razões de desempenho e tratar dos possíveis erros de transmissão diretamente dentro da aplicação. No Quadro 4.3 é possível observar algumas das principais características (comparativo) de cada um dos protocolos.

Quadro 4.3: Diferenças entre os protocolos TCP e UDP

TCP	UDP
Orientado a conexão	Não orientado a conexão
Ponto a ponto	Ponto a ponto
Confiável, controle de erros	Não confiável, sem controle de erros
Full duplex	*Full duplex*
Entrega ordenada	Não garante entrega ordenada
Controle de fluxo	Sem mecanismo de controle de fluxo

Fonte: Tanenbaum, 2003

O TCP e o UDP usam o protocolo IP, da camada de rede (internet) para a entrega dos pacotes. Os pacotes TCP ou os datagramas do UDP são encapsulados em datagramas IP e encaminhados (roteados) da origem até o destino. Após o encapsulamento, os roteadores usam basicamente os campos do IP.

Vale ressaltar que o protocolo UDP possibilita além da comunicação ponto-a-ponto, realizar a comunicação de um para muitos, o que significa que um computador origem através do protocolo UDP pode entregar pacotes para diversos computadores destino em uma rede. Este é um diferencial bastante relevante do protocolo UDP.

4.4 Protocolos da camada internet da arquitetura TCP/IP

Estudaremos nesta seção os principais protocolos da camada internet (camada de rede no modelo de referência OSI), os protocolos relacionados ou auxiliares e os mecanismos de roteamento.

4.4.1 O Protocolo da Internet – IP

O IP (*Internet Protocol* – Protocolo da Internet) é o protocolo essencial da arquitetura TCP/IP e o principal protocolo da camada de rede. A função principal do IP é a transferência de dados, na forma de datagramas, entre os nós (computador, roteador) da rede.

O serviço oferecido pelo IP não é confiável, também chamado de "melhor esforço". O protocolo tentará entregar o datagrama no destino, mas não há garantia de que os datagramas cheguem ordenados (pois podem seguir caminhos diferentes na rede e ter a ordem de entrega alterada), duplicados,

não há garantia nem mesmo que o datagrama chegue ao destino. Embora o IP ofereça um serviço de datagrama não confiável, a confiabilidade na transferência dos dados é uma função que pode ser adicionada nas outras camadas da arquitetura, como é estudado nas demais seções. Os roteadores, nesta camada de rede são responsáveis pela escolha do caminho que os datagramas utilizam até chegarem ao seu destino (inter-redes ou internet).

A Figura 4.3, representa os campos do cabeçalho de um datagrama IP, na sua versão 4, a versão mais usada na atualidade. Cada campo do cabeçalho está ligado a uma função dentro do protocolo:

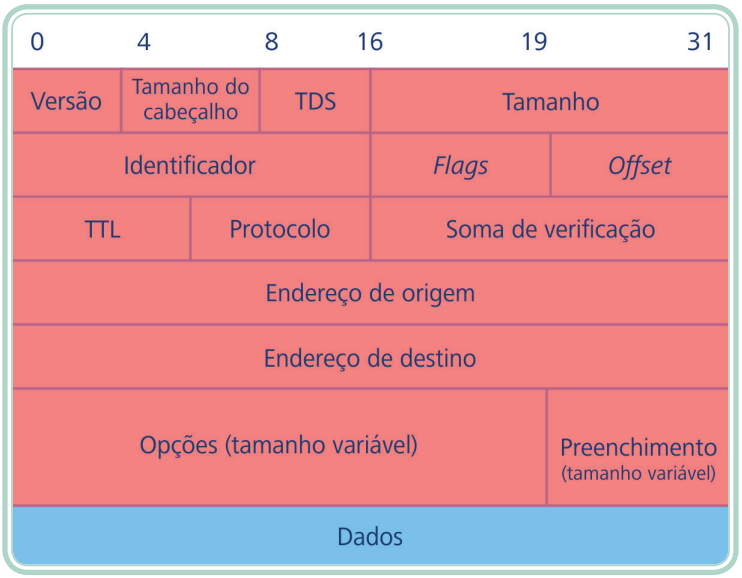

Figura 4.3: Formato de um pacote IPv4
Fonte: CTISM, adaptado de Davie e Bruce, 2004, p. 173

- **Versão** – com quatro *bits* identifica a versão do protocolo. Atualmente a versão 4 (IPv4) é a mais usada, mas a implantação da versão 6 (IPv6) está crescendo rapidamente.

- **Tamanho do cabeçalho** – essencialmente serve para especificar onde começa a porção de dados do datagrama.

- **TDS, tipo de serviço** – basicamente serve para definir diferentes tipos de prioridades aos datagramas de diferentes serviços da internet.

- **Tamanho** – comprimento total do datagrama, incluindo cabeçalho e dados. Quando o tamanho do datagrama é maior que o tamanho máximo de datagrama que a rede suporta, o datagrama é quebrado em fragmentos menores.

- **Identificador** – usado para identificar fragmentos de um mesmo datagrama original.

- ***Flags*** – usado para controlar e identificar fragmentos.

- ***Offset*** – permite ao receptor identificar o local de um fragmento no datagrama original.

- **TTL (*Time To Live* – tempo de vida)** – determina o número máximo de nós que um datagrama pode passar antes de ser descartado. O objetivo desse campo é evitar que um datagrama fique circulando pelas redes (internet) infinitamente. Cada vez que o datagrama passa (roteado) por um nó da rede, o valor do campo TTL é diminuído em uma unidade (decrementado). Quando o valor do TTL chega a zero o datagrama é descartado. Essa situação pode acontecer, por exemplo, quando há algum erro de roteamento e os datagramas são encaminhados indefinidamente (*loop*). Dessa forma o campo TTL evita problemas maiores nas redes.

- **Protocolo** – campo usado para identificar o protocolo usado junto com o IP, por exemplo, TCP (6) ou o ICMP (1).

- **Soma de verificação (*checksum*)** – usado para a verificação da integridade do cabeçalho IP. Esse valor é recalculado em cada nó (roteador).

- **Endereço IP de origem – endereço IP de destino** – usados para identificar as máquinas de origem e destino respectivamente.

- **Opções** – Campos de cabeçalhos adicionais, normalmente não são usados (DAVIE; BRUCE, 2004).

4.4.1.1 Endereçamento IP

O endereçamento IP permite identificar um dispositivo pertencente a uma rede de computadores. Para que isso seja possível cada um destes equipamentos conectados a uma rede (computadores, servidores, *notebooks*, *smartphones*, entre outros) deve possuir um número de identificação único (endereço IP) para que os roteadores possam fazer a entrega de pacotes de forma correta.

a) IPv4

Atualmente o endereçamento IPv4 ainda é o mais utilizado, sendo gradativamente substituído pelo endereçamento IPv6 (que será abordado na sequência).

Os endereços IPv4 são constituídos por 32 *bits*, divididos em quatro octetos, em outras palavras, quatro seções de 08 *bits*, separados por ponto que formam o endereço IP na versão 4 (IPv4). Destes quatro octetos uma parte representa a rede enquanto outra representa a quantidade de computadores que podem estar presentes em cada rede.

Um número IP pode variar do endereço 0.0.0.0 ao endereço 255.255.255.255, embora vejamos que existem algumas particularidades tanto na utilização, quando distribuição dos números IPs nas redes de computadores.

Como forma de organização e funcionamento inicial das redes de computadores, os endereços IPs foram divididos em classes (A, B, C, D e E), conforme a representação no Quadro 4.4.

Quadro 4.4: Classes de endereços IPv4

Classe	Faixa	N° endereços
A	1.0.0.0 – 126.255.255.255	16.777.216
B	128.0.0.0 – 191.255.0.0	65.536
C	192.0.0.0 – 223.255.255.0	256
D	224.0.0.0 – 239.255.255.255	***Multicast***
E	240.0.0.0 – 255.255.255.254	Testes (IETF) e uso futuro

Fonte: Silva, 2010

A-Z

Multicast
Tecnologia que permite que um fluxo de dados seja enviado a múltiplos destinos simultaneamente. Pode ser utilizada tanto em aplicações um-para-muitos, como muitos-para-muitos.
Um exemplo de utilização da tecnologia multicast esta nas aplicações distribuídas, especialmente multimídias, como videoconferências ou ensino a distância, tornando-as mais eficientes e economizando recursos.

As classes **A**, **B** e **C** foram distribuídas e são utilizadas por redes de computadores de diferentes tamanhos. Conforme pode ser visualizado no Quadro 4.4, faixas da classe **A**, possuem uma maior quantidade de IPs disponíveis que podem ser utilizados por computadores em uma rede, enquanto nas classes **B** e **C** estes valores decrescem gradativamente (SILVA, 2010).

Os endereços da classe **D** são utilizados para *multicast* em redes de computadores.

Já, os endereços da classe **E**, são utilizados para testes e como reserva futura quando da escassez dos endereços das classes anteriores.

Além dos endereços IPs válidos, citados acima, existem os endereços IPs chamados de não-roteáveis que são reservados para redes privadas (LAN, por exemplo). Dessa forma, é possível montar redes de computadores que funcionam entre si, com a utilização de endereços não-roteáveis. No Quadro 4.5, são apresentados alguns dos endereços reservados a redes privadas.

Quadro 4.5: Faixas de endereços IPv4 não roteáveis		
Classe	**Menor endereço**	**Maior endereço**
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Fonte: Silva, 2010

b) CIDR

Distribuir endereços IP através de classes (A, B, C, D e E) fazia com que inúmeros endereços IPv4 fossem desperdiçados. Como medida para uma melhor utilização dos endereços IPv4 e dada a escassez dos mesmos, foi implementada a notação CIDR (*Classless Inter-Domain Routing*).

Ao utilizar o CIDR ao invés das classes de IPs tradicionais temos a inserção de máscaras de tamanho variáveis, permitindo desta forma uma melhor utilização dos endereços e um menor desperdício de faixas IP.

Outra mudança que ocorre com a utilização do CIDR é a inexistências do conceito de faixas de endereços IP.

Exemplo: uma faixa de endereços IP, com máscara "/24" é equivalente a uma faixa de endereços de classe C, porém esta faixa pode começar com qualquer dígito e não somente de 192 a 223 que era o estipulado para esta faixa antes da utilização da notação CIDR.

É importante salientar que a máscara de rede determina qual parte do endereço IP é destinado a identificar a rede e qual delas endereçam os *hosts*. Em um endereço IP "200.153.132.3", com máscara "255.255.255.0" (/24), os primeiros 24 *bits* (200.153.132) referem-se a rede, enquanto os últimos 08 *bits* (3) referem-se ao *host*.

No Quadro 4.6, é possível visualizar exemplos da aplicação de CIDR e máscaras de tamanho variável, quanto aos endereços de rede e *host* que podem ser formados.

Quadro 4.6: Máscaras de rede

Máscara	*Bits* da rede	*Bits* do *host*	Número de redes	Número de *hosts*
255.255.255.0 (/24)	Nenhum	00000000	nenhuma	254 endereços (do 1 ao 254)
255.255.255.192 (/26)	11	000000	2 endereços (2 e 3)	62 endereços (de 1 a 62)
255.255.255.224 (/27)	111	00000	6 endereços (de 1 a 6)	30 endereços (de 1 a 30)
255.255.255.240 (/28)	1111	0000	14 endereços (de 1 a 14)	14 endereços (de 1 a 14)
255.255.255.248 (/29)	11111	000	30 endereços (de 1 a 30)	6 endereços (de 1 a 6)
255.255.255.252 (/30)	111111	00	62 endereços (de 1 a 62)	2 endereços (2 e 3)

Fonte: Morimoto, 2007

Para saber mais sobre faixas de endereços IP. CIDR e máscara de tamanho variável, acesse: http://www.hardware.com.br/tutoriais/endereco-ip-cidr/>

É importante lembrar que é possível utilizar a notação CIDR a qualquer momento na configuração de placas de rede, servidores e configurações de rede em geral. Ao escrever um *script* de *firewall*, por exemplo, o computador reconhece se escrevermos "192.168.0.0/255.255.255.0", quanto se utilizarmos a notação CIDR, escrevendo "192.168.0.0./24" (MORIMOTO, 2007).

c) IPv6

O IPv6, também conhecido como IP versão 6, é uma espécie de atualização do IPv4, oferecendo inúmeras vantagens para seus utilizadores, como por exemplo, um maior número de endereços IPs disponíveis. A ideia do IPv6 surgiu basicamente por dois motivos principais: a escassez dos endereços IPv4 e pelo fato de empresas deterem faixas de endereços IPv4 classe A, inteiras.

Em um endereço IPv6 são utilizados 128 *bits*, o que permite um total de 340.282.366.920, endereços disponíveis seguidos de mais 27 casas decimais (diferentemente do IPv4, onde são utilizados 32 *bits*, para formar o endereço IP).

Os endereços IPv6 são formados por oito quartetos de caracteres hexadecimais, separados pelo caractere ":" (dois pontos).

Exemplo: **2800 : 03f0 : 4001 : 0804 : 0000 : 0000 : 0000 : 101f**

Considerando o sistema hexadecimal, cada caractere representa 04 *bits*, ou 16 combinações. Ainda, considerando uma base hexadecimal temos a representação de 0 a 9 e a utilização das letras A, B, C, D, E e F, que são as representações das 16 combinações possíveis.

No IPv6 os endereços são divididos (assim como no IPv4) em dois blocos: os primeiros 64 *bits* identificando a rede (os primeiros 04 octetos) e os últimos 64 *bits* identificando os *hosts*. Vale lembrar aqui, que diferentemente do IPv4, no IPv6 não existem mais as máscaras de tamanho variável (CIDR) visto anteriormente.

Pode ser um pouco complicado armazenar na memória um endereço IPv6, devido a quantidade de caracteres existentes em cada endereço. Para ajudar nestas situações foram criadas técnicas que permitem abreviar estes endereços, conforme veremos nos exemplos a seguir:

- Exemplo 1: todos os zeros à esquerda (dentro de cada quarteto) do endereço podem ser omitidos. Exemplo: ao invés de escrever "0262", é possível escrever somente "262". Ao invés de escrever "0004", é possível escrever apenas "4" e ao invés de escrever "0000" é possível escrever apenas "0". Todas estas formas de abreviação são válidas e não alteram em nada o significado e funcionamento da rede.

- Exemplo 2: endereços do tipo "0:0:0:0:0:0:0:1" podem ser reduzidos para "::1".

Para configurar endereços em uma rede local de computadores, existem algumas opções, tais como:

a) Utilizar endereços sequenciais: "2001:cde1::1", "2001:cde1::2", "2001:cde1::3" e assim sucessivamente para os micros da rede.

b) Utilizar os endereços MAC das interfaces de rede, para utilizá-los também como endereços IPs. Exemplo: endereço MAC do computador "0C-EE-E6-8D-4D-7D" e tomamos como exemplo que o endereço de rede é "2001:bce4:0:0". A primeira tarefa a ser feita seria a conversão do endereço MAC em um endereço hexadecimal, simplesmente fazendo a inserção dos caracteres "ffff" entre o sexto e sétimo dígito. Desta forma, teríamos no exemplo "0CEE:E6ff:ff8D:4D7D". Fazendo a inserção do endereço de rede, teríamos o endereço IPv6 completo, tal como: 2001:bce4:0000:0000:0CEE:E6ff:ff8D:4D7D. O interessante desta técnica é que agilizamos e simplificamos a tarefa constante de buscarmos saber o endereço MAC e IP da interface da rede, em locais distintos.

Semelhante ao que ocorre no IPv4, no IPv6 temos faixas de endereços reservadas, ou seja, que podem ser utilizadas somente em redes locais, para testes, entre outros. Confira os exemplos no Quadro 4.7:

Quadro 4.7: Endereços IPv6 reservados

Endereço IP	Utilização
Iniciados por "2001:"	Reservados para provedores de acesso
Iniciados por "3fff : ffff" e "2001 : 0DB8"	Reservados para uso em documentação, exemplos e testes (não são roteáveis)
0:0:0:0:0:0:0:1	Endereço de *loopback* (semelhante ao 127.0.0.1 no IPv4)

Fonte: Morimoto, 2007

Para testar a conectividade do IPv6, tanto em sistemas operacionais Windows quanto Linux, basta acessar o *prompt* de comando (Windows) e o terminal (Linux) e digitar respectivamente (MORIMOTO, 2007):

- ping ::1 (Windows)
- ping6 fee::1 (Linux)

4.4.1.2 Máscara de rede

Uma máscara de rede, também conhecida por *netmask*, corresponde a um número de 32 *bits*, semelhante a um endereço IP, com a finalidade de identificar a rede na qual está inserido determinado computador e quantidade de *hosts* (computadores) que podem estar nesta mesma rede.

Os computadores que fazem parte de uma rede possuem além de um número IP que identifica o mesmo, uma máscara de rede e um *gateway* de rede.

As máscaras de rede possuem padrões para cada classe (faixa de endereços IPs), conforme Quadro 4.8:

Quadro 4.8: Classes de endereço IPv4

Classe	Máscara a ser utilizada
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Fonte: Morimoto, 2007

Para efeitos de exemplificação se tivéssemos um computador com o IP 200.132.36.3 a máscara de rede correspondente seria 255.255.255.0. Computadores que queiram comunicar-se e estejam em uma mesma máscara de

rede, fazendo a comunicação diretamente utilizando o protocolo apropriado para tal procedimento. Computadores que queiram comunicar-se, mas que estão configurados com máscaras diferentes necessitam de comunicação através de roteadores para intermediar a comunicação entre ambos.

4.4.2 O protocolo de controle de erros – ICMP

O protocolo ICMP (*Internet Control Message Protocol*) tem a função de identificar erros em uma rede de computadores. Computadores, servidores, *gateways*, entre outros dispositivos da rede utilizam-se do protocolo ICMP para enviar mensagens e comunicar-se entre si.

Como exemplo da utilização deste protocolo, estão dois comandos bastante conhecidos no contexto das redes de computadores, independente de sistema operacional. Estes comandos são o ping e o traceroute.

- O comando ping, permite saber se determinado computador está acessível, se existe conexão a internet, entre outros.

- O comando traceroute, permite fazer o rastreamento de um pacote na rede, listando os servidores, roteadores, entre outros dispositivos que este pacote "passa" até chegar ao seu destino.

Vale salientar que muitos *firewalls*, servidores e mecanismos de proteção de rede bloqueiam respostas a requisições ICMP (por meio dos comandos ping e traceroute), como forma de proteger estes equipamentos e a rede como um todo de tentativas de mapeamento e posteriormente ataques.

O protocolo ICMP é padronizado pela RFC 792, onde é possível visualizar, por exemplo, as principais funções e características detalhadas do funcionamento deste protocolo.

4.4.3 Tradução de endereços – ARP

Agora que compreendemos como funciona o endereçamento IP, percebemos que teremos duas formas distintas de endereçamento para os computadores da rede local: o endereço da camada de enlace, também conhecido como endereço MAC (corresponde ao endereço físico do computador) e o endereço da camada internet, também conhecido como endereço lógico ou endereço IP. Você pode estar se perguntando agora: "As duas formas de endereçamento são usadas na mesma rede?". A resposta à pergunta é "Sim!". Nas redes locais TCP/IP, usamos ambas as formas de endereçamento, em camadas diferentes.

O endereçamento na camada de enlace (o endereço MAC ou endereço Ethernet) é conhecido como endereçamento físico, pois é usado na camada de enlace ou endereço de *hardware*, está gravado no *firmware* da placa de rede e não pode ser alterado. O endereço da camada de rede (o endereço IP) é conhecido como endereço lógico, pois pode ser escolhido arbitrariamente. Sendo mais específico, o endereço físico e o endereço lógico, estão associados a uma mesma interface de rede de um computador conectado na rede, porém usados em camadas diferentes da arquitetura.

A comunicação entre os computadores da rede ocorre realmente na camada de enlace, ou seja, em uma rede local (computadores em uma mesma rede lógica), como a Ethernet, as máquinas se conhecem de fato pelo endereço físico. Por outro lado, na grande rede (internet) para cada computador do usuário é atribuído um endereço lógico distinto, o endereço IP.

Um item importante a ser questionado neste momento é: "Se cada camada usa um padrão de endereçamento diferente, como os protocolos de rede se entendem?". Percebemos que precisa existir uma forma de associar um endereço lógico a um endereço físico. O protocolo de tradução de endereços mais usado é o ARP (*Address Resolution Protocol* – Protocolo de Resolução de Endereços).

O ARP é um protocolo distribuído, pois não precisa de um computador central gerenciando. Ele está implantado em cada máquina da rede. Conceitualmente, o ARP trabalha na camada de rede, pois traduz endereços da camada de rede em endereços da camada de enlace.

Analisaremos agora o funcionamento do ARP, por meio de um exemplo, passo-a-passo:

a) O computador A possui o endereço IP 192.168.1.3 e deseja enviar um pacote ao computador B, com o endereço 192.168.1.4.

b) O computador A, então, envia uma mensagem especial a todos "perguntando": "Qual o endereço físico (MAC) do computador com endereço lógico (IP) 192.168.1.4?". A mensagem é enviada a todos (*broadcast*), pois ele não sabe, obviamente, o endereço que está procurando.

c) O computador B recebe o pedido de A e envia outra mensagem informando seu endereço MAC.

d) O computador A então envia o pacote que estava desejando enviar de início.

No nível de enlace, o endereço de *broadcast* MAC é FF:FF:FF:FF:FF:FF, ou seja, um endereço MAC com todos os 48 *bits* do endereço marcados (setados). Uma mensagem de *broadcast* é recebida por todos os computadores presentes na rede. A Figura 4.4 a seguir mostra os campos existentes em um pacote do tipo ARP.

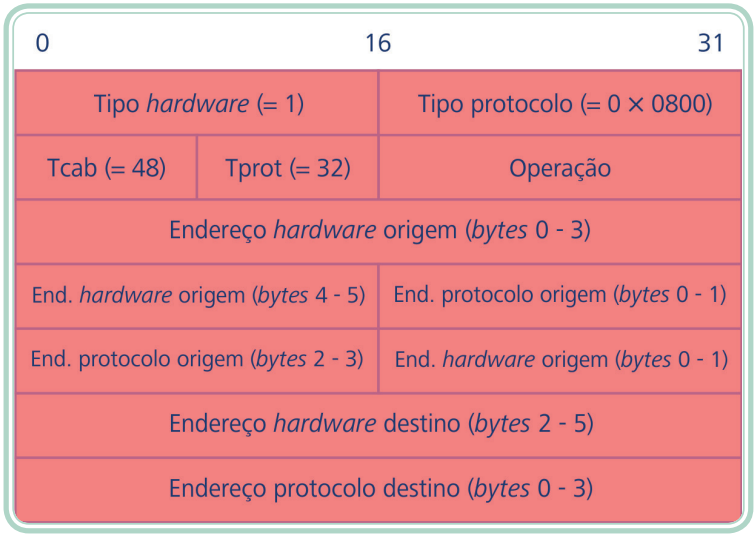

Figura 4.4: Campos de um pacote ARP
Fonte: CTISM, adaptado de Davie e Bruce, 2004, p. 188

No quadro da Figura 4.4 representamos o formato padrão de um pacote do protocolo ARP. O ARP foi projetado para ser genérico e permitir traduzir qualquer endereço lógico em endereço físico, porém na prática, o grande uso é na tradução de endereços IP em endereços MAC (endereço Ethernet). O campo Tipo *hardware* especifica a rede física, o 1 significa rede Ethernet. O campo Tipo protocolo especifica o protocolo da camada superior, neste caso o IP. TCab significa o tamanho do endereço de *hardware* (endereço MAC) e Tprot determina o tamanho do endereço do protocolo (endereço IP). Operação especifica se o pacote corresponde a uma pergunta ou uma resposta. Os demais campos representam os endereços de origem MAC e IP (do computador que está enviando o pacote) e os endereços de destino MAC e IP (de quem recebe).

Os computadores mantém uma lista (*cache*) com os endereços MAC associados aos endereços IP dos outros computadores na rede. Assim, o computador não precisa ficar "perguntando" pelo endereço MAC de outro computador, toda vez que quiser enviar um pacote. O ARP é um protocolo onde os computadores

podem "ouvir" os pedidos dos outros computadores, pois as mensagens são enviadas em *broadcast* e usar essas informações para criar sua própria lista de endereços. Um computador pode também responder, consultando sua própria lista, a um pedido de endereço de outro computador.

O ARP está condicionado à rede local. Não há o encaminhamento de pacotes ARP para outras redes, como ocorre com pacotes do nível de rede. No nível de rede, os pacotes são encaminhados aos roteados entre as redes (DAVIE; BRUCE, 2004).

4.4.4 RARP

O protocolo RARP (*Reverse Address Resolution Protocol*) intitulado como Protocolo de Resolução Reversa de Endereços, tem a função de associar um endereço Ethernet (MAC) a um endereço IP. Graças ao protocolo RARP um dispositivo de rede pode fazer uma solicitação a esta mesma rede para saber qual o endereço IP de determinada interface. Diferentemente do protocolo ARP, para dispositivos da rede que utilizam o protocolo RARP é necessário um servidor RARP que responda pelas solicitações encaminhadas a este servidor.

Na Figura 4.5, um esquema simples da diferença e função dos dois protocolos.

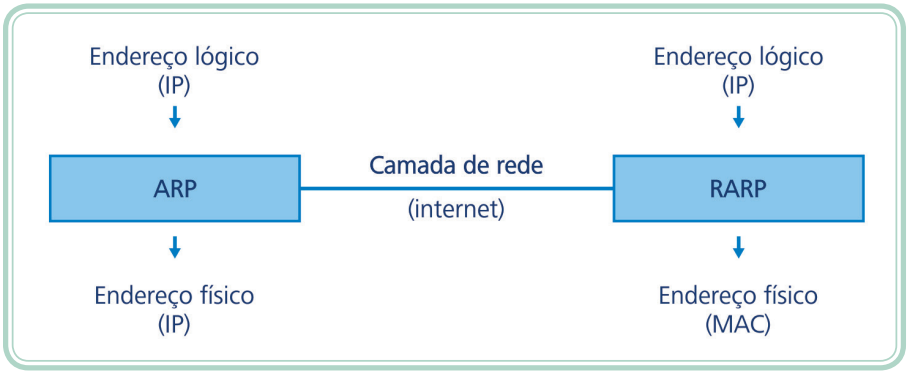

Figura 4.5: Protocolos ARP e RARP
Fonte: CTISM, adaptado dos autores

4.5 Protocolos da camada física (interface de rede)

Nesta quarta e última parte estudaremos os principais protocolos da camada de interface de rede do modelo TCP/IP, também conhecida como camada física. Esta camada aborda protocolos que trabalham no nível mais próximo ao *hardware* (interfaces, periféricos, entre outros).

4.5.1 Ethernet

Padronizada pelo padrão IEEE 802.3, o protocolo Ethernet é amplamente utilizado nas redes locais (LAN). Este protocolo, baseado no envio de pacotes é utilizado na interconexão destas redes. Dentre as características deste protocolo estão:

- Definição de cabeamento e sinais elétricos (camada física).
- Protocolos e formato de pacotes.

O padrão Ethernet baseia-se na ideia de dispositivos de rede enviando mensagens entre si. Cada um destes pontos de rede (nós da rede) possui um endereço de 48 *bits*, gravado de fábrica (endereço único mundialmente), também conhecido como endereço MAC, que permite identificar uma máquina na rede e ao mesmo tempo manter os computadores com endereços distintos entre si.

Um endereço MAC, gravado na memória ROM do computador é um endereço de 48 *bits*, composto por caracteres hexadecimais que vão de 0 à F. Destes 48 *bits* 24 são a representação de um código fornecido pelo IEEE, repassado a cada fabricante de interfaces de rede. Os outros 24 *bits* são atribuídos pela própria fabricante das placas de rede. Dessa forma, tem-se um endereço formado semelhante ao endereço mostrado na Figura 4.6.

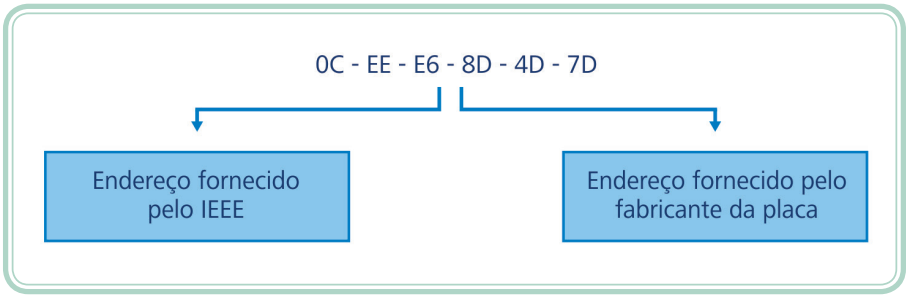

Figura 4.6: Componentes da criação de um endereço MAC
Fonte: CTISM, adaptado dos autores

Vale salientar que para identificar este endereço em um computador com sistema operacional Windows, basta acessar o *prompt* de comando e digitar o comando: "ipconfig /all".

Existem diferentes classificações para o padrão Ethernet, que vão desde padrões para cabeamento metálico, fibra óptica e interfaces *wireless*. Estes variam quanto ao tipo de tecnologia, velocidade, entre outras características. A seguir listamos as principais.

- 10Base-T Ethernet (padronizada pelo padrão IEEE 802.3). Velocidade de 10 *megabits* por segundo, utilizada em redes de par trançado.

- Fast Ethernet (padronizada pelo padrão IEEE 802.3u). Velocidade de 100 *megabits* por segundo, utilizada em redes de par trançado.

- *Gigabit* Ethernet (padronizada pelo padrão IEEE 802.3z). Velocidade de 01 *gigabit* por segundo.

- 10 *gigabit* Ethernet (padronizada pelo padrão IEEE 802.3ae). Velocidade de 10 *gigabits* por segundo.

- 100BASE-FX. Velocidade de 100 *megabits* por segundo, utilizada em redes de fibra óptica.

- 1000BASE-SX. Velocidade 01 *gigabit* por segundo, utilizada em redes de fibra óptica.

- 10GBASE-SR. Velocidade 10 *gigabits* por segundo, utilizada em redes de fibra óptica.

- *Wireless* Ethernet (padronizada pelo padrão IEEE 802.11). Oferece diferentes categorias, com características distintas (velocidade, canal de operação, frequência, etc.):
  - 02 *megabits* por segundo, no padrão 802.11.
  - 11 *megabits* por segundo, no padrão 802.11b.
  - 54 *megabits* por segundo, no padrão 802.11g.
  - De 65 a 300 *megabits* por segundo, no padrão 802.11n.

Resumo

Nessa aula, foi possível conhecer os principais protocolos utilizados nas redes de computadores, bem como, a função de cada um deles. Além disso, foi possível entender como esses protocolos funcionam e em qual camada operam. Como parte principal desta aula foi apresentado em detalhes os protocolos TCP e IP, fundamentais para o funcionamento lógico da rede.

Atividades de aprendizagem

1. Dada as camadas do modelo TCP/IP, liste os principais protocolos que operam em cada uma destas camadas.

2. Diferencie o protocolo TCP do protocolo UDP, citando três diferenças entre eles.

3. Com relação ao IPv4 e ao IPv6, qual a diferença entre estes protocolos? O que muda de um para o outro e como são formados?

4. Para que serve a notação CIDR e porque foi criada?

5. Qual a função do protocolo ICMP?

6. Cite três protocolos da camada de aplicação, o que fazem e para que servem.