).

- **Mensagem RS** - Enviada por um host que inicia na rede para obter informações de endereçamento.

- **Mensagem RA** - São enviadas pelos roteadores a cada 200 segundos, ou em resposta a uma mensagem RS, para fornecer informações de endereçamento para hosts IPv6 com informações de endereçamento, como o prefixo da rede, e seu comprimento, endereço DNS e nome de domínio. Um host que usa a Configuração Automática de Endereço sem Estado (SLAAC) definirá seu gateway padrão para o endereço local do link do roteador que enviou o RA.

- **Mensagem NS** - Enviada por um host IPv6 para verificar se seu endereço IP é idêntico (duplicado) a algum outro host

- **Mensagem NA** - Enviada em resposta a uma mensagem NS caso haja duplicação de endereço IPv6

**Destaque**: As mensagens ICMPv6 também são utilizadas para resolução de endereços MAC, estabelecimento e manutenção de rotas.