Arquitetura TCP/IP

Objetivos	• Fornecer os fundamentos necessários à compreensão do funcionamento de redes de computadores baseadas no conjunto de protocolos TCP/IP. • Familiarizar o aluno com a terminologia e conceitos básicos dos serviços e protocolos TCP/IP • Explorar e administrar redes de computadores baseadas em protocolos TCP/IP
Público Alvo:	• Administradores de redes TCP/IP • Administradores de serviços de informação baseados em tecnologia Internet • Profissionais de informática em geral.
Carga Horária	• 16 horas
Material Distribuído	• Notas de aula

Maiores informações sobre inscrições e custos podem ser obtidas no servidor Web da Gerência de Atendimento ao Cliente do Centro de Computação da Unicamp

Sumário

- **Repetidores, Pontes e Roteadores**
- **Protocolos da Família TCP/IP**
- **IP (Internet Protocol)**
- **ICMP - Internet Control Message Protocol**
- **Aplicações de Rede**
- **UDP e TCP**
- **ARP - Address Resolution Protocol (1)**
- **ARP - Address Resolution Protocol (2)**
- **Roteamento IP**
- **Algoritmo de Roteamento**
- **Telnet**
- **FTP - File Transfer Protocol**
- **TFTP - Trivial FTP**
- **[NFS] Network File System**
- **[NFS] Ambiente Centralizado**
- **[NFS] Ambiente Distribuído**
- **[NFS] Implementação**
- **[NFS] Características**
- **[NFS] Protocolo de Mount**
- **[NFS] Servidor NFS**
- **[NFS] Cliente NFS**
- **[NFS] Interação Cliente/Servidor**
- **[NIS] Network Information Service**
- **[NIS] Servidores e Clientes**

Autor: Rubens Queiroz de Almeida
Gerência de Suporte de Software
Centro de Computação
Unicamp
Última Modificação: 20/06/97

HISTÓRICO TCP/IP

- Criado pelo DARPA em meados de 1970
- Surgimento da ARPANET e da MILNET
- Integração ao UNIX/BSD
- Surgimento da NSFNET
- Comitê Organizador - IAB
- Documentação - RFCs e IENs
- SRI-NIC

NOTAS

A plataforma TCP/IP surgiu através dos trabalhos do DARPA (Defense Advanced Research Projects Agency) dos Estados Unidos, em meados da década de 70, constituindo a ARPANET, que mais tarde se desmembrou em ARPANET, para pesquisa, e MILNET, para instituições militares.

Para encorajar os pesquisadores universitários a adotar o TCPIP, o DARPA fez uma implementação de baixo custo, integrando-o ao UNIX da Universidade de Berkeley (BSD) já em uso em todas as universidades americanas. Além disso, teve-se o cuidado de definir aplicações de rede similares às já conhecidas em Unix, como *rusers* e *rcp*.

Mais tarde a NSF (National Science Foundation) estimulou o seu crescimento criando a NSFNET, que ligava centros de supercomputação espalhados por todo o país, numa rede de longa distância, também com os protocolos TCP/IP.

Existe um grupo chamado IAB (Internet Activities Board) que coordena os esforços de pesquisa na área, através de vários grupos de trabalho.

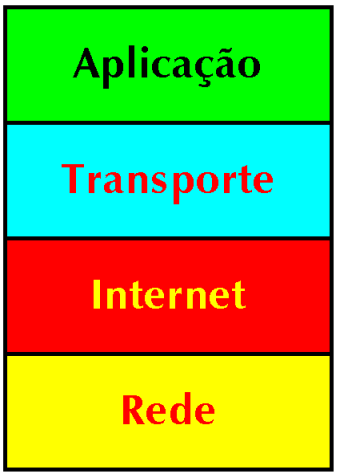
A documentação dos trabalhos, propostas para novos protocolos ou alteração de outros já existentes é feita através de artigos conhecidos como RFCs (Request for Comments). Propostas ainda em estudos são chamadas de IEN (Internet Engineering Notes) ou *Internet Drafts*.

Tanto as RFCs quanto as IENs são numeradas sequencialmente e em ordem cronológica. São distribuídas

pelo SRI-NIC, órgão que executa várias tarefas administrativas na INTERNET.

Centro de Computação
UNICAMP

Introdução à Arquitetura TCP/IP



NOTAS

Uma arquitetura de rede é definida pelas camadas ou níveis que a compõem, pela interface entre essas camadas e pelas regras de comunição entre camadas de mesmo nível em máquinas distintas, regras estas conhecidas como *protocolo*.

O objetivo da divisão em camadas é permitir a modularização do software, permitindo que as alterações sejam localizadas e transparentes aos outros níveis não afetados.

Os módulos de software de protocolo em cada máquina podem ser representados como camadas empilhadas. Cada camada cuida de uma parte do problema.

Existem duas regras importantes para o entendimento da divisão do software de rede em camadas:

- A camada inferior fornece serviços á camada superior.
- O protocolo de nível N no nó destino tem que receber o mesmo objeto enviado pelo protocolo de nível N no nó origem.

A Introdução à Arquitetura TCP/IP possui apenas 4 níveis:

- nível 1: interface de rede

- nível 2: internet ou camada IP
- nível 3: transporte
- nível 4: aplicação

O nível 1 lida com o meio de comunicação, utilizando endereços físicos. Os níveis 2 e 3 são incorporados ao sistema operacional. O nível 4 pode ser escrito por usuários. Os níveis 2,3 e 4 usam endereços IP.

O diagrama conceitual da primeira figura mostra a camada Internet entre uma camada de protocolo superior e uma camada de interface de rede. A segunda figura é mais realística e mostra que o software IP pode se comunicar com múltiplos protocolos de nível superior e múltiplas interfaces de rede.

Centro de Computação
UNICAMP

Modelo de Camadas ISO

Camada ISO	**Função**
Aplicação	Serviços de rede
Apresentação	Apresentação de dados
Sessão	Estabelece o elo de comunicação entre a origem e o destino
Transporte	Conecta processos em computadores diferentes
Rede	Fornece o endereço de uma máquina na rede
Enlace de Dados	Agrupa bits para transmissão
Fisica	Hardware que compõe uma rede

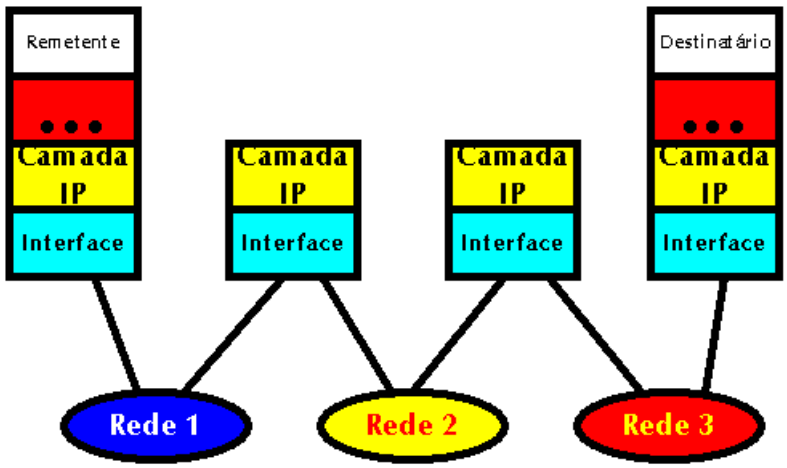
Centro de Computação
UNICAMP

Modelo de Camadas ISO x TCP/IP

Camada ISO	Serviços RPC	Serviços não RPC
Aplicação	NFS, YP, mount, etc.	rlogin,rcp,tftp,etc
Apresentação	XDR (eXternal Data Representation)	
Sessão	Remote Procedure Call (RPC)	
Transporte	TCP, UDP	Protocolos TCP/UDP
Rede	Internet Protocol (IP)	Internet Protocol (IP)
Enlace de Dados	Ethenet ou outro controlador	Ethernet ou outro controlador
Fisica	Ethernet ou outro meio físico	Ethernet ou outro meio físico

Centro de Computação
UNICAMP

FLUXO DE MENSAGENS (1)



NOTAS

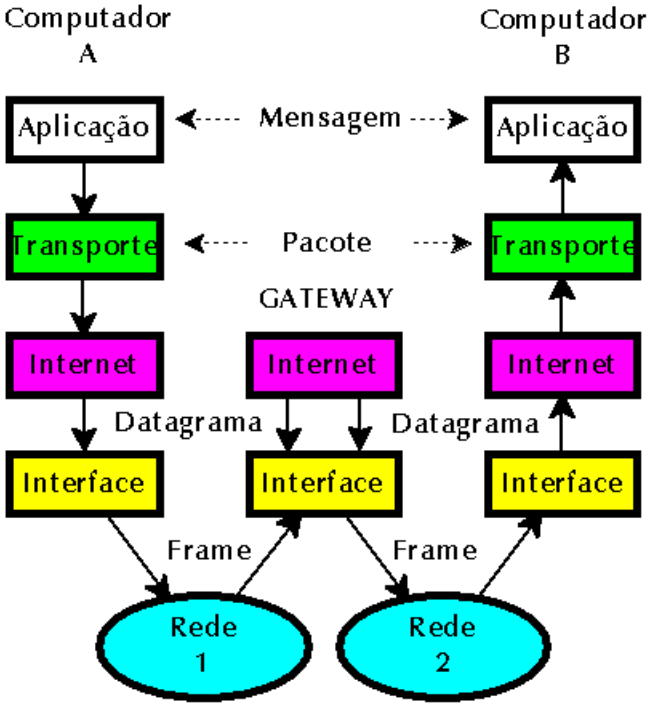
Transferir uma mensagem de uma aplicação numa máquina para outra aplicação em outra máquina significa transferir a mensagem para sucessivas camadas inferiores na máquina do transmissor, transferir a mensagem através da rede e transferir a mensagem para sucessivas camadas superiores na máquina destino.

Nas máquinas intermediárias o datagrama que chega através de uma camada de interface de rede sobe at a camada IP que o roteará de volta para uma outra rede através de sua outra interface de rede. Este datagrama será capturado por outra máquina intermediária e passará pelo mesmo processo até chegar á máquina destino. Essas máquinas*intermediárias* são chamadas GATEWAYS na nomenclatura Internet.

Conforme a mensagem passa por diferentes camadas de rede e é encapsulada por diferentes protocolos, ela assume diferentes nomes como pacote, datagrama, e frame.

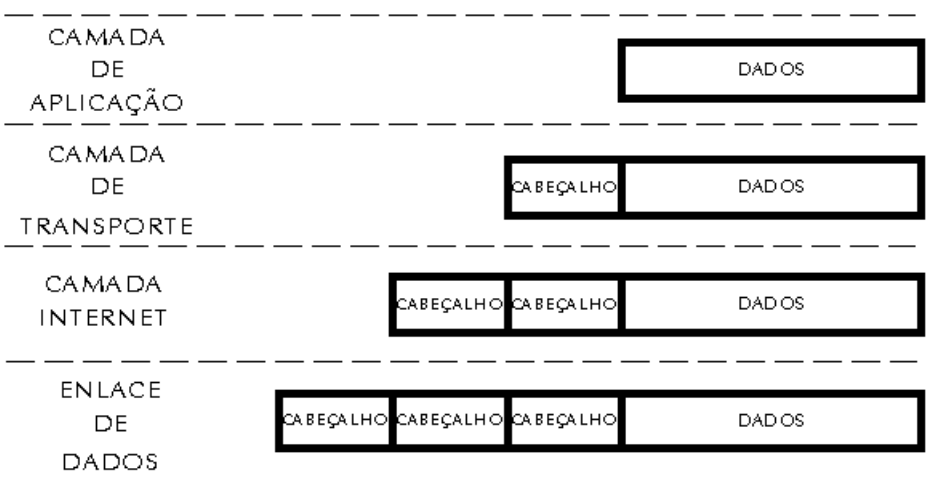
Centro de Computação
UNICAMP

FLUXO DE MENSAGENS (2)



Centro de Computação
UNICAMP

Encapsulamento TCP/IP-Ethernet



Centro de Computação
UNICAMP

ENDEREÇOS ETHERNET

- Endereço único no mundo, estabelecido pelo IEEE
- 6 bytes
- Codificado por hardware

  Ex. 00-00-1D - 00-26-A3

  Onde:

  00-00-1D identifica o fabricante
  00-26-A3 identifica o número de série

Multicast

- Para enviar uma msg a vários dispositivos numa rede simultaneamente

  AA-00-80-xx-xx-xx
  AB-00-80-xx-xx-xx

Broadcast

Recebido por todas as estações no mesmo segmento de rede

FF-FF-FF-FF-FF-FF

NOTAS

Quando um endereço Ethernet é utilizado como endereço destino num pacote, este só será decodificado pela estação que possuir aquele específico endereço.

O endereço multicast é formado modificando o último bit do primeiro byte de identificação do fabricante.

O endereço broadcast é utilizado por certos protocolos para comunicação com todos os nós da rede, quando não se conhece qual o nó que pode atender uma solicitação.

OBS. Não serve para localização de máquinas na rede.

Centro de Computação
UNICAMP

ENDEREÇAMENTO IP

- Distribuídos pelo SRI-NIC
- Representados em notação decimal
- Intervalo de 0.0.0.0 a 255.255.255.255
- Máscara separa parte "rede" da parte "máquina" e segue o mesmo padrão numérico do número IP
- Endereço de rede e de máquina com valor 0 são inválidos
- 127.0.0.0 é reservado para teste de loopback
- Qualquer porção do endereço formada por 1's é considerada um broadcast

NOTAS

Como os endereços IP codificam a rede e a máquina dentro da rede, eles não especificam uma máquina, mas sim uma conexão á rede.

Problema: se uma máquina muda de uma rede para outra o seu endereço IP deve mudar.

O endereço IP broadcast é mapeado ao broadcast do hardware.

Centro de Computação
UNICAMP

CLASSES DE REDES IP

Classe	Faixa de Enderecos	Representacao Binaria	Utilizacao
A	1-126.x.x.x	0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh	
B	128-191.x.x.x	10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh	
C	192-223.x.x.x	110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh	
D	224 -239.x.x.x	1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx	Enderecos Multicast
E	240-247.x.x.x	11110xxx.xxxxxxxx.xxxxxxxx.xxxxxxxx	Reservado
		n=bits rede	
		h=bits host	

NOTAS

Gateways usam o endereço de rede para o roteamento de datagramas IP.

A parte "máquina" do endereço identifica unicamente uma estação dentro de uma rede específica.

Centro de Computação
UNICAMP

MÁSCARAS E SUBNETTING (1)

143	106	1	45
10001111	01101010	00000001	00101101
11111111	11111111	00000000	00000000

Subnetting

Permite que se divida a porção de máquina em 2 partes:

- mais bits para rede
- menos bits para máquinas
- Utiliza-se uma nova máscara para identificar a nova parte de redes
- A nova porção do endereço usada para rede é conhecida como subnet

143	106	1	45
10001111	01101010	0000001	00101101
11111111	11111111	11111111	11000000

Classe B -> máscara 255.255.255.192

NOTAS

Máscara 255.255.0.0 possui 65.534 máquinas na mesma rede.

Máscara 255.255.255.192 possui 1022 subredes com 62 máquinas cada.

Centro de Computação
UNICAMP

Máscaras e Subnetting (2)

Dado o número IP 143.106.1.45 e a máscara 255.255.0.0

- Endereço de rede: 143.106.0.0
- Broadcast nesta rede: 143.106.255.255

Dada a máscara 255.255.255.192

- Endereço de rede: 143.106.1.0
- Broadcast nesta rede: 143.106.1.63

Equação genérica:

número de máquinas/subredes na rede:

2 **n-2 ,onde n é igual ao número de bits para subnet ou número de bits de máquina

Centro de Computação
UNICAMP

Tabela de Subredes/Computadores

Classe B

# de bits	*Mascara Decimal*	*Mascara Hexa*	*Subredes*	*Hosts*
2	255.255.192.0	FFFFC000	2	16382
3	255.255.224.0	FFFFE000	6	8190
4	255.255.240.0	FFFFF000	14	4094
5	255.255.248.0	FFFFF800	30	2046
6	255.255.252.0	FFFFFC00	62	1022
7	255.255.254.0	FFFFFE00	126	510
8	255.255.255.0	FFFFFF00	254	254
9	255.255.255.128	FFFFFF80	510	126
10	255.255.255.192	FFFFFFC0	1022	62
11	255.255.255.224	FFFFFFE0	2046	30
12	255.255.255.240	FFFFFFF0	4094	14
13	255.255.255.248	FFFFFFF8	8190	6
14	255.255.255.252	FFFFFFFC	16382	2

Classe C

# de bits	*Mascara Decimal*	*Mascara Hexa*	*Subnets*	*Hosts*
2	255.255.255.192	FFFFFFC0	2	62
3	255.255.255.224	FFFFFFE0	6	30
4	255.255.255.240	FFFFFFF0	14	14
5	255.255.255.248	FFFFFFF8	30	6
6	255.255.255.252	FFFFFFFC	62	2

Centro de Computação
UNICAMP

Repetidores, Pontes e Roteadores

Repetidor:

- nível 1 OSI
- estende um segmento de rede
- regenera os sinais recebidos
- máximo 2 repetidores (4 em IRLs)

Ponte:

- nível 2 OSI
- armazena os frames
- analisa o endereço de destino
- transmite apenas se necessário
- transparente a protocolo de rede
- Spanning Tree

Roteador:

- nível 3 OSI
- recebe somente frames a ele endereçados
- toma decisão baseado no endereço de rede do pacote

NOTAS

O repetidor opera a nível dos cabos e sinais elétricos. Gera o preâmbulo Ethernet, amplifica e ressincroniza o sinal. Assim, todo o tráfego em um segmento da rede é passado para o outro. No caso de colisões o repetidor gera um JAM no lado em que não houve a colisão para garantir que todos percebam que o meio está ocupado. Pode ligar redes com meios de transmissão díspares, por exemplo, cabo coaxial com fibra óptica ou com pares trançados, porém o nível 2 da rede tem que ser o mesmo.

IRLs (Inter-Repeater Links) são segmentos de rede que conectam apenas 2 repetidores. Esses segmentos de rede devem obedecer ás restrições de tamanho máximo para cada tipo de meio físico.

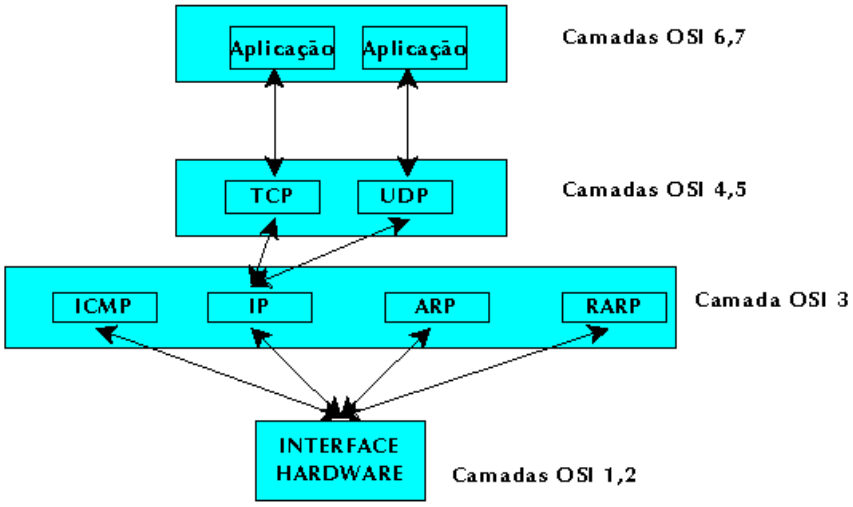
As pontes examinam os endereços de destino de todos os frames (nível 2 - Ethernet ou Token-ring) e tomam decisões quanto á necessidade de transferir cada frame para os circuitos que interligam as redes, através de uma lista de endereços associada a cada segmento de rede, criada dinamicamente. No caso de não existir o endereço na tabela o frame é transmitido (caso inicial). As pontes são totalmente

transparentes para os outros dispositivos de rede e por isso diversas redes locais interligadas por uma ponte formam uma única rede lógica.Não há limite no número de pontes como no caso de repetidores.

Os roteadores não examinam todo frame existente na rede como as pontes.Como são nós da rede, eles recebem apenas os frames a eles endereçados. Abrem cada frame e leêm as informações de endereçamento nível 3 (no caso do TCP/IP, o endereço IP) e extraindo informação sobre a rede para qual esse pacote deve ser endereçado, enviando-o para uma de suas interfaces de rede. Diferentemente dos repetidores e pontes, exigem conhecimento técnico para sua instalação e operação. Atualmente todos os roteadores do mercado são multiprotocolares, com IP, DECNET, APPLETALK, XNS, IPX e outros.

Centro de Computação
UNICAMP

Protocolos da Família TCP/IP



Centro de Computação
UNICAMP

IP (INTERNET PROTOCOL)

- Não confiável: entrega não garantida, sem controle de sequenciamento, não detecta erros nem informa o transmissor.
- Orientado a pacote - "connectionless": cada pacote é tratado independentemente dos outros
- "Bem intencionado": os pacotes só são descartados quando todos os recursos são exauridos
- Unidade básica: datagrama - que é quebrado em fragmentos para se adequar ao MTU do hardware
- Time-to-live: Cada datagrama tem um campo que diz que após determinado tempo o datagrama pode ser descartado. Cada gateway decrementa 1 ao recebê-lo e a cada segundo. TTL = 0 , datagrama é retornado.

Centro de Computação
UNICAMP

ICMP

- ICMP - Internet Control Message Protocol
- ICMP permite que gateways enviem mensagem de erro ou de controle para outros gateways ou máquinas
- Provê comunicação entre o protocolo Internet (IP) em uma máquina e o IP em outra.
- Muitas vezes não ajuda a localizar onde está o erro, pois ele responde apenas á máquina que originou o pacote errôneo e o erro pode estar em algum gateway no caminho.
- Pode ser perdido como qualquer outro pacote IP
- PING : pacote ICMP do tipo "echo request" e "echo reply "

Centro de Computação
UNICAMP

APLICAÇÕES DE REDE

- Processos clientes X servidores
- Servidores estão sempre ativos esperando conexões
- Clientes são criados assincronamente
- Identificação da conexão:
  - IP origem
  - Ip destino
  - Porta origem
  - Porta destino
- Porta destino: *Well-known ports*
- Porta origem: alocação dinâmica
- Arquivos:
  - **`/etc/services`**
  - **`/etc/inetd.conf`**

NOTAS

Além das falhas de linhas de comunicação e processadores, o IP falha também ao entregar datagramas quando a máquina destino está temporariamente ou permanentemente desconectada da rede, quando o contador "time-to-live" expira ou quando gateways intermediários tornam-se tão congestionados que não podem processar o tráfego de entrada.

Para permitir que gateways possam reportar erros para as máquinas de origem ou prover informação sobre circunstâncias inesperadas, existe o protocolo ICMP que tem que estar dentro de qualquer implementação de IP.

Como todo outro tráfego, mensagens ICMP trafegam na internet na porção de dado de datagramas IP. O destino de uma mensagem IP não é um programa de aplicação ou usuário e sim o próprio protocolo IP da máquina destino.

Fragilidades: ICMP só reporta erros á fonte original, não a intermediários. Suponha um datagrama que

siga uma rota através de uma série de gateways G1, G2, ..., GK. Se GK tem rotas incorretas e envia o datagrama para o gateway GE, GE reporta o erro de volta para a origem do datagrama.Porém a origem não tem nenhuma responsabilidade sobre esse erro nem controle sobre o gateway problemático. Pode inclusive nem saber qual é esse gateway. Além disso, o próprio pacote ICMP pode se perder como qualquer datagrama IP.

O comando PING faz uso de um dos tipos de pacote ICMP. A máquina origem envia pacote ICMP do tipo "echo request" . A máquina que recebe essa mensagem responde com ICMP do tipo "echo reply" . Algumas versões de PING enviam vários pacotes e devolvem estatísticas. Se o ping tem sucesso, significa que as principais partes do sistema de transporte estão funcionando.

Centro de Computação
UNICAMP

UDP e TCP

- UDP - User Datagram Protocol
- TCP - Transmission Control Protocol
- Nível de transporte (sobre o IP)
- UDP não é orientado á conexão e não tem tratamento de erros
- TCP utiliza número nas mensagens ,*janelas deslizantes*, temporização e controle de fluxo para garantir confiabilidade.
- Ambos utilizam portas de protocolo para identificar os processos comunicantes de maneira unívoca.

NOTAS

Nas aplicações de rede existe sempre um processo cliente numa máquina que dispara uma conexão, e ur processo servidor em outra que tem que estar preparado para aceitar várias conexões simultâneas. Para isso existe para cada tipo de processo servidor o conceito de um processo "master" que aceita novas conexões e cria processos escravos do mesmo tipo para lidar com cada conexão. O processo "master"nunca morre (exceto em condições excepcionais) e o processo cliente tem uma duração finita.

Esse processos servidores são chamados "daemons"na linguagem UNIX e seus nomes terminam com a letra "d". Existe um daemon genérico chamado inetd que aceita conexões "em nome de" vários tipos de processos, como telnet e finger.

Surge a questão: como identificar uma conexão unicamente, tanto na máquina origem quanto na máquina destino ? Da explanação anterior fica claro que apenas os IP de destino e origem não bastam. Solução: associar a cada aplicação (ou serviço) um número de porta padronizado. Assim por exemplo, telnet tem o número 23; ftp, 21 e SMTP, 25. O melhor meio de pensar numa porta é como uma fila. Quando uma aplicaçãop negocia com o sistema operacional uma determinada porta, o S.O. cria uma fila interna para armazenar as mensagens que chegam.

Porém isso não é suficiente: e se na máquina origem existir mais de um telnet com a mesma máquina destino? Solução: associar a cada cliente na máquina origem um múmero de porta único, obtido dinâmicamente. Para isso em cada máquina existe um processo chamado portmap que "escolhe" uma porta disponível. Os números de porta até 1024 são reservados para portas pré-definidas (alguns valores são

reservados para aplicações criadas por usuários) e acima deste valor a alocação é dinâmica.

Centro de Computação
UNICAMP

ARP e RARP

ARP - Adress Resolution Protocol

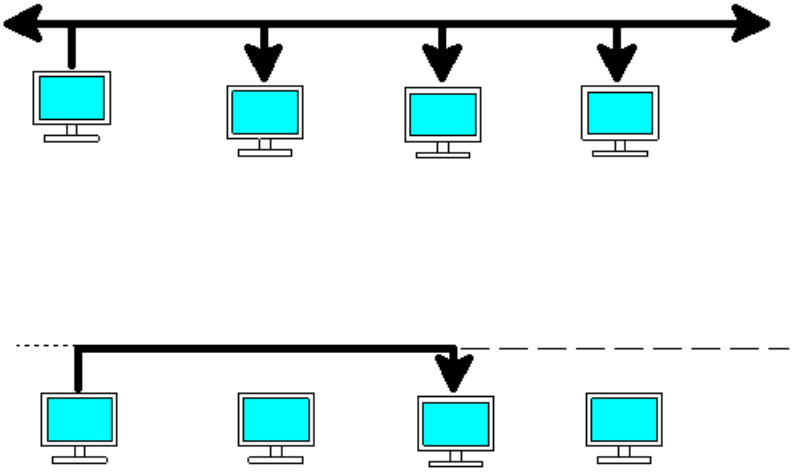
- A quer enviar mensagem para B, com endereço IP_B
- envia requisição broadcast
- obtém endereço físico de B, F_B
- guarda F_B em cache
- envia mensagem para F_B

RARP - Reverse ARP

- máquinas diskless precisam saber seu número IP
- servidores RARP possuem database com mapeamento IP X Ethernet
- enviam requisição broadcast
- recebe endereço IP fornecido por um servidor RARP
- armazena em memória até o próximo reboot

Centro de Computação
UNICAMP

ARP



```
% arp -a
  gilda.cmp.unicamp.br (143.106.30.16) at 8:0:5a:cd:56:f6 [ethernet]
  roma.cmp.unicamp.br (143.106.30.9) at 14:3:10:6:30:0 [ethernet]
  panoramix.cmp.unicamp.br (143.106.30.11) at 8:0:20:9:71:6f [ethernet]
```

Centro de Computação
UNICAMP

Roteamento IP

Decisão:

Baseada em tabelas de rotas que ficam no kernel do sistema operacional

RIP

Tabela pode ser estática ou dinâmica

Roteamento Dinâmico:

- routed - **`/etc/gateways`**
- gated - **`/etc/gated.conf`**

Hops

Número de gateways até a rede específica

Comando`netstat -r`

```
Routing Table:
  Destination           Gateway           Flags  Ref   Use   Interface
-------------------- -------------------- ----- ----- ------ ---------
127.0.0.1            127.0.0.1             UH       0 249140  lo0
```

```
143.106.2.0          143.106.1.1          UG        0     18  le0
143.106.20.0         143.106.10.35        UG        0    103  le0
143.106.20.64        143.106.10.34        UG        0    330  le0
143.106.28.128       143.106.1.1          UG        0    456  le0
143.106.30.128       143.106.10.9         UG        0    135  le0
224.0.0.0            143.106.10.11        U         3      0  le0
143.106.10.255       143.106.10.14        UGHD      0     83  le0
143.106.20.1         143.106.10.35        UGHDM     0      6  le0
default              143.106.10.10        UG        0  63655  le0
```

Centro de Computação
UNICAMP

Algoritmo de Roteamento

Rotear_datagrama_IP ( )

Extrair endereço IP de destino, I_D, do datagrama

- Calcular endereço IP da rede destino, I_R
- Se I_R é qualquer rede diretamente conectada
  - envie datagrama para o destino sobre esta rede (envolve "resolver" o endereço I_D para um endereço físico, encapsular o datagrama e enviá-lo)
- Senão Se I_D aparece aparece como uma rota específica
  - roteie datagrama como especificado na tabela
- Senão Se I_R aparece na tabela de roteamento
  - roteie datagrama como especificado na tabela
- Senão Se uma rota default está especificada
  - roteie datagrama para o gateway default
- Senão declare "Erro de Roteamento"

NOTAS

Quando se diz "roteie de acordo com a tabela" pretende-se dizer: pegue o endereço do gateway que está na tabela, que necessáriamente pertence á alguma rede da máquina onde está o pacote , use ARP para traduzir esse endereço IP para um endereço físico, encapsule esse datagrama num frame e envie para a interface de rede adequada.

Centro de Computação
UNICAMP

Telnet

- Estabelece uma sessão de login remoto interativa
- Utiliza a porta 23 TCP

- O cliente ignora caracteres de controle com exceção de um que funcionará como escape

- Permite independência de tipos de terminais

- Desvantagem: ineficiência. Cada caractere transmitido força várias trocas de contexto de processos dentro do sistema operacional local e remoto.

- TN3270 - telnet com emulação de terminal IBM 3270

Centro de Computação
UNICAMP

FTP - FILE TRANSFER PROTOCOL

- Filosofia Cliente-Servidor
- Acesso Interativo
- Usuário especifica máquina destino, username e password
- Eficiente
- Transferência nem sempre pode ser revertida
- Duas portas de protocolo:
  - Processo de controle (baseado em telnet)
  - Processo de transferência dos dados
- FTP anonimo para arquivos públicos

NOTAS

Protocolos confiáveis como TCP permitem que se faça uso interativo de máquinas remotas. A aplicação telnet faz com que usuários estabeleçam uma sessão de login com outra máquina que não aquela onde estão fisicamente conectados e tenham acesso a todos os comandos disponíveis na máquina remota, utilizando a porta de protocolo 23 para comunicação entre os processos.

O processo cliente tem que ignorar o funcionamento de todas os caracteres de controle locais, como CTRL/C, CTRL/Z, para que esses possam ser usados na máquina remota. Deve existir apenas uma sequência de ESCAPE para possibilitar o encerramento da própria sessão telnet, caso ocorra algum problema.

Telnet usa o conceito de Terminal Virtual de Rede para obter independência de tipos de terminais físicos.

Por ser um programa a nível de aplicação, tem suas vantagens e desvantagens. - Vantagem: possibilita que a modificação de seu código seja feita mais facilmente do que se o seu código pertencesse ao sistema operacional. - Desvantagem:Ineficiência. Cada tecla pressionada no lado do cliente viaja do terminal do

usuário atavés do sistema operacional até o programa cliente. Daí volta para o S.O. e atravessa a rede até chegar á máquina destino servidora. Lá, o caractere vai através do S.O. até o programa servidor e do programa servidor até a um ponto-de-entrada de um pseudo-terminal do sistema. Finalmente o S.O. entrega o caractere para a aplicação que o usuário esteja executando na máquina remota.

Centro de Computação
UNICAMP

TFTP - TRIVIAL FTP

- FTP sem autenticação
- Código menor que FTP
- Utilizado em estações diskless (gravado na ROM)
- Utiliza UDP
- Pacotes numerados sequencialmente com timeout e retransmissão

---

NOTAS

Dentro da filosofia cliente-servidor, o usuário chama um programa cliente para iniciar a transferência. Nessa chamada o usuário especifica o computador remoto onde o arquivo desejado reside e uma autorização para obter acesso (username e password). O cliente então contacta o servidor na máquina remota e requisita uma cópia do arquivo. Uma vez transferido, o usuário pode encerrar o software cliente.

A vantagem da cópia do arquivo todo está na eficiência da operação.

Transferência entre máquinas heterogêneas é mais complicada, pois cliente e servidor têm que entrar em acordo com relação ao proprietário do arquivo, proteção de acesso e formato do dado. Porém, mesmo assim nem sempre a transmissão inversa é possível. Por ex., pode ser impossível converter o ponto flutuante de uma máquina para outra sem perder a precisão.

Como outros servidores, o servidor ftpd aceita várias conexões simultâneas, Um único processo servidor espera conexões e cria processos escravos para lidar com cada uma delas. Contudo o processo escravo não faz tudo sozinho. Ele apenas gerencia a parte de controle (porta 21) e usa um outro processo separado (porta 20) para trabalhar com a tarefa de transferência de dados. Para cada transparência o FTP estabelece uma nova conexão na porta 20. Quando a conexão de controle é encerrada a sessão termina.

Para a parte de controle, o FTP usa o protocolo telnet simplificado, sem negociação de opções.

Para prover acesso irrestrito a arquivos públicos, muitas instalações usam FTP anonymous, o que significa que o usuário não precisa de conta ou password para ter acesso. O username usado é "anonymous" e a password normalmente é o endereço da pessoa (para fins de contabilidade). O acesso fica restrito a apenas um especificado filesystem.

Centro de Computação
UNICAMP

Network File System

- Serviço de rede que permite o compartilhamento transparente de sistemas de arquivos ou diretórios entre os nós de uma rede

- Implementado usando RPC (Remote Procedure Call), cujos protocolos são descritos usando XDR (eXternal Data Representation)

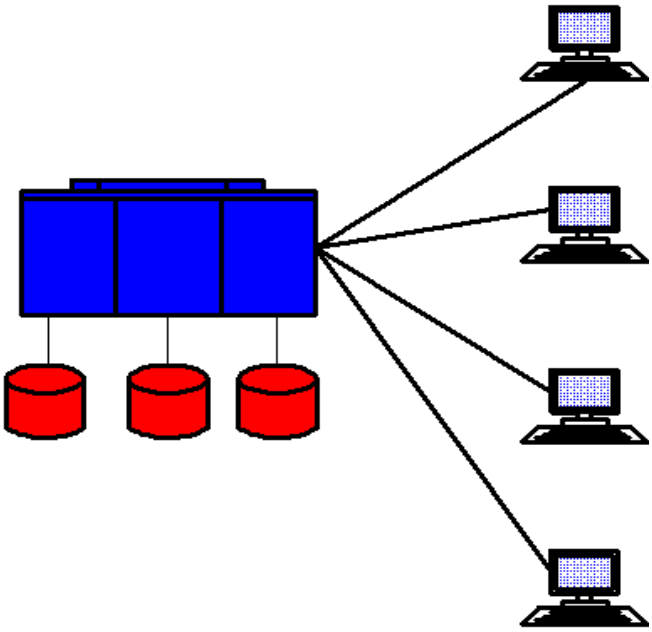
NOTAS

RPC, ou *Remote Procedure Call*, é uma biblioteca de procedimentos que prove um meio através do qual um processo (processo cliente) possa fazer com que um outro processo (processo servidor) execute uma chamada a um procedimento, como se o processo cliente tivesse executado a chamada em seu próprio espaço de endereçamento. Devido ao fato de que o cliente e o servidor serem processos separados, eles não precisam residir na mesma máquina.

XDR ou eXternal Data Representation é a especificação de um padrão para formato de dados portável. O RPC utiliza o XDR para assegurar que os dados são representados da mesma maneira em computadores, sistemas operacionais e linguagens de programação diferentes.

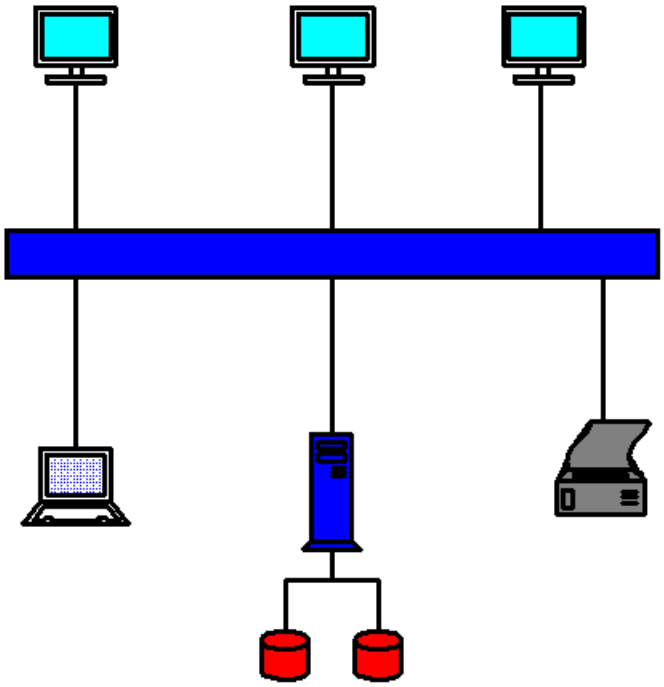
Centro de Computação
UNICAMP

Ambiente Centralizado



Centro de Computação
UNICAMP

Ambiente Distribuído

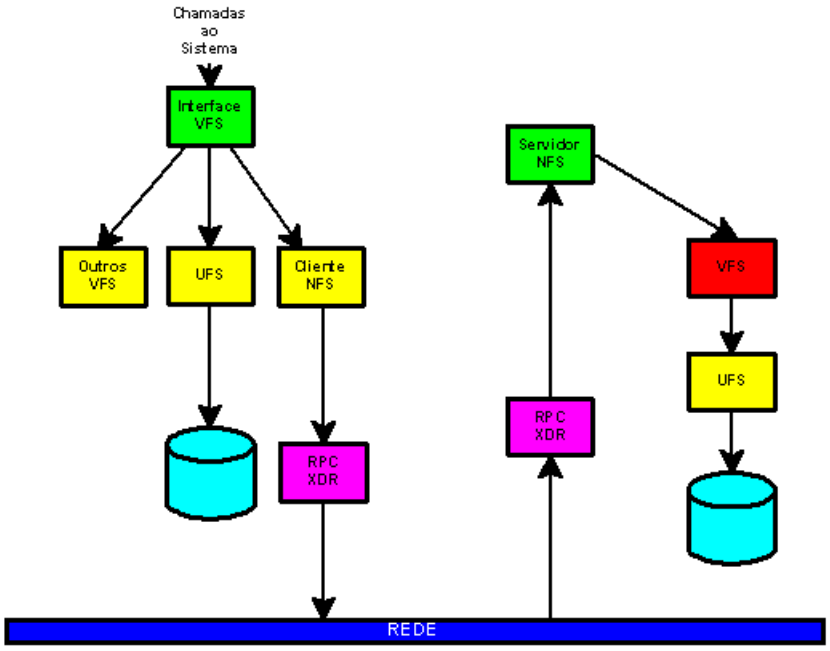


NOTAS

O objetivo principal do NFS era tornar todos os discos disponíveis onde necessário. Estações de trabalho individuais têm acesso a toda informação, independente de sua localização. Impressoras e supercomputadores tornam-se também disponíveis aonde quer que estejam localizados na rede.

Centro de Computação
UNICAMP

NFS - Implementação



NOTAS

Na implementação do NFS realizada pela SUN, existem três entidades a serem consideradas: a interfac com o sistema operacional, o sistema de arquivos virtual (VFS - Virtual File System) e a interface com o sistema de arquivos de rede (NFS - Network File System). A interface com o sistema operacional Unix foi preservada, assegurando desta forma compatibilidade com aplicações existentes. As aplicações continuam usando funções tais como read e write para acessar arquivos NFS da mesma forma que utilizam para acessar arquivos locais.

O VFS é melhor visualizado como uma camada que foi acrescida ao sistema de arquivos Unix tradicional. Os filesystems Unix são compostos de diretórios e arquivos, cada um dos quais possuindo um inode (index node) que contém informações sobre o arquivo tais como localização, tamanho, propriedade, permissões e datas de acesso. Cada inode recebe um número único dentro do sistema operacional. Arquivos ou diretórios em sistemas diferentes todavia podem possuir o mesmo identificador. Este é um problem existente em um ambiente de rede, devido ao fato de que sistemas remotos precisam ser

montados dinamicamente e conflitos de endereçamento ocasionariam enormes transtornos. Para resolver este problema foi criado o VFS, o qual é baseado em uma estrutura de dados chamada vnode. No VFS se assegura que arquivos possuem identificações númericas únicas, mesmo dentro de um ambiente de rede. Os vnodes separam as operações no filesystem da semântica de sua implementação. Acima da interface com o VFS, o sistema operacional opera em termos de vnodes; abaixo desta interface, o sistema operacional pode ou não implementar inodes. A interface VFS pode conectar o sistema operacional a uma grande diversidade de sistemas de arquivos, como por exemplo, sistemas FAT, NTFS, HPFS, etc. O VFS local conecta o sistema de arquivos a um dispositivo local.

O VFS remoto define e implementa a interface NFS baseado nos protocolos RPC e XDR.

No caso de acesso através de um VFS local, os pedidos são direcionados ao sistema de arquivos em dispositivos conectados à máquina cliente. No caso de acesso remoto, o pedido passa através das camadas RPC e XDR chegando à rede. Originalmente o protocolo utilizado para o transporte era o UDP/IP. O NFS versão 3.0 utiliza TCP/IP. Do lado do servidor, os pedidos passam pelas camadas RPC e XDR até chegar ao servidor NFS; o servidor utiliza vnodes para acessar um de seus vfs locais e atender ao pedido.

Centro de Computação
UNICAMP

Características

A implementação do NFS oferece cinco tipos de transparência:

- Tipos de sistemas de arquivos
- Localização dos sistemas de arquivos
- Tipo de sistema operacional
- Tipo de máquina
- Tipo de rede

NOTAS

O protocolo NFS, como implementado pela SUN, oferece cinco tipos de transparência:

- **Sistema de arquivos:**

  O vnode, em conjunção com um mais VFSs locais (e possivelmente VFSs remotos) permite que um sistema operacional se comunique transparentemente com uma grande variedade de sistemas de arquivos.

- **Localização de sistemas de arquivos:**

  Desde que não se diferenciam VFSs remotos e locais, a localização de um sistema de arquivos é transparente.

- **Tipo de sistema operacional:**

  O protocolo RPC permite interconexão de uma grande variedade de sistemas operacionais na rede, e torna o tipo de sistema operacional remoto de um servidor remoto transparente.

- **Tipo de máquina:**

O XDR permite que uma variedade de máquinas se comuniquem em uma rede e torna o tipo de máquina de um servidor remoto transparente.

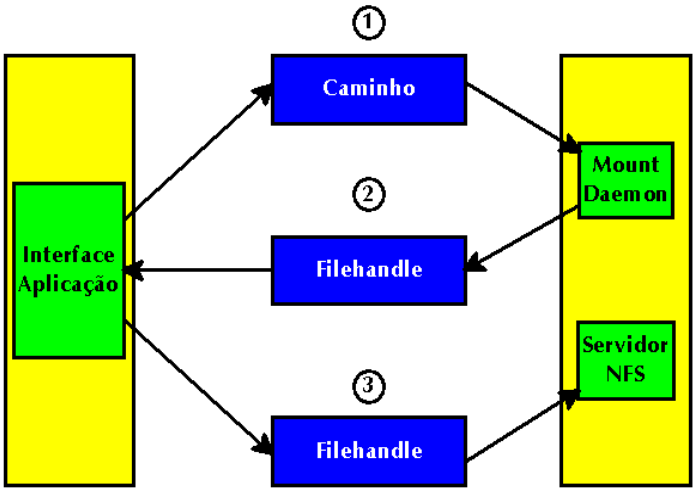
- **Tipo de rede:**

  o RPC e o XDR podem ser implementados sobre uma grande variedade de protocolos de transporte, tornando assim o tipo de rede empregada transparente.

Uma das grandes vantagens da implementação do NFS é sua capacidade de combinar tipos de sistemas de arquivos diferentes. As especificações dos protocolos RPC e XDR são públicas, abertas e de domínio público. Desta forma, qualquer empresa que queira implementar o NFS em seus produtos pode fazê-lo sem despesas que não aquelas necessárias para o desenvolvimento das aplicações.

Centro de Computação
UNICAMP

Protocolo de Mount



1. Cliente envia o caminho de um arquivo ou diretório ao servidor NFS

2. O servidor responde retornando o filehandle correspondente

3. O cliente envia o filehandle ao servidor NFS

NOTAS

O NFS define as operações tradicionais de acesso ao sistema de arquivos para leitura, criação e deleção de arquivos e diretórios, e atribuição de atributos. A interface foi projetada de modo a que as operações em arquivos acessem estes arquivos por meio de um identicador chamado filehandle, um endereço de início e um tamanho em bytes. O NFS nunca trabalha com caminhos, apenas com filehandles. Mais precisamente, o NFS nunca interpreta os caminhos (pathnames).

Dado um filehandle para um diretório, um programa cliente pode usar procedimentos do NFS para obter outros filehandles para poder navegar através dos diretórios e arquivos de um sistema de arquivos. O cliente entretanto precisa obter o filehandle para um sistema de arquivos utilizando RPC para invocar o mount daemon do servidor. O mount daemon irá retornar um filehandle que garantirá acesso ao sistema de arquivos.

Centro de Computação
UNICAMP

Servidor NFS

- Exporta sistemas de arquivos para tornar seu uso transparente a aplicações de clientes NFS
- Lê ou grava arquivos em resposta a pedidos de clientes NFS
- Não mantém informação relativa a arquivos abertos por clientes
- Pode servir a clientes NFS ou a outros servidores
- Não faz cache de pedidos de write de clientes NFS

Centro de Computação
UNICAMP

Cliente NFS

- Monta sistemas de arquivos compartilhados exportados pelo servidor NFS
- Arquivos são lidos ou gravados através de pedidos ao servidor NFS
- Mantém toda informação a respeito de seus arquivos abertos
- Pode utilizar os serviços de vários servidores NFS
- Pode se comunicar com servidores NFS através de nós na Ethernet
- Realiza cache para gravação

Centro de Computação
UNICAMP

Interação Cliente/Servidor

- O **`/etc/exports`** determina os sistemas de arquivos a serem exportados
- O comando **`exportfs`** torna os sistemas de arquivos disponíveis
- O arquivo **`/etc/xtab`** contém a lista dos sistemas de arquivos exportados
- O servidor inicializa o daemon do NFS (**`nfsd`**) e o daemon para mount (**`mountd`**)
- O daemon **`rpc.mountd`** do servidor retorna um indicador (*file handle*) para o diretório ou sistema de arquivos solicitado
- O *file handle* do cliente é colocado na tabela de mounts do kernel
- Todas as referências posteriores são passadas ao daemon NFS rodando no servidor usando o file handle do cliente
- O read ahead/write behind do NFS é gerenciado pelo *block i/o daemon* (**`biod`**)

Centro de Computação
UNICAMP

NIS

- Banco de dados com informacoes da rede
- Servidores e clientes
- Dominio NIS

Centro de Computação
UNICAMP

Servidores e Clientes

- Servidor Mestre
  - Contém os mapas NIS
  - Atualiza os mapas NIS
  - Propaga os mapas NIS
  - Fornece mapas NIS para clientes
- Servidor Escravo
  - Recebe mapas NIS do servidor
  - Fornece mapas NIS para clientes
- Clientes

NOTAS

Um servidor NIS é uma máquina que contém um grupo de mapas que são postos à disposição da rede. O servidor de arquivos não precisa ser o servidor NIS, a menos que ele seja a única máquina na rede que possua discos. Existem dois tipos de servidores NIS, mestres e escravos.

O servidor mestre:

- contém o grupo mestre de mapas NIS
- atualiza o grupo mestre de mapas NIS
- propaga o grupo mestre de mapas NIS para os servidores escravos
- fornece serviços NIS aos clientes do domínio NIS

O servidor mestre atualiza os mapas dos servidores escravos As mudanças serão propagadas do servidor mestre para os servidores escravos. Se mapas NIS são criados ou alterados em servidores escravos ao invés de no servidor mestre, o algoritmo do NIS será quebrado. Sempre faça todas as modificações e

criações de dados no servidor mestre. Teoricamente uma máquina pode ser mestre de um mapa e escravo de outro. Recomenda-se com vigor que uma única máquina deve ser a mestre de todos os mapas criados dentro de um domínio.

O servidor escravo:

- contém um grupo adicional de mapas NIS
- recebe o grupo adicional de mapas do servidor mestre NIS
- fornece serviços de NIS aos clientes do domínio NIS

Um cliente NIS

- é uma máquina que faz uso do serviço NIS
- roda processos que solicitam dados dos mapas dos servidores

Centro de Computação
UNICAMP

ypbind/ypserv

- Os clientes NIS inicializam o binding daemon (**/usr/etc/ypbind**) durante o boot
- O daemon ypbind emite para a rede um pedido para se ligar a um servidor NIS
- A máquina rodando o processo mestre (**/usr/etc/ypserv**) se liga ao cliente que fez o pedido.
- Todas as consultas feitas pelo cliente serão transmitidas pelo processo **ypbind** a um daemon **ypserv** rodando em uma servidora
- Se um servidor não responde após um binding bem sucedido, o daemon **ypbind** retorna ao modo *broadcast* para tentar se conectar a um outro servidor.

NOTAS

Os clientes NIS obtem informações de um servidor NIS através de um processo de binding. O binding é a associação de um domínio com o endereço Internet do servidor e da porta naquele servidor através da qual o processo **ypserv** ouve os pedidos de serviço. Esta informação é armazenada no diretório **/var/yp/binding** usando um arquivo do tipo *domainname.versão.*

O processo de binding é dirigido por pedidos de clientes. Como o bind é estabelecido por*broadcasting*, deve existir ao menos um processo **ypserv** em cada rede.

Bindings e rebindings são tratados transparentemente pelas rotinas de biblioteca. Se o processo **ypbind** é incapaz de falar com o processo **ypserv** ao qual se conectou, ele marca o domínio como *unbound* e tenta se ligar ao domínio novamente.

Se o arquivo **`/var/yp/ypserv.log`** existe quando o processo **`ypserv`** é inicializado, informações de erro serão registradas neste arquivo quando do aparecimento de condições de erro.

Os arquivos **`/var/yp/binding/`** *domainname.version* são criados para acelerar o processo de binding. Estes arquivos fazem um cache do último binding bem sucedido criado para o domínio; quando um binding é solicitado estes arquivos são verificados quanto à sua validade e então usados.

Centro de Computação
UNICAMP

Sendmail

Características

- Entrega imediata de mensagens
- Mudança de endereços imediata
- Interação com DNS através de registros MX
- Mensagens podem ser entregues a partir de outros serviços

NOTAS

Mensagens enviadas a partir do correio eletrônico demoram apenas alguns segundos para serem entregues (no melhor caso). Como conseqüencia deste fato o correio comum é denominado pela comunidade Internet de *snail mail*.

A mudança de endereços não implica em transtornos para os usuários visto que pela criação de um arquivo chamado **`.forward`** em seu diretório de trabalho todo o mail pode ser redirecionado de um computador para outro.

O programa sendmail pode utilizar o *Domain Naming System* (DNS) para descobrir o local para onde enviar as mensagens. Registros do tipo MX (Mail Exchanger) permitem com que mensagens sejam facilmente redirecionadas de um computador para outro.

Finalmente, as mensagens podem ser roteadas para outros tipos de redes. O programa sendmail pode entregar mensagens para redes como UUCP, Bitnet, DECNET, SNA e várias outras.

Centro de Computação
UNICAMP

MUA x MTA

- **MUA - Mail User Agent**
  - MUAs são quaisquer dos programas utilizados para ler, responder, compor e dispor de mensagens eletrônicas.
  - Exemplos
    - mush
    - pine
    - mail
    - ...
- **MTA - Mail Transport Agent**
  - MTAs são programas que se encarregam de entregar mensagens a vários usuários e redirecionar mensagens entre computadores como por exemplo o programa sendmail.

NOTAS

Existem diversos programas para se lidar com o correio eletrônico (MUA). O programa que normalmente existe em todos os ambientes unix chama-se mail e é apenas para os iniciados devido á sua complexidade. É recomendável entretanto que todos os administradores de sistemas saibam como utilizá-lo devido á sua universalidade, ou seja, podem ser encontrados em praticamente todas as variantes de sistemas Unix.

Existem outros programas tais como pine e elm que tornam o trabalho com o correio eletrônico extremamente simples para usuários comuns. As opções, tanto de domínio público como comerciais são numerosas. Interfaces gráficas com suporte a MIME (Multipurpose Internet Mail Extensions) estão também se tornando cada vez mais comuns.

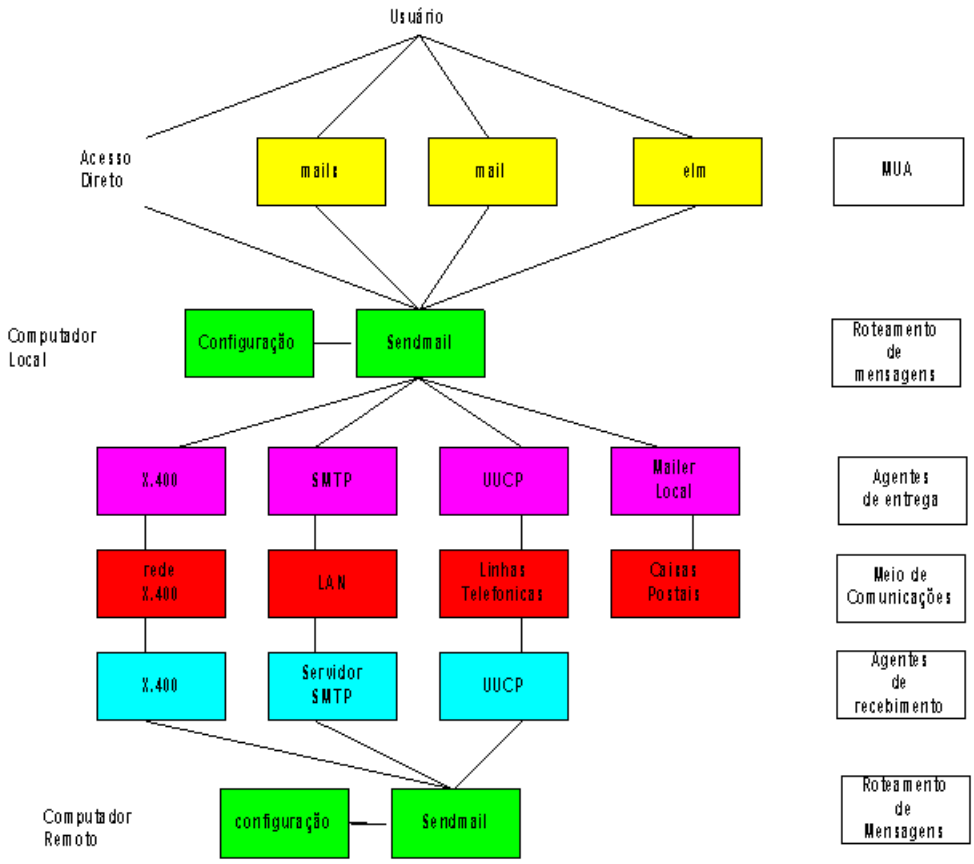
Recomenda-se que todos os administradores configurem um programa diferente do mail do sistema na criação das contas. O programa **`sendmail`** (MTA) é necessário porque a entrega de correio eletrônico raramente é uma tarefa simples. Algumas instituições podem desejar que todas as mensagens sejam direcionadas para um servidor central de correio eletrônico.

Como a tarefa de transportar mensagens frequentemente se extende além dos domínios da máquina local, a necessidade de um MTA separado de um MUA aumenta. O programa **`sendmail`** pode enviar

mensagens de uma máquina para outra na mesma rede e pode também direcionar mensagens da rede em que se encontra para redes de arquitetura radicalmente diferentes.

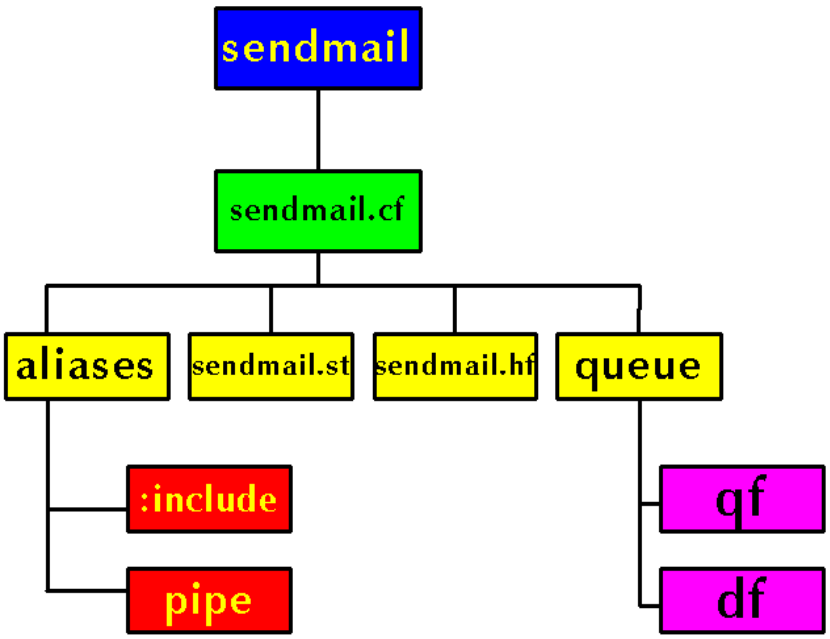
Centro de Computação
UNICAMP

Fluxo de Processamento



Centro de Computação
UNICAMP

O programa Sendmail



NOTAS

O programa sendmail tem como uma de suas tarefas monitorar a rede á espera de mensagens e envia mensagens para outros computadores. Mensagens locais são enviadas a programas locais para entrega acrescentando estas mensagens a arquivos já existentes ou processando-as através de outros programas. Mensagens podem ser enfileiradas para entrega posterior. O sendmail possui também a função de aliasing na qual um recipiente pode destinar suas mensagens a outros usuários ou programas.

A posição do programa sendmail na hierarquia do sistema de arquivos pode ser entendida como uma árvore invertida. Quando o programa sendmail é executado, ele le primeiramente o seu arquivo de configuração (sendmail.cf). Dentre os diversos itens definidos neste arquivo encontra-se a localização de todos os outros arquivos e diretórios que o programa sendmail necessita.

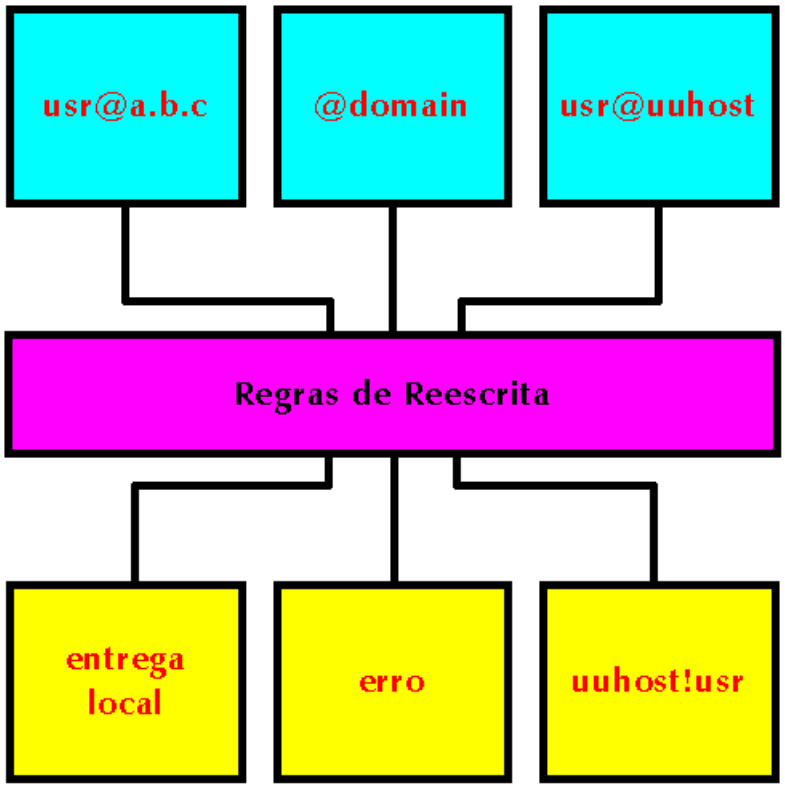
Centro de Computação

UNICAMP

Regras (Rules)

As regras no arquivo /etc/sendmail.cf são utilizadas para:

- modificar endereços eletrônicos
- detectar erros de endereçamento
- selecionar agentes para entrega de mensagens



Centro de Computação
UNICAMP

Domain Name Service
CONCEITOS
(1)

Nomes e Endereços

Toda interface de rede ligada a uma rede TCP/IP é identificada por um endereço IP formado por 32 bits. Um nome pode ser atribuído a qualquer dispositivo que possua um endereço IP. A atribuição de nomes aos endereços se deve ao fato de que é muito mais fácil uma pessoa se lembrar de nomes do que de números. O software de rede entretanto trabalha apenas com os números.

Na maior parte dos casos, os nomes e números podem ser usados indistintamente. Desta forma, os comandos `telnet wuarchive.wustl.edu` e `telnet 128.252.135.4` conduzem ao mesmo computador.

Quando se utilizam nomes é necessário que exista um serviço que efetue a conversão deste nome em um número IP para que se estabeleça a conexão.

Tradução Número x Nome

A tradução entre nomes (mais facilmente memorizáveis) e números passou por diversos estágios durante o desenvolvimento da Internet e das redes que a precederam.Inicialmente existia uma tabela, chamada *hosts.txt*, mantida pelo DDN-NIC e que era distribuída a todos os computadores da Internet. Com o crescimento da Internet este esquema se tornou inviável, exigindo a criação de um serviço mais eficiente para a resolução de nomes. A tabela*hosts.txt* foi substituída por um banco de dados distribuído denominado*Domain Name Service* concebido por Paul Mockapetris. As especificações encontram-se descritas naRFC 1034.

DNS - Domain Name Service

O DNS, ou *Domain Name Service*, foi desenvolvido para oferecer uma alternativa à resolução de nomes através do arquivo *hosts.txt* que pudesse garantir seu funcionamento eficiente mesmo em face do crescimento explosivo por que vem passando a Internet, permitindo ao mesmo tempo que informações sobre computadores novos sejam rapidamente disseminadas conforme a necessidade.

Centro de Computação
UNICAMP

Domain Name Service
CONCEITOS
(2)

BIND (Berkeley Internet Name Domain)

No Unix, o serviço DNS é implementado através do software BIND. O BIND é um sistema cliente servidor. O lado cliente do BIND é chamado resolver. Ele envia perguntas relativas a informações contidas no DNS a servidores de nomes (nameservers). O servidor DNS responde à estas perguntas. O lado servidor do DNS chama-se named.

Zonas

O termo zona (zone) se refere a informações contidas em um arquivo do banco de dados do DNS.

Domínio

Parte da hierarquia de domínios identificada por um nome de domínio.

Centro de Computação
UNICAMP

Configurações BIND (Servidor)

O software BIND pode ser configurado de diversas maneiras. São as seguintes as configurações mais comuns:

caching-only

Caching-only são servidore que rodam o programa **named** mas não são fontes oficiais de informação a respeito de domínios. Estes servidores obtem a resposta a todas as perguntas que lhe são direcionadas a partir de algum servidor remoto.

Servidores Primários

O servidor primário é a fonte oficial de todas as informações a respeito de um domínio específico. Ele carrega as informações a respeito do domínio a partir de arquivos locais mantidos pelo administrador do domínio. O servidor primário é o servidor mestre devido ao fato de que pode responder a qualquer pergunta sobre seu domínio com total autoridade.

Servidores secundários

Servidores secundários são aqueles que transferem um conjunto completo de informações a partir do servidor primário. Os arquivos descrevendo as zonas são transferidos do servidor primário e armazenados no servidor secundário como um arquivo local. Esta transferência chama-se **zone transfer**. O servidor secundário mantem uma cópia completa de todas as informações a respeito do domínio e responde a perguntas com autoridade. Consequentemente, um servidor secundário também é considerado um servidor mestre.

Centro de Computação
UNICAMP

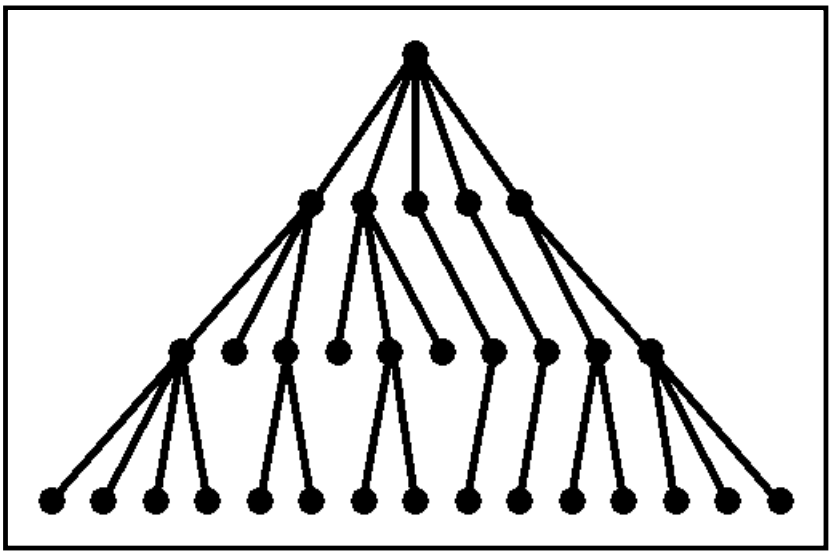
Domínios

O DNS é um sistema hierárquico distribuído concebido para realizar a tradução de nomes para números necessária ao estabelecimento de conexões entre computadores ligados à Internet.

Sob este sistema não existe nenhum repositório central que contenha informações sobre todos os computadores ligados à Internet.

Esta informação é distribuída por milhares de computadores, denominados servidores de nomes, ou name servers. Estes servidores de nomes encontram-se organizados de maneira similar ao sistema de arquivos do Unix.

Esta hierarquia pode ser representada da seguinte forma:



O DNS possui um domínio raiz, localizado no topo da hierarquia de domínios, que é servido por um grupo de servidores denominados ***root name servers .***

Centro de Computação
UNICAMP

Criação de Domínios e Subdomínios

O NIC (*Network Information Center* dos Estados Unidos tem a autoridade para alocar domínios. Para obter um domínio, o interessado precisa submeter um pedido ao NIC para criar um domínio sob um dos domínios de alto nível (net, gov, mil, org, com, edu).

O NIC americano delegou à Fundação de Amparo à Pesquisa do Estado de São Paulo (*FAPESP*, a autoridade para alocar domínios dentro do domínio .br
(net.br, gov.br, mil.br, org.br, com.br e edu.br).

O registro de um domínio é feito preenchendo-se o formulário domain-template.txt. Este formulário é uma versão adaptada do modelo distribuído pelo NIC americano e contem instruções para seu preenchimento

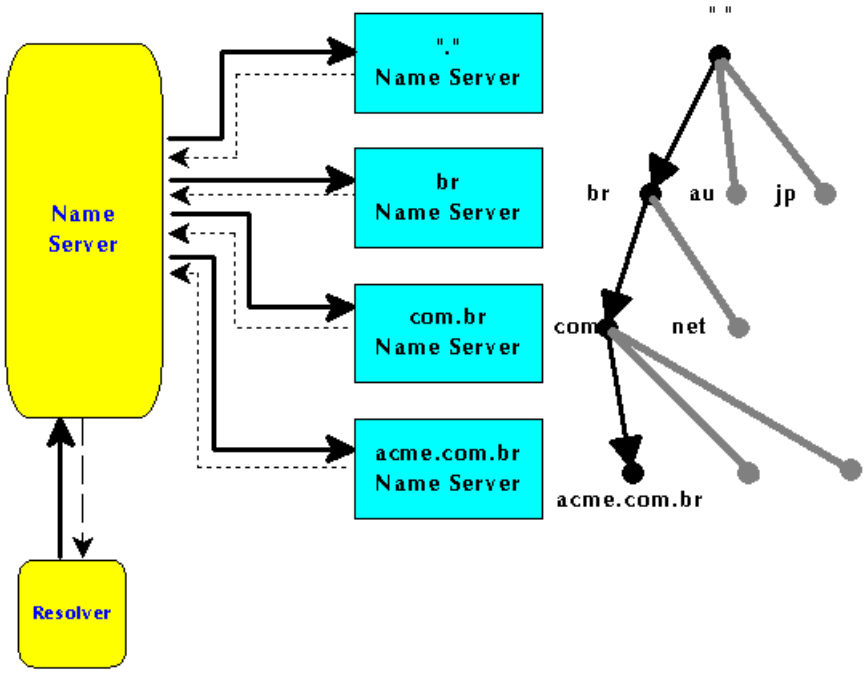
Diferentemente das normas adotadas nos EUA, a FAPESP não autoriza o domínio de registros em nome de pessoas físicas. Apenas empresas ou órgãos registrados de qualquer espécie podem se candidatar ao registro de domínios. O serviço de registro de domínios é realizado gratuitamente pela FAPESP.

Obviamente, um domínio somente será registrado caso não exista um registro anterior feito por outra entidade. Para determinar se já existe registro de um domínio utilize o programa whois.

O servidor whois com informações do domínio .br está localizado na FAPESP

Centro de Computação
UNICAMP

Resolução de Nomes



Centro de Computação
UNICAMP

Domain Name System Ferramentas de Gerenciamento

(traduzido e adaptado de Tools to manage DNS)

Diagnósticos Básicos

nslookup
: Ferramenta para interrogar servidores de nomes

dig
: Mais abrangente que nslookup, é usado por diversas outras ferramentas.

host
: Desenvolvido como uma evolução das ferramentas nslookup e dig.

Diagnósticos Gerais

Checker
: Utilizado para uma análise, do lado do servidor, de servidores remotos mal configurados.

DDT
: Desenvolvido por Jorge Frazao e Artur Romao, para debugar dados no cache.

dnswalk
: Desenvolvido por David Barr, verifica a árvore do DNS.

doc
: Desenvolvido por Steve Hotz e Paul Mockapetris. Verifica a integridade de um domínio.

lamers
: De Bryan Beecher, verifica e avisa os administradores sobre servidores que estão gerando informações errôneas.

nslint
: Desenvolvido por Craig Leres, identifica inconsistencias em arquivos do DNS.

ZoneCheck
: Faz verificação de zonas.

Ferramentas para manutenção de Zonas

Accugraph's IP Address Management
: Ferramenta comercial

addhost
: Realiza o gerenciamento de tabelas de hosts utilizando uma interface curses.Por John Hardt.

GASH
: Ferramenta de administração de sistemas que inclui o DNS.

gencidrzone
: Gera zonas reversas CIDR .

h2n
: Automatiza o procedimento de geração de arquivos DNS a partir do arquivo /etc/hosts, descrito

no livro DNS and Bind .

makezones
: Auxilia a manutenção de arquivos DNS.

NetID
: Produto comercial para gerenciamento do DNS

QIP e QNS
: Ferramentas comerciais para gerenciamento de endereços IP e DNS. Quadritek, utilizando Sybase .

SENDS
: Desenvolvida por Paul Vixie para o gerenciamento de bases DNS complexas.

Utah Tools
: Conjunto de ferramentas para gerenciamento do DNS em uso na Universidade de Utah.

webdns
: Manutenção DNS através de um WWW browser.

zsu
: Incrementa os números seriais das zonas de modo sensato.

Ferramentas Diversas

bindgraph
: Gera gráficos no formato xgraph para monitorar as estatísticas de servidores de nomes. Escrito por Nigel Campbell.

Brad's Tools
: Conjunto de ferramentas para gerenciamento de DNS.

dns-peers
: Gera arquivos de configuração baseado em arquivos de servidores remotos. Útil para sites que trocam serviços secundários para muitas zonas.

Paul's tools
: Desenvolvidas por Paul Balyoz: domtools, hiermap, dlint and cachebuild.

resolv+
: resolver para SunOS 4.1.x

Watch
: Ferramenta para análise do syslog que mantem e sumariza filas de eventos relacionados ao DNS.

Ferramentas de Sistema

Perl
: Linguagem de administração de sistemas utilizada por várias das ferramentas acima.

Centro de Computação
UNICAMP

DNS - Bibliografia

- Setting up a basic DNS server for a domain
- Domain Names - Concepts and Facilities - RFC 1034
- Domain Names - Implementation and Specification - RFC 1035
- DNS Resource Directory
- Common DNS Operational and Configuration Errors - RFC 1912
- DNS Extensions to support IP version 6 - RFC 1886
- DNS Support for Load Balancing - RFC 1794
- Tools for DNS debugging - RFC 1713
- Common DNS Data File Configuration Error - RFC 1537
- Common DNS Implementation Errors and Suggested Fixes - RFC 1536
- DNS encoding of network names and other types - RFC 1101
- A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY) - RFC 1996
- Incremental Zone Transfer in DNS - RFC 1995
- Name Server Operations Guide for BIND
- DNS server software
- Common DNS Errors
- Dealing with Lame Delegations
- DNS Database Files
- Style Guide for Zone Files
- The Domain Name System
- Tricks of the BIND Trade

- Linux DNS HOWTO
- A Survey of DNS Tools
- Keeping track of names and information: the domain system
- Domain Name System Structure and Delegation - RFC 1591
- DNS Tricks and Tips
- DNS Background Materials: Suggested Reading
- DNS and BIND
  Paul Albitz and Cricket Liu
  O'Reilly & Associates
  ISBN: 1-56592-010-4

Centro de Computação
UNICAMP