Apostila de "Internet e Arquitetura TCP/IP"
volume I I

Curso de Redes de Computadores

2ª edição

Carlos Antonio Silva Junior

1. Protocolos da camada de Rede e Protocolos auxiliares de TCP/IP

Este protocolos são agrupados neste capítulo, por fornecerem serviços auxiliares para TCP/IP, tanto a nível de enlace OSI quanto a nível a de aplicação.

BOOTP e DHCP

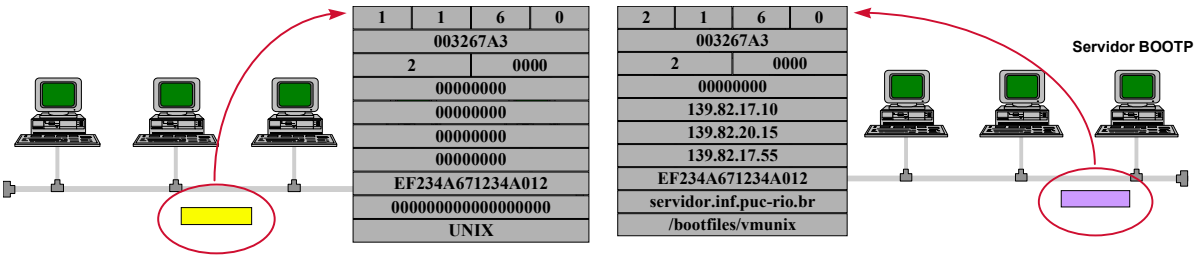
Este protocolos fornecem aos protocolos TCP/IP, as informações iniciais de configuração da máquina tais como endereço IP, máscara de sub-rede, roteadores default, rotas, servidores de Boot, servidores de nome e diversas outras informações. Eles são utilizados principalmente para realizar a administração centralizada de máquinas TCP/IP e possibilitar o BOOT de máquinas sem rígido e sem informações iniciais de configuração. O BOOTP (Bootstrap Protocol) é o protocolo mais antigo e o DHCP (Dynamic Host Control Protocol) está aos poucos o substituindo. O BOOTP é bastante utilizado para o boot inicial de dispositivos de rede, como roteadores, switches, hubs gerenciáveis, além de estações Unix diskless (sem disco e cada vez mais raras hoje). O DHCP é um pouco mais complexo e mais versátil e vem sendo utilizado principalmente para simplificar a administração de endereços e outros parâmetros de configuração de grandes instalações de máquinas TCP/IP.

Protocolo BOOTP

A mensagem BOOTP é encapsulada em UDP e possui o seguinte formato:

0	7	15	23	31
Octeto 1	Octeto 2	Octeto 3	Octeto 4	
OP (1=Req,2=Rep)	HW TYPE	HLENGTH	HOPS	
TRANSACTION ID				
SECONDS (tempo desde o boot)	UNUSED			
CLIENT IP ADDRESS (se cliente souber)				
YOUR IP ADDRESS				
SERVER IP ADDRESS				
GATEWAY IP ADDRESS				
CLIENT HARDWARE ADDRESS (16 OCTETS)				
SERVER HOST NAME (64 OCTETS)				
BOOT FILE NAME (128 OCTETS)				
VENDOR-SPECIFIC AREA (64 OCTETS)				

As mensagens BOOTP Request e BOOTP Reply tem o mesmo formato mas no Request alguns campos não são preeenchidos. Uma estação que deseja obter informações de configuração pode enviar uma mensagem BOOTP Request por broadcast. Um servidor de BOOTP pré configurado na rede com os parâmetros de cada cliente, receberá a mensagem e enviará os dados previamente armazenados para o cliente. Este procedimento é mostrado nas duas figuras abaixo:



Na área Vendor-Specific da mensagem BOOTP podem ser colocadas uma série de variáveis possíveis adicionais para configuração da estação cliente de BOOTP. Estas opções são definidas em RFCs adicionais e servem tanto para BOOTP quanto para DHCP.

Protocolo DHCP

O DHCP tem como principal vantagem em relação ao BOOTP a sua capacidade de configuração automática de estações, sem necessidade de criação de uma tabela de configuração para cada máquina (com seus parâmetros e endereços MAC respectivos, como é o caso de BOOTP). Desta forma, um administrador de rede pode configurar as diversas estações IP existentes na rede de modo genérico, sem especificar uma tabela para cada uma.

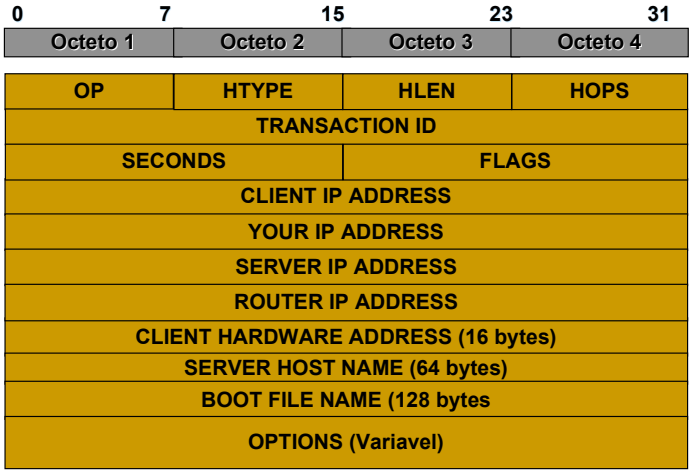
O DHCP tem a capacidade de distribuir endereços de forma dinâmica para as estações, usando três métodos de fornecimento distintos:

- Empréstimo (leasing) de endereço aleatório por tempo limitado: Neste tipo de fornecimento de endereço IP, o servidor fornece ao cliente um endereço IP obtido de um conjunto pré-definido de endereços (p.ex. 192.168.0.10 a 192.168.0.90) por um tempo pré determinado.

- Empréstimo de endereço aleatório por tempo infinito: Neste tipo, o servidor associa um endereço obtido do conjunto de endereços a um cliente na primeira vez que este cliente contactar o servidor. Nas demais vezes, será fornecido o mesmo endereço a este cliente (associado através do endereço MAC), mesmo que as duas máquinas sejam desligadas e ligadas. Este método simplifica a atribuição de endereços para uma quantidade grande de máquinas.

- Empréstimo de endereço fixo: Neste tipo de fornecimento, o DHCP opera como o BOOTP, onde há a associação explícita entre o endereço IP e o endereço MAC da máquina origem, estipulado em uma tabela de configuração

A mensagem DHCP é compatível com BOOTP e possui o formato abaixo:



Ao contrário da mensagem BOOTP que possui apenas dois tipos de comandos (REQUEST e REPLY), a mensagem DHCP possui 8 tipos de comandos. Este comandos não são colocados no campo OP, como em

BOOTP, mas para manter a compatibilidade, são colocados como uma opção especial no campo OPTIONS, a de código 53, associado a um dos comandos abaixo:

DHCP DISCOVER - Enviado pelo cliente para solicitar uma resposta de algum servidor DHCP
DHCP OFFER - Oferta de endereço IP de um servidor para um cliente. Um cliente pode receber várias ofertas de diferentes servidores DHCP
DHCP REQUEST - Requisição de um endereço específico daqueles oferecidos pelos servidores. É enviado por broadcast apesar de ser endereçado a um único servidor para que os demais tomem conhecimento da escolha.
DHCP DECLINE - Informa que a oferta contêm parâmetros incorretos (Erro)
DHCP ACK - Confirmação do servidor sobre a atribuição do endereço para a requisição do cliente.
DHCP NAK - Servidor nega o fornecimento do endereço previamente oferecido, geralmente causado por um erro ou pelo fato do cliente ter demorado muito a requisitar o endereço solicitado.
DHCP RELEASE - Cliente libera o endereço IP utilizado. Ë raramente utilizado na prática, pois geralmente o cliente é desligado sem liberar o endereço. Ele retorna ao conjunto de endereços disponíveis no servidor devido ao estouro do tempo de leasing.
DHCP INFORM - Cliente que já possui endereço IP pode requisitar outras informações de configuração respectivas àquele endereço.

A operação de DHCP define diversos estados de funcionamento, quando o cliente está executando alguma ação e enviando uma das mensagens acima:

1. INITIALIZE
   - Configura interface com valor zero pois não tem endereço disponível - 0.0.0.0
   - Envia DHCPDISCOVER(UDP 67) como broadcast e muda para estado SELECT. Nesta mensagem, pode colocar opções de configurações desejadas
2. SELECT
   - Pode receber uma ou várias mensagens DHCPOFFER, cada uma com seus parâmetros distintos
   - Escolhe uma, envia DHCPREQUEST como broadcast e vai para estado REQUEST
3. REQUEST
   - Aguarda até receber DHCPACK do servidor escolhido. Se não receber, escolhe outra oferta e a solicita
   - Vai para o estado BOUND.
4. BOUND
   - É o estado normal de funcionamento.
   - Passa a utilizar o endereço, durante o tempo especificado pelo servidor
   - Quando o tempo atingir 50%, envia novo DHCPRequest para o servidor e passa para estado RENEW
   - Para cancelar o uso da endereço envia DHCPRelease
5. RENEW
   - Servidor pode enviar DHCPNAK, DHCPACK ou nenhuma resposta à solicitação de Request
   - Se receber ACK, volta para o estado BOUND
   - Se não receber resposta nenhuma, o cliente envia DHCPREQUEST em broadcast para que outros servidores possam enviar ofertas.
   - Se receber DHCPNAK, libera IP e vai para estado INITIALIZE

Opções DHCP

As opções DHCP tem o formato abaixo:

CODE	LENGTH	VARIÁVEL ...

O código indica o tipo da opção. Os comandos DHCP tem sempre o código 53 e tamanho 1, sendo o próximo byte o código específico do comando:

1 = DHCPDISCOVER
2 = DHCPOFFER
3 = DHCPREQUEST
4 = DHCPDECLINE
5 = DHCPPACK
6 = DHCPNACK
7 = DHCPRELEASE
8 = DHCPINFORM

As opções de DHCP e BOOTP informam dados úteis para as diversas camadas TCP/IP, desde o nível de Reda ao Nível de Aplicação. Enumera-se algumas abaixo:

Opções Básicas:

Code	Param	Descrição
0		Pad - alinhamento
255		Fim das opções
1	MASK	Máscara a ser utilizada pela estação
3	IP1, IP2, ...	Lista de roteadores default para a estação
6	IP1, IP2, …	Lista de servidores de DNS
9	IP1, IP2, …	Lista de servidores de impressão LPR
12	nome	Nome da máquina
13	número	Tamanho do arquivo de boot
15	nome	Nome do domínio
16	IP	Endereço do servidor de swap
17	nome	Path do diretório / da máquina

Opções de DHCP

Code	Param	Descrição
50	IP	Endereço IP requerido preferencialmente
51	tempo (s)	Tempo de empréstimo de endereço
53	**mensagem**	**Mensagem DHCP**
54	IP	Identificação do servidor DHCP remetente
55	COD1, …	Cliente requisita opções ao servidor
56	texto	Mensagem de erro
57	número	Tamanho máximo da mensagem DHCP
58	tempo	T1 - Tempo de espera para estado RENEWING
59	tempo	T2 - Tempo de espera para estado REBINDING

Opções de IP

Code	Param	Descrição
19	1/0	Habilita IP Forwarding na estação
20	1/0	Habilita Source Routing na estação
22	número	Tamanho máximo do datagrama que cliente deve receber
23	número	Tamanho do TTL default da máquina
26	número	MTU da interface
27	1/0	Todas as interfaces tem o mesmo MTU ?
28	IP	Endereço de broadacst da rede
29	1/0	Realizar ICMP Mask Discovery ?
31	1/0	Realizar ICMP Router Discovery ?
33	IP1/DEST1, IP2/DEST2, ..	Rotas estáticas

Protocolo PPP

O protocolo PPP (Point-to-Point Protocol) é o principal protocolo para o transporte de IP sobre ligações ponto a ponto, criando um nível de enlace em um meio que não o possua. O PPP é empregado como protocolo de

enlace nos seguintes tipos de meio: ligações seriais discadas, ligações seriais dedicadas (enlaces telefônicos, satélite, rádio), ligações ISDN e outras.

Pode-se diferenciar o funcionamento de PPP em dois grupos principais: quando empregado em ligações discadas ele provê os mecanismos de autenticação, com a correspondente interação com os dispositivos para verificar a autenticidade do originador da chamada, além de que as mensagens trocadas diferenciam o originador da chamada do receptor da chamada. Quando empregado em ligações dedicadas, geralmente não são trocadas mensagens de autenticação e o funcionamento do protocolo é praticamente simétrico em relação às mensagens trocadas.

PPP é genérico podendo carregar diversos protocolos de nível de rede OSI, além de possuir uma série de opções que podem ser negociadas pelos dois lados da conexão. PPP provê três tipos de funcionalidade:

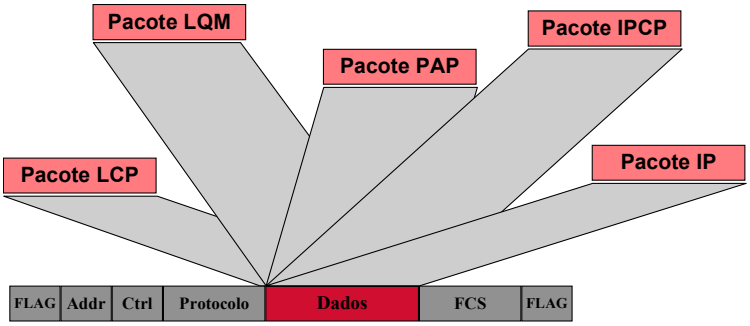
- Encapsulamento
- Protocolos de Controle do Enlace PPP (protocolo LCP, PAP, CHAP, LQM)
- Protocolos de Controle do Protocolo de Nível 3 sendo carregado (protocolos IPCP, IPXCP, …)

O Encapsulamento de PPP na verdade não faz parte do protocolo, permitindo que ele se encaixe em outros protocolos de nível de enlace. O PPP pode utilizar diversos tipos de encapsulamento compatíveis com HDLC, ISDN e outros. Na sua forma default, o encapsulamento de PPP é similar ao início de um pacote HDLC, conforma a figura abaixo:

7E FF 03 7E

Os campos FLAG, ADDR e CTRL são similares a HDLC. Os campos Protocolo, Dados e FCS são comuns a todo pacote PPP. Protocolo contém o protocolo sendo carregado no campo de dados, sendo por exemplo os valores: **LCP = C021, IPCP = 8021, IPXCP = 802B, PAP = C023, CHAP = C223, LQR = C025, IP = 0021, IPX = 002B, Bridging NCP = 8031, Netbios = 803F, ...**

O encapsulamento dos diversos protocolos sobre PPP é mostrado na figura abaixo:



Pacote PPP

Protocolo LCP - Link Control Protocol

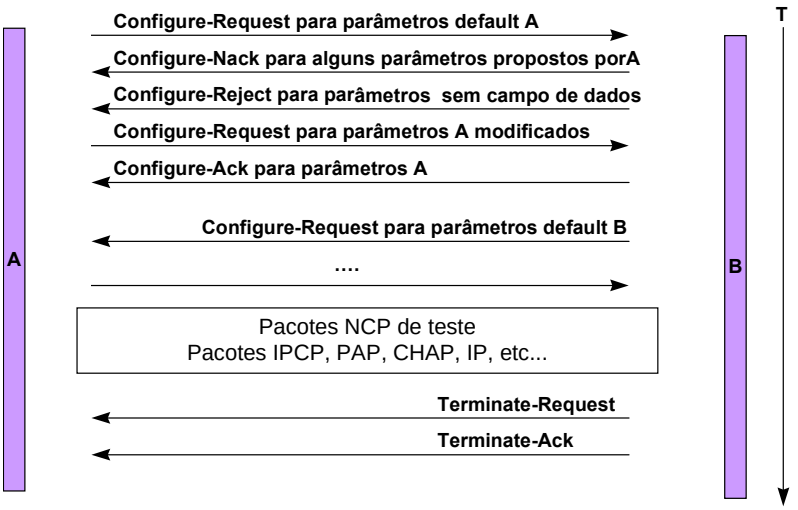
Este protocolo controla o enlace PPP. O formato de sua mensagem é dado abaixo:

COMANDO	ID	Length	Dados Variáveis

O Comando pode ser um dos seguintes tipos:

- Configure-Request: Solicita o aceite para as opções especificadas no campo de dados
- Configure-Ack: Concorda com as opções, para serem utilizadas pelo outro lado
- Configure-Nack: Rejeita as opções, enumerando-as no campo de dados
- Configure-Reject: Rejeita as opções que não possuem um campo de valor
- Terminate-Request: Informa o fim da conexão PPP
- Terminate-Ack: Concorda com o fim da conexão
- Code-Reject: Informa erro no código do comando LCP
- Protocol-Reject: Informa erro no protocolo da mensagem PPP
- Echo-Request
- Echo-Reply
- Discard-Request

A troca de dados em uma conexão PPP é realizada conforme a figura abaixo. Os comandos de configuração do link PPP (LCP) são trocados com o objetivo de estabelecer os parâmetros de operação da ligação. Após o acordo dos comandos de configuração, são passados os comandos de configuração do protocolo de dados (IPCP) e, apóes estes, são finalmente passados os pacotes do protocolo IP.



As opções de configuração LCP mais utilizadas são:

- Maximum Receive Unit
- Authentication Protocol
- Quality Protocol
- Magic Number
- Protocol Field Compression
- Address Control Field Compression

Em ligações discadas é comum os servidores de acesso remoto possuírem a opção de detecção automática de PPP. Neste caso, como, geralmente os primeiros pacotes PPP trocados são os Configure-Request, basta que o receptor verifique se os dados correspondem aos códigos deste comando e, então, iniciem automaticamente o PPP.

Protocolo IPCP - Network Control Protocol

Os comandos possíveis no protocolo IPCP são:

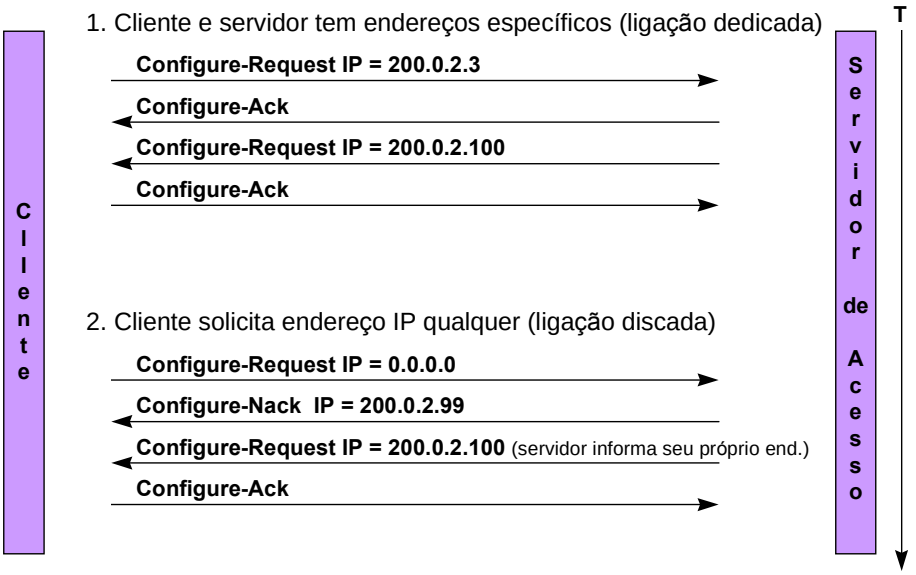
- Configure-Request: Solicita o aceite para as opções especificadas no campo de dados
- Configure-Ack: Concorda com as opções, para serem utilizadas pelo outro lado
- Configure-Nack: Rejeita as opções, enumerando-as no campo de dados
- Configure-Reject: Rejeita as opções que não possuem um campo de valor
- Terminate-Request: Informa o fim da troca de dados IP
- Terminate-Ack: Concorda com o fim da troca de dados
- Code-Reject: Informa erro no código do comando IPCP

Este comandos são trocados de forma semelhante ao LCP, sendo que ao término da fase de acordo do IPCP, passam os dados do protocolo IP.

As principais opções de configuração de IPCP são:

- IP Compression Protocol: Informa se será utilizado algum protocolo de compressão (e qual) para o cabeçalho IP
- IP Address: origem informa ao destino o endereço IP a ser utilizado pela origem. No caso de conter 0.0.0.0 (que ocorre tipicamente na estação que realiza uma ligação serial discada), o outro lado (neste caso o servidor de acesso remoto) fornece o endereço IP a ser utilizado pela origem, através do comando Configure Nack.

As possíveis formas de negociação de endereço IP são dadas pela figura abaixo:



Protocolo SLIP

SLIP fornece apenas o encapsulamento para um enlace serial. Sua mensagem é dado na forma abaixo:

0xDB - ESC **0xC0 - END**

O funcionamento de SLIP ocorre da seguinte forma:

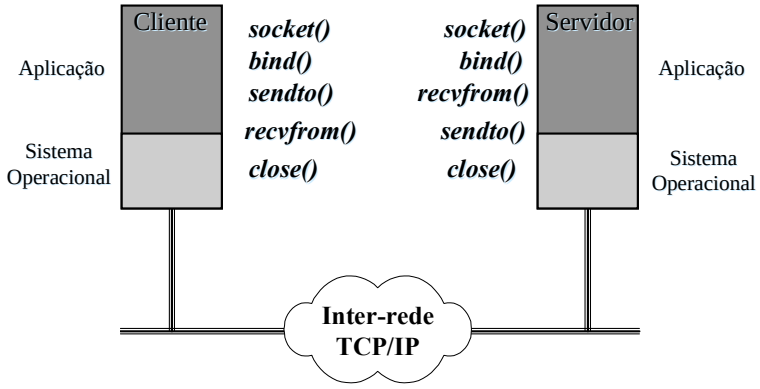
- Transmite ESC
- Transmite datagrama, caracter por caracter, substituindo um ESC nos dados por ESC ESC
- Transmite END

3. Interfaces do Nível de Transporte (socket, WinSock)

A interface de socket do Unix é um conjunto de funções para permitir a utilização do sistema de comunicação por processos (programas) neste sistema operacional. A interface Winsock é composta de funções semelhantes a socket, para o ambiente Windows.

A interface socket possui funções distintas para a comunicação com e sem conexão.

A utilização das funções de socket para a comunicação **sem conexão** é dada abaixo:



A utilização destas funções é dada abaixo:

- socket: Inicializa a estrutura de dados do socket (equivalente ao SAP - Ponto de acesso de serviço), determinando qual o protocolo (PF_INET = TCP/IP) e o tipo do serviço (DGRAM = UDP e STREAM = TCP)

- bind: associa o socket a uma porta USP ou TCP - pode-se dizer que para o programador, a porta do protocolo TCP ou UDP é efetivamente o socket.

- sendto: solicita ao sistema de comunicação o envio de dados, especificando o endereço IP destino e a porta destino, além dos próprios dados.

- recvfrom: informa ao sistema de comunicação que o programa está aguardando dados. O programa será congelado enquanto não houverem dados para receber, sendo reativado quando chegarem dados.

- close: desassocia a porta do socket e desativa o socket.

Deve-se observar que nem todas as funções geram mensagens de rede. De fato, apenas a função sendto gera uma mensagem.

A sintaxe destas funções é mostrada abaixo:

```
sock1 = socket (pf, type, protocol)
      pf = PF_INET | PF_APPLETALK | PF_NETW | PF_UNIX
      type = SOCK_STREAM | SOCK_DGRAM | SOCK_RAW | SOCK_RDGRAM

close (sock1)

bind (sock1, localaddr, addrlen)
      localaddr = struct {ADDR_FMLY, PROTO_PORT, IP_ADDR}

sendto (sock1, message, length, flags, destaddr, addrlen)
```

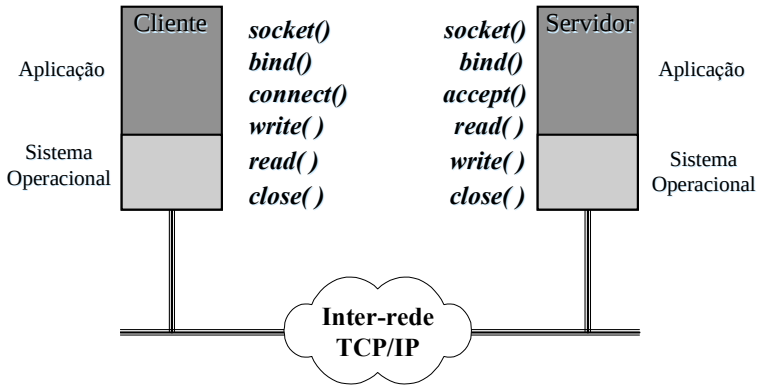
```
recvfrom (sock1, buffer. length, flags, fromaddr, addrlen)

nptr = gethostbyname (name)
      nptr = struct {name, aliases, address_type, address}

nptr = gethostbyaddr (addr, len, type)

sptr = getservbyname (servname, proto)
      sptr = struct {name, protocol, port)
```

No caso de comunicação utilizando conexão, a utilização das funções é dada na figura abaixo:



A sintaxe das funções adicionais é dada abaixo:

```
connect (sock1, destaddr, addrlen)
      destaddr = struct {ADDR_FMLY, PROTO_PORT, IP_ADDR}

write (sock1, data, length)

read (sock1, buffer, length)

listen (sock1, qlength)

newsocket = accept (sock1, addr, addrlen)

ready = select (ndesc, indesc, outdesc, excdesc, timeout)
```

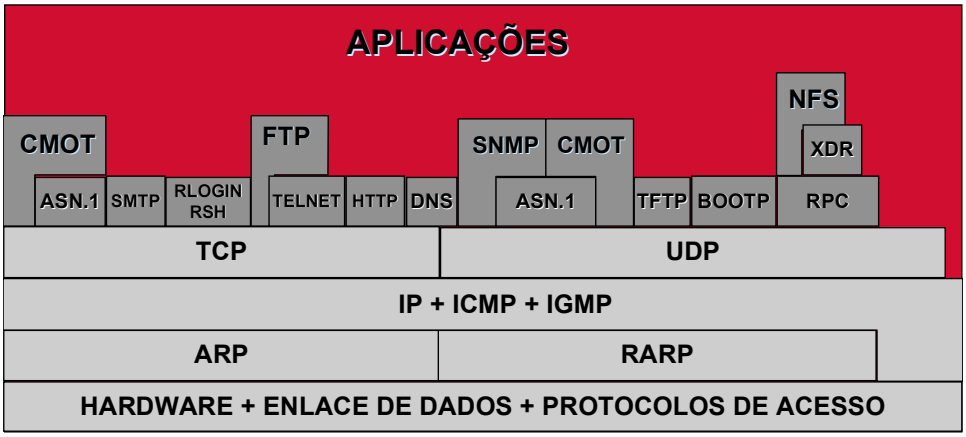
ndesc = numero de descritores a serem examinados
indesc = descritores examinados
excdesc = descritores examinados para exceção
timeout = tempo máximo de espera

4. Protocolos de Nível de Aplicação

Os protocolos de aplicação TCP/IP são aqueles que realizam as funções de alto-nível e que utilizam os serviços da camada de transporte UDP ou TCP para a comunicação.

Os protocolos de aplicação podem realizar funções diretamente acessíveis pelo usuário como FTP, HTTP, SMTP, POP3, IMAP4, Finger, Telnet, Chat, NFS, TFTP, NNTP e outros. Além disto, podem também realizar funções mais próximas do sistema de comunicação, tais como os protocolos DNS, BOOTP, DHCP, SNMP, BGP4, e outros.

As aplicações são ilustradas na figuira abaixo:



Protocolo DNS

O protocolo DNS (Domain Name System) especifica duas partes principais: regras de sintaxe para a definição de domínios e o protocolo utilizado para a consulta de nomes.

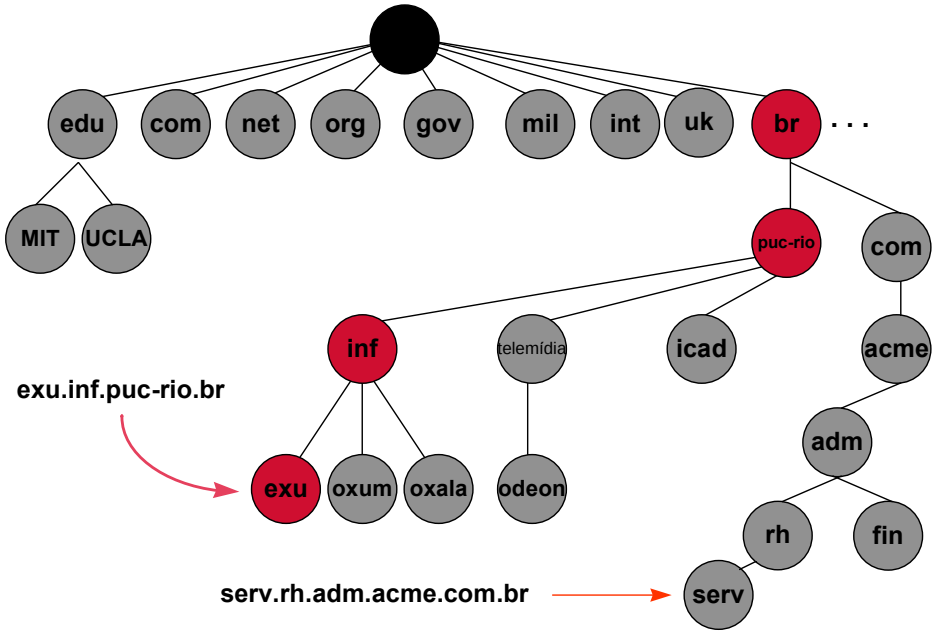
O DNS é basicamente um mapeamento entre endereços IP e nomes. A abordagem inicial para este mapeamento era a utilização de nomes planos, ou seja, sem hierarquia. Esta abordagem possui limitações intrínsecas quanto a escalabilidade e a manutenção. O sistema de nomes utilizado na Internet tem o objetivo de ser escalável, suportando a deinição de nomes únicos para todas as redes e máquinas na Internet e permitir que a administração seja descentralizada.

A estrutura de nomes na Internet tem o formato de uma árvore invertida onde a raiz não possui nome. Os ramos imediatamante inferiores à raiz são chamados de TLDs (Top-Level Domain Names) e são por exemplo .com, .edu., .org, .gov, .net, .mil, .br, .fr, .us, uk, etc… Os TLDs que não designam países são utilizados nos EUA. Os diversos países utilizam a sua própria designação para as classificações internas. No Brasil, por exemplo, temos os nomes .com.br., .gov.br, .net.br, .org.br e outros.

Cada ramo completo até a raiz como, por exemplo, puc-rio.br, acme.com.br, nasa.gov, e outros são chamados de domínios. Um domínio é a área administrativa englobando ele próprio e os subdomínios abaixo dele. Por exemplo o domínio .br engloba todos os subdomínios do Brasil. O domínio acme.com.br tem a responsabilidade por todos os domínios abaixo dele.

A delegação de responsabilidade de um domínio é a capacidade do DNS de simplificar a administração. Ao invés do domínio .br ser responsável diretamente por todos os seus sub-domínios e os que vierem abaixo deles, há na verdade uma delegação na atribuição de nomes para os diversos sub-domínios. No exemplo acima, a empresa Acme possui a responsabilidade de administração do domínio acme.com.br.

A hierarquia de domínios pode ser observada na figura abaixo:



Os domínios principais genéricos, chamados de GTLDs (Generic Top Level Domain Names) que são .net, .com e .org são administrados pelo Internic (Internet Network Information Center) que também é responsável pela administração do espaço de endereçamento IP. Recentemente foram criados novos nomes de domínio genéricos que serão utilizado a partir de 98. São eles: .firm, .store, .web, .arts, .rec, .infor, .nom.

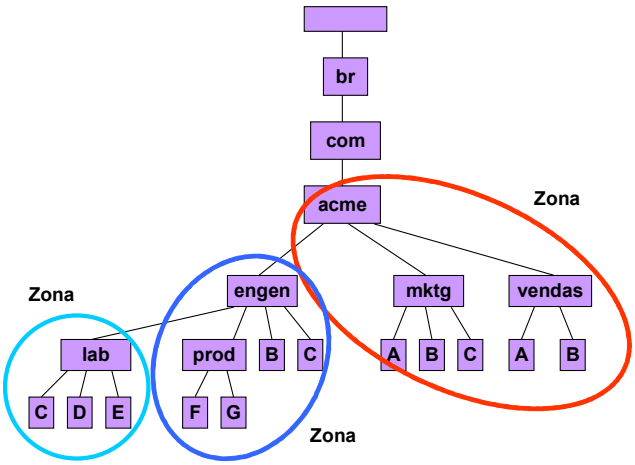
Os domínios são completamente independentes da estrutura de rede utilizada. Não existe necessariamente algum relacionamento entre eles. O DNS possui uma estrutura inversa para poder representar o endereçamento de rede, ou permitir que seja feito o mapemento do endereço IP correspondente a um nome. Esta estrutura possui como raiz principal a notação .arpa e possui como único ramo o .in-addr. Abaixo deste são colocados em ordem os bytes do endereço IP.

Implementação do DNS

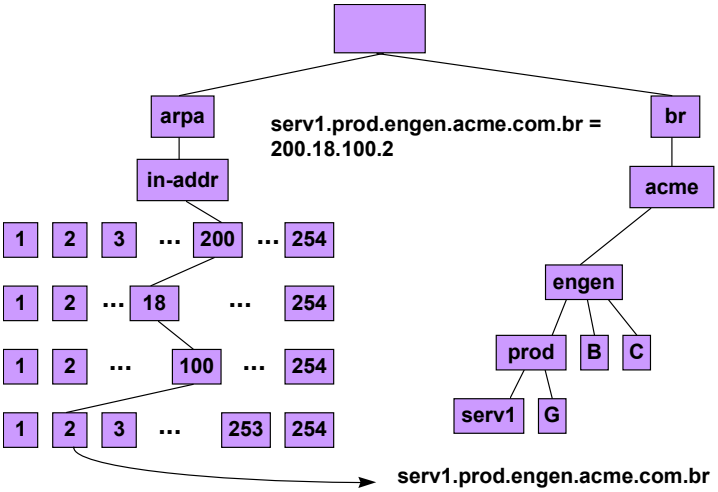
O DNS é implementado por meio de uma aplicação cliente-servidor. O cliente é o **resolver** (conjunto de rotinas em uma implementação de TCP/IP que permite a aconsulta a um servidor) e um servidor geralmente é o programa **bind** ou uma implementação específica de um servidor de DNS (Windows NT).

Um servidor de DNS pode ser responsável pela resolução de uma ou mais nomes de domínios (ex. acme.com.br, presid.acme.com.br). Seu escopo de atuação define a Zona de atuação de um servidor DNS. Por exemplo, para resolver o domínio acme.com.br e seus sub-domínios existem três zonas: a primeira resolve o próprio domínio principal e os subdomínios mktg.acme e vendas.acme; a segunda resolve os domínios engen.acme e prod.engen.acme; e a terceira resolve o domínio lab.engen.acme. Cada zona possui um servidor de nomes principal ou primário, que mantêm em tabelas o mapeamento dos nomes em endereços IP daquele domínio. Uma zona pode ter servidores secundários que possam substituir os primários em caso de falha. Os secundários, entretanto não possuem fisicamente as tabelas de mapeamento mas carregam regularmente as informações do primário.

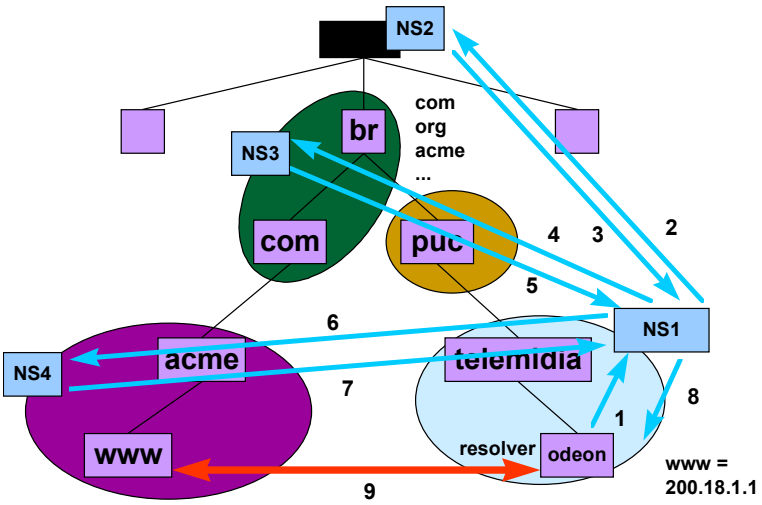
Veja figura abaixo:



Por outro lado, a representação do domínio reverso .in-addr.arpa para uma das máquinas de prod.engen.acme.com.br é visto abaixo:



A resolução de um nome é realizada de forma recursiva, consultando diversos servidores de nome até chegar àquele responsável pelo domínio consultado. Por exemplo a resolução do endereço www.lab.acme.com.br, será realizado pelo servidor da zona responsável por lab.acme.com.br. A figura abaixo ilustra o processo de consulta:


NS2
com
org
acme
...
br
NS3
com
puc
4
3
2
5
6
NS1
NS4
acme
telemidia
7
8
1
www
resolver
odeon
www =
200.18.1.1
9

Protocolos de Roteamento

Protocolo RIP

Conforme citado em capítulos anteriores, o IP possui vários mecanismos para obter informações para sua tabela de rotas (específicas de cada máquina). A tabela de rotas de IP pode ser preeenchida por meio de:

- Rotas default por meio de configuração estática (manual)
- Rotas específicas por meio de configuração estática (manual)
- Rotas default por meio do protocolo ICMP Router Advertisement
- Rotas específicas para estação por meio de ICMP Redirect
- Rotas aprendidas dinâmicamente por meio de protocolos de roteamento (ex. RIP, OSPF, BGP-4)

A última forma de aprendizado se aplica normalmente aos próprios roteadores, quando situados em redes complexas, já que suas tabelas de rota devem conter os detalhes de roteamento da rede (Uma estação por outro lado, pode ter rotas para um único roteador default e aprender rotas melhores por meio de ICMP Redirect).

O protocolo RIP é do tipo Vetor de Distância, já que baseia a escolha de rotas por meio da distância em número de roteadores. O funcionamento do protocolo RIP é bem simples, consistindo na divulgação de rotas de cada roteador para seus vizinhos (situados na mesma rede).

Cada roteador divulga sua tabela de rotas através de um broadcast na rede. Os demais roteadores situados na mesma rede recebem a divulgação e verificam se possuem todas as rotas divulgadas, com pelo menos o mesmo custo (custo é a quantidade de roteadores até o destino).

Se não possuírem rota para determinada rede divulgada, incluem mais uma entrada na sua tabela de rotas e colocam o roteador que a divulgou como o gateway para aquela rede. Em seguida, sua própria divulgação de rotas já conterá a rota nova aprendida. Este processo se repete para todos os roteadores em um conjunto de redes, de modo que, após várias interações, todos já possuem rotas para todas as redes. Uma rota aprendida é mantida enquanto o roteador que a originou continuar divulgando. Caso o roteador pare de divulgar a rota ou nenhuma mensagem de divulgação seja recebida dele, o roteador que havia aprendido a rota a mantêm por 160 segundos, findos os quais a rota é retirada da tabela de rotas. Neste caso, se outro roteador divulgar uma rota para aquela rede específica, esta será utilizada.

No caso em que um roteador, recebe rotas para uma mesma rede divulgadas por roteadores diferentes, a com menor custo é usada, sendo as demais descartadas.

O protocolo RIP não possui suporte para sub-rede (máscara de rede), o que só vem a ser suportado no protocolo RIPv2.

O custo de uma rota é a quantidade de roteadores que uma mensagem terá que atravessar desde o roteador que possui a rota até a rede destino. O custo máximo em RIP tem o valor de 16, que significa infinito. Por isto, o diâmetro máximo de uma rede com protocolo RIP é de 14 roteadores.

A mensagem RIP tem o seguinte formato:

0	7	15	23	31
Octeto 1	Octeto 1	Octeto 1	Octeto 1	

COMMAND	VERSION	MUST BE ZERO
FAMILY OF NET 1		MUST BE ZERO
IP ADDRESS OF NET 1		
MUST BE ZERO		
MUST BE ZERO		
DISTANCE TO NET 1		
FAMILY OF NET 2		MUST BE ZERO
IP ADDRESS OF NET 2		
MUST BE ZERO		
MUST BE ZERO		
DISTANCE TO NET 2		
. . .		

Nesta mensagem, as rotas divulgadas por cada roteador são incluídas na parte IP ADDRESS OF NET X ….

As figuras abaixo mostram a divulgação de rotas por meio do protocolo RIP. Os roteadores divulgam e recebem informações de rotas via RIP, enquanto as estações apenas aprendem as rotas (RIP passivo).

1. Roteador G1 divulga sua tabela de rotas, que inicialmente contêm apenas as rotas diretas, para as redes ligadas diretamente.

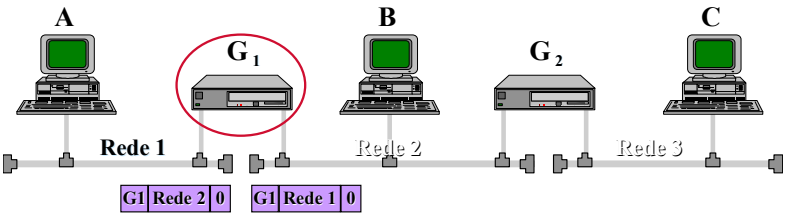


Tabela de Rotas

Rede	GW	M
Rede 1	-	0

Rede	GW	M
Rede 1	-	0
Rede 2	-	0

Rede	GW	M
Rede 2	-	0

Rede	GW	M

Rede	GW	M
Rede 3	-	0

2. O roteador G2, possui rotas para as redes ligadas diretamente, mas recebe um pacote de divulgação de rotas de R1, com uma rede nova (Rede 1). O roteador G2 instala a rota nova na sua tabela de rotas.

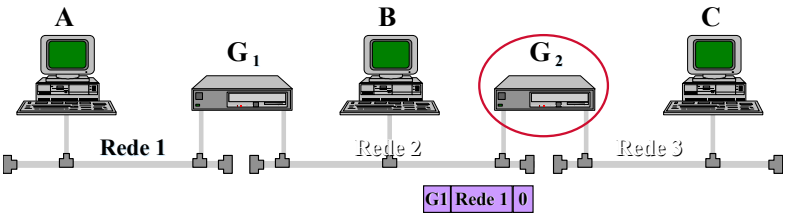


Tabela de Rotas

Rede	GW	M
Rede 1	-	0
Rede 2	G1	1

Rede	GW	M
Rede 1	-	0
Rede 2	-	0

Rede	GW	M
Rede 2	-	0
Rede 1	G1	1

Rede	GW	M
Rede 2	-	0
Rede 3	-	0
Rede 1	G1	1

Rede	GW	M
Rede 3	-	0

3. O Roteador G2 divulga suas rotas para as redes ligadas diretamente, incluindo a rota nova aprendida de G1. G1, recebendo esta divulgação, instala uma rota nova para a Rede 3.

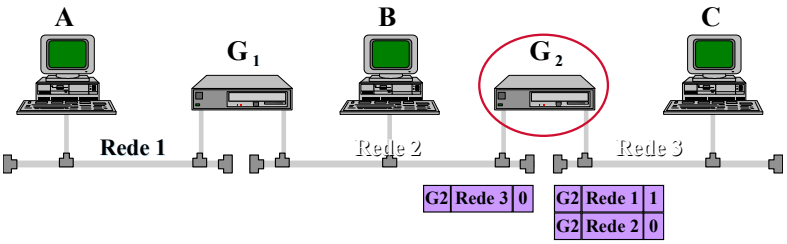


Tabela de Rotas

Rede	GW	M
Rede 1	-	0
Rede 2	G1	1

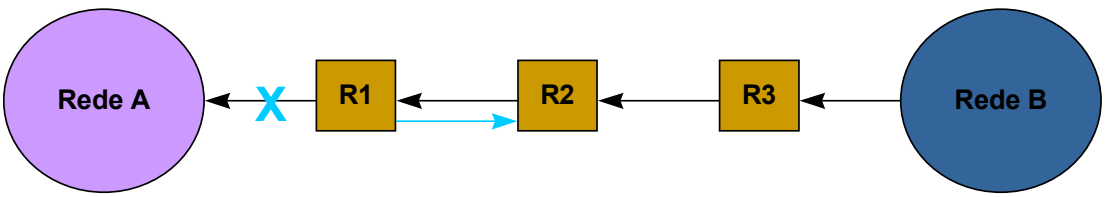
Rede	GW	M
Rede 1	-	0
Rede 2	-	0

Rede	GW	M
Rede 2	-	0
Rede 1	G1	1

Rede	GW	M
Rede 2	-	0
Rede 3	-	0
Rede 1	G1	1

Rede	GW	M
Rede 3	-	0

O protocolo RIP possui problemas intrínsecos de loop e convergência. O problema de convergência ocorre no seguinte caso:



O roteador R2 havia aprendido uma rota para a Rede A, através de R1. Tanto R1 quanto R2 divulgam de 30 em 30 segundos a sua tabela de rotas por meio de RIP. No funcionamento normal, se R1 perder a rota para a

Rede A, o roteador R1 divulgará uma mensagem RIP contendo uma rota para a Rede A com custo infinito (=16). O roteador R2, ao receber esta rota, verificará que ela veio de R1, de onde havia aprendido a rota para a rede A. Ele então procederá como determina o protocolo RIP e colocar a rota também com custo = 16.

Entretanto se, quando R1 perder a rota para a Rede A, R2 enviar sua tabela de rotas por RIP antes que R1 o tenha feito, R1 verificará que R2 possui uma rota melhor que ele para a rede A, com custo = 2 (já que R2 enviaria por meio de R1). R1 então instala uma rota para a rede A com custo = 3, sendo R2 o gateway da rota. Na próxima divulgação de R1, R2 constatará uma rota para a rede A com custo = 3. Ele então atualizará sua própria rota (já que a havia aprendido de R1), com custo = 4. A próxima divulgação de R2, causará a respectiva alteração do custo da rota em R1 para 5. Isto ocorre até que o custo desta rota atinja o valor 16.

O problema de convergência pode ser reduzido adotando-se as seguintes técnicas:

- *split -horizon update:* não divulga rotas de volta para a interface de onde recebeu a informação de rota
- hold-down: não aceita por 60s informações sobre uma rede após ela ser dada como não -alcançável
- poison-reverse: divulga rotas de volta para a interface de onde recebeu a rota, mas com métrica 16 (não -alcançável e mantém este estado durante um tempo mínimo, mesmo recebendo rota para a rede
- riggered-updates: força um roteador a divulgar imediatamente as rotas quando recebe rede não-alcançável

Protocolo RIP2

O protocolo RIP2 é bastante semelhante ao RIP, com as seguintes adições:

- As rotas contêm a máscara da rede destino, permitindo divulgar rotas para subredes
- O protocolo pode ser autenticado, adicionando segurança
- RIP2 pode carregar informações de outros roteadores adjacentes, que funcionam com outros protocolos (como OSPF e BGP-4)

A mensagem RIP é mostrada abaixo: