

**IESPLAN – Instituto de Ensino Superior Planalto**  
**Departamento de Ciência da Computação**  
**Curso: Ciência da Computação**  
**Disciplina: Engenharia de Software**  
**Professor: Marcel Augustus**

## **O Protocolo ARP**

Brasília, DF, setembro de 2003.

**IESPLAN – Instituto de Ensino Superior Planalto**  
**Departamento de Ciência da Computação**  
**Curso: Ciência da Computação**  
**Disciplina: Redes de Computadores II**  
**Professor: Marcel Augustus**

## **O Protocolo ARP**

Alunos: Cláudio, Nilson e Alexandre.

Brasília, DF, setembro de 2003.

# Sumário

<b>INTRODUÇÃO.....</b>	<b>4</b>
<b>PROTOCOLO ARP.....</b>	<b>5</b>
ARP - ADDRESS RESOLUTION PROTOCOL.....	5
FUNCIONAMENTO DO PROTOCOLO ARP.....	5
<b>CACHE ARP.....</b>	<b>6</b>
<b>ARP – ENCAPSULAMENTO E IDENTIFICAÇÃO.....</b>	<b>7</b>
<b>FORMATO DO ARP.....</b>	<b>7</b>
<b>DESCRIÇÃO DOS CAMPOS.....</b>	<b>7</b>
<b>CONCLUSÃO.....</b>	<b>9</b>
<b>BIBLIOGRAFIA.....</b>	<b>10</b>
<b>APÊNDICE 1 – UTILITÁRIO ARP.....</b>	<b>11</b>
<b>APÊNCIDE 2 – UTILITÁRIO CODEVIEW.....</b>	<b>12</b>
<b>ANEXO 1 – RFC 826.....</b>	<b>13</b>

## **Introdução**

Neste trabalho, apresentaremos o Protocolo ARP – Address Resolution Protocol: seu papel na comunicação de dados na Internet, seu funcionamento e a estrutura de dados que utiliza. Apresentaremos também a RFC 826 que o definiu e os utilitários ARP e CodeView, usados para visualizar suas informações e capturar seu datagrama.

# Protocolo ARP

## ***ARP - Address Resolution Protocol***

O endereço IP é utilizado para roteamento, ou seja, a escolha do caminho ideal em determinada circunstância e o instante para a conexão entre dois nós. Para solucionar o problema de mapear o endereço de nível superior (IP) para endereço físico (Ethernet) foi proposto (e aceito) através da **RFC826** o Address Resolution Protocol (ARP). O ARP permite que um host encontre o endereço físico de um host destino, tendo apenas o seu endereço IP. Apesar de ter sido criado especificamente para uso com IP sobre Ethernet, devido à forma que foi implementado, seu uso não está restrito a este ambiente. O mapeamento de endereços pode ser feito de duas maneiras:

- Mapeamento direto
- Mapeamento dinâmico

O ARP é dividido em duas partes: a primeira determina endereços físicos quando manda um pacote, e a segunda responde os pedidos de outros hosts. Geralmente antes de enviar, o host consulta seu cache ARP procurando o endereço físico. Se encontrar o endereço, anexa-o no frame e envia acrescentando os dados. Se o host não encontrar o endereço, é realizado um broadcast de pedido ARP. A segunda parte do código do ARP manuseia os pacotes recebidos da rede. Quando chega um pacote, o programa extrai e examina o endereço físico e IP para verificar se já existe a entrada no cache e atualiza novamente sobrescrevendo os endereços. Depois, o receptor começa a processar o resto do pacote. O receptor processa dois tipos de entrada de pacotes ARP:

- Pedido ARP de um outro host: o receptor envia o endereço físico ao emissor e armazena o endereço do emissor no cache. Se o endereço IP do pacote recebido não for igual do receptor, o pacote ARP é ignorado.
- Resposta de um pedido ARP: Após verificar a entrada no cache ARP, o receptor verifica primeiro a resposta com o pedido ARP enviado anteriormente. Enquanto o receptor espera pela resposta, as aplicações podem gerar outros pacotes que geralmente esperam na fila. Após verificar o endereço IP, o receptor atualiza os pacotes com o mesmo. O ARP retira os pacotes da fila depois de fornecer os endereços.

Se durante o broadcast o destinatário não puder aceitar um pedido, o host emissor deve armazenar o pacote enviado para retransmiti-lo. Pode acontecer, também, de o hardware de um host ter sido substituído. Se algum host tentar enviar dados para ele, utilizará um endereço não existente na rede, por isso é importante atualizar e remover os endereços no cache em períodos regulares.

## ***Funcionamento do protocolo ARP***

Consiste no envio de um frame em broadcasting com endereço IP do destino, o qual responde com um datagrama contendo o seu endereço IP e o endereço físico. A máquina que gerou o broadcasting passa a usar o endereço físico do destino para enviar seus datagramas.

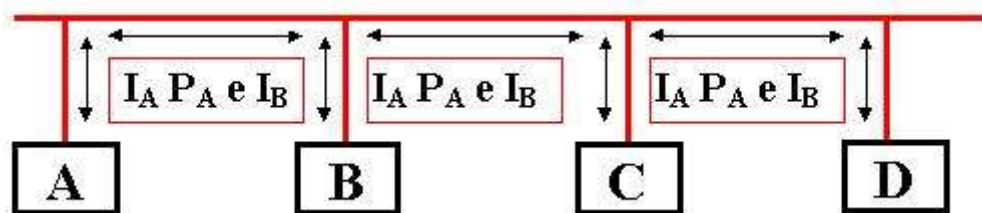


Figura 1 - o host envia o pacote para todos os hosts

O host A, cujo endereço IP é  $I_A$  e endereço físico  $P_A$ , deseja enviar dados ao host B, cujo IP é  $I_B$ , porém de endereço físico desconhecido. O host A envia um datagrama especial em broadcast.

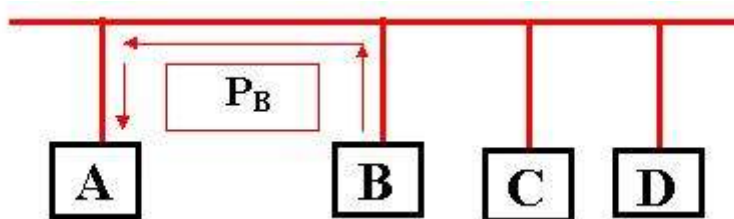


Figura 2 - Somente o host B responde com o seu  $P_B$

Apenas o host B responde, pois o datagrama foi endereçado via IP. O datagrama resposta é constituído do endereço IP ( $I_B$ ) mais o endereço físico  $P_B$ . A partir desse instante o host A passa a endereçar o host B apenas com seus endereços já conhecidos ( $P_B$  e  $I_B$ ). Resumidamente, o ARP funciona da seguinte forma:

- Quando uma máquina A quer falar com uma máquina B e não sabe seu endereço físico, envia um pacote ARP de request em modo broadcast.
- Todas as máquinas em operação recebem o pedido, mas somente a máquina B responde, pois ela reconhece que o endereço pedido é o seu.
- A guarda o endereço físico de B  $P_B$  em cache.
- A envia mensagem para  $P_B$ .

## Cache ARP

Em uma rede de grande porte e ocupada, o envio de pacotes em broadcasting interromperá todos os hosts para que eles processem cada pacote da rede. Essa interrupção prejudicará de maneira significativa a eficiência da rede e a tornaria mais lenta. Para reduzir os broadcasts, os hosts de redes que necessitam utilizar o ARP mantêm uma lista de endereços IP e Ethernet que correspondem a eles obtidos por solicitações anteriores. Isto é listado como Cache ARP e é atualizado sempre que uma solicitação for enviada. Depois de algum tempo o endereço no ARP Cache é removido, independentemente de estar sendo usado ou não. Isto é chamado de **Aging**.

## ARP – Encapsulamento e Identificação

As mensagens ARP devem ser transmitidas nos frames. Para identificar se os frames ARP estão carregando o pedido (request) ou a resposta, o campo do tipo do cabeçalho (header) recebe um valor específico, e a mensagem ARP é enviada no campo dos dados. Quando o frame é recebido, o host checa o tipo de frame para determinar seu conteúdo.

### Formato do ARP

Os dados nos pacotes do ARP não possuem um cabeçalho de formato fixo, ao contrário de outros protocolos. A mensagem é montada para ser utilizada em diferentes redes. Por isso, o primeiro campo no cabeçalho indica os comprimentos dos campos seguintes. O ARP pode ser usado com endereços físicos e protocolos arbitrários. Ao contrário da maioria dos protocolos, o pacote ARP não alinha no tamanho de 32-bits. Por exemplo, o endereço do emissor (sender) ocupa 6 octetos contíguos, expandindo-se para próxima linha.

### Descrição dos Campos

0	8	16	24	31
HARDWARE TYPE		PROTOCOL TYPE		
HLEN	PLEN	OPERATION		
SENDER HA(OCTETS 0-3)				
SENDER HA(OCTETS 4-5)		SENDER IP(OCTETS 0-1)		
SENDER IP (OCTETS 2-3)		TARGET HA(OCTETS 0-1)		
TARGET HA(OCTETS 2-5)				
TARGET IP(OCTETS 0-3)				

Figura 3 - Formato do ARP

- Hardware Type (tipo do hardware): composto de dois octetos, especifica o tipo de hardware utilizado na rede física. Se for 1, é rede Ethernet.
- Protocol Type (tipo do protocolo): composto de dois octetos, especifica o endereço do protocolo utilizado no nível superior do emissor.
- Operation (operação) : especifica se o datagrama é um pedido ARP (request 1 ) ou uma resposta ARP (reply 2), ou ainda um RARP (request 3, reply 4).
- HLEN e PLEN: habilitam o ARP para ser usado com redes arbitrárias porque eles especificam o comprimento dos endereços do hardware e dos protocolos do nível superior. O HLEN (Hardware Length) é utilizado para identificar o tamanho dos campos SENDER HA e TARGET HA. PLEN (Protocol Length) especifica o tamanho dos campos SENDER IP e TARGET IP.
- SENDER HA (Sender Hardware Address) : endereço físico (Ethernet) de quem envia o pacote.
- SENDER IP (Sender Protocol Address): endereço lógico (IP) de quem envia o pacote.
- TARGET HA (Target Hardware Address) : Endereço físico desejado. Na operação de request vai em branco, e, quem responder preenche este campo.
- TARGET IP (Target Protocol Address) : Endereço lógico da máquina desejada.

Quando um emissor faz um pedido, envia o endereço TARGET IP (ARP) ou o endereço físico TARGET HA (RARP). Antes de responder, o destinatário atualiza os endereços recebidos e muda a operação para resposta (reply). Assim, a resposta carrega os endereços do emissor assim como os endereços IP e físico do destinatário.



## **Conclusão**

Como se pode ver, o protocolo ARP tem um papel importante auxiliando a Internet responder às necessidades de comunicações de dados mundiais, apesar da multiplicidade de protocolos de acesso ao meio e transmissão, oferecendo uma tecnologia robusta e eficaz.

## **Bibliografia**

- Comer, Douglas E.; Internetworking with TCP/IP Volume I (Principles, Protocols and Architecture); Prentice Hall, 1991.

## Apêndice 1 – Utilitário ARP

```
C:>arp -a
```

```
Interface: 10.8.17.180 on Interface 0x10000003
  Endereço IP      Endereço físico      Tipo
  10.8.16.1        00-d0-04-86-c3-fc      dinâmico
  10.8.17.222      00-50-ba-8b-48-42      dinâmico
  10.8.21.57       00-d0-b7-af-84-e9      dinâmico
  10.8.23.140      00-50-ba-8b-64-3d      dinâmico
```

```
C:>ipconfig
```

Configuração de IP do Windows 2000

Ethernet adaptador Conexão de rede local:

```
Sufixo DNS específico de conexão . : ac.correiosnet.int
Endereço IP. . . . . : 10.8.17.180

M scara de sub-rede. . . . . : 255.255.248.0

Gateway padrão . . . . . : 10.8.16.1
```

## Apêndice 2 – Utilitário CodeView

**CommView - Evaluation Version**

File Search View Tools Settings Rules Help

Realtek RTL8139(A) PCI Fast Ethernet Adap...

IP Statistics Packets Logging Rules Alarms

**Rules Configuration:**

- Enable ethernet protocol rules:**
  - Description: IP, ARP, SNMP, NCHLL, IFFFWND
  - Action: Capture, Ignore
- Enable direction rules:**
  - Capture inbound packets
  - Capture outbound packets
  - Capture pass-through packets
- Enable IP protocol rules:**
  - Description: ICMP, IGMP, GGP, IP-ENCAP, ST, TCP, EGP, IGP, PUP, UDP, HMP
  - Action: Capture, Ignore

**Packet List:**

No	Protocol	MAC Addresses	IP Addresses	Ports
4722	ARP REQ	00:50:BA:8B:48:B1 => Broadcast	10.8.17.180 -> 10.8.16.118	N/A
4723	ARP RESP	00:50:BA:8B:48:B1 <= 00:50:BA:8B:48:B1	10.8.16.118 -> 10.8.17.180	N/A
5707	ARP REQ	00:50:BA:8B:48:B1 => Broadcast	10.8.17.180 -> 10.8.16.213	N/A
5767	ARP REQ	00:50:BA:8B:48:B1 => Broadcast	10.8.17.180 -> 10.8.16.213	N/A
5900	ARP REQ	00:50:BA:8B:48:B1 => Broadcast	10.8.17.180 -> 10.8.16.213	N/A
6196	ARP REQ	00:50:BA:8B:48:B1 => Broadcast	10.8.17.180 -> 10.8.17.156	N/A
6226	ARP REQ	00:50:BA:8B:48:B1 => Broadcast	10.8.17.180 -> 10.8.17.156	N/A
6333	ARP REQ	00:50:BA:8B:48:B1 => Broadcast	10.8.17.180 -> 10.8.17.156	N/A
7190	ARP REQ	00:50:BA:8B:48:B1 => Broadcast	10.8.17.180 -> 10.8.16.199	N/A
7226	ARP REQ	00:50:BA:8B:48:B1 => Broadcast	10.8.17.180 -> 10.8.16.199	N/A
7293	ARP REQ	00:50:BA:8B:48:B1 => Broadcast	10.8.17.180 -> 10.8.16.199	N/A
10034	ARP REQ	00:50:BA:8B:48:B1 => Broadcast	10.8.17.180 -> 10.8.17.245	N/A
10121	ARP REQ	00:50:BA:8B:48:B1 => Broadcast	10.8.17.180 -> 10.8.17.245	N/A
10190	ARP REQ	00:50:BA:8B:48:B1 => Broadcast	10.8.17.180 -> 10.8.17.245	N/A

**Packet Details (No. 4722):**

- Ethernet II: Destination MAC: FF:FF:FF:FF:FF:FF, Source MAC: 00:50:BA:8B:48:B1, Ethertype: 0806 (2054) - ARP, Direction: Out, Time / Delta Time: 17:59:56.529 / 0.000, Frame size: 42 bytes, Frame number: 4722
- ARP: Hardware: 00001 (1) - Ethernet, Protocol: 00900 (2048) - IP, Hardware address length: 0x06 (6), Protocol address length: 0x04 (4), Operation: 00001 (1) - ARP Request, Sender MAC address: 00:50:BA:8B:48:B1, Sender IP address: 10.8.17.180, Target MAC address: 00:00:00:00:00:00, Target IP address: 10.8.16.118

**Packet Details (No. 4723):**

- Ethernet II: Destination MAC: 00:50:BA:8B:48:B1, Source MAC: 00:50:BA:8B:48:B1, Ethertype: 0806 (2054) - ARP, Direction: In, Time / Delta Time: 17:59:56.529 / 0.000, Frame size: 60 bytes, Frame number: 4723
- ARP: Hardware: 00001 (1) - Ethernet, Protocol: 00900 (2048) - IP, Hardware address length: 0x06 (6), Protocol address length: 0x04 (4), Operation: 00002 (2) - ARP Response, Sender MAC address: 00:50:BA:8B:48:B1, Sender IP address: 10.8.16.118, Target MAC address: 00:50:BA:8B:48:B1, Target IP address: 10.8.17.180

**Hex Dump (No. 4723):**

```
0x0000  00 50 BA 8B 48 B1 00 50 BA 8B 68 8A 08 06 00 01  .P<Hh.P<hS...v
0x0010  08 00 06 04 00 02 00 50 BA 8B 68 8A 0A 08 10 76  ....P<hS...v
0x0020  00 50 BA 8B B1 0A 08 11 B4 20 20 20 20 20 20 20  .P<Hh...
0x0030  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
```

## **Anexo 1 – RFC 826**