DlteC do Brasil®
www.dltec.com.br
info@dltec.com.br | 41 3045.7810

DLTEC DO BRASIL

PROTOCOLO IPV4 E CLASSES

Protocolo IPv4 e Classes

O conteúdo dessa apostila é uma adaptação da matéria online do Curso Protocolo IPv4 e Classes.

Para mais informação visite www.dltec.com.br

Seja muito bem-vindo(a) ao curso Curso Protocolo IPv4 e Classes, o qual é uma continuação do curso sobre o protocolo TCP/IP.

Nesse curso você aprenderá mais sobre a operação do protocolo IPv4, assim como o funcionamento dos protocolos ICMP, ARP e RARP.

Aproveite muito bem o material, pois é com uma base sólida que os verdadeiros profissionais conseguem se diferenciar e chegar mais longe!

Lembre-se que o conteúdo é vasto, mas DlteC estará com você em todos os momentos dessa jornada!

Bons estudos!

Introdução

Olá!

Seja bem vindo ao **Curso Protocolo IPv4 e Classes**.

Nesse curso vamos nos aprofundar no estudo do TCP/IP focando no endereçamento IPv4, assim como nos protocolos ICMP, ARP e RARP para entender melhor a operação da camada de Internet.

O foco desse curso são as classes de endereçamento IP e o uso dessas classes sem a divisão em sub-redes, conhecido como Roteamento Classful.

Esperamos que você aproveite ao máximo este material, que foi idealizado com o intuito verdadeiro de fazê-lo(a) um verdadeiro profissional da Infra de TI!

Estamos torcendo pelo seu sucesso!

Bons estudos!

Curso Protocolo IPv4 e Classes/IP

Objetivos

Ao final desse curso você deverá ter conhecimentos sobre:

- Explicar o formato do cabeçalho IPv4 e seus campos.
- Entender funciona o sistema de numeração binário.
- Realizar a conversão binário-decimal e decimal-binário.
- Como os endereços IPv4 são divididos nas classes:
  - Classe A
  - Classe B
  - Classe C
  - Classe D
  - Classe E
- Explicar a relação entre as classes de IPv4 e a Internet
- Entender o conceito de máscara de rede e prefixo de rede
- Realizar a análise quantitativa de redes e hosts em cada uma das classes de endereço IP
- Saber como identificar as porções de rede e host dado um endereço IP e máscara de rede
- Saber identificar as faixas de endereço de uso especial, tais como RFC 1918 e endereços de loopback
- Saber como endereçar uma rede IPv4 utilizando o conceito de roteamento Classful
- Explicar como operam os protocolos:
  - ICMP
  - ARP
  - RARP

Sumário

1 Introdução ao Curso

Bem-vindo ao **Curso Protocolo IPv4 e Classes**!

O **Curso Protocolo Ipv4 e Classes** possui como objetivo fornecer ao aluno conhecimento sobre o endereçamento IPv4, como as classes são divididas, endereços especiais e a operação do protocolo IPv4 através dos protocolos ICMP, ARP e RARP.

Ao final do curso, você deverá ser capaz de:

- Explicar o formato do cabeçalho IPv4 e seus campos.
- Entender funciona o sistema de numeração binário.
- Realizar a conversão binário-decimal e decimal-binário.
- Como os endereços IPv4 são divididos nas classes:
  - Classe A
  - Classe B
  - Classe C
  - Classe D
  - Classe E
- Explicar a relação entre as classes de IPv4 e a Internet
- Entender o conceito de máscara de rede e prefixo de rede
- Realizar a análise quantitativa de redes e hosts em cada uma das classes de endereço IP
- Saber como identificar as porções de rede e host dado um endereço IP e máscara de rede
- Saber identificar as faixas de endereço de uso especial, tais como RFC 1918 e endereços de loopback
- Saber como endereçar uma rede IPv4 utilizando o conceito de roteamento Classful
- Explicar como operam os protocolos:
  - ICMP
  - ARP
  - RARP

Não esqueça que ao final do curso você poderá emitir o seu certificado!

1.1 Como Estudar com o Material da DlteC do Brasil

Nesse curso você terá **vídeo aulas** e **material de leitura** para o aprendizado do conteúdo.

Posso somente ler ou assistir aos vídeos? NÃO RECOMENDAMOS!

O ideal é você assistir aos vídeos e na sequência ler os conteúdos ou...

... se preferir leia os conteúdos e depois assistia aos vídeos, tanto faz.

POR QUE LER E ASSISTIR?

Simples, porque **um conteúdo complementa o outro**. Principalmente se você está se preparando para a prova de certificação é crucial que você tanto veja os vídeos como a matéria de leitura!

2 Revisão do Formato e Cabeçalho do Protocolo IPv4

Abaixo segue o cabeçalho do protocolo IP versão 4 e logo abaixo a descrição dos campos.

+	0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Versão	Tamanho do cabeçalho	*Tipo de Serviço* (ToS) (agora DiffServ e ECN)	Comprimento (pacote)	
32	Identificador			*Flags*	*Offset*
64	*Tempo de Vida* (TTL)		Protocolo	*Checksum*	
96	Endereço origem				
128	Endereço destino				
160	Opções				
192	*Dados*				

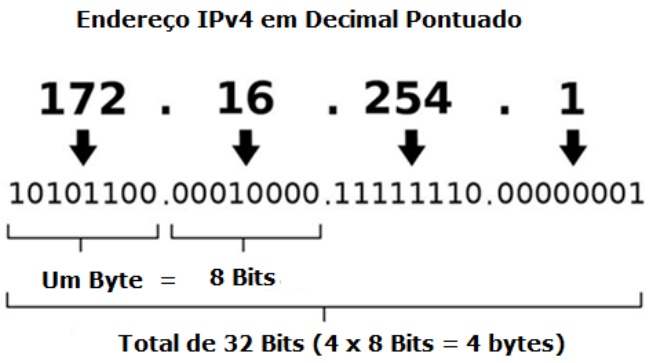
- **Versão (version)**: Definido como 4.
- **IHL (header length)**: Comprimento do Cabeçalho da Internet com o número de palavras de 32 bits no cabeçalho IPv4.
- **Tipo de serviço**: Definido na RFC 791 e define o tipo de serviço (ToS – Type of Service), agora DiffServ e ECN utilizados para definir marcação de QoS.

- **Tamanho total (total length)**: Define todo o tamanho do datagrama incluindo cabeçalho e dados. O tamanho mínimo do datagrama ou pacote IP é de vinte bytes e o máximo é 64 Kbytes, porém o MTU mínimo que os hosts precisam suportar é de 576 bytes. Se os pacotes ultrapassarem o MTU precisam ser "fragmentados", ou seja, quebrados em pedaços menores para caberem dentro do tamanho máximo do protocolo do caminho. No IPv4 a fragmentação pode ser feita pelos computadores ou diretamente nos roteadores.
- **Identificador (identifier)**: Usado principalmente para identificar fragmentos do pacote IP original.
- **Flags**: Usado para controlar ou identificar fragmentos.
- **Offset do fragmento**: permite que um receptor determine o local de um fragmento em particular no datagrama IP original.
- **Tempo de vida**: Chamado de TTL (time to live) ajuda a prevenir que os pacotes IP entrem em loop na rede. Utilizado para o teste de traceroute.
- **Protocolo (protocol)**: Define o protocolo que será transportado no pacote, sendo que os protocolos comuns e os seus valores decimais incluem o ICMP (1) e o TCP (6).
- **Checksum**: Campo de verificação de erros para o cabeçalho do datagrama IPv4. Cobre apenas verificação do cabeçalho, não dos dados.
- **Endereço de origem (source)/destino (destination)**: Campos que trazem os endereços de origem (transmissor) e de destino (receptor) de 32 bits cada um. Os endereços IP têm seus campos divididos em 4 conjuntos de 8 bits, ou seja, 4 bytes escritos em decimal pontuado, por exemplo, 192.168.1.1.
- **Opções (options)**: Normalmente não utilizados.
- **Dados (data ou payload)**: Informações das camadas superiores, por exemplo, segmentos TCP ou datagramas UDP.

Sem dúvida alguma os campos de endereçamento de origem e destino são os mais importantes do cabeçalho IP, pois eles que fornecem o endereçamento lógico utilizado para transporte do pacote através da rede.

Lembre-se que o quadro de camada-2 é trocado durante a viagem do IP pela rede conforme o protocolo utilizado pelo link local, já o pacote IP é aberto somente pelo destino da transmissão.

Abaixo segue como um endereço IP é escrito em decimal pontuado e depois em bits.



Com 32 bits temos um total de 2^32 bits ou 4.294.967.296 de possíveis endereços IP. Portanto, o primeiro endereço IP versão 4 possível tem todos os bits em zero e o último todos os bits em 1:

- 1º endereço IP: 00000000.00000000.00000000.00000000 -> 0.0.0.0
- Último endereço IP: 11111111.11111111.11111111.11111111 -> 255.255.255.255

A faixa de variação dos endereços entre o primeiro 0.0.0.0 e o último 255.255.255.255 corresponde a todo espaço de endereçamento IPv4 disponível.

Essa faixa foi dividida no início em classes (A, B, C, D e E) para possibilitar a divisão dos endereços entre instituições e empresas para possibilitar o endereçamento dos computadores na Internet. As classes A, B e C são as faixas de endereços utilizadas para endereçar hosts e navegar nas Intranets e Internet. Nessas classes temos endereços de Unicast e Broadcast.

A classe D é reservada para a comunicação em Multicast, sendo que a classe E é reservada.

Atualmente a Internet não segue mais o padrão de classes, pois ela é "Classless", ou seja, a divisão dos endereços não depende mais desse padrão de classes, seguindo um padrão chamado CIDR ou "Classless Inter-Domain Routing".

3 Sistemas de Numeração

Vamos iniciar com o tópico "Matemática para Redes de Computadores", onde iremos rapidamente abordar os seguintes assuntos:

- Sistema de Numeração Decimal.
- Sistema de Numeração Binário.
- Sistema Hexadecimal (apenas em vídeo).

3.1.1 Sistema Decimal

Os sistemas numéricos consistem em símbolos e regras para a utilização destes símbolos. O sistema numérico mais frequentemente utilizado é o sistema numérico Base 10 ou decimal.
Um sistema dito de base 10 significa que são utilizados dez símbolos para sua representação (0, 1, 2, 3, 4, 5, 6, 7, 8 e 9). Estes símbolos podem ser combinados para representar todos os valores numéricos possíveis.

O sistema numérico decimal é baseado em potências de 10. Cada posição colunar de um valor, da direita para a esquerda, é multiplicada pelo número 10, que é o número base, elevado a uma potência, que é o expoente.

A potência à qual é elevado o valor 10 depende da sua posição à esquerda do ponto decimal. Quando um número decimal é lido da direita para a esquerda, a primeira posição, ou a mais à direita representa 10 elevado por 0 (1), a segunda posição representa 10 elevado por 1 (10 x 1 = 10). A terceira posição representa 10 elevado por 2 (10 x 10 = 100). A sétima posição à esquerda representa 10 elevado por 6 (10 x 10 x 10 x 10 x 10 x 10 = 1,000,000). Esta é a verdade independentemente de quantas colunas sejam ocupadas pelo número.

Sistema de Numeração Base 10
Símbolos: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

1	3	4	5
10^3	10^2	10^1	10^0

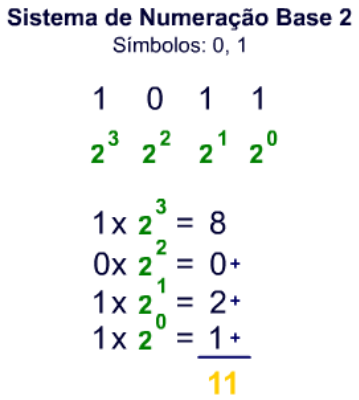
$1 \times 10^3 = 1000$
$3 \times 10^2 = +300$
$4 \times 10^1 = +\ 40$
$5 \times 10^0 = +\ 5$
1345

3.1.2 Sistema Binário

Os computadores reconhecem e processam dados, utilizando-se o sistema binário ou Base 2. O sistema binário utiliza dois símbolos, 0 e 1, em vez dos dez símbolos utilizados no sistema numérico decimal.

A posição, ou casa, de cada algarismo da direita para a esquerda em um número binário representa 2, o número base, elevado a uma potência ou expoente, começando com 0.

Exemplo: 1011 base 2 = (1 x 2 elevado por 3 = 8) + (0 x 2 elevado por 2 = 0) + (1 x 2 elevado por 1 = 2) + (1 x 2 elevado por 0 = 1) = 11 (8 + 0 + 2 + 1).



Observação: Os computadores foram concebidos para utilizarem grupos de oito bits. Este grupo de oito bits é denominado byte. Em um computador, um byte representa um único local de armazenamento endereçável. Estes locais de armazenamento representam um valor ou um único caractere de dados, por exemplo, um código ASCII.

O número total de combinações de oito chaves ou bits ligadas ou desligadas é de 256. Já a faixa de valores de um byte é de 0 a 255. Veja abaixo como é o crescimento em binário da sequência entre 0 e 255:

```
00000000 -> 0
00000001 -> 1
00000010 -> 2
00000011 -> 3
00000100 -> 4
00000101 -> 5
00000110 -> 6
00000111 -> 7
00001000 -> 8
00001001 -> 9
00001010 -> 10
00001011 -> 11
00001100 -> 12
00001101 -> 13
00001110 -> 14
00001111 -> 15
00010000 -> 16
...
11111100 -> 252
11111101 -> 253
11111110 -> 254
11111111 -> 255
```

Os valores em binário dentro de um byte crescem da esquerda para direita somando-se um a cada passo. Por esse motivo cada campo do endereço IP pode ir apenas de 0 a 255, não existe IP 1.1.1.256, por exemplo, pois o valor do quarto byte não é possível com apenas 8 bits!

Outra dica interessante é que os números pares têm o último bit sempre em zero e os ímpares em 1, note na sequência mostrada anteriormente esse fato.

É importante entender o conceito do byte ao trabalhar com computadores e redes.

3.1.3 Conversão Binária

Vamos ver agora um pouco de como realizar conversão de sistemas numéricos começando pela conversão decimal-binário e na sequência veremos a conversão binário-decimal.

Conversão Decimal-Binário
Existem várias maneiras de realizar a conversão de decimal para binário, vamos mostrar nesse tópico um método simples de comparar o número decimal que queremos converter em binário com os valores de cada bit. A dica é verificar se o número decimal é maior ou menor que cada bit e ir subtraindo antes de passar ao próximo caso ele seja maior. Veja abaixo os valores em decimal de cada bit em um octeto (byte):

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

Sempre comece comparando o decimal a ser convertido com o valor do bit mais significativo (**128**). Veja o exemplo prático a seguir para converter o número decimal 168 em número binário de oito bits utilizando esse método:

- 128 cabe dentro de 168? Sim. Portanto, o bit mais à esquerda do número binário é um.
- Agora fazemos a diferença 168 – 128 = 40.
- 64 cabe dentro de 40? Não cabe. Portanto, o segundo bit da esquerda é zero.
- 32 cabe dentro de 40? Sim. Portanto, o terceiro bit da esquerda é um.
- Agora subtraímos 40 – 32 = 8.
- 16 cabe dentro de 8? Não cabe. Portanto, o segundo bit da esquerda é zero.
- 8 cabe dentro de 8? Sim. Portanto, o quinto bit da esquerda é um.
- Agora subtraímos 8 – 8 = 0. Como o resto foi zero todos os bits à direita serão zero, mesmo assim vamos continuar a análise até o final.
- 4 cabe dentro de 0? Não cabe. Portanto o sexto bit é zero.
- 2 cabe dentro de 0? Não cabe. Portanto o sétimo bit é zero.
- 1 cabe dentro de 0? Não cabe. Portanto o oitavo bit mais à esquerda também é zero.
- Resultado: 10101000 = 168 decimal

Conversão Binário-Decimal:
Os números binários podem ser convertidos em números decimais, multiplicando os dígitos binários pelo número base do sistema, o qual é Base 2, e elevando-os ao expoente da sua posição.

Exemplo: Para converter o número binário 01110000 em um número decimal fazemos o seguinte:
0 x 2 elevado a 0 = 0
0 x 2 elevado a 1 = 0
0 x 2 elevado a 2 = 0
0 x 2 elevado a 3 = 0
1 x 2 elevado a 4 = 16
1 x 2 elevado a 5 = 32
1 x 2 elevado a 6 = 64
0 x 2 elevado a 7 = 0

Agora é só somar o valor dos bits e temos o resultado: 0+0+0+0+16+32+64+0 = 112

Lembre-se que as provas da Cisco não permitem uso de calculadora, por isso é importante que você entenda bem as conversões em binário e interpretar números Hexadecimais (estudados no IPv6).

4 Endereçamento IP e a Internet

No início da Internet não era prevista essa taxa de adesão tanto de empresas como do setor público em geral, por isso os IP utilizados para endereçar as redes foram divididos em três classes de tamanhos fixos chamadas: **classes A, B e C**.

- **Classe A**: varia de 1.0.0.0 a 127.0.0.0, onde o primeiro octeto (os primeiros 8 bits) do endereço IP identifica a rede e os 3 octetos restantes (24 bits) identificarão o host específico da rede.
- **Classe B**: tem um conjunto de endereços que varia de 128.0.0.0 a 191.255.0.0. Os primeiros dois octetos (16 bits) do endereço IP identificam a rede e os dois octetos restantes (16 bits) identificarão o host.
- **Classe C**: varia de 192.0.0.0 a 223.255.255.0, sendo que os primeiros três octetos (24 bits) do endereço IP identificam a rede e os octetos restantes (8 bits) identificarão o host específico da rede.

Além dessas três classes, existem mais duas classes que são utilizadas para Multicast (**Classe D** – redes de 224.x.x.x a 239.x.x.x) e reservada para fins especiais pela IANA (**Classe E** – redes a partir de 240.x.x.x).

Essas classes foram baseadas na premissa que teríamos na Internet poucas redes de grande porte (126 redes com mais de 16 milhões de hosts cada uma), as quais estão na classe A, uma quantidade maior de redes de médio porte (aproximadamente 16 mil redes com mais de 65 mil hosts cada uma) que ficariam dentro da classe B e uma quantidade muito maior de redes de pequeno porte que ficariam dentro da classe C (aproximadamente 2 milhões de redes com apenas 254 hosts cada uma).

Para termos uma ideia de como a alocação de IPs foi realizada nos primórdios da Internet as faixas classe A foram distribuídas entre grandes instituições como AT&T, IBM, Xerox, HP, Apple, MIT, Ford, dentre outras. É isso mesmo que você está pensando uma empresa apenas com uma classe A inteira, ou seja, mais de **dezesseis milhões de hosts**!

Outras duas classes foram definidas além das citadas anteriormente, a classe D dedicada a serviços de Multicast e a classe E reservada para estudos e pesquisas.

O roteamento com base em classes é chamado de **Classful**.

Com o crescimento da Internet esse tipo de classificação e distribuição de IPs passou a não ser mais eficiente, pois as classes acabaram ficando muito limitadas em termos de tamanho de rede e flexibilidade.

Atualmente o mundo está vivendo uma fase em que os endereços IP versão 4 disponíveis estão com seus dias contados e já foi dado o início à implementação do IP versão 6, porém como os dois ainda irão conviver por muito tempo temos que saber sobre as duas versões.

Alguns outros fatos históricos interessantes sobre o crescimento da Internet:

- Em 1990 já existiam 313.000 hosts conectados à Internet.
- Em maio de 1992 38% das faixas de endereços classe A, 43% da classe B e 2% da classe C já estavam alocados, sendo que a rede já possuía 1.136.000 hosts conectados.
- Em 1993, com a criação do protocolo HTTP e a liberação por parte do Governo estadunidense para a utilização comercial da Internet, a quantidade de hosts na Internet passou de 2.056.000 em 1993 para mais de 26.000.000 em 1997.
- Em 2012 a ISC (Internet System Consortium) estimou que existissem até o mês de julho de 2012 aproximadamente **908.585.739** hosts na Internet.

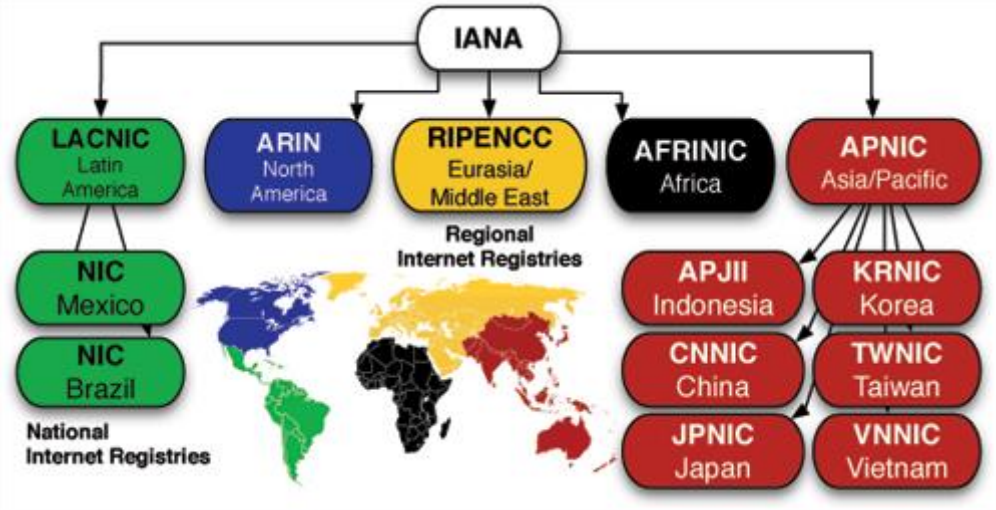
Em novembro de 1991 é formado o grupo de trabalho ROAD (Routing and Addressing) para atuar sobre o problema da escassez de endereços IP versão 4, o qual apresenta como solução a estes problemas a utilização do **CIDR** (**Classless Inter-domain Routing**). Basicamente o CIDR tem como ideia central o **fim do uso das classes de endereços**, por isso o nome **classless** ou "**sem classess**", possibilitando a alocação de blocos de tamanho apropriado conforme a real necessidade de cada rede na Internet.

Outras duas técnicas foram desenvolvidas para desacelerar o esgotamento de IPs válidos da Internet foi a introdução dos **endereços IP privados** (RFC 1918 – Private Addresses) e o uso do **NAT** (Network Address Translation).

Private Addresses		
Class	**RFC 1918 Internal Address Range**	**CIDR Prefix**
A	10.0.0.0–10.255.255.255	10.0.0.0/8
B	172.16.0.0–172.31.255.255	172.16.0.0/12
C	192.168.0.0–192.168.255.255	192.168.0.0/16

Mundialmente quem administra os IPs é a entidade chamada **IANA** (Internet Assigned Numbers Authority), a qual repassa as responsabilidades de alocação em cada região do mundo para outras cinco entidades, sendo que para a América Latina a **LACNIC** é a responsável.

No Brasil a LACNIC delegou a administração dos endereços IP para o **Registro BR** (http://registro.br), nesse link você pode registrar domínios, solicitar endereços IPs e verificar a disponibilidade de domínios. Veja na figura abaixo um organograma das entidades que administram a alocação de IPs ao redor do mundo.



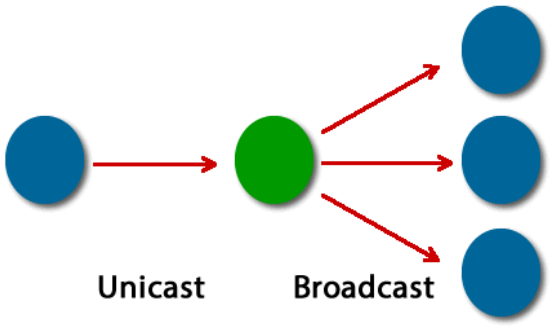
5 Tipos de Comunicação Suportada pelo Protocolo IPv4

Conforme vimos anteriormente os endereços IP foram divididos em classes, sendo que nas **Classes A, B e C** temos os endereços utilizados pelos computadores para que eles possam se comunicar em rede, chamados de endereços de **Unicast**.

Além disso, nessas três classes de IP temos também os endereços de **Broadcast**, utilizados para comunicação com **todos os hosts** de uma rede.

Portanto, a comunicação **Unicast** é realizada de **um para um**, ou seja, **host a host**, já a comunicação em **broadcast** é de **um para todos**, ou seja, quando um pacote é endereçado no destino para um endereço de broadcast **todos os hosts** daquela rede **irão receber e processar** aquele pacote IP.

Veja a figura ao lado.



Em uma rede IP o primeiro endereço representa a própria rede para o roteamento e **não pode ser utilizado para endereçar hosts**. Este endereço recebe o nome de "**endereço de rede**" ou "**endereço de subrede**" e é utilizado para criar "**rotas**" para as redes IP.

Os endereços de Unicast vão do segundo ao penúltimo IP de cada rede ou sub-rede, por exemplo, na rede classe C 192.168.1.0 os endereços de Unicast vão de 192.168.1.1 até 192.168.1.254, pois o endereço 192.168.1.0 é o endereço de rede e o último IP 192.168.1.255 é o endereço de broadcast dessa rede.

Os endereços de Unicast são chamados de **endereços de Host** (**hosts válidos** ou **IPs válidos**) e podem ser **utilizados para endereçar os hosts ou interfaces de rede**, já os **endereços de rede e broadcast NÃO podem ser utilizados para endereçar os hosts** ou interfaces dos roteadores.

O endereço de broadcast que representa **todos os IPs** (de qualquer classe) é o endereço IP **255.255.255.255**, porém cada rede ou sub-rede IP tem também um endereço de broadcast que representa todos os IPs daquela rede ou sub-rede específica, o qual é o **último IP de cada rede ou subrede**.

Por exemplo, na rede classe C 192.168.1.0 o IP 192.168.1.255 é o broadcast direcionado dessa rede, o que significa se você fizer um "ping 192.168.1.255" todos os IPs dessa rede irão responder, ou seja, os computadores configurados com IPs de 192.168.1.1 até 192.168.1.254.

Normalmente esse teste proposto acima não deve funcionar, pois ele permite um tipo de ataque chamado de Smurf e por isso normalmente o ping para endereços de broadcast não são respondidos por muitos sistemas operacionais.

Os **broadcasts direcionados** a uma sub-rede específica, ou seja, para o **último IP** de uma rede ou sub-rede, por padrão não são encaminhados entre interfaces de um roteador, porém esse comportamento pode ser alterado via configuração (consulte o fabricante).

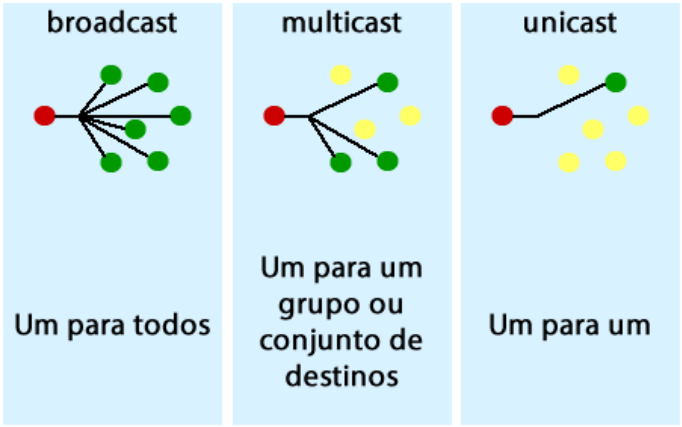
Essa função normalmente vem por padrão desabilitado.

Já uma mensagem de broadcast para o endereço **255.255.255.255** nunca será encaminhado pelas interfaces, mesmo com a configuração citada anteriormente.

Na camada-2, o endereço MAC de um IP de broadcast é ffff.ffff.ffff, já o MAC de Unicast é o enderço gravado na placa ou interface de rede do host.

Já os endereços de **Classe D** são utilizados para a comunicação Multicast, a qual é uma comunicação de **um para um grupo**, ou seja, utilizada para **comunicação em um grupo** de elementos que possuem o **mesmo endereço de Multicast**.

Veja a figura abaixo com a diferença entre os três tipos de comunicação.



Por exemplo, quando um roteador é configurado com o EIGRP como protocolo de roteamento, as informações de roteamento trocadas entre os roteadores são feitas utilizando o **multicasting**.

Os roteadores que estão rodando o EIGRP recebem o endereço IP classe D 224.0.0.10 e se um roteador em uma rede LAN enviar uma mensagem de roteamento e houver mais roteadores OSPF todos receberão essa mensagem, porém diferente do broadcast somente os roteadores com o IP 224.0.0.10 irão processar essa informação.

Note que todos os roteadores EIGRP enviam e recebem informações de roteamento pelo mesmo endereço classe D 224.0.0.10, por isso o termo "**grupo de multicast**".

No Unicast precisamos ter um IP de origem e outro de destino **únicos** na rede, já no broadcast temos um endereço de origem do host que está enviando o pacote e o destino será 255.255.255.255 ou um dos endereços de broadcast direcionados de uma rede, por exemplo, 192.168.1.255.

Os endereços MAC de quadros de multicast normalmente iniciam com "01-00-5E" em comunicações IPv4.

6 Classes de Endereços IPv4: A, B, C, D e E

Ao todo foram definidas cinco classes de endereços IP, ou seja, classes A, B, C, D e E.

Veja a figura abaixo com as classes e como identificá-las.

O que caracteriza cada classe é o primeiro octeto do endereço IP, sendo que para a Classe A ele sempre inicia em zero, para a Classe B inicia em 10, para a Classe C em 110, na Classe D em 1110 e finalmente para a Classe E em 1111.

Aqui temos o primeiro uso da conversão de decimal para binário, se você enfrentar uma pergunta querendo saber a classe de um endereço IP é só converter o primeiro octeto em binário e seguir a regra estudada anteriormente!

Na figura também podemos tirar uma importante informação sobre quantas redes e endereços de host que as classes A, B e C podem fornecer.

Note que para a classe A temos o primeiro octeto para rede e os demais para host, na B temos dois octetos para rede e dois para host e na classe C são três para rede e um para host, o que nos fornece a máscara de rede padrão de cada uma das classes:

- **Classe A** -> Rede.Host.Host.Host = 255.0.0.0
- **Classe B** -> Rede.Rede.Host.Host = 255.255.0.0
- **Classe C** -> Rede.Rede.Rede.Host = 255.255.255.0

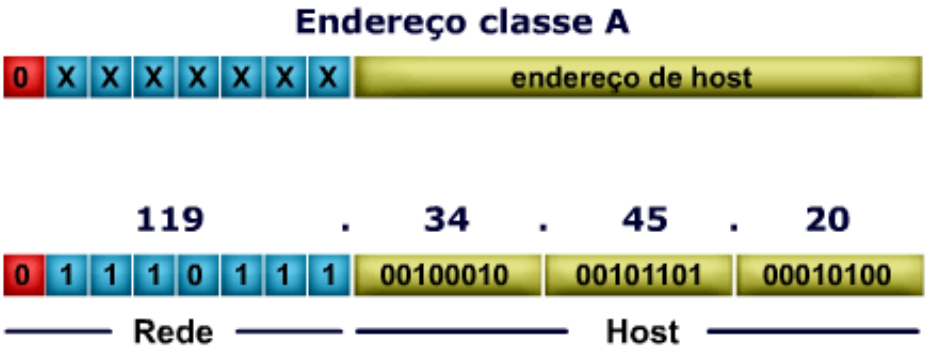
As classes D e E não utilizam o conceito de rede e host, elas utilizam somente endereçamento de host, por isso não possuem máscara de rede.

Portanto, a faixa de endereços de Internet não vai de 0.0.0.0 a 255.255.255.255, ela está limitada aos endereços das classes A, B e C.

Agora vamos estudar cada uma das classes com mais detalhes.

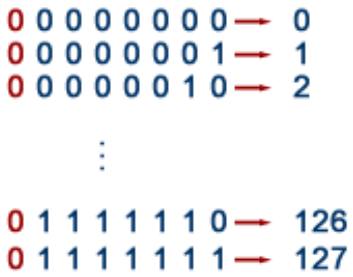
6.1 Endereço IP Classe A

Os endereços da classe A sempre terão o primeiro bit do primeiro octeto igual a 0 (0xxxxxxx), veja figura abaixo ilustrando o endereço.



Ao lado segue a variação completa do primeiro octeto que representa as redes da classe A.

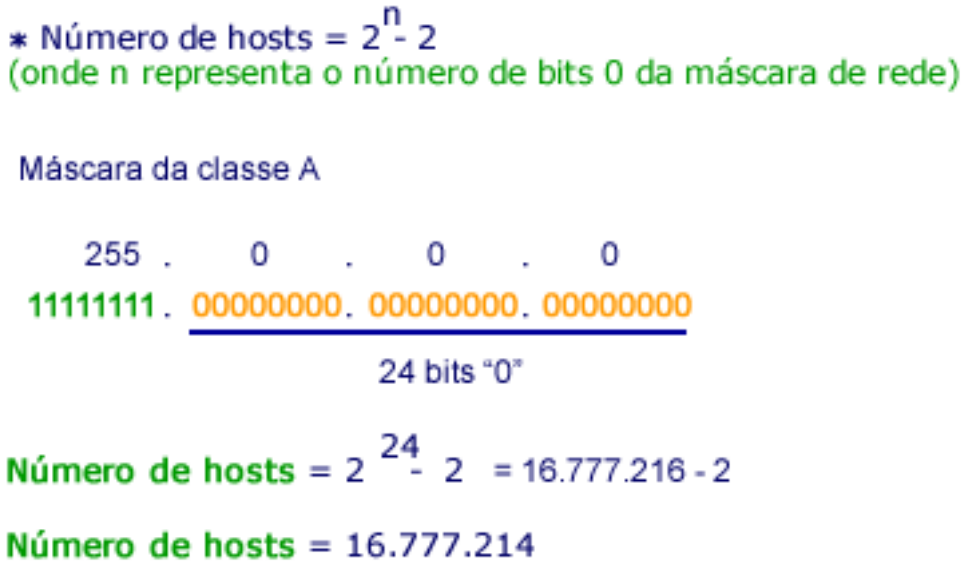
Note que o primeiro bit nunca será diferente de "0". Uma dica interessante para descobrir em que classe o endereço IP está situado é converter o primeiro octeto em binário e verificar os primeiros bits.



Os endereços de classe A pertencem das redes **1.0.0.0** até a **126.0.0.0**. As redes 0.0.0.0 (Internet) e 127.0.0.0 (127.0.0.0) são de uso especial e não podem ser utilizadas para endereçar redes, conforme já estudamos anteriormente.

A máscara de rede padrão de uma classe A é **255.0.0.0**. Outra forma de representar uma máscara de rede é utilizando a notação decimal, onde a máscara será representada pela quantidade de bits "1" nela contidos, para a classe A o prefixo é "/8".

Para determinar a quantidade de hosts que uma classe possui, ou seja, o número de computadores que ela pode endereçar utiliza-se a fórmula abaixo:

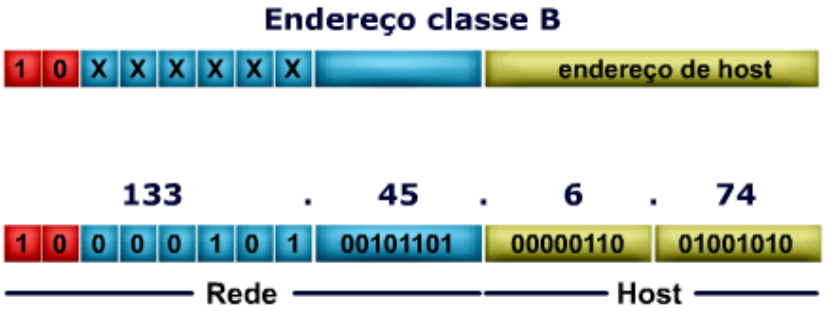


Note que na fórmula diminuímos dois endereços IPs do total, isso porque o primeiro representa a própria rede e o último representa o endereço de broadcast, e ambos não podem ser utilizados para endereçar computadores.

As **126** redes da classe A possuem endereços suficientes para endereçar até **16.777.214** hosts (computadores) cada uma.

6.2 Endereço IP Classe B

Os endereços da classe B sempre terão os dois primeiros bits do primeiro octeto igual a 10 (10xxxxxx), veja ilustração abaixo.



Abaixo segue a variação completa dos dois primeiros octetos que representam as redes da classe B.

Conforme mostrado acima, as redes classe B variam de 128.0.0.0 até 191.255.0.0, sendo que a máscara de rede padrão de uma classe B é 255.255.0.0 ou /16.

O número de redes classe B é o número de bits 1 que podem variar na máscara elevado a dois, ou seja, como temos 16 bits de rede e dois deles são fixos (**10**xxxxxx.xxxxxxxx) temos 2^14 endereços de classe B o que dão **16.384 redes**.

Para determinar a quantidade de hosts que uma classe possui, ou seja, o número de computadores que ela pode endereçar utiliza-se a fórmula abaixo (mesma conta utilizada para a classe A):

* Número de hosts = $2^n - 2$
(onde n representa o número de bits 0 da máscara de rede)

Máscara da classe B

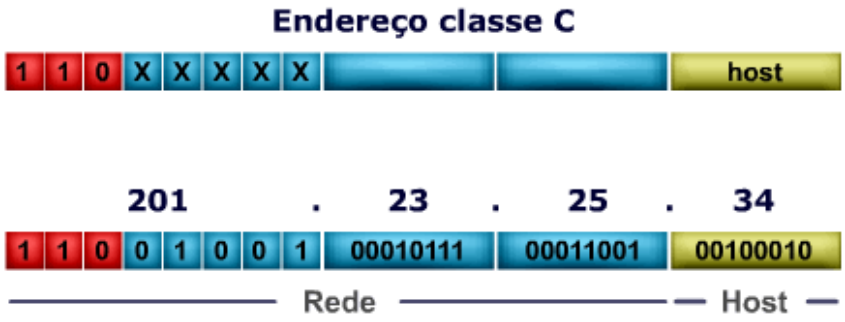
255 . 255 . 0 . 0
11111111 . 11111111 . 00000000 . 00000000
16 bits "0"

Número de hosts = $2^{16} - 2$ = 65.536 - 2
Número de hosts = 65.534

Portando a classe B possui endereços suficientes para endereçar **16.384 redes** diferentes com até **65.534 hosts** (estações) cada uma.

6.3 Endereço IP Classe C e RFC 1918

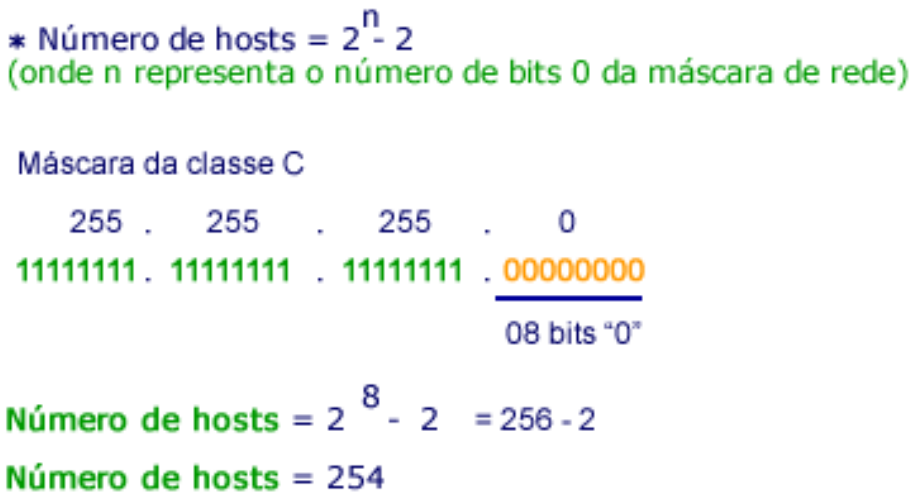
Os endereços da classe C sempre terão os três primeiros bits do primeiro octeto igual a 110 (110xxxxx), conforme figura abaixo.



As redes classe C variam de 192.0.0.0 (**110**00000.00000000.00000000.00000000) até a 223.255.255.0 (**110**11111.11111111.11111111.00000000), sendo que a máscara de rede padrão de uma classe C é 255.255.255.0 ou /24.

O número de redes classe C segue o mesmo princípio que utilizamos para a classe B, ou seja, temos 24 bits de host com os três primeiros do primeiro octeto fixos em "110", portanto podemos ter 2^21 (24-3) redes classe C, ou seja, um total de **2.097.152 redes**.

Para determinar a quantidade de hosts que uma classe possui, ou seja, o número de computadores que ela pode endereçar utiliza-se a mesma fórmula das classes A e B (***o cálculo de host nunca varia!***):



Portando a classe C possui endereços suficientes para endereçar **2.097.152** redes diferentes com até **254** hosts cada uma.

Além disso, temos diversas faixas de endereços reservados em cada uma das classes A, B e C.

A mais conhecida é a **RFC 1918** que define endereços para uso privativo, ou seja, para criação de Intranets, evitando o uso de endereços válidos para Internet em ambientes corporativos.

Abaixo seguem as faixas de endereços privados:

- **Classe A**: de 10.0.0.0 até 10.255.255.255
- **Classe B**: de 172.16.0.0 até 172.31.255.255
- **Classe C**: de 192.168.0.0 até 192.168.255.255

Os endereços começados em zero também não são utilizados para endereçar computadores, pois a rede 0.0.0.0 com a máscara 0.0.0.0 representa a Internet.

Outra faixa reservada é a 127.0.0.0 a 127.255.255.255, a qual representa a faixa de loopback utilizada pelos computadores para endereçar a própria interface de rede.

Se você pingar o endereço 127.0.0.1 no Windows, Linux ou MAC OS-X deve receber 100% de retorno, pois você está pingando sua própria placa de rede, portanto se ela não responder você está com sérios problemas.

Outra faixa de endereço reservada e não utilizada na Internet é a iniciada em 169.254.0.0 com a máscara 255.255.0.0, esses endereços são reservados para o **Zeroconf**, uma autoconfiguração da placa de rede quando o computador não encontra um servidor DHCP na rede.

Se você entrar com um ipconfig no Windows ou ifconfig no Linux e verificar um endereço na faixa de 169.254.0.1 a 169.254.255.254 é sinal de que sua placa de rede são encontrou um servidor DHCP para fornecer os dados necessários para seu correto funcionamento.

6.4 Endereço IP Classes D e E

Os endereços da classe D são utilizados para **multicasting** e variam dos Ips 224.0.0.0 até 239.255.255.255. Os demais IPs pertencem à classe E, à qual é reservada para testes e estudos.

7 Hosts, Redes e Máscara de Rede

Como já estudamos, um endereço IP é representado por um número binário de 32 bits, divididos em quatro conjuntos de oito bits, chamados de octetos ou bytes.

Todo endereço IP é dividido em duas partes, sendo que a inicial identifica a rede e a final é o endereço do host de rede, chamado também de Host-ID (Host Identification ou identificação do host).

A melhor analogia para entender o endereçamento IP é o endereçamento postal, onde para encontrar um destino você necessita do nome da rua e do número da casa, ou seja, o endereço de rede seria o nome da rua e o endereço de host o número da casa.

Portanto a principal função do endereçamento IP é **identificar um dispositivo** (micro, roteador, servidor, etc.) **dentro de uma rede**, a qual é um conjunto de computadores.

Quem delimita a porção de rede e de host em um endereço IP é a **máscara de rede** também chamada de **máscara de sub-rede**.

Na realidade **não existe endereço IP sem uma máscara de rede**.

A máscara de rede também é representada por 32 bits, sendo que os bits "0" representam a porção de host e os bits "1" a de rede.

A máscara sempre inicia com uma sequência de bits 1 e depois têm uma sequência de zeros, nunca veremos bits um e zero intercalados, isso porque o que é rede é rede, não existe uma rede-host para o endereçamento IP.

Por exemplo, uma máscara 11111111.00000000.00000000.00000000 = 255.0.0.0 é válida, já a máscara 11111110.00000000.00000000.11111111 = 254.0.0.255 não é válida.

Usando a mesma máscara acima, se tivermos o endereço IP 1.2.3.4 com a máscara 255.0.0.0 podemos tirar que a porção de rede desse endereço é "**1**" e o host-ID "**.2.3.4**".

A rede que um endereço IP pertence pode ser definida com uma conta binária chamada AND lógico entre o endereço e sua máscara.

No AND lógico qualquer número AND zero é zero e um AND um é igual a um, portanto se fizermos o cálculo teremos:

- 1.2.3.4 AND 255.0.0.0
- 00000001.00000010.00000011.00000100 AND
  11111111.00000000.00000000.00000000
- 00000001.00000000.00000000.00000000 = 1.0.0.0

Portanto a rede que o IP 1.2.3.4 pertence é 1.0.0.0 com a máscara 255.0.0.0.

Podemos também representar o IP e máscara através da notação de prefixo de rede com a máscara não em decimal, mas representada por uma barra (/) mais o número de bits um nela contidos.

Por exemplo, a rede calculada acima pode ser escrita 1.0.0.0/8, porque na máscara 255.0.0.0 temos oito bits um.

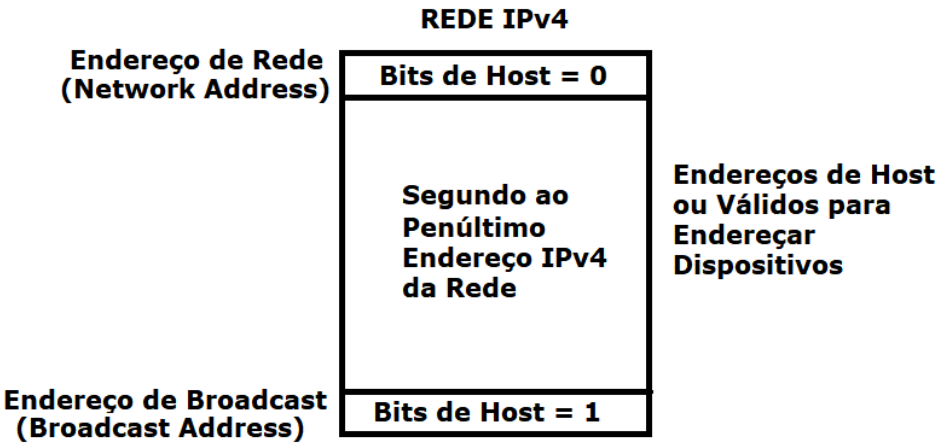
Observação: Lembre-se que um endereço IP identifica não uma máquina, mas **uma conexão à rede**.

Máquinas com mais de uma interface de rede (roteadores, por exemplo) possuem um endereço IP para cada interface.

Até mesmo um computador pode possuir vários endereços IP.

Lembre-se que uma rede IPv4 é dividida entre:

- **Endereço de rede**, onde todos os bits de host da máscara são iguais a zero. Ele é o primeiro endereço IPv4 de uma rede ou sub-rede.
- **Endereço de broadcast**, onde todos os endereços de host da máscara são iguais a "um". Ele é o último endereço IPv4 de uma rede ou sub-rede.
- **Endereços de hosts** ou **endereço de Unicast** (endereços válidos para endereçar dispositivos de rede) que estão na faixa entre o endereço de rede e o endereço de broadcast. Endereços que vão do segundo ao penúltimo IPv4 da rede ou sub-rede.



Lembre-se que os bits de Host são os os bits "zero" na máscara de rede ou sub-rede, já a rede ou sub-rede é indicada pelos bits "uns" (1) na máscara ou prefixo.

8 Introdução ao Planejamento de Redes IPv4

Primeiro vamos pensar em quem devemos endereçar em uma Rede IP? Que dispositivos precisam de endereços?

A resposta está abaixo:

- Interfaces L3 de roteadores e switches L3 (Portas roteadas e SVIs ou Switched Virtual Interfaces – interfaces virtuais em switches L3)
- Interfaces de gerenciamento em switches L2 e APs (Access Points)
- Placas de Rede dos Endpoints (Computadores, Servidores/VMs, Telefones IP, Câmeras IP, Dispositivos Móveis, Impressoras...)

Portanto, cada domínio de broadcast em uma rede IPv4, seja ela uma rede LAN, WAN ou uma VLAN (LAN Virtual criada em switches) necessita de uma rede IPv4 exclusiva.

Lembre-se que os endereços em uma rede IPv4, ou até mesmo em redes IPv6, deve ser único naquela rede!

Existem várias áreas, setores, unidades dentro de uma empresa e cada uma pode ter requisitos e características diferentes, por isso mesmo é comum a divisão dessas redes, ou seja, separar redes IP para diferentes usos e usuários.

Cada domínio de broadcast em uma rede IPv4 precisa de uma rede exclusiva como boa prática, por isso mesmo você precisa planejar sua rede e saber como e quem precisa de endereçamento.

Na prática um endereço IP versão 4 possui 32 bits e é dividido em quatro "**octetos**", ou seja, quatro conjuntos de oito bits e escritos em formato decimal. O que define que parte do endereço é rede ou host é a "**máscara de rede**" ou "**máscara de sub-rede**".

Por exemplo, se tivermos o endereço **192.168.10.65** e não dermos mais nenhuma característica não seria nada mais que um número qualquer, pois se não pudéssemos dividir os endereços IPs em redes não teríamos uma "**hierarquia**" e não poderíamos dividir as redes entre as diversas empresas e corporações.

Tenha em mente que a "**rede IP**" representa um **conjunto de endereços**, assim como no endereçamento postal de um país se não tivéssemos os Estados, Cidades, Ruas e números das casas não conseguiríamos enviar cartas.

Imagine se tivéssemos apenas o País Brasil e você deseja enviar uma carta para uma pessoa, como seria possível encontrar o João da Silva que tem seu endereço "Brasil"?

Precisamos de uma hierarquia, ou seja, vamos mandar uma carta para o Sr João da Silva, que mora no Brasil, na cidade de São Paulo, na rua tal, número tal apartamento 100, agora sim faz sentido concorda?

A mesma coisa acontece com as redes IP, para que possamos encontrar um host, que é relativo a uma pessoa ou casa no endereçamento postal, precisamos saber onde ele está e isso quem nos diz é a rede ou sub-rede IP e quem nos mostra isso é a máscara de rede ou de sub-rede.

Vamos completar agora o endereço 192.168.10.65 com a máscara padrão de um endereço de **classe C** que é o **255.255.255.0**.

Veja que cada octeto da máscara corresponde ao octeto do endereço, portanto onde temos o bit um na máscara indica que o número que está no endereço IP representa uma rede, convertendo a máscara em binário temos 11111111.11111111.11111111.**00000000**, ou seja, os três primeiros octetos representam a rede e o último octeto o host.

Isso significa que temos um conjunto de micros dentro da rede 192.168.10 e o que procuramos é o que tem o final 65.

Na prática uma rede é quando **todos os bits de host estão zerados**, portanto representamos a rede que o host final 65 pertence como: 192.168.10.**0**, pois é no último octeto que estão os bits de host.

Os Hosts, ou seja, os endereços que posso configurar em um computador, laptop, impressora, switch ou interface de um roteador vão do primeiro IP após o endereço de rede até o penúltimo número da sequência (um antes do broadcast).

Lembrem-se endereços de host são também chamados de endereços de **Unicast**, para utilização de comunicação entre dois terminais apenas, já o último valor representa o **broadcast direcionado** daquela rede, ou seja, se enviarmos um ping para o último valor da sequência de IPs de uma rede todos os hosts que estiverem ativos dessa rede deveriam responder.

Colocamos a palavra "**deveriam**" porque essa ação pode ser bloqueada em algumas redes por questões de segurança.

Vamos então entender o que é uma rede IP finalizando a análise do endereço 192.168.10.65 com a máscara 255.255.255.0.

Já sabemos que sua rede é o 192.168.10.0, que o broadcast é o último valor da sequência (quando todos os bits de host estão em um) e os hosts válidos estão entre a rede e o broadcast, portanto teremos:

- **Rede**: 192.168.10.0 (192.168.10.**00000000** - quando todos os bits de host estão zerados).
- **Broadcast (último valor)**: 192.168.10.255 (192.168.10.**11111111** -> o último valor é quando todos os bits de host estão setados em um).
- **Endereços que podemos utilizar nos hosts**: 192.168.10.1 (192.168.1.**00000001** - o próximo após a rede) até 192.168.10.254 (192.168.10.**11111110** - um a menos que o broadcast).

Portanto essa é a definição de uma rede IP, ou seja, ela possui um **endereço de rede** (todos os bits de host estão zerados), os **hosts válidos** (um após a rede até um antes do broadcast) e um **endereço de broadcast** (todos os bits de host estão em 1 – último IP antes da próxima rede).

Lembre-se que outra maneira de encontrar a rede que um endereço pertence, a qual é utilizada pelos roteadores e computadores, é fazendo o **AND lógico** entre o IP e a máscara.

Um AND lógico é uma conta em binário que diz que qualquer valor AND zero dá zero e um AND um dá um. Vamos fazer a conta com o endereço 192.168.10.65 AND 255.255.255.0.

Onde temos 255 é tudo 1 e onde temos zero é tudo zero, ou seja, temos oito bits um no número 255 e oito bits zero no ponto zero. Fazendo o AND temos que:

- 192 AND 255 = 192
- 168 AND 255 = 168
- 10 AND 255 = 10
- 65 AND 0 = 0

Portanto a rede é a 192.168.10.0 com a máscara 255.255.255.0.

Outro ponto importante é a quantidade de redes e hosts por rede e como isso tudo pode ser calculado. Se você conhecer bem o binário conseguirá responder essa pergunta sozinho, senão vamos aprender ou revisar na sequência.

Quem dá a quantidade de redes ou hosts que teremos são quantos bits vamos utilizar para fazer as redes e hosts, ou seja, os **bits um** da máscara que podemos utilizar dão a quantidade de **redes** e os **bits zero** dão a quantidade de **hosts**.

Por exemplo, foi citado que uma classe C tem sempre os três primeiros bits fixos em "110" e como ela utiliza os três primeiros octetos para rede e somente o quarto octeto para host temos o seguinte cenário:

- 21 bits 1 (r - rede) para redes (24 menos 3 que são fixos) e 8 bits (h - hosts) para fazer os hosts.
- 110rrrrr.rrrrrrrr.rrrrrrrr.hhhhhhhh

Para calcular as redes basta você fazer dois (base do binário) elevado à quantidade de bits de rede que sobraram nesse caso 21, ou seja, 2^21 (dois elevado a vinte e um) será igual a 2.097.152 de redes classe C.

Já para os hosts temos um detalhe importantíssimo, pois o primeiro IP é utilizado para dar o endereço rede e o último o broadcast, portanto temos que descontar dois IPs da conta, por isso a fórmula para hosts são dois elevados ao número de bits zero da máscara menos dois, pois temos que descontar a rede e o broadcast que não são utilizados para endereçar hosts. No caso da classe C temos (2^8 – 2) = (256 – 2) = 254 IPs.

Seguindo o mesmo princípio, se tivermos que escolher redes Classe A e B o que variam são as quantidades de redes e hosts que temos por classe.

Por exemplo, se fossemos endereçar uma LAN com a rede 172.16.0.0 classe B, a qual tem a máscara padrão 255.255.0.0 ou o prefixo /16 temos as seguintes características:

- 172.16.0.0 é o endereço de rede, ou seja, quando todos os bits de host estão em zero.
- Como máscara é 255.255.0.0 temos os dois últimos octetos variando como host, pois ela é uma classe B (**10**rrrrrr.rrrrrrrr.hhhhhhhh.hhhhhhhh).
- O último endereço IP é o broadcast dessa rede (todos os bits de host estão em um), o qual será 172.16.11111111.11111111 ou 172.16.255.255.
- Tudo que está entre 172.16.0.0 e 172.16.255.255 você pode utilizar para endereçar hosts.
- Portanto temos os endereços válidos iniciando em 172.16.0.1 e o último 172.16.255.254 (um a menos que o broadcast).

Em termos quantitativos, para uma classe B temos 14 bits (pois os dois primeiros do primeiro octeto são sempre 10) de rede e 16 bits de host. O que nos dá 2^14 redes (16.384) e "2^16 – 2" endereços de host (65.534 hosts válidos).

Agora vamos a um exemplo com a classe A, endereçando uma LAN com a rede 10.0.0.0, a qual tem a máscara padrão 255.0.0.0 ou /8 temos as seguintes características:

- 10.0.0.0 é o endereço de rede, ou seja, quando todos os bits de host estão em zero.
- Como máscara é 255.0.0.0 temos os dois últimos octetos variando como host, pois ela é uma classe A (10rrrrrr.hhhhhhhh.hhhhhhhh.hhhhhhhh).
- O último endereço IP é o broadcast dessa rede (todos os bits de host estão em um), o qual será 10.11111111.11111111.11111111 ou 10.255.255.255.
- Tudo que está entre 10.0.0.0 e 10.255.255.255 você pode utilizar para endereçar hosts.
- Portanto temos os endereços válidos iniciando em 10.0.0.1 e o último 10.255.255.254 (um a menos que o broadcast).

Em termos quantitativos, para uma classe A temos 7 bits de rede (pois o primeiro octeto é sempre 0 na classe A) e 24 bits de host.

O que nos dá 2^7 redes (128) e "2^24 – 2" endereços de host (16.777.214 hosts válidos). Porém ao invés de termos 128 temos 126 redes na classe A, pois temos que descontar as redes iniciadas com zero (0.0.0.0) e com 127 (127.0.0.0).

Lembre-se que elas são redes especiais, sendo que a zero é reservada para representar todas as redes ou a Internet e a 127 é reservada para loopback.

Na prática cada rede LAN, VLAN ou WAN precisa de uma rede IP **própria e única**, portanto endereçar é atribuir uma rede a uma interface de um roteador ou a uma VLAN e distribuir os endereços de host para essas interfaces e demais terminais.

O que estudamos aqui são as **redes IP baseadas em classes** ou **Classful**.

Nesse curso não serão abordadas técnicas de divisão em sub-redes como VLSM ou CIDR, pois teremos um curso específico para tratar desses assuntos.

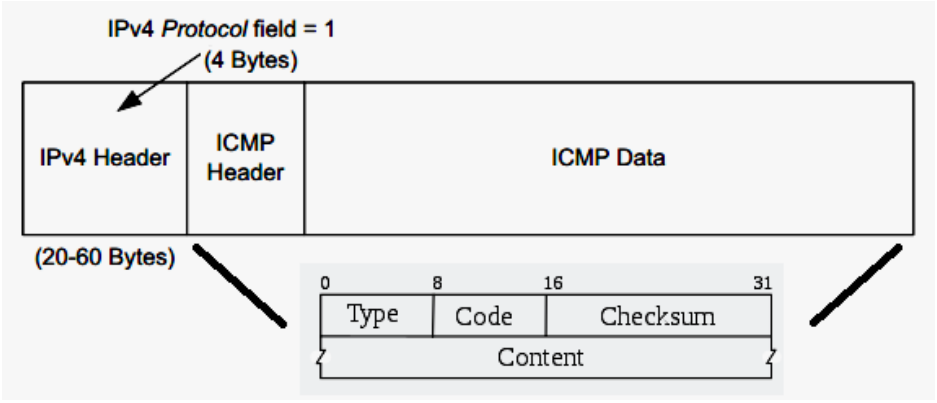
9 Protocolo ICMP

O **ICMP** ou **Internet Control Message Protocol** (em português, Protocolo de Mensagens de Controle da Internet) é um protocolo integrante do IPv4, definido pela RFC 792 e utilizado para fornecer relatórios de erros ao host que deu origem aos pacotes enviados na rede.

Qualquer computador que utilize IPv4 precisa aceitar as mensagens ICMP e alterar o seu comportamento de acordo com o erro relatado.

Os gateways (roteadores) devem estar programados para enviar mensagens ICMP quando receberem pacotes que provoquem algum tipo de erro.

O protocolo ICMP é encapsulado diretamente dentro de um pacote IP com o código de protocolo 1 (0x01), conforme imagem a seguir.



Abaixo segue uma descrição breve dos campos do protocolo ICMP:

- **Type** (Tipo da Mensagem - 8 bits): especifica o significado da mensagem e o formato do restante do pacote. Abaixo seguem os principais tipos de mensagens do ICMP:

    - **0 - Echo Reply**: utilizado no teste de ping como resposta a uma solicitação.
    - **3 - Destination Unreachable**: indica problemas de alcance a redes ou hosts remotos.
    - 4 - Source Quench: indica problemas com controle de fluxo e volume de dados enviado é muito grande.
    - 5 – Redirect: enviado pelo roteador inidicando um redirecionamento de rota ou rede.
    - **8 – Echo (request)**: utilizado para solicitar o ping, ou seja, mensagem enviada quando utilizamos o comando ping.
    - **11 - Time Exceeded**: Esta mensagem é enviada quando o tempo de vida de um datagrama é ultrapassado. Normalmente esse tempo de vida ou time to live é definido pelos sistemas operacionais.
    - 12 - Parameter Problem: Esta mensagem é enviada quando o campo de um cabeçalho está errado.
    - 13 – Timestamp (request): Uma máquina pede para outra a sua hora e a sua data do sistema (universal).
    - 14 - Timestamp Reply: resposta ao pedido de timespamp.
    - 15 - Information Request: Esta mensagem permite pedir à rede um endereço IP.
    - 16 - Information Reply: resposta ao information request.

Code (Código da mensagem - 8 bits): contém o código de erro para o datagrama, reportado pela mensagem ICMP. A interpretação desse campo depende do tipo da mensagem, portanto, cada tipo de mensagem pode conter vários códigos ou codes, os quais representam informações ou erros, por exemplo, veja abaixo os códigos que podem ser gerados para o tipo 3 de mensagem ICMP ou Destination Unreachable:

- 0 = net unreachable ou rede não está acessível
- 1 = host unreachable ou máquina não está acessível
- 2 = protocol unreachable ou protocolo não está acessível
- 3 = port unreachable ou porta não está acessível
- 4 = fragmentation needed and DF set ou fragmentação necessária
- 5 = source route failed ou o encaminhamento falhou

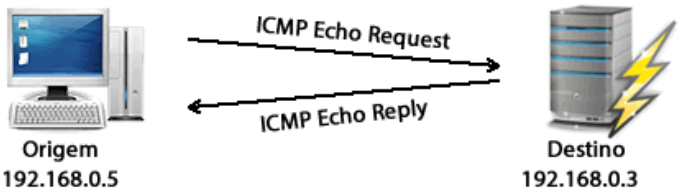
- **Checksum** (16 bits): é aplicado à toda mensagem, iniciando a partir do campo TYPE. O algoritmo é o mesmo usado pelo IP para cálculo do checksum do cabeçalho IP.
- **ICMP Data** (Dados ou Content – Conteúdo da mensagem): contém informações específicas da mensagem ICMP. Normalmente o conteúdo da mensagem é a descrição do código, por exemplo, em um teste de ping o gateway não consegue encontrar a rede de destino em sua tabela de roteamento. Ele enviará ao cliente que fez o ping uma mensagem de Destination Unreachble, com o código 0 e a mensagem "**rede não está acessível**".

A seguir vamos estudar os dois testes mais conhecidos em uma rede, os quais são implementados através de mensagens do ICMP: Ping e Traceroute.

9.1 Ping: Echo Request e Echo Reply

Como você já deve ter percebido, o ICMP fornece ferramentas comumente usadas para testes de rede como o Ping e Traceroute através das suas mensagens, tipos e códigos.

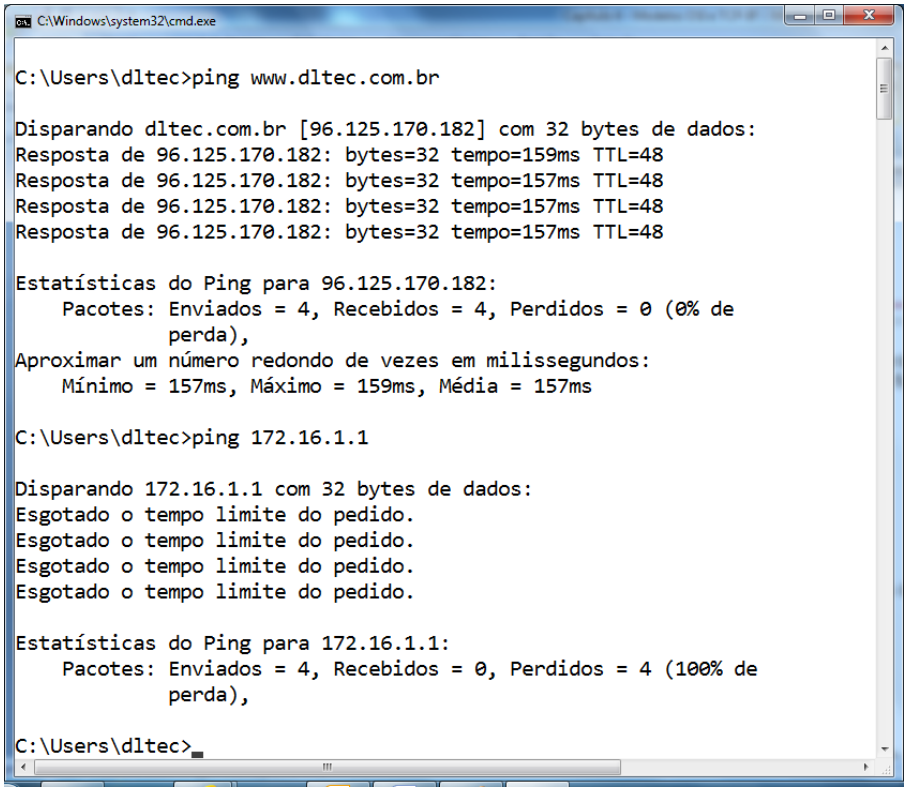
Por exemplo, o tão utilizado no dia a dia de qualquer profissional de redes "Ping" é baseado em duas mensagens, o echo request e echo reply.



Quando você entra no prompt de comandos do Windows, por exemplo, e digita "ping www.exemplo.com.br", na realidade seu computador está enviando mensagens de "echo request" ao servidor onde a página da Exemplo está hospedada e ao receber essa mensagem o servidor responde com um "echo reply".

Caso o servidor não responda seu computador mostrará um timeout (tempo de resposta expirado), indicando que não houve resposta.

Veja a tela a seguir com dois exemplos de ping, o primeiro obteve resposta (0% de perda) e o segundo não (100% de perda).



O teste de ping é utilizado para verificar se há comunicação fim a fim, ou seja, entre origem e destino, sem se importar com os dispositivos (roteadores e switches) que estão no meio do caminho.

Vale a pena lembrar que as mensagens de ping podem ser bloqueadas por firewalls e IPSs, portanto nem sempre não obter uma resposta a um ping significa necessariamente um erro, pode ser que esse teste esteja bloqueado por motivos de segurança.

9.2 Traceroute

Já o trace ou traceroute tem a função de testar o **caminho** que o pacote está seguindo até seu destino, ou seja, ele é um **teste ponto a ponto**.

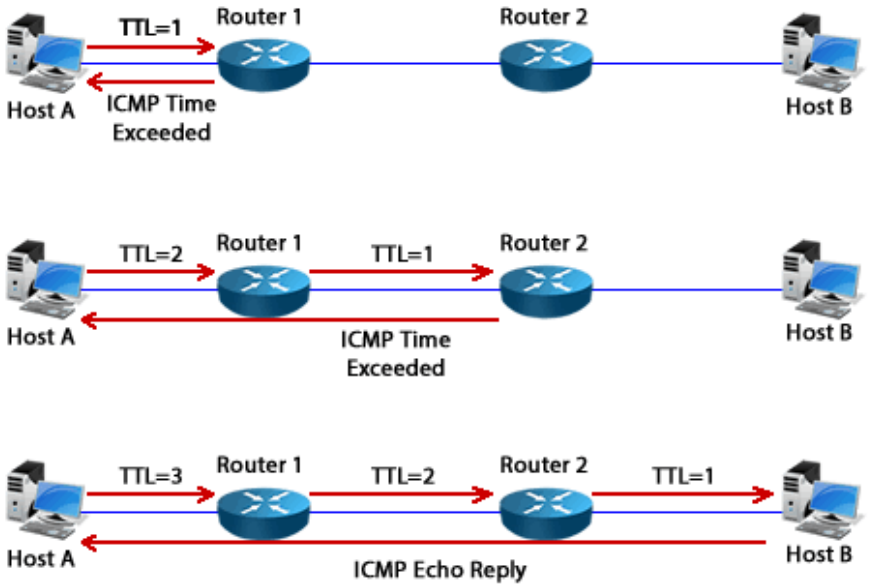
O trace está baseado no funcionamento do campo TTL do protocolo IP, pois quando um pacote IP tem seu tempo de vida expirado o roteador deve enviar uma mensagem ICMP à origem do pacote indicando esse problema com a mensagem tipo 11 ou "Time Exceeded", código (code) 0 informando a mensagem de "Tempo ultrapassado".

Nessa mensagem vem o IP do roteador e com isso o computador consegue saber por onde o pacote está passando, pois o endereço IP de destino é do dispositivo que encaminhou a mensagem de erro.

Resumindo, o host onde foi originado o trace manda um pacote com TTL igual a 1, no primeiro salto o pacote expira e o roteador responde.

Depois envia um pacote com TTL igual a 2, aí ele conhece o roteador que está no segundo salto, sendo que esse processo se repete até que o pacote atinja seu destino e o caminho é traçado.

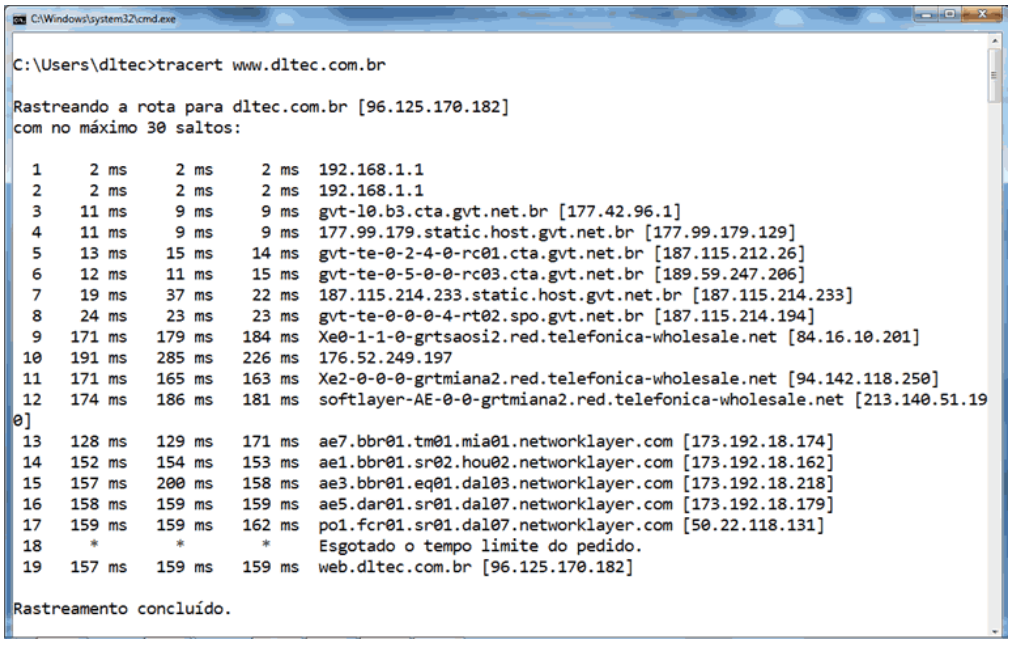
Veja a figura abaixo, onde o host de destino está a 3 saltos da origem.



Acompanhe na tela mostrada a seguir onde temos um exemplo do "tracert" que é o comando do Windows para o traceroute (Cisco e Linux).

Note que no décimo oitavo salto o computador não obteve resposta, pois provavelmente existe um bloqueio por motivos de segurança nesse roteador.

Para alcançar o destino nosso pacote teve que percorrer 19 saltos, ou seja, passou por 19 roteadores entre a origem e o destino.



10 Protocolos ARP e RARP

O **ARP** (Address Resolution Protocol – protocolo de resolução de endereços) e o **RARP** (Reverse Address Resolution Protocol – protocolo de resolução de endereços reverso) são dois protocolos utilizados para resolução de endereços físicos

Eles têm a função de mapear qual endereço físico está vinculado a um determinando endereço IP de um host remoto.

Isto é necessário em redes da família Ethernet para que o quadro de camada 2 possa ser montado e enviado localmente até seu destino ou então até o roteador que tem a saída para a rede de destino (que pode ser a Internet, por exemplo).

10.1 Protocolo ARP

Lembre-se que para que dois hosts se comuniquem, no quadro da camada 2 deve estar indicado os endereços MAC de origem e destino. Sem isso não tem como a rede local, por exemplo, um switch determinar para que porta ele deve encaminhar o quadro e também quando o quadro chegar ao destino este host não conseguiria saber que o quadro é para ele.

Veja a figura a seguir com o quadro da camada 2 genérico para a família Ethernet.

Protocolo Ethernet (Quadro)

Preâmbulo	Endereço de Destino	Endereço de Origem	Tipo	Dados	Sequência de Verificação do Quadro
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

Note que no segundo campo temos o MAC do destino (computador que vai receber os dados) e no terceiro campo do quadro o MAC de origem, ou seja, de quem está enviando os quadros.

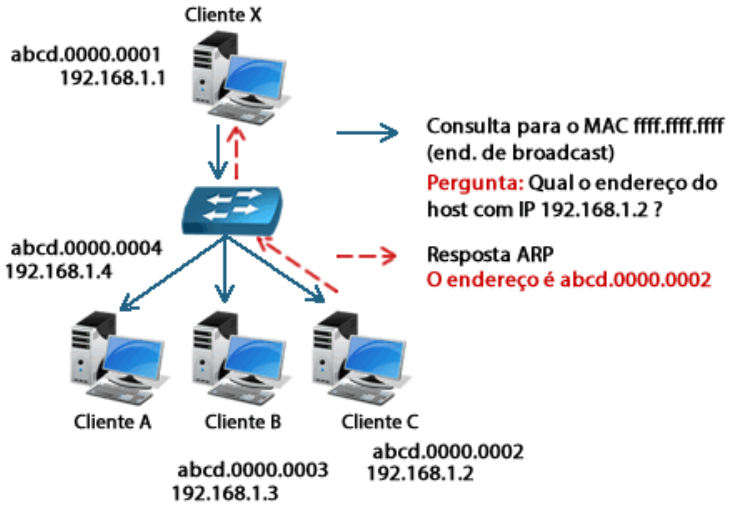
Quando a comunicação se dá entre dois computadores na mesma LAN, por exemplo, na sua casa você quer fazer um ping do seu computador para o computador de seu Pai ou Irmão, nesse caso eles estão na mesma rede que você e normalmente você sabe os endereços IP, portanto você digita "ping 192.168.1.2".

Com isso o seu computador tem o seu próprio IP, pois ele está configurado na placa de rede, seu endereço MAC que também está gravado na placa de rede, conhece o IP remoto, porque você o digitou e falta o endereço MAC do computador remoto.

É aí que entra o protocolo chamado ARP, pois ele envia uma requisição na rede em broadcast, ou seja, todos os micros da mesma rede irão receber essa requisição, solicitando o endereço MAC do IP que você digitou no ping.

Todos os micros recebem a requisição, mas quem responde é aquele que tem o IP 192.168.1.2. Ao receber a informação o computador de origem consegue montar o quadro e enviar as informações.

Acompanhe na figura a seguir a ilustração do funcionamento do protocolo ARP.



Logo abaixo da figura para ver como é o formato do quadro do ARP com a resposta do host com IP 192.168.1.2 informando seu MAC ao host de origem, note que a resposta do ARP é enviada diretamente para o solicitante, ou seja, não mais em broadcast e sim em unicast.

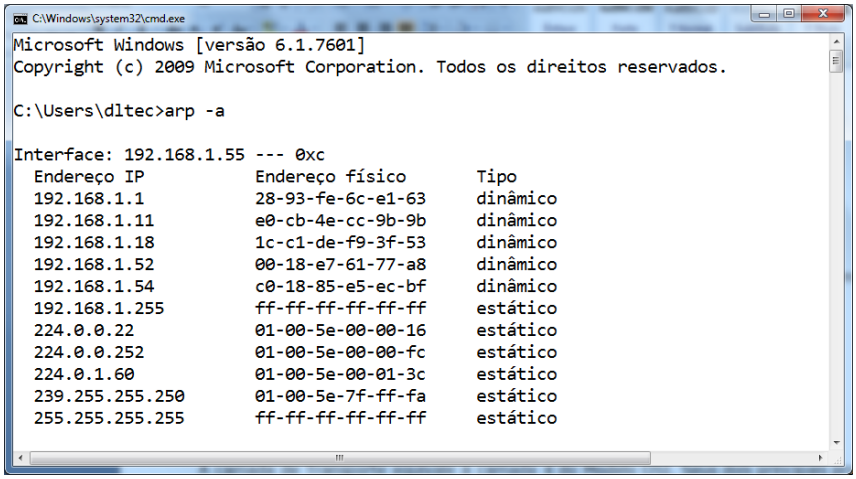
Na sequência você verá a figura com quadro já finalizado e que será enviado entre o host ClienteX e o ClienteC.

bits 0-7	bits 8-15	bits 16-31
Hardware Type (HTYPE) 0x0001 (ethernet)		Protocal Type (PTYPE) 0x0806 (ARP)
Hardware Length (HLEN) 0x06	Protocol Legth (PLEN) 0x04	Operation (OPER) 0x0002 (REPLY)
Sender Hardware Address (SHA) abcd.0000.0002		
Sender Protocol Address (SPA) 192.168.1.2		
Target Hardware Address (SHA) abcd.0000.0001		
Target Protocol Address (SPA) 192.168.1.1		

Quadro entre ClienteX e Cliente C

Preâmbulo	Endereço de Destino	Endereço de Origem	Tipo	Dados	Sequência de Verificação do Quadro
01010101 (x8)	abcd.0000.0002	abcd.0000.0001	0x0800	IP	CRC
8 bytes	6 bytes	6 bytes	2 bytes		4 bytes

No seu computador a tabela ARP pode ser visualizada abrindo o prompt de comando e digitando "arp –a".



Na tabela ARP ficam apenas os endereços MAC dos computadores que estão na mesma rede local e alguns endereços especiais que são configurados nos dispositivos, como os de broadcast (255.255.255.255 – ffff.ffff.ffff) e multicast (veremos no capítulo de endereçamento IP mais detalhes sobre a faixa de endereços IP).

Quando a comunicação é realizada com um host que não pertence à mesma LAN o roteador local entra em cena servindo de intermediário, pois como já vimos anteriormente é o roteador que conhece as rotas para demais redes.

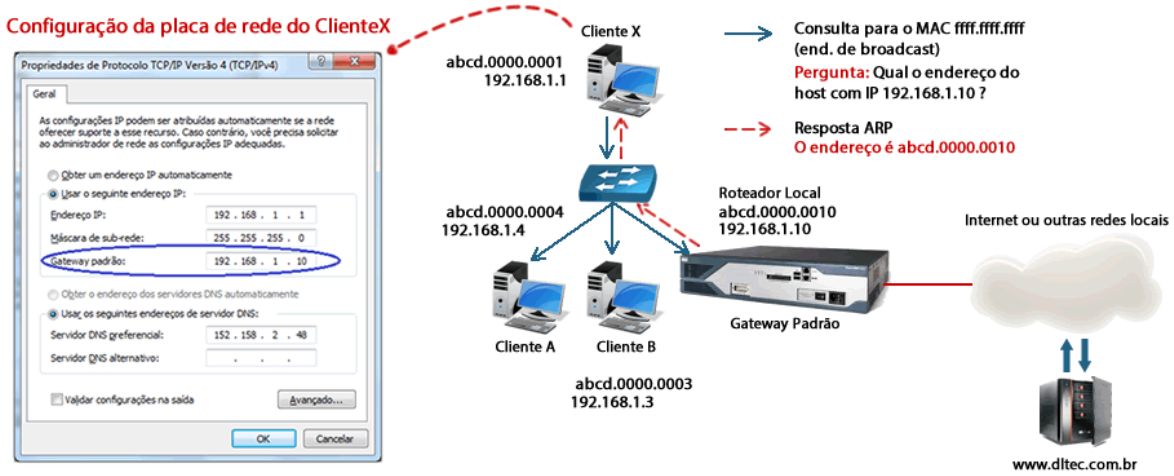
Nesse caso o computador que deseja enviar as informações para fora da rede consegue distinguir que o destino não pertence à mesma rede e envia uma requisição ARP solicitando o endereço MAC do roteador local, o qual está configurado em sua placa de rede como "roteador padrão" ou "gateway padrão".

Quando o roteador recebe a solicitação ele envia seu MAC ao solicitante e a partir daí serve como intermediário da comunicação.

Portanto, o quadro terá o MAC de origem do computador solicitante e o MAC de destino será o endereço do roteador local.

Porém, no protocolo IP, o endereço de destino não será o do roteador local, e sim o endereço IP do computador de destino, senão não haveria comunicação, pois o roteador não saberia para que interface encaminhar aquele pacote!

Veja a figura com a ilustração do funcionamento do ARP quando os hosts comunicantes estão em LANs distintas.



Mais para frente você verá que para o computador descobrir o IP do website www.dltec.com.br ele precisará utilizar primeiro o protocolo de resolução de nomes de Internet, chamado DNS.

10.2 Protocolo RARP

Já o Reverse Address Resolution Protocol (RARP) ou Protocolo de Resolução Reversa de Endereços associa um **endereço MAC conhecido a um endereço IP**.

Permite que os dispositivos de rede encapsulem os dados antes de enviá-los à rede. Um dispositivo de rede, como uma estação de trabalho sem disco, por exemplo, pode conhecer seu endereço MAC, mas não seu endereço IP.

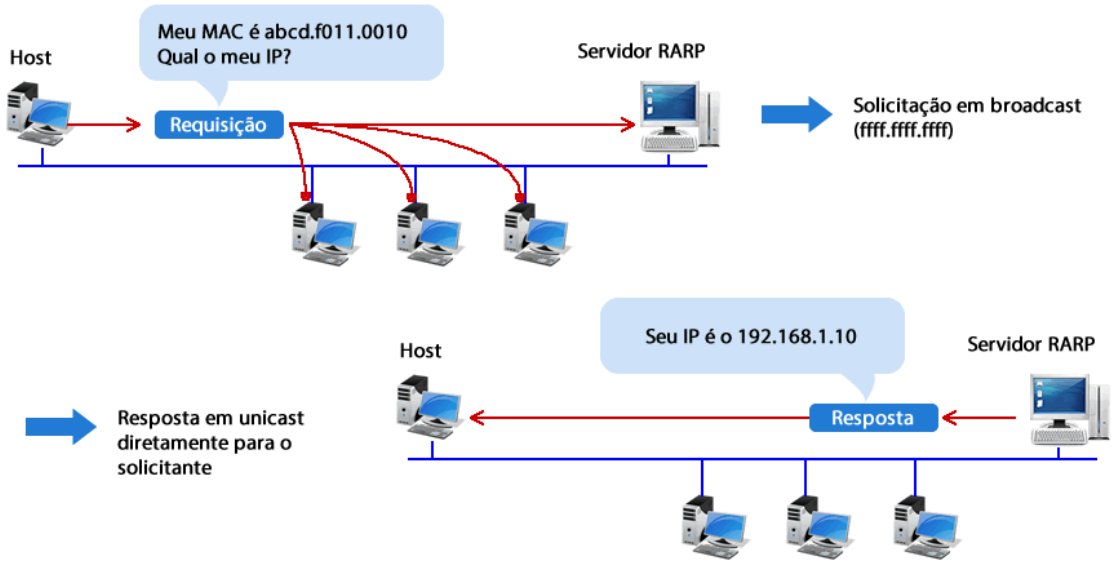
Além disso, o IPv4 pode utilizar na detecção de IPs duplicados através do protocolo ARP utilizando ARPs gratuitos ou "Gratuitous ARP" (GARP).

O RARP permite que o dispositivo faça uma solicitação para saber seu endereço IP.

Os dispositivos que usam o RARP exigem que haja um **servidor RARP** presente na rede para responder às solicitações RARP.

O RARP caiu em desuso devido a sua função ser praticamente a mesma que a dos servidores de DHCP (atribuição dinâmica de endereços IP para hosts).

Veja a figura a seguir com uma ilustração do funcionamento do RARP.



No servidor RARP o administrador de rede deve ter pré-configurado todos os MACs dos micros que participam desse processo de inicialização e vinculado IPs a essas máquinas.

11 Conclusão e Certificado

Parabéns por ter chegado ao final do curso **Protocolo IPv4 e Classes**!

Tenha certeza de que compreendeu todos os conceitos aqui mostrados, pois ao final desse curso você deve ser capaz de:

- Explicar o formato do cabeçalho IPv4 e seus campos.
- Entender funciona o sistema de numeração binário.
- Realizar a conversão binário-decimal e decimal-binário.
- Como os endereços IPv4 são divididos nas classes:
  - Classe A
  - Classe B
  - Classe C
  - Classe D
  - Classe E
- Explicar a relação entre as classes de IPv4 e a Internet
- Entender o conceito de máscara de rede e prefixo de rede
- Realizar a análise quantitativa de redes e hosts em cada uma das classes de endereço IP
- Saber como identificar as porções de rede e host dado um endereço IP e máscara de rede
- Saber identificar as faixas de endereço de uso especial, tais como RFC 1918 e endereços de loopback
- Saber como endereçar uma rede IPv4 utilizando o conceito de roteamento Classful
- Explicar como operam os protocolos:
  - ICMP
  - ARP
  - RARP

Não esqueça que você deve ler e assistir tudo para obter o seu certificado de conclusão do curso.

Ficamos por aqui e nos encontramos nos próximos cursos!!!!!