


Arquiteturas e Protocolos de Comunicação



Funções da camada de rede

As duas funções fundamentais desta camada são:


- 1. Endereçamento ou addressing**

atribuição de um código único a cada interface de estação, tornando possível enviar e receber pacotes através desse interface destinados a ou originados de qualquer outro interface ligado à Internet
- 2. Encaminhamento ou routing**

mecanismo que permite a cada sistema na Internet determinar a melhor rota (caminho) para enviar um pacote para determinado destino

Paulo Almeida/José Oliveira @2005 Acetatos 1

Arquiteturas e Protocolos de Comunicação



Funções da camada de rede

Uma LAN não é uma rede porque funciona por difusão (broadcast) e portanto não faz entrega selectiva de pacotes (PDU - Protocol Data Units)


O endereçamento em LAN não tem estrutura: é feito por força bruta. Cada interface possui um endereço único num espaço plano sem capacidade de suportar o encaminhamento porque é atribuído por fabricante. Os endereços ethernet de 48 bits são atribuídos pelo IEEE em que os três primeiros octetos identificam o fabricante

- 00-0D-88-9C-8A-8F Realtek
- 00-08-02-D6-38-93 D-Link

O encaminhamento em LAN não existe o que não deve ser confundido com a filtragem feita pelas bridges para passar tramas selectivamente entre segmentos da LAN

Paulo Almeida/José Oliveira @2005 Acetatos 2

Arquiteturas e protocolos de comunicação



Endereços IP

Cada interface ligado à Internet possui um endereço IP de 32 bits (IPv4) ou de 128 bits (IPv6)

Os endereços IP são atribuídos em blocos a ISP (Internet Service Providers), isto é, são atribuídos a redes e não a organizações ou fabricantes, assim:


O prefixo do endereço permite calcular o encaminhamento;

Os blocos de endereços são atribuídos pela IANA (IANA - Internet Addressing and Naming Authority (www.iana.org) que subdelega em quatro RIR, Regional Internet Registries:

- ARIN – American Registry for Internet Numbers
- APNIC - Asia Pacific Network Information Centre
- LACNIC - Latin American Caribbean IP address Regional Registry
- RIPE NCC - Réseaux IP Européens Network Coordination Centre (www.ripe.net)

Paulo Almeida/José Oliveira @2005 Acetatos 3

Arquiteturas e protocolos de comunicação



Formato do datagrama IP

A unidade básica de dados na camada de rede é o pacote ou datagrama IP (N-PDU, Network Protocol Data Unit);

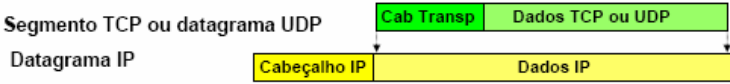
Em geral, um datagrama define-se como uma unidade de dados pequena, que é transmitida independentemente de qualquer outra e sem garantia de entrega no destino;

Cada PDU possui um cabeçalho e uma parte de dados;

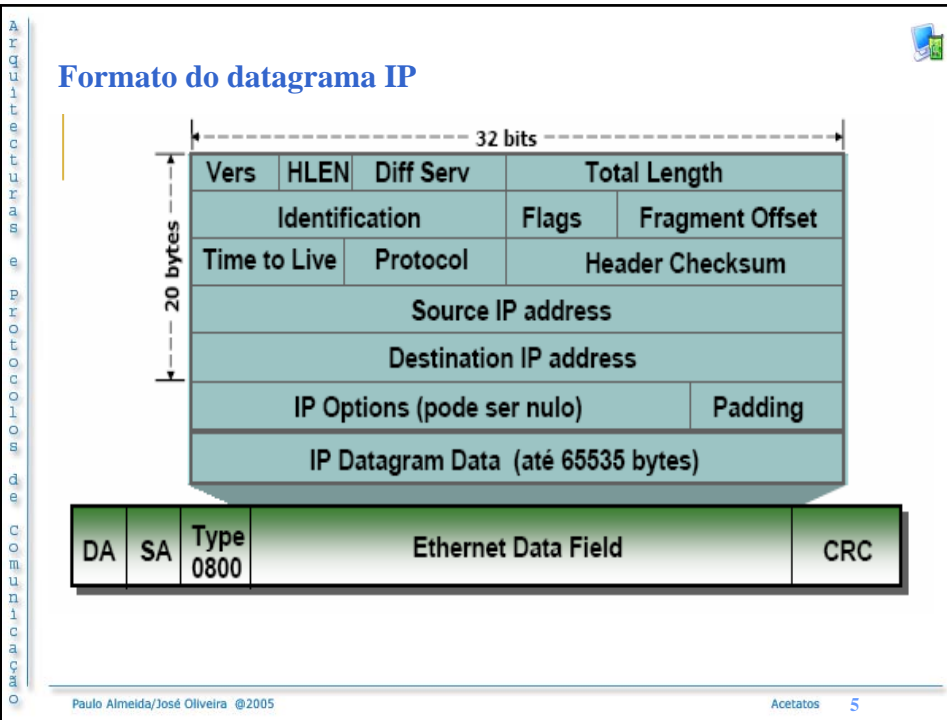
A parte de dados (payload) contém o PDU da camada protocolar superior que é a camada de transporte (T-PDU):

- Um segmento TCP ou
- Um datagrama UDP

Assim, o protocolo IP encapsula um protocolo de transporte



Paulo Almeida/José Oliveira @2005 Acetatos 4



Arquiteturas e Protocolos de Comunicação

Formato do datagrama IP

Version (4b): versão corrente é a 4 (IPv4). A versão seguinte (IPv6) altera o formato do pacote;

Header Length (4b): N^o de palavras de 32 bits do cabeçalho => tamanho máximo do cabeçalho = 60 bytes

Type of Service (8b):

- 4 bits (TOS) usados para minimizar o atraso, maximizar eficiência, maximizar a fiabilidade ou minimizar os custos (RFC 1349)
- 6 bits (DiffServ) diferenciar classes de serviços para o tráfego internet (RFC 2474). ← Actualmente

Total Length (16b): N^o de bytes de todo o pacote => tamanho máximo do pacote = 65535 bytes

Identification (16b): identifica univocamente cada pacote que sai do sistema (fragmentação e agrupamento)

Paulo Almeida/José Oliveira @2005 Acetatos 6



Formato do datagrama IP

Flags (3b): usadas quando ocorre fragmentação

Fragment Offset (13b): posição dos dados no pacote original antes da fragmentação

Time-To-Live (8b): N^o máximo de routers que o pacote pode passar (cada router decreta o valor deste campo)

Protocol (8b): Identifica o protocolo destinatário dos dados (Ex: icmp(1), tcp(6), udp(17), ..., IPinIP(4), IPv6(41), ...)

Header Checksum (16b): verificar integridade do cabeçalho (soma, complemento de 1, de cada 16b do cabeçalho)

Source IP Address (32b): endereço do remetente

Destination IP Address (32b): endereço do destinatário

Options (Nx32b): opções do protocolo ($0 \leq N \leq 10$)

Data (Nx32b): dados do protocolo servido



Fragmentação

Um datagrama cujo comprimento exceda o MTU definido para a LAN, é dividido em datagramas mais curtos, chamados fragmentos, que serão reagrupados no destino de modo a reconstituírem o datagrama original;

Os fragmentos são datagramas IP e são encaminhados como tal como qualquer outro datagrama IP;

MTU (Maximum Transfer Unit): é o número máximo de bytes aceites no campo de dados da trama da LAN;

A fragmentação não depende dos routers, mas sim das características das LAN ligadas aos seus interfaces;

Os campos identification e fragment offset permitem reconstituir o datagrama IP original



Formato do endereço IP

IPv4: utiliza endereços de 32 bits

bbbbbbbbbbbbbbbbbbbbbbbbbbbb

é usada uma notação decimal (dot decimal notation)

bbbbbbb.bbbbbbb.bbbbbbb.bbbbbbb



b = dígito binário
d = dígito decimal

o endereço é dividido em duas partes lógicas:

- uma parte (o prefixo) identifica a rede, ou subrede, e
- a parte restante, que identifica o interface da estação (host) nessa subrede

Podemos definir os endereços por tipos:

- Unicast: identifica um único sistema
- Multicast: identifica um grupo de sistemas
- Broadcast: identifica todos os sistemas de uma rede

Endereçamento com classes

esquema original, baseado na RFC 791 (Set 1981)

usa os primeiros bits como identificadores de classe obsoleto

Identificador da classe	Parte do Endereço de Rede	Parte do Endereço de Estação
-------------------------	---------------------------	------------------------------

Classe A

0	7 bits de endereço de rede	24 bits de endereço de estação
---	----------------------------	--------------------------------

Classe B

10	14 bits de endereço de rede	16 bits de endereço de estação
----	-----------------------------	--------------------------------

Classe C

110	21 bits de endereço de rede	8 bits endereço de estação
-----	-----------------------------	----------------------------


Classe D

1110	Endereços Multicast no intervalo 224.0.0.0 - 239.255.255.255	
------	--	--

Classe E

11110	Classe E – Reservado para utilização futura	
-------	---	--

Arquiteturas e protocolos de comunicação



Espaço de endereços IPv4 com classes


a atribuição de blocos de endereços é rígida

muitos endereços desperdiçados o que conduziu ao esgotamento de endereços

	Nets(1ºB)	Nº Nets	Nº Hosts/Net
Classe A	0-127	$2^7=128$	$2^{24}-2=16.777.214$
Classe B	128-191	$2^{14}=16.384$	$2^{16}-2=65.534$
Classe C	192-223	$2^{21}=2.097.152$	$2^8-2=254$

Paulo Almeida/José Oliveira @2005 Acetatos 11

Arquiteturas e protocolos de comunicação



Máscaras de endereço

Máscara: padrão que conjugado com o endereço IP, devolve a parte do endereço de rede (sub-rede);

No endereçamento por classes as máscaras são:

Classe A: 11111111.00000000.00000000.00000000
 notação decimal: 255.0.0.0 notação CIDR: /8

Classe B: 11111111.11111111.00000000.00000000
 notação decimal: 255.255.0.0 notação CIDR: /16

Classe C: 11111111.11111111.11111111.00000000
 notação decimal: 255.255.255.0 notação CIDR: /24

No endereçamento sem classes as máscaras têm qualquer outro valor permitindo a criação de sub redes (subnetts) da classe original.

Paulo Almeida/José Oliveira @2005 Acetatos 12

Subnetting com classes



Necessidade de criar sub redes dentro de uma instituição

A partir de uma rede de classe A, B ou C, utilizar os bits mais significativos destinados aos sistemas (hosts) e criar sub redes

Exemplo:

Class B	Net(16)	Subnet(8)	Host(8)
---------	---------	-----------	---------

Antes do *subnetting* um sistema sabia a que rede pertencia através do seu endereço IP. Analisava os bits mais significativos para saber a que classe pertencia e assim determinar quais os bits destinados à identificação da rede

Com *subnetting* é necessário utilizar uma máscara para identificar os bits que correspondem à identificação da rede

Máscaras de endereço



Exemplo:

193.137.7.0/255.255.255.0 criar 4 sub redes


193.137.7.0; 193.137.7.64; 193.137.7.128 e 193.137.7.192
todas com a máscara 255.255.255.192 (...11000000)

cada sub rede suporta no máximo $2^6 - 2 = 62$ sistemas ($62 * 4 = 248 < 254$)

Actualmente, todos os sistemas devem suportar a utilização de máscaras e consequentemente o *subnetting*

Arquiteturas e Protocolos de Comunicação

Restrições a endereços IP



Endereços reservados:

- os primeiros 4 bits não podem ser todos 1
- 127.x.x.x é o endereço reservado para *loopback*
- bits de *host* a 0s ou 1s são reservados (rede e broadcast)
- bits de *subnet* a 0s ou 1s são reservados

Endereços privados:


atribuídos para intranets privadas (sem conectividade global, não devem ser visíveis, ié, não são encaminhados na Internet), RFC1918:

- bloco 192.168.0.0 - 192.168.255.255 (prefixo 192.168 /16)
- bloco 172.16.0.0 - 172.31.255.255 (prefixo 172.16 /12)
- bloco 10.0.0.0 - 10.255.255.255 (prefixo 10 /8)

Paulo Almeida/José Oliveira @2005 Acetatos 15

Arquiteturas e Protocolos de Comunicação

Endereçamento sem classes



Motivos:

Esgotamento do endereçamento IP (redes atribuídas mas poucos endereços usados, 3% segundo um estudo efectuado)

Esgotamento da capacidade nas tabelas de routing globais (capacidade teórica: 60.000 entradas)

Solução:

Reestruturação da atribuição de endereços (acabar com as classes e atribuir redes que variam entre 13 a 27 bits)

Agregação de rotas (ainda melhor se houver uma estrutura hierárquica na distribuição de blocos de endereços)

Paulo Almeida/José Oliveira @2005 Acetatos 16

Endereçamento sem classes



- esquema actual, baseado na RFC 1519 (Set 1993)
- não considera os bits de classe utilizando uma máscara de 32 bits para determinar o endereço de rede;
- permite *routing* mais eficiente por agregação de rotas, designado CIDR (*Classless Internet Domain Routing*)
- as rotas são agregadas por grupos de endereços adjacentes, baseado na RFC 2519 (Fev 1999)
- tabelas de encaminhamento mais pequenas
- usado na prática nas tabelas de *routing*

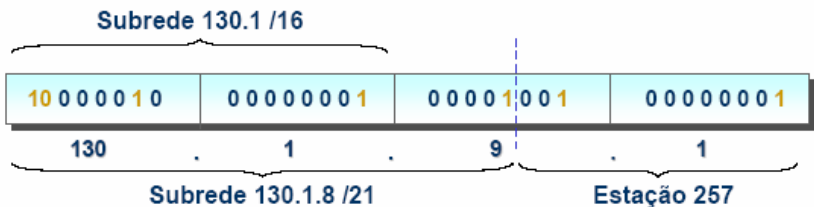
Endereçamento sem classes



Considere-se a sub rede IP 130.1 /16

Considere-se o endereço IP 130.1.9.1 /21

- é o endereço da estação 257 da sub rede 130.1.8 /21 ou
- é o endereço da estação 257 da sub rede 8 da sub rede 130.1 /16



Máscara de subrede com 21 bits:
 $11111111.11111111.11111000.00000000_2 = 255.255.248.0_{10}$

Arquiteturas e Protocolos de Comunicação

Endereçamento com e sem classes

Considere-se o endereço IP 130.1.5.1
é o endereço da estação 5.1 da rede 130.1.0.0 (classe B)

Considere-se o endereço IP 130.1.5.1 /24
é o endereço da estação 1 da sub rede 5 da rede 130.1.0.0
interpretação sem classes: estação 1 da sub rede 130.1.5 /24

(máscara com múltiplo de 8 bits) interpretação sem classe (CIDR)

Rede		Estação	Máscara de subrede			Rede	Subrede	Estação
130.1	5.1	255.255.255.0	130.1	5	1			
interpretação original por classe		interpretação como subrede de classe						

Acetatos 19

Arquiteturas e Protocolos de Comunicação

Subnetting

permite melhor aproveitamento, organização e gestão do espaço de endereços

introduz níveis hierárquicos no *routing*

exemplificação da criação de sub redes utilizando a máscara /24 no bloco 130.1 /16

Acetatos 20

Arquiteturas e Protocolos de Comunicação

Subnetting

exemplo de criação de sub redes utilizando a máscara /27 no bloco 130.1 /16

Este segmento (subrede) apenas tem duas estações (os dois routers)

Não é permitido separar subendereços com igual prefixo por subredes não-contíguas

router
subrede

Paulo Almeida/José Oliveira @2005 Acetatos 21

Arquiteturas e Protocolos de Comunicação

Encaminhamento IP

O encaminhamento na internet é feito por *routers*.
Um router executa duas funções fundamentais:

- Routing;
- Forwarding;

Routing – o processo pelo qual o *router* calcula o conjunto de rotas, ou caminhos, para endereços Internet e o prepara para utilizar sob a forma de uma tabela de encaminhamento.

Forwarding – a forma como um *router* utiliza a tabela de encaminhamento para (re)enviar cada pacote recebido no seu salto seguinte.

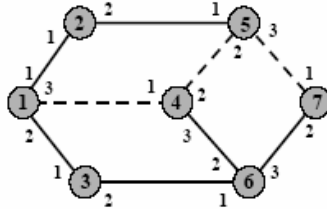
A informação que cada *router* necessita é a seguinte: para cada endereço de destino que figure num pacote, qual o interface pelo qual enviar esse pacote?

Paulo Almeida/José Oliveira @2005 Acetatos 22

Encaminhamento IP



Considere-se a rota tracejado entre os routers 1 e 7:



Para o nó 1 enviar um pacote ao nó 7, precisa saber:

- que a rota para 7 é através do nó vizinho 4;
- que para isso tem de enviar o pacote pelo interface 3;

Não necessita conhecer a rota completa 1-4-5-7 pois:

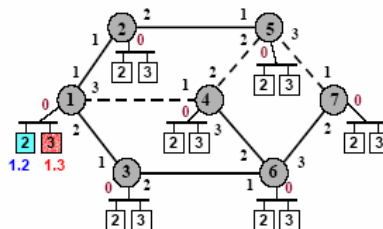
- confia no nó 4 para reenviar o pacote correctamente
- a rota vista por 4 poderá ser outra, por exêmplo, 4-6-7

Encaminhamento IP



Consideraremos nesta rede de exemplo que:

- cada router apenas liga uma sub rede;
- o interface de cada router na sua sub rede tem o número 0;
- há duas estações em cada sub rede (modelo usado no NW);
- o número da sub rede (n) é o número do router;
- o endereço global de cada estação (h) é n.h;
- por ex, a estação 2 ligada ao router 1 tem endereço 1.2;



Os datagramas originados na sub rede 1 destinados à sub rede 7 seguem através do interface 3, para o router 4

Encaminhamento IP



Como é que um router decide qual a melhor rota para um determinado router de destino?

Se o destinatário está na mesma rede, então o pacote IP é enviado directamente para o destino;

Caso contrário, se a tabela de encaminhamento estiver vazia, o pacote IP é enviado para o router por omissão;

Se a tabela de encaminhamento não estiver vazia, procura na tabela a rota destino (a rota mais específica é a utilizada).

As rotas são calculadas otimizando alguma medida ao longo dos caminhos que possam ser percorridos.

A medida é designada por função custo

Funções custo mais usadas no encaminhamento:

Número de Saltos (hop count)

Atraso (delay)

Encaminhamento IP



A actualização da tabela de encaminhamento pode ser feita das seguintes formas:

Estática:

as rotas são introduzidas manualmente na tabela
as rotas permanecem fixas

Dinâmica:

o router calcula automaticamente as rotas óptimas
as rotas mudam ao longo do tempo

A configuração automática das rotas é feita por um protocolo:

Interior - Gateway Protocol (IGP), usado dentro de um sistema autónomo (AS). Protocolos: RIP, OSPF

Exterior Gateway Protocol (EGP), usado entre AS's.
Protocolos: BGP

Encaminhamento IP



Tabela de encaminhamento:

- Endereço IP destino (host ou rede);
- Endereço IP do next-hop router;
- Flags, definem o tipo de entrada (directa ou next-hop);
- Métrica ou custo, define a melhor rota;
- Interface a usar para chegar ao next-hop router.

exemplo:

Destino	Next-hop	Flags	Métrica	Interface
172.17.0.0/24		U	0	eth0
192.168.130.1/32	172.17.0.254	UG	0	eth0
193.137.7.0/24	172.17.0.253	UG	0	
* 0.0.0.0/0	172.17.0.1	UG	0	

* por omissão (default); U rota activa (up); G usar next-hop (gateway)

Encaminhamento IP



Rota de defeito é a rota a seguir caso não exista uma entrada específica na tabela para a rede de destino:
 é um caso particular de encaminhamento estático
 é identificado pelo termo default ou pela subrede 0.0.0.0 /0

exemplo:

```
> netstat -nr
```

destination	gateway	use	interface
default	192.110.1.254	102410	tu0
192.110.1.0	192.110.1.240	234576	tu0
192.168.1.0	192.110.1.253	124586	tu1


Leitura da terceira linha:

Um datagrama gerado na estação que seja destinado à subrede 192.168.1.0 será entregue ao nó de endereço 192.110.1.253 saindo pela interface local tu1

Obs: Trata-se de uma estação com dois interfaces (tu0 e tu1), na mesma subrede

Arquiteturas e Protocolos de Comunicação

ARP -Address Resolution Protocol



Endereço IP → Endereço físico
Necessário para algumas tecnologias

O protocolo IP tem de passar à tecnologia subjacente o endereço físico do sistema ao qual deve ser entregue o pacote IP. Para tal recorre ao protocolo ARP

Uma vez que os sistemas podem mudar de endereços IP ou mudar de interface de rede é necessário um mapeamento dinâmico


Modo de funcionamento típico:

- O IP pede ao ARP o endereço físico correspondente a um dado endereço IP
- O ARP procura o endereço IP na sua tabela de mapeamento:
Se encontrar, devolve o respectivo endereço físico se não:
- Constrói uma mensagem ARP e utiliza a tecnologia subjacente para enviar essa mensagem a todos os sistemas da rede (broadcast)
- Espera resposta do sistema cujo endereço IP é o pretendido
- Adiciona o mapeamento à tabela
- Devolve o endereço físico ao IP

Paulo Almeida/José Oliveira @2005Acetatos 29

Arquiteturas e Protocolos de Comunicação

ARP -Address Resolution Protocol



Formato da mensagem

	0	8	16	31	
Header	Hardware type		Protocol type		4 bytes
	Hw length	Prot. length	Opcode		
	Source hardware address				n bytes (variável)
	Source protocol address				
	Destination hardware address				
	Destination protocol address				

Paulo Almeida/José Oliveira @2005Acetatos 30

ARP -Address Resolution Protocol



Formato do pacote (cont.)

Hardware type (16b) – tipo de endereço físico (ethernet=0x1)

Protocol type (16b) – tipo de protocolo (ip=0x800)

Hardware address length (8b) – tamanho do endereço de hardware (ethernet=6B)

Protocol address length (8b) – tamanho do endereço de protocolo (ip=4B)

Opcode (16b) – tipo de mensagem ARP: Request , Reply

Source hardware address – identifica remetente (MAC)

Source protocol address – identifica remetente (IP)

Destination hardware address – identifica destinatário ou vazio

Destination protocol address – identifica destinatário (IP)

ARP -Address Resolution Protocol



Exemplo:

172.17.0.2 → Endereço físico

Pedido (enviado por 172.17.0.1 para todos os sistemas)

- Request(
 - 00:B0:D0:38:AB:B9, a quem devem responder (MAC)
 - 172.17.0.1, a quem devem responder (IP)
 - 0, endereço MAC a determinar
 - 172.17.0.2) destinatário do pedido

Resposta (do sistema 172.17.0.2)

- Reply (
 - 00:C0:E0:11:22:33, o meu endereço MAC
 - 172.17.0.2, o meu endereço IP
 - 00:B0:D0:38:AB:B9, quem solicitou (MAC)
 - 172.17.0.1) quem solicitou (IP)

Arquiteturas e Protocolos de Comunicação

ARP -Address Resolution Protocol

Exemplo (cont.):

- Trama ethernet:
- Ethernet header
- ARP header
- ARP data

Trama ethernet (pedido):

FF:FF:FF:FF:FF:FF (dst), 00:B0:D0:38:AB:B9 (src), 0x806 (arp), 0x1 (ethernet), 0x800 (ip), 0x6 (mac len), 0x4 (ip len), 0x1 (request), 00:B0:D0:38:AB:B9, 172.17.0.1, 0, 172.17.0.2

Trama ethernet (resposta):

00:B0:D0:38:AB:B9 (dst), 00:C0:E0:11:22:33 (src), 0x806 (arp), 0x1 (ethernet), 0x800 (ip), 0x6 (mac len), 0x4 (ip len), 0x2 (reply), 00:C0:E0:11:22:33, 172.17.0.2, 00:B0:D0:38:AB:B9, 172.17.0.1

Paulo Almeida/José Oliveira @2005Acetatos 33

Arquiteturas e Protocolos de Comunicação

ARP -Address Resolution Protocol

Sistema destinatário ausente

- ARP envia pedido e espera um determinado tempo pela resposta;
- Se resposta não chega, repete o processo com um tempo de espera maior;
- Se ocorrer um *timeout* o processo termina

Tabela de mapeamento

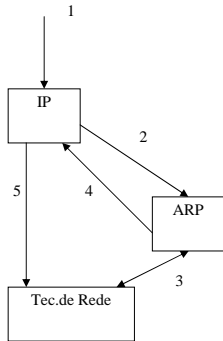
- Por cada pedido de resolução satisfeito é guardado o mapeamento numa tabela com um tempo de vida (TTL).
- Se o TTL acabar, a entrada é removida

Gratuitous ARP

- O sistema envia um pedido com o seu próprio endereço IP.
- Usado no arranque do sistema para verificar se não existe outro sistema activo com o mesmo endereço

Paulo Almeida/José Oliveira @2005Acetatos 34

Interacção entre o IP e o ARP



1. **Enviar (End. IP; Dados)**
2. **Resolver (End. IP)**
Consulta tabela, existe entrada?
Não, constrói pacote ARP com End. IP
3. **Enviar (Broadcast, Pacote ARP)**
Recebe pacote ARP do sistema destinatário
Actualiza tabela → 4.
- Sim,
4. **Resposta (End. IP, End. Físico)**
Constrói pacote IP
5. **Enviar (End. Físico, Pacote IP)**

Interacção entre o IP e o ARP



Destinatário e remetente na mesma rede

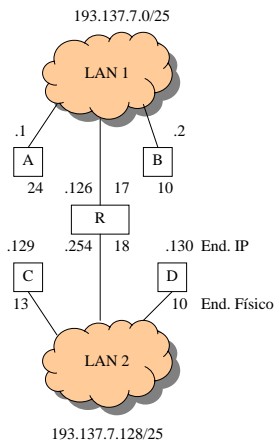


Tabela ARP de A

IP	Físico
193.137.7.126	0A 3B 44 C2 EF 17

- A → B
1. Enviar (193.137.7.2; Dados)
 2. Resolver (193.137.7.2)
 3. Enviar (FF FF FF FF FF FF, Pacote ARP)
 4. Resposta (193.137.7.2, 0A 3B 44 C2 EF 10)
 5. Enviar (0A 3B 44 C2 EF 10, Pacote IP)

Interacção entre o IP e o ARP



Destinatário e remetente em redes distintas

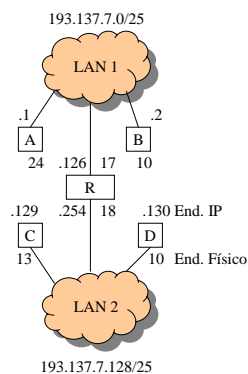


Tabela ARP de A

IP	Físico
193.137.7.126	0A 3B 44 C2 EF 17
193.137.7.2	0A 3B 44 C2 EF 10

- A → D (A → R; R → D)
1. Enviar (193.137.7.130; Dados)
IP determina que D está noutra rede
 2. Resolver (193.137.7.126)
 4. Resposta (.126, 17)
 5. Enviar (17, Pacote IP)
-
2. Resolver (.130)
 3. Enviar(FF, Pacote ARP)
 4. Resposta (.130, 10)
 5. Enviar(10, Pacote IP)

Reverse ARP



Endereço físico → Endereço IP

Utilizado por sistemas sem disco. Sabe o seu endereço físico (embutido na interface de rede) e necessita do endereço IP

Constrói uma mensagem RARP e envia por *broadcast*

Formato da mensagem RARP igual ao ARP (trama ethernet com o campo type=0x8035)

Servidor na rede com todos os mapeamentos de endereços físicos para endereços IP

Preferível usar o protocolo de aplicação BOOTP (*Bootstrap Protocol*)

Internet Control Message Protocol -ICMP



Parte integrante do pacote IP

Serve principalmente para enviar mensagens de erro bem como outras condições que mereçam atenção

Normalmente, para reportar erros ocorridos no processamento de pacotes IP

Utiliza o IP para enviar as mensagens

As mensagens ICMP são construídas/usadas pelos protocolos IP, TCP e UDP e às vezes pelo próprio processo do utilizador.

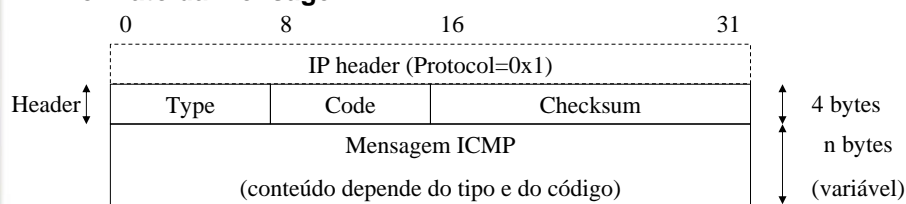
Não pretende tornar o protocolo IP fiável, apenas acrescentar ferramentas que lhe permitam obter retorno sobre problemas na rede

Qualquer problema com uma mensagem ICMP não deve gerar outra mensagem ICMP

Internet Control Message Protocol -ICMP



Formato da mensagem



- Type – identifica o tipo de mensagem
- Code – distingue dentro de um tipo as várias mensagens
- Checksum – serve para detectar erros de paridade

Arquiteturas e Protocolos de Comunicação

Internet Control Message Protocol -ICMP

Mensagens (tipo, código):

- Echo reply (0,0)/request (8,0)
- Destination unreachable (3,):
 - 0-network/1-host/2-protocol/3-port unreachable, ...
 - 6-network unknown/7-host unknown/admin. prohibited(9/10),
 - 13-communication admin. prohibited by filtering, ...
- Source quench (4,0) – GW/Dst Host: sugerir controlo de fluxo
- Redirect (5,0-network/1-host/...) – GW: sugerir rota alternativa
- Router advertisement (9,0)/solicitation(10,0)
- Time exceeded (11,0-transit(TTL=0)/1-reassembly)
- Parameter problem (12,0-ip header/1-ip option)
- Timestamp request (13,0)/reply (14,0)
- ...

Paulo Almeida/José Oliveira @2005Acetatos 41

Arquiteturas e Protocolos de Comunicação

Internet Control Message Protocol -ICMP

Mensagem ICMP e segurança

Muitos sistemas intermédios (routers) e destinatários não enviam alguns tipos de mensagem para evitarem:

- Negação de serviço
- Conhecimento de serviços disponibilizados
- Conhecimento das políticas de segurança
- Aumento excessivo de tráfego

Utilização de *firewalls* para proteger o sistema ou a rede:

- Pode e deve negar algumas das mensagens ICMP, por exemplo o Echo request
- Deve no entanto deixar passar outras, por exemplo o Source quench. Esta mensagem é enviada pelo router quando tem as filas de espera cheias (congestionado) ou por sistemas destinatários que estejam a atingir a sua capacidade máxima de processamento. Os sistemas remetentes devem diminuir o fluxo de pacotes

Paulo Almeida/José Oliveira @2005Acetatos 42

Camada de rede



Interação entre camadas (níveis)

