

Administração UNIX

Roberto de **Beauclair** Seixas
tron@lncc.br

Administração UNIX

- Introdução
- Sistema de Arquivos
- Ligando e Desligando
- Configuração do Kernel
- Redes
- Segurança
- Utilitários Importantes
- NFS
- NIS (Yellow Pages)
- DNS
- Manutenção
- Backup
- AIX
- SGI
- SunOS/Solaris
- Linux

Introdução

- Administrador

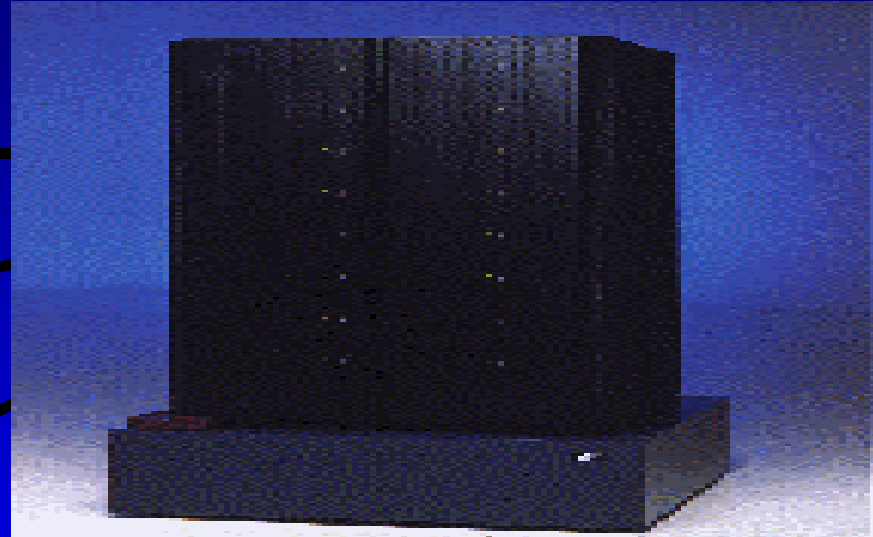
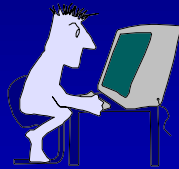
- Organiza e controla o uso de um recurso computacional, podendo ser este recurso um simples computador, um sistema de computadores ou uma rede de computadores;
- Pode servir como operador, conhecedor de comandos UNIX, suporte, apoio, homem-manual, detectador de problemas de hardware, enfim, um **solucionador de problemas**.

Introdução

- Funções

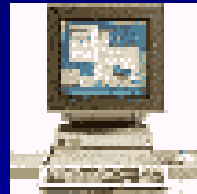
- *Startup/Shutdown*
- Manutenção do Sistema de Arquivos
- Configuração para:
 - » contas de usuários, formas de acesso, redes, impressoras, *scripts*, ...
- Monitoração de Atividades do Sistema
- Balanceamento das necessidades dos Usuários
- Estabelecer e Manter a Segurança do Sistema
- Corrigir Erros e Problemas

Ambiente Tradicional

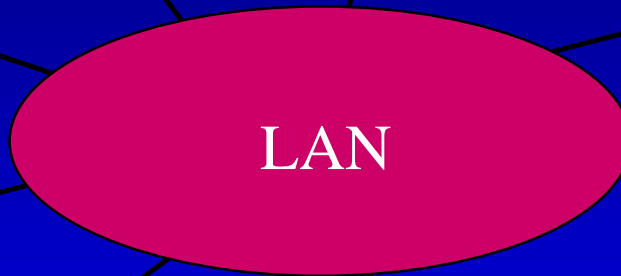


- CPU única e discos compartilhados
- Backup envolvia apenas 1 sistema
- Apenas um usuário privilegiado
- Softwares e versões únicos

Ambiente UNIX



?



- cada usuário tem sua própria CPU, memória e I/O
- diferentes categorias de uso
- backup pode envolver vários sistemas e vários discos
- cada “estação” possui seu próprio usuário privilegiado
- vários tipos de sistemas

Ambiente UNIX

- Facilidades:

- Utilitários para facilitar a administração de um sistema em rede - NFS, NIS, DNS, ...;
- Suporte de múltiplas arquiteturas de equipamentos;
- Várias versões de Sistemas Operacionais podem estar rodando na rede ao mesmo tempo.

Ambiente UNIX

- Tipos de Sistemas

- **servidor**: é uma estação que possui espaço em disco suficiente para suportar outros sistemas que estão na rede.
- **standalone**: possui sistema de arquivos completo para o *root*, *swap* e *usr* num disco próprio.
- **diskless**: não possui disco e por isso depende de outros sistemas na rede para poder funcionar.
- **dataless**: é uma estação que possui um pequeno disco com apenas o *root* e *swap*. As outras partições residem em outros sistemas.

Administração

A administração do Sistema inclui manter a versão mais atual do software instalada (o UNIX e os aplicativos). Existem utilitários para instalação e atualização dos Sistemas.

Quando novos Sistemas são adicionados à rede, eles precisam ser configurados, conforme a conveniência, como servidores, *standalone*, *diskless* ou *dataless*.

Administração

- Instalação do Software
 - UNIX
 - Aplicativos
 - Atualizações
- Configuração
 - Kernel
 - Impressoras
- Manutenção
 - *Backup / Restore*
- Segurança
 - Usuários e Grupos
 - Acessos privilegiados
- Comunicação e Redes
 - TCP/IP
 - E-Mail
 - NFS
 - NIS
 - DNS

Sistema de Arquivos

- Tipos de Discos

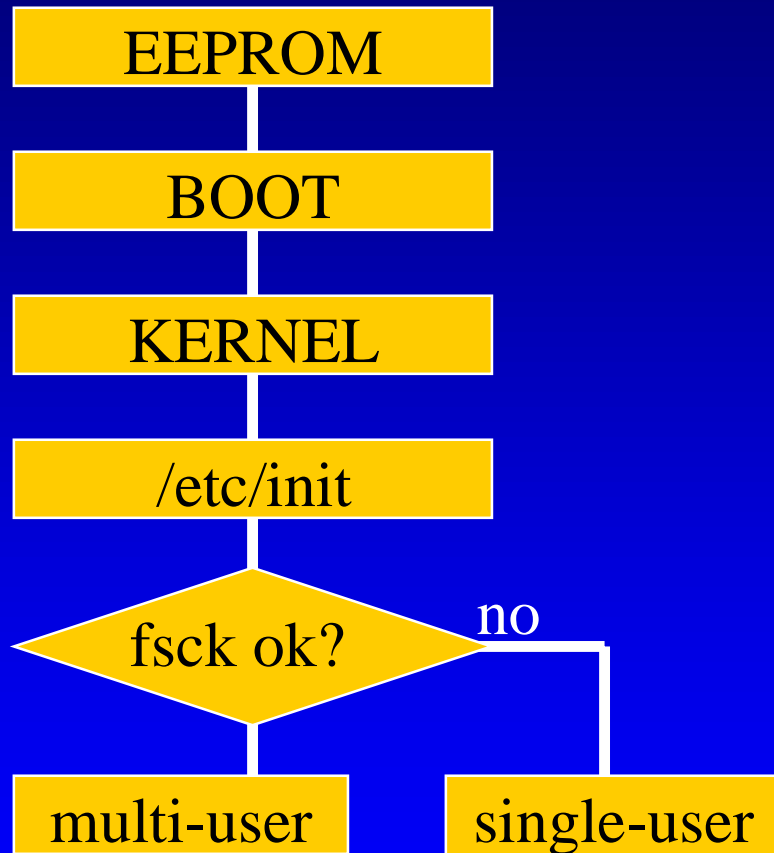
- SCSI: Small Computer System Interface
- IDE: Integrated Drive Electronic
- IPI: Intelligent Peripheral Interface

- Particionamento dos Discos

- Os discos são organizados em forma de partições; as partições são usadas para ajudar a interpretar as informações pelo *device driver*. Para o *device driver* cada partição corresponde a um dispositivo, como se fosse um disco.

Sun: /dev/sd0a **SGI:** /dev/root **AIX:** /dev/hd1 **Linux:** /dev/hda1

Startup e Shutdown



- testa o hardware;
- partição de *boot*;
- verifica dispositivos;
- identifica *root*, *swap* e *usr*;
- executa funções do sistema;
- verifica consistência dos sistemas de arquivos
- multi-user + rede + r/w ou single-user + r/o

Startup e Shutdown

- *halt, fasthalt, reboot e fastboot*
 - Todos estes comandos não mandam aviso quando estão desativando o sistema. O *fasthalt* e o *fastboot* criam um arquivo “/fastboot” que faz com que não se execute o *fsck* no próximo boot.
- *shutdown*
 - Executa o procedimento de desativar o sistema e avisa os usuários.

Ex: # shutdown 1400 Manutenção do Sistema

shutdown +15 Sistema será desativado em minutos.

Configuração do Kernel

- O Kernel ocupa espaço em memória. Logo, para reduzirmos o tamanho do código do kernel, devemos colocar apenas os módulos necessários. Isto vai liberar espaço em memória e aumentará o desempenho e velocidade do sistema como um todo.
- Qualquer hardware que for ligado ao Sistema precisa ser “suportado” pelo Kernel. Isto pode ser verdade também para software, uma vez que alguns fabricantes podem ter seu próprio *driver* para incluir no Kernel.
- Não deixe de fazer uma cópia do Kernel original, para qualquer eventualidade inesperada.
- Podem ocorrer problemas com o Kernel e a máquina apresentar erros no reboot. Isto significa que algo deve ser corrigido no Kernel e regenerado. Caso não seja identificado o problema, retorne o kernel antigo até que a solução seja encontrada.

Configuração do Kernel

● SunOS

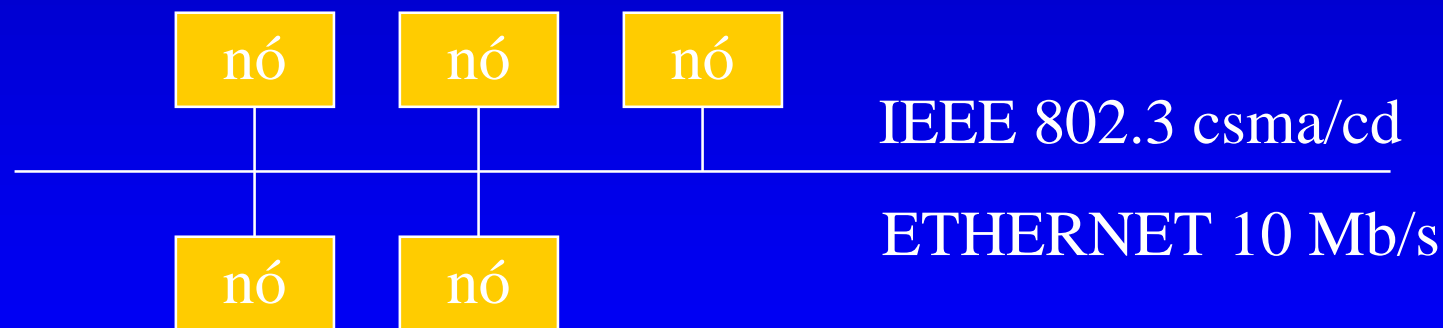
```
# cd /usr/share/sys/sun4/conf
# cp GENERIC NEW_KERNEL
# vi NEW_KERNEL
# config NEW_KERNEL
# cd ../NEW_KERNEL
# make
# mv /vmunix /vmunix.old
# cp vmunix /vmunix
# reboot
```

● Linux

```
# cd /usr/src/linux
# vi module_subdir/source_file.c
# make config
# make dep
# make Image
# make zImage
# mv vmlinux /vmlinux
# (LILO config - /vmlinuz)
# reboot
```

Redes

7. application	MAIL	FTP	TELNET	NFS	NIS	DNS
6. presentation	XDR					
5. session	RPC					
4. transport	TCP			UDP		
3. network	IP (INTERNETWORK)					
2. datalink	ETHERNET			Point-to-Point		
1. physical	ETHERNET			Point-to-Point		



Ethernet e Internet

- Ethernet

- É único para cada equipamento fabricado no mundo todo e possui 48 bits. Este endereço é gravado em PROMS nas placas de CPU e rede.

Ex: 8:0:20:1:39:31 (/etc/ethers)

- Internet

- É formado por um número de 32 bits, representando a rede, sub-rede e nó dentro da rede.
- Existem 3 classes (A, B e C) conforme número de nós.

Ex: 146.134.8.9 (/etc/hosts)

Redes

- Gateway (cisco = 146.134.8.254)
 - permite que redes de protocolos diferentes se comuniquem.
- Router
 - conecta duas redes locais
 - dois números IP (dois hostnames)
 - dois controladores Ethernet

(Rede de Pesquisa com a Rede Administrativa)

Monitoramento da Rede

ping < <i>hostname</i> >	envia um pacote de dados e relata se a informação foi recebida.
netstat	mostra o status de várias estruturas da rede.
telnet < <i>hostname</i> >	aplicação para se conectar a computadores remotos.
ftp < <i>hostname</i> >	aplicação para a transferência de arquivos

Segurança do Sistema

- login
- password
- userid
- groupid
- nome completo
- diretório
- shell

} /etc/passwd
/etc/group
/etc/shells
ou
NIS

Segurança do Sistema

● arquivos

```
-rw-r--r--  root  wheel  file1  
-rw-r--r--  root   wheel  file2  
-rw-r--r--  root   wheel  file3
```

● diretórios

```
drwxr-x--x  tron  prjcds  diretório
```

rwX dono pode ler, escrever e procurar.

r-x grupo pode ler e procurar.

--x outros podem procurar mas não podem ler.

Segurança do Sistema

- Set user id

- A permissão **setuid** significa que quando o programa for executado, o *userid* será o do dono do programa. Isto permite que usuários executem algumas atividades que requerem acesso a arquivos e diretórios que eles não poderiam acessar.

```
-rwsr-xr-x  root  staff  passwd
```

Segurança do Sistema

- Set group id

- A permissão **setgid** funciona da mesma forma que o **setuid**, mas para grupos ao invés de usuários. Quando em execução, substitui o *groupid* para o do programa.

```
-rwxr-sr-x  root  kmem  ps
```

Segurança do Sistema

- Set user id **and** Set group id
 - O comando de impressão (*lpd*) precisa ser definido para **setuid** do *root* para acessar todos os arquivos necessários da área de *spool* e para **setgid** do *daemon*, porque todos os dispositivos pertencem a este grupo .

```
-r-sr-s--x  root  daemon  lpd
```


Segurança do Sistema

- Set stick bit

- O **stick-bit** representa que o uma imagem do processo é retido em memória ou em swap, quando não está sendo executado. Este procedimento é feito para que o programa se torne disponível mais rapidamente para os usuários. Para diretórios, indica que apenas o *root* pode removê-lo. A intenção é para que os diretórios públicos não sejam removidos inadvertidamente.

```
-rw-----t  root  staff  swapfile  
drwxrwxrwt  root  staff  tmp
```

Segurança do Sistema

- **chmod**

- **setuid** chmod **4751** file (u+s)
- **setgid** chmod **2751** file (g+s)
- **stick-bit** chmod **1751** file (o+t)

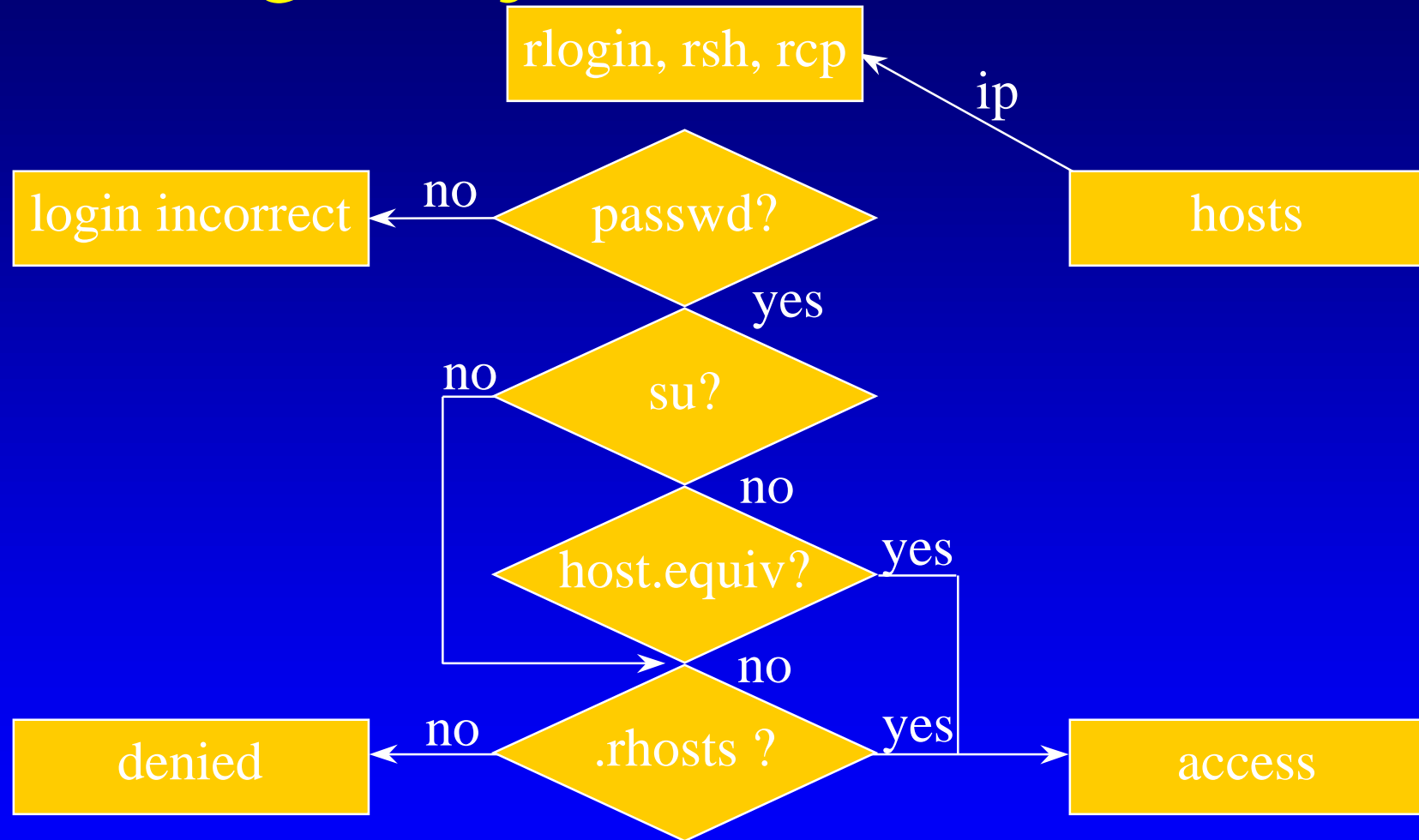
- **chown e chgrp**

- Altera o dono/grupo de arquivos ou diretórios.
Também é permitido utilizar o *userid/groupid*.

Segurança do Sistema

- `su [-] <user>`
 - Cria um novo *shell* que possui o *userid* do usuário especificado. Se nenhum usuário for especificado, o usuário será o *root*. Para que o comando tenha efeito, é necessário conhecer a *password* do usuário. Com este comando é possível obter as permissões do novo usuário.
 - Caso o parâmetro “-” seja incluído, os *scripts* do usuário serão executados.

Segurança Através da Rede



Segurança Através da Rede

- /etc/hosts.equiv

- Contém uma lista dos *hosts* e usuários “confiáveis”. Se o usuário e o nome do nó estão neste arquivo, então o *password* não será necessário. A exceção será quando o usuário for o *root*. Neste caso, o arquivo checado será o “*.rhosts*”.

- /etc/netgroup

- Define um grupo de máquinas da rede que são usados para estabelecer permissões de comandos remotos.

Utilitários Importante

- ps - Mostra o status dos processos
 - PID: número do processo
 - STAT: status do processo
 - » R em execução
 - » T parado
 - » P aguardando paginação
 - » D aguardando o disco
 - » S inativo por menos de 20 segundos
 - » I inativo por mais de 20 segundos
 - » W em área de swap
 - » Z aguardando processo pai (zombie)

Todos processos: Sun/Linux/SGI: ps -aux AIX: ps -elf

Utilitários Importante

- `kill [signal] <pid>` - Sinaliza processos
 - Este comando envia sinais para processos. É utilizado, normalmente, para parar processos mas pode ser usado para enviar sinais do UNIX para qualquer processo. Para verificar os sinais possíveis use “kill -list”.
 - Para usar o comando *kill* é necessário conhecer o *pid* do processo a ser interrompido. É recomendado que se tente terminar um processo de uma maneira que permita o fechamento dos arquivos pendentes, antes de executar o encerramento incondicional: “kill -kill”

Utilitários Importante

- *pstat*
 - Mostra o conteúdo de várias tabelas do kernel. As tabelas de *inodes*, *stream*, arquivos e processos podem ser verificados. O *pstat* pode ser usado para analisar o *dump* de sistemas em que ocorreram *crash dumps*.
- *uptime* e *rup*
 - Mostra a quanto tempo um sistema está ativo desde o último *reboot*. É mostrado também a média de carga da CPU, baseado no último minuto, cinco minutos e quinze minutos.
- *rusers*
 - Mostra os usuários conectados em “todos” os nós da rede. (nós remotos devem ter *ruserd*)
- *wall* e *rwall*
 - Permite que usuários enviem mensagens para todos os usuários conectados no sistema.

Network File System

- O **NFS** é um serviço de rede que permite o compartilhamento de sistemas de arquivos ou diretórios através da rede, de forma totalmente transparente.
- O **NFS** é implementado através do mecanismo de RPC (*Remote Procedure Call*), com o protocolo XDR (*eXternal Data Representation*), tornando-o independente do tipo de máquina.

Network File System

- Servidor NFS

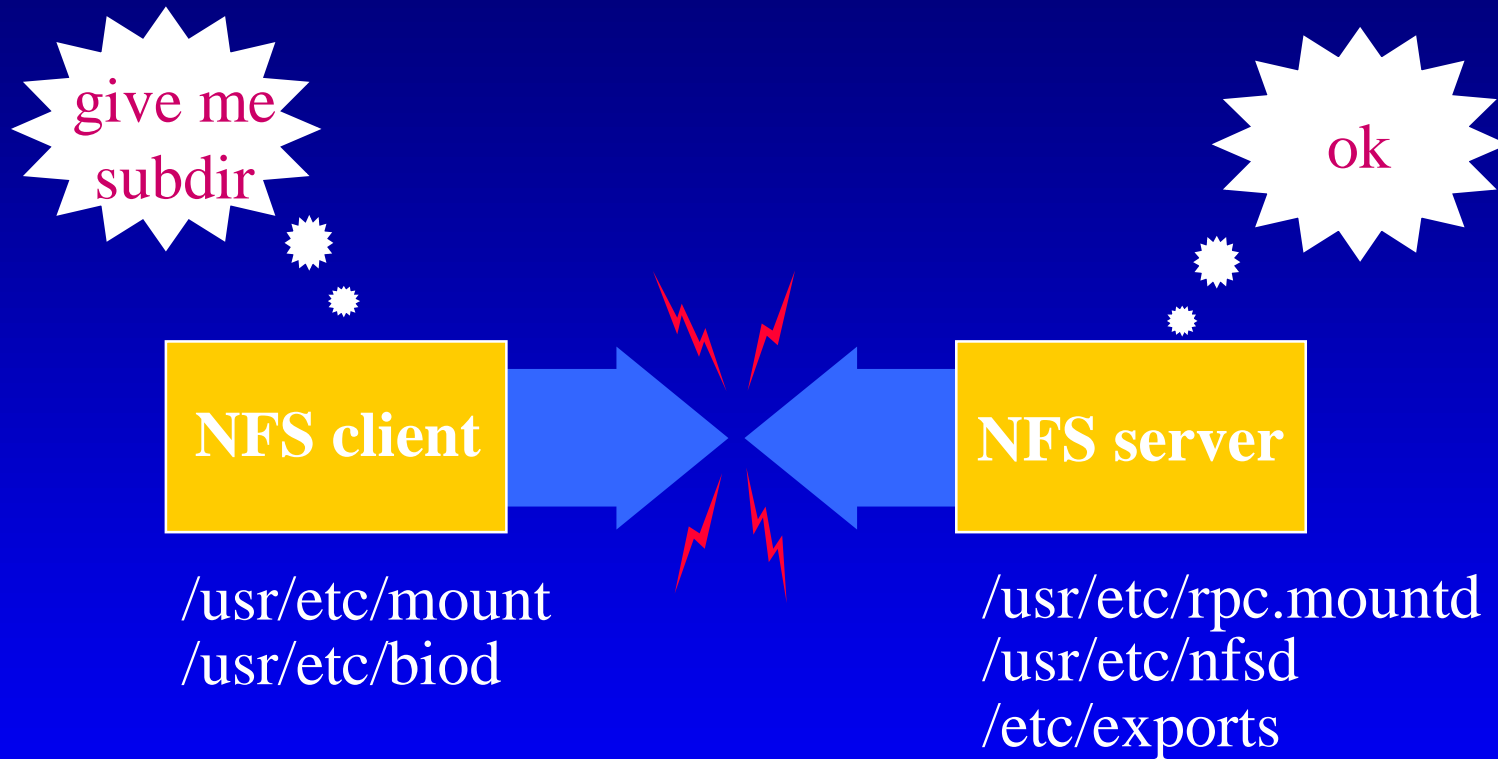
- É a máquina que permite a “montagem” de seus sistemas de arquivos por outras máquinas na rede.
- O servidor “exporta” o sistema de arquivo para fazê-lo disponível para compartilhamento remoto.
- Tarefas:
 - » ler ou escrever arquivos em resposta as requisições;
 - » não mantém nenhum status dos arquivos abertos;
 - » não armazenar requisições de escrita;
 - » se comunicar através de *routers*;

Network File System

- Cliente NFS

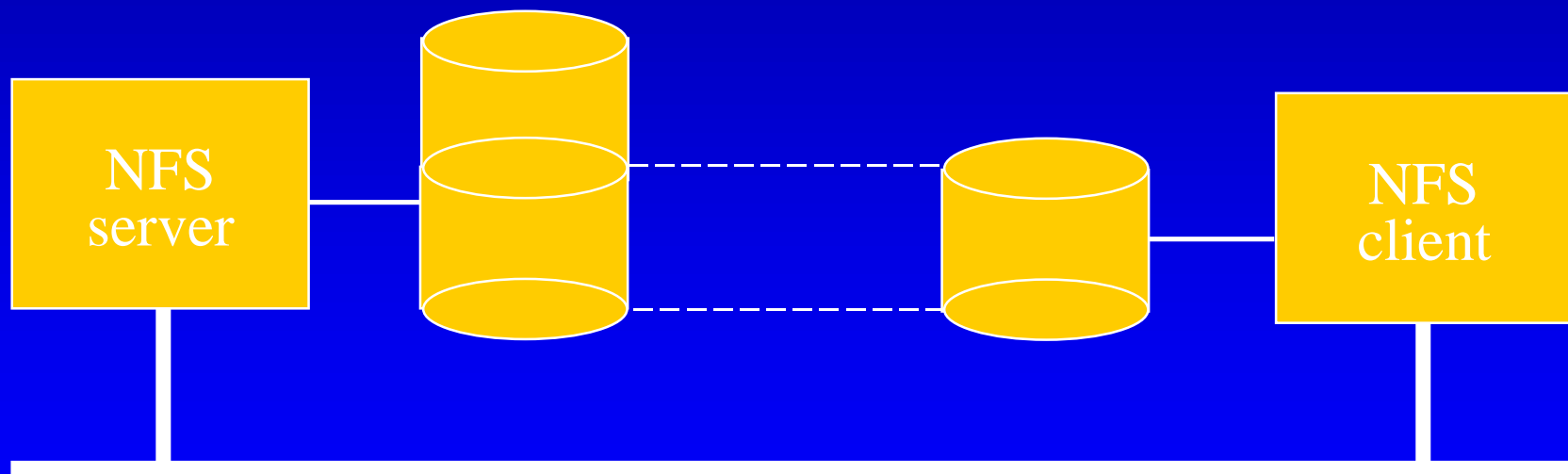
- É a máquina que compartilha (“monta”) os sistemas de arquivos ou diretórios disponibilizados (“exportados”) pelos servidores NFS. Os arquivos são escritos e lidos através de requisições feitas ao servidor NFS.
- Tarefas:
 - » manter o status dos arquivos abertos;
 - » controlar as requisições de escrita;
 - » se comunicar através de *routers*;

Network File System



Network File System

O *daemon* “`rpc.mountd`” no servidor retorna um *handle* do sistema de arquivos requisitado. O *handle* do cliente é colocado na tabela de montagens do kernel. Todas as referências futuras serão passadas para o *daemon* do NFS rodando no servidor, usando o *handle* do cliente.



Network File System

- `/etc/exports`

- Se este arquivo existir, automaticamente os sistemas de arquivos serão “exportados” e os *daemons* “`nfsd`” e “`rpc.mountd`” serão ativados.

- `exportfs`

- É usado para “exportar” sistemas de arquivos a qualquer instante.

- `mount`

- É usado para “montar” sistemas de arquivos locais ou remotos.

- `/etc/fstab` (SunOs/Linux/IRIX) `/etc/filesystems` (AIX)

- Contém uma lista dos sistemas de arquivos a serem “montados”.

Network File System

- Exemplos:

 - # exportfs -a

 - # exportfs -u /home/soft

 - # mount -t nfs -o rw,soft fs1:/home/fs1 /u

 - # mount -t iso9660 -o ro /dev/sd0 /cdrom

- showmount <*host*>

 - Mostra uma lista de clientes NFS de *host*.

- nfsstat

 - Mostra algumas estatísticas do NFS

Network Information Service

- O **NIS** é um serviço de informações distribuído, que controla dados importantes ao funcionamento da rede.
- O antigo nome “Yellow Pages” mudou devido ao fato de ser marca registrada da *British Telecommunications*. No entanto, os comandos e muitos manuais ainda fazem referências a este nome.

Network Information Service

- Um domínio **NIS** é um grupo de nós na rede que utilizam o mesmo banco de dados.
- Domínios **NIS** podem ser estabelecidos independentes de domínios Internet (DNS).
- Um domínio **NIS** é simplesmente um diretório em “/var/yp” contendo um conjunto de “mapas”. O nome do diretório é o nome do domínio.
- Cada máquina na rede pertence a um único domínio, definido nos *scripts* de inicialização durante o *boot*.

Network Information Service

- Servidores e Clientes

- Um cliente NIS é uma máquina que utiliza os serviços de rede dos servidores NIS;
- Um servidor mestre NIS oferece os serviços do NIS, atualiza e propaga os mapas para os servidores escravos;
- Um servidor escravo NIS fornece os serviços do NIS, caso o servidor mestre não esteja disponível.

- Mapas Principais

passwd, group, hosts, netgroup, netmasks e networks.

Network Information Service

- Inicializando o servidor NIS
 - defina o nome do domínio
 - # domainname <*domain*>
 - atualize os arquivos dos mapas no /etc
 - crie o banco de dados
 - # ypinit -m
 - ative os *daemons* do NIS
 - # ypserv
 - # ypbind

Network Information Service

- Inicializando o cliente NIS
 - defina o nome do domínio
 - # domainname <*domain*>
 - ative o *daemon* do NIS
 - # ypbind

Network Information Service

- Atualizando o NIS

- Qualquer alteração do banco de dados do NIS tem que ser feito no servidor mestre. Para isto, deve-se editar os arquivos necessários (/etc) e executar o comando *make* (*ypmake*) no diretório “/var/yp”.
- O *make* refaz os mapas alterados e quando estiverem completas faz um “yppush” para atualizar os mapas dos servidores escravos e dos clientes.

Network Information Service

- Comandos úteis

- `ypwhich` mostra quem é o servidor usado
- `ypwhich -m` mostra quem é o servidor mestre
- `ypwhich -x` mostra os apelidos dos mapas
- `ypcat <map>` mostra o conteúdo do mapa

Domain Name Service

- O **DNS** é o serviço responsável pela resolução de nomes na rede, ou seja, responsável pela tradução do nome simbólico para um número IP.

Ex: **vishnu** para **146.134.8.251**
 www2 ou **brahma** para **146.134.8.182**

- É executado, através do *daemon* “named” que consulta uma tabela de nomes com os *hosts* do domínio e os números IP, e uma tabela de números IP com os *hosts* (domínio reverso).
- O arquivo “/etc/resolv.conf” é usado para informar qual o servidor DNS e qual a ordem a ser utilizada. Por exemplo, no caso da procura de um *host*, a consulta pode ser local (/etc/passwd), NIS (bind) ou DNS.

Domain Name Service

- *nslookup*
 - É o utilitário usado para a resolução interativa de nomes, inclusive para domínio reverso.

Manutenção do Sistema de Arquivos

- Problemas

- Não sincronização dos sistemas de arquivos em caso de desligamento;
- Não verificação e reparo de arquivos inconsistentes no momento do *boot*;
- Problemas eventuais no disco (*bad blocks*);
- Falhas e Oscilações na rede elétrica;
- Falhas de Hardware.

Manutenção do Sistema de Arquivos

- *fsck*

- Verifica as inconsistências nos sistemas de arquivos e faz os reparos necessários de forma interativa ou automática.
- O *fsck* se baseia no fato de que não deve haver inconsistências nos sistemas de arquivos. Por exemplo, o número de *inodes* é especificado no superbloco do disco. Qualquer informação contraditória é considerada suspeita e tentar-se-á eliminá-la.
- Os arquivos e diretórios encontrados como “órfãos” serão reconectados ao sistema de arquivos no diretórios “lost+found”. O nome do arquivo é o seu antigo *inode*.

Backup e Restore

- tar

- É utilizado para salvar e recuperar arquivos. No caso de se especificar um diretório, a operação será recursiva.

- Criação: `tar cvf <device> <files/dir>`

- Listagem: `tar tvf <device>`

- Extração: `tar xvf <device> [<files/dir>]`

- Criação remota:

 - `tar cvf - <files/dir> | rsh <host> dd of=<device>`

- Extração remota:

 - `rsh <host> dd if=<device> | tar xvBf -`

Backup e Restore

- Controle das Unidades de Fita (Tape/DAT)

`mt -f <device> <command>`

onde <command> pode ser:

- » `rewind` rebobina a fita
- » `status` mostra o status da fita
- » `retension` retensiona
- » `fsb <n>` avança <n> registros na fita
- » `bsb <n>` retrocede <n> registros na fita