

ADMINISTRAÇÃO DE REDES



Airton Kuada
airton@fesppr.br

AGENDA

CONFIGURAÇÃO DE
AMBIENTE DE REDE NO
LINUX

GERENCIAMENTO DE
SERVIÇOS

REDES PEER2PEER
WINDOWS

SAMBA
(COMPARTILHAMENTO DE
ARQUIVOS)

QUOTA DE DISCO

DHCP

BIND (SERVIDOR DE DNS)

POSTFIX (CORREIO
ELETRÔNICO)

APACHE (SERVIDOR HTTP)

SQUID – PROXY INTERNET

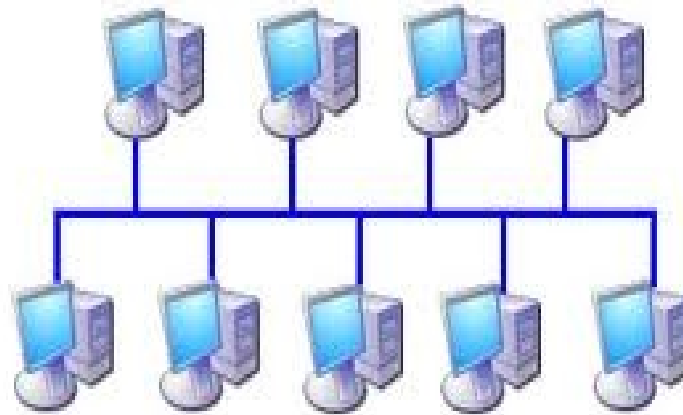


CONFIGURAÇÃO BÁSICA DE REDES LINUX



■ CONEXÕES DE REDE

- UMA REDE LOCAL É COMPOSTA PELA INTERCONEXÃO DE DIVERSOS ELEMENTOS (NÓS DE REDE) ATRAVÉS DE UM MEIO FÍSICO



■ CONEXÕES DE REDE

- CADA ESTAÇÃO OU SERVIDOR UTILIZADO UMA PLACA DE REDE PARA SE CONECTAR AO MEIO FÍSICO



■ COMANDOS DE INTERFACES DE REDE

- NO LINUX, CADA PLACA DE REDE RECEBE UMA IDENTIFICAÇÃO COMO:

- eth0 – PRIMEIRA INTERFACE DE REDE

- eth1 – SEGUNDA INTERFACE DE REDE

- eth2 – TERCEIRA INTERFACE DE REDE

- eth3 – QUARTA INTERFACE DE REDE

- O COMANDO UTILIZADO PARA MOSTRAR TODAS AS INTERFACES DE REDE É:

- # ifconfig -a

- O COMANDO UTILIZADO PARA MOSTRAR DETALHES DE UMA INTERFACE ESPECÍFICA É:

- # ifconfig eth1

- OBSERVAÇÃO IMPORTANTE É QUE SOMENTE O USUÁRIO “root” PODE UTILIZAR ESTES COMANDOS



■ COMANDOS DE INTERFACES DE REDE

■ EXEMPLO DE SAÍDA DE UM COMANDO

■ # ifconfig eth0

Link encap:Ethernet *Endereço de HW 00:11:5b:fc:d5:2a*

inet end.: 192.168.1.100 Bcast:192.168.1.255 Masc:255.255.255.0

endereço inet6: fe80::211:5bff:fefc:d52a/64 Escopo:Link

UP BROADCAST RUNNING MULTICAST **MTU:1500** Métrica:1

RX packets:5266063 errors:0 dropped:0 overruns:0 frame:0

TX packets:1846647 errors:0 dropped:0 overruns:0 carrier:0

colisões:0 txqueuelen:1000

RX bytes:2663170854 (2.4 GiB) TX bytes:145663092 (138.9 MiB)

IRQ:23 Endereço de E/S:0xc800



■ COMANDOS DE INTERFACES DE REDE

- A INTERFACE DE REDE PODE SER CONFIGURADA MANUALMENTE (CONFIGURAÇÃO TEMPORÁRIA) ATRAVÉS DO COMANDO “ifconfig” COMO MOSTRADO ABAIXO, PORÉM O MAIS COMUM É UTILIZAR ARQUIVOS DE CONFIGURAÇÃO (CONFIGURAÇÃO PERMANENTE) QUE SÃO UTILIZADOS NA INICIALIZAÇÃO DO SISTEMA OPERACIONAL

```
# ifconfig eth1 172.16.1.10 netmask 255.255.0.0
```



■ COMANDOS DE INTERFACES DE REDE

- A CONFIGURAÇÃO AUTOMÁTICA UTILIZA O ARQUIVO “/etc/network/interfaces”

- CONFIGURANDO UM ENDEREÇO ESTÁTICO

```
auto eth0
```

```
iface eth0 inet static
```

```
address 172.16.1.10
```

```
netmask 255.255.0.0
```

```
network 172.16.0.0
```

```
broadcast 172.16.255.255
```

```
gateway 172.16.1.1
```

- CONFIGURANDO UM ENDEREÇO COM DHCP

```
auto eth0
```

```
iface eth0 inet dhcp
```



■ COMANDOS DE INTERFACES DE REDE

■ DESABILITANDO LÓGICAMENTE UMA INTERFACE

- EM DETERMINADOS MOMENTOS É NECESSÁRIO RETIRAR A MÁQUINA DA REDE TORNANDO-A INATIGÍVEL POR QUALQUER OUTRA MÁQUINA (POR EXEMPLO: A MÁQUINA ESTÁ SENDO ATACADA)
- ESTA ATIVIDADE PODE SER REALIZADA DE DUAS FORMAS:
 - PODEMOS RETIRAR FISICAMENTE, O CABO DA REDE
 - PODEMOS DESABILITAR LOGICAMENTE A INTERFACE DE REDE
- QUANDO DESABILITAMOS LOGICAMENTE A INTERFACE DE REDE, ELA ESTARÁ CONECTADO A REDE, MAS NÃO ESTARÁ OPERACIONAL



■ COMANDOS DE INTERFACES DE REDE

■ DESABILITANDO LÓGICAMENTE UMA INTERFACE

□ # ifdown eth0

■ HABILITANDO LÓGICAMENTE UMA INTERFACE DE REDE

□ # ifup eth0



■ UTILIZANDO COMANDOS DE REDE

- UMA VEZ QUE A INTERFACE DE REDE ESTEJA OPERACIONAL E A CONEXÃO FÍSICA COM A REDE ESTEJA REALIZADA, PODEMOS INICIAR A COMUNICAÇÃO COM OUTRA MÁQUINA NA REDE
- A PRIMEIRA OPERAÇÃO É VERIFICAR SE A MAQUINA POSSUI CONECTIVIDADE COM OUTRAS MÁQUINAS DA REDE E PARA ISSO, UTILIZAMOS COMANDO “ping”
- O COMANDO “ping” ENVIA UMA PACOTE (ECHO REQUEST) PARA O HOST REMOTO QUE POR SUA VEZ DEVOLVE UM PACOTE DE RESPOSTA (ECHO RESPONSE)
- EXEMPLO DE UTILIZAÇÃO

□ ping 172.17.1.1

□ ONDE

□ ping É O COMANDO

□ 172.17.1.1 É O HOST DE DESTINO (REMOTO)



■ UTILIZANDO COMANDOS DE REDE

■ EXEMPLO DE UTILIZAÇÃO DO COMANDO “ping”

```
#ping 10.15.16.1
```

```
PING 10.15.16.1 (10.15.16.1) 56(84) bytes of data.
```

```
64 bytes from 10.15.16.1: icmp_req=1 ttl=255 time=1.31 ms
```

```
64 bytes from 10.15.16.1: icmp_req=2 ttl=255 time=1.47 ms
```

■ PARA ENCERRAR O COMANDO “ping”, UTILIZE A COMBINAÇÃO DE TECLA “ctrl c”

■ AO FINAL SERÁ MOSTRADO UMA ESTATÍSTICA SOBRE O COMANDO “ping” ANTERIORMENTE EXECUTADO

```
--- 10.15.16.1 ping statistics ---
```

```
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
```

```
rtt min/avg/max/mdev = 1.315/1.393/1.472/0.086 ms
```



■ UTILIZANDO COMANDOS DE REDE

■ MANIPULANDO A TABELA ARP

- A TABELA ARP ARMAZENA OS ENDEREÇOS MAC DE TODOS OS HOSTS QUE ESTÃO NA MESMA REDE IP QUE SE COMUNICARAM COM A HOST LOCAL
- A TABELA ARP É MOSTRADA ATRAVÉS DO COMANDO “arp” CONFORME MOSTRADO ABAIXO:

```
# arp -an
```

```
? (10.15.18.36) em 00:30:67:9c:6a:4f [ether] em eth0
```

```
? (10.15.16.6) em 00:00:5e:00:01:16 [ether] em eth0
```

```
? (10.15.18.93) em 00:22:15:ea:2e:05 [ether] em eth0
```

```
? (10.15.16.1) em 00:0f:23:c0:5d:ff [ether] em eth0
```



■ UTILIZANDO COMANDOS DE REDE

■ MANIPULANDO A TABELA ARP

□ UMA ENTRADA PODE SER ELIMINADA DA TABELA “arp”

```
# arp -d 10.15.18.36
```

```
# arp -an
```

```
? (10.15.18.36) em <incompleto> em eth0
```

```
? (10.15.16.6) em 00:00:5e:00:01:16 [ether] em eth0
```

```
? (10.15.18.93) em 00:22:15:ea:2e:05 [ether] em eth0
```

```
? (10.15.16.1) em 00:0f:23:c0:5d:ff [ether] em eth0
```



■ UTILIZANDO COMANDOS DE REDE

■ MANIPULANDO A TABELA ARP

□ UMA ENTRADA PODE SER ADICIONADA MANUALMENTE NA TABELA “arp”

```
# arp -s 10.15.18.36 00:0f:24:44:ab:cd
```

```
# arp -an
```

```
? (10.15.18.36) em 00:0f:24:44:ab:cd [ether] PERM em eth0
```

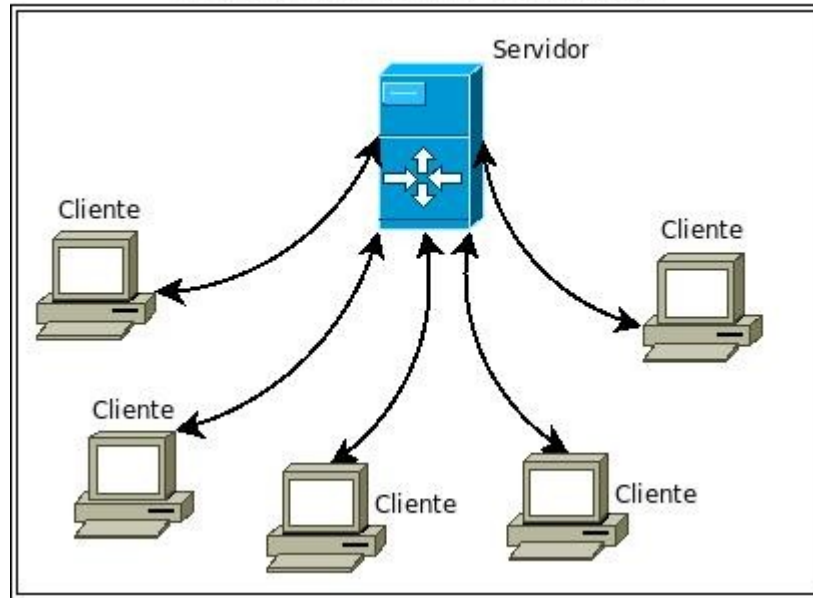
```
? (10.15.16.6) em 00:00:5e:00:01:16 [ether] em eth0
```

```
? (10.15.18.93) em 00:22:15:ea:2e:05 [ether] em eth0
```

```
? (10.15.16.1) em 00:0f:23:c0:5d:ff [ether] em eth0
```



Modelo Cliente-Servidor



■ SERVIÇOS DE REDE

- UM SERVIÇO DE REDE É UMA FUNCIONALIDADE QUE É FORNECIDA EM UMA REDE DE COMPUTADORES
- ESTA FUNCIONALIDADE PODE SER UTILIZADA PARA ATENDER AS NECESSIDADE DE ADMINISTRAÇÃO DA PRÓPRIA REDE DE COMPUTADORES OU PARA ATENDER AS NECESSIDADES DOS USUÁRIOS
- TIPOS DE SERVIÇOS DE REDE
 - RECUPERAÇÃO DE CONTEÚDO – HTTP/FTP
 - ACESSO REMOTO – SSH/TELNET/VNC
 - CONFIGURAÇÃO – DHCP/LDAP/DNS
 - MONITORAÇÃO E GERENCIA - SNMP
 - COMPARTILHAMENTO DE RECURSOS – NFS/SMB/IPP
 - COMUNICAÇÃO ENTRE USUÁRIOS – SMTP/POP3/IMAP/SIP



■ SERVIÇOS DE REDE

■ CADA SERVIÇO DE REDE É COMPOSTO

□ CLIENTE

□ COMPUTADOR QUE SOLICITA O SERVIÇO ATRAVÉS DA REDE

□ SERVIDOR

□ SERVIDOR QUE ATENDE A SOLICITAÇÃO DO USUÁRIO E REALIZA O PROCESSAMENTO PRINCIPAL

□ PROTOCOLO

□ CONJUNTO DE MENSAGENS QUE SÃO TROCADAS ENTRE O CLIENTE E O SERVIDOR PARA A REALIZAÇÃO DO SERVIÇO

□ MIDDLEWARE

□ É O AMBIENTE QUE FORNECE SUPORTE PARA A IMPLEMENTAÇÃO DO SERVIÇO, ISTO É, OS SISTEMAS OPERACIONAIS E PROTOCOLOS DE COMUNICAÇÃO QUE ENCAMINHAM AS MENSAGENS ATRAVÉS DA REDE



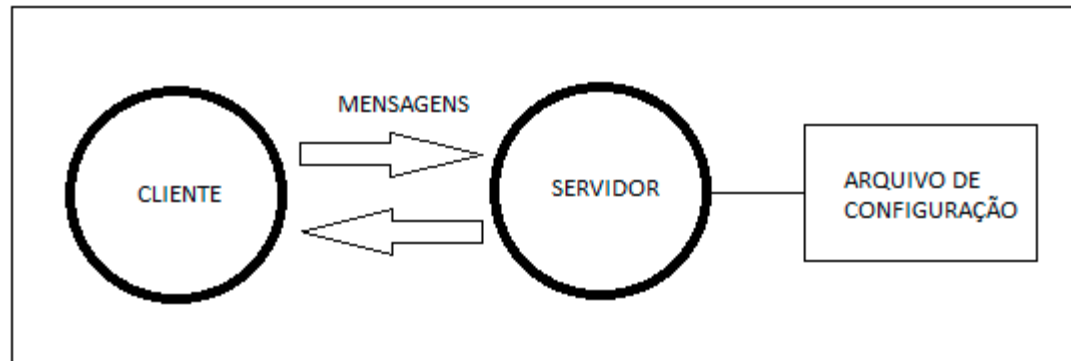
■ SERVIÇOS DE REDE

- EXEMPLO DE FORNECIMENTO DE SERVIÇO DE PÁGINAS (HTTP)
 - ESTAÇÃO COM WINDOWS 7, EXECUTANDO O BROWSER INTERNET EXPLORER (IE) NO BRASIL, ACESSANDO O SITE www.asus.tw
 - SERVIDOR HTTP QUE HOSPEDA O SITE www.asus.tw EXECUTA UM SISTEMA OPERACIONAL LINUX COM O SERVIÇO APACHE ESTÁ LOCALIZADO EM TAIWAN
 - NESTE CASO, O BROWSER (CLIENTE) REQUISITA E MOSTRA A PÁGINA SOLICITADA PELO USUÁRIO, O APACHE (SERVIDOR) RECEBE A SOLICITAÇÃO DO BROWSER, E ENVIA O CONTEÚDO QUE SERÁ MOSTRADO NO BROWSER



■ SERVIÇOS DE REDE

- O SERVIDOR PODE TRATAR DIVERSAS REQUISIÇÕES SIMULTANEAMENTE, ISTO PERMITE QUE DIVERSOS CLIENTES SEJAM ATENDIDOS NO MESMO INSTANTE
- CLIENTE E SERVIDOR COMUNICAM-SE ATRAVÉS DA REDE, TROCANDO MENSAGENS
- CADA SERVIDOR POSSUI UM ARQUIVO DE CONFIGURAÇÃO QUE DEFINE A FORMA DE TRABALHO



■ SERVIÇOS DE REDE

■ ARQUITETURA DE SERVIÇOS DE REDE

□ TWO-TIER – ARQUITETURA COM DOIS COMPONENTES

□ O SERVIDOR É RESPONSÁVEL PELA EXECUÇÃO DO SERVIÇO

□ CLIENTE É RESPONSÁVEL PELA APRESENTAÇÃO DOS RESULTADOS E INTERAÇÃO COM O USUÁRIO

□ SE O CLIENTE É RESPONSÁVEL SOMENTE PELA APRESENTAÇÃO DOS DADOS, ISTO É, NÃO REALIZA NENHUM PROCESSAMENTO SIGNIFICATIVO, É CHAMADO DE CLIENTE MAGRO

□ EXEMPLO: WEBMAIL, VNC

□ SE O CLIENTE É RESPONSÁVEL POR PARTE DA LÓGICA DA APLICAÇÃO, ISTO É, É RESPONSÁVEL POR ALGUMA PARTE DO PROCESSAMENTO FINAL DO SERVIÇO, É CHAMADO DE CLIENTE GORDO

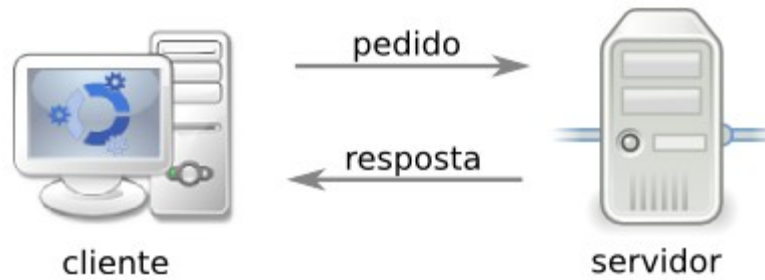
□ EXEMPLO: OUTLOOK



■ SERVIÇOS DE REDE

■ ARQUITETURA DE SERVIÇOS DE REDE

□ TWO-TIER – ARQUITETURA COM DOIS COMPONENTES



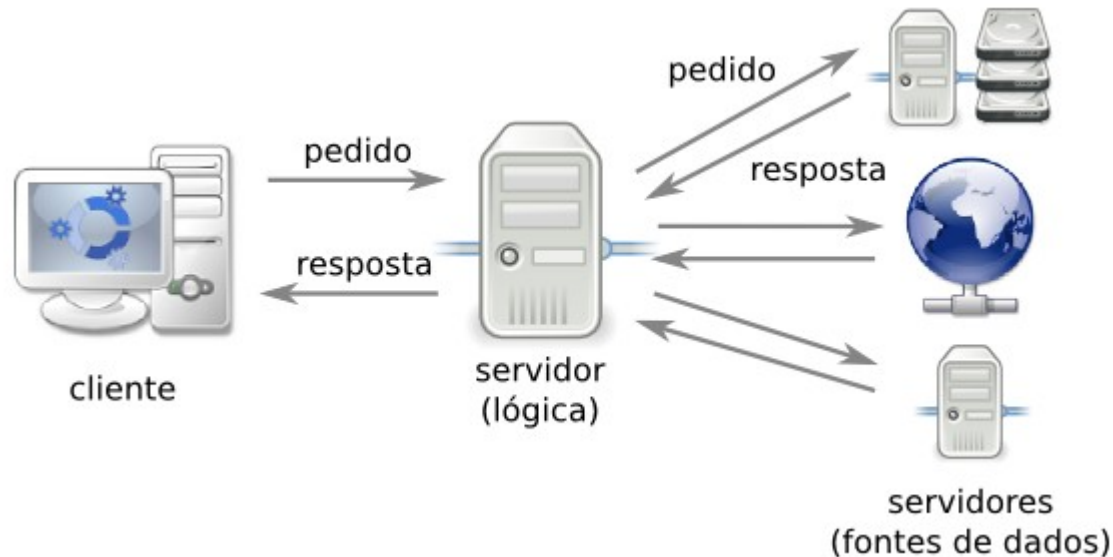
■ SERVIÇOS DE REDE

■ ARQUITETURA DE SERVIÇOS DE REDE

□ THREE-TIER – ARQUITETURA COM TRÊS COMPONENTES

□ O CLIENTE É RESPONSÁVEL PELA INTERFACE COM O USUÁRIO

□ O SERVIDOR É RESPONSÁVEL PELA LÓGICA DA APLICAÇÃO E OS REPOSITÓRIOS DE DADOS

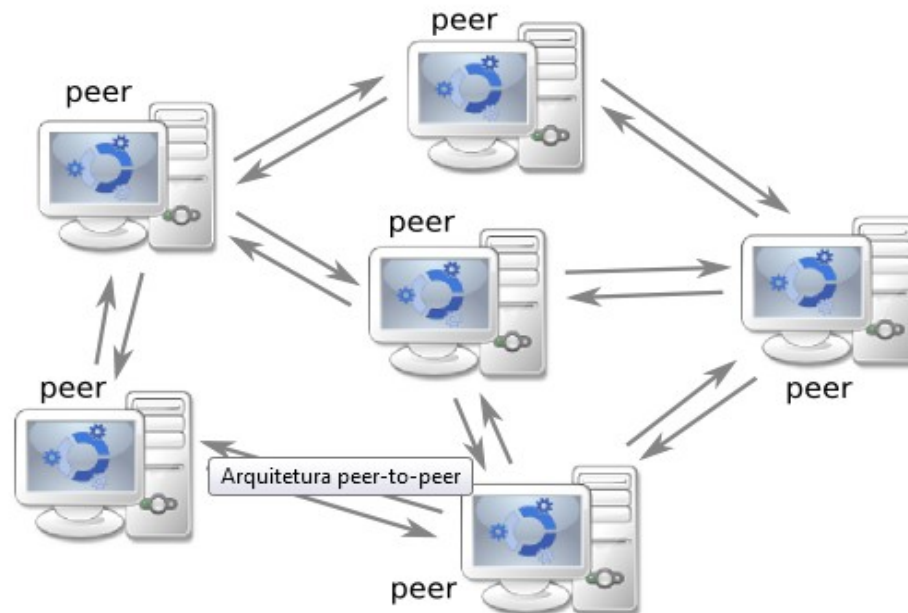


■ SERVIÇOS DE REDE

■ ARQUITETURA DE SERVIÇOS DE REDE

□ PEER-TO-PEER

□ NESTA ARQUITETURA TODOS PARTICIPANTES SÃO AO MESMO TEMPO SERVIDORES (OFERECEM RECURSOS E SERVIÇOS) E CLIENTES (UTILIZAM SERVIÇOS E RECURSOS) UNS DOS OUTROS



■ SERVIÇOS DE REDE

□ PORTAS DE COMUNICAÇÃO

SERVIÇO	PORTA	PROTOCOLO
HTTP	80	TCP
DNS	53	UDP
SSH	22	TCP
SMTP	25	TCP
FTP	21 E 20	TCP
SNMP	161 E 162	UDP
VNC	5900	TCP



■ SERVIÇOS DE REDE

□ SERVIÇOS DE REDE NO AMBIENTE LINUX

- UM SERVIÇO DE REDE É INSTALADO NO SISTEMA OPERACIONAL LINUX DEBIAN ATRAVÉS DA APLICAÇÃO APT COMO MOSTRADO NO EXEMPLO ABAIXO:

- # apt-get install apache2

- DURANTE O PROCESSO DE INSTALAÇÃO DIVERSOS ARQUIVOS (BINÁRIOS, BIBLIOTECAS E ARQUIVOS DE CONFIGURAÇÃO) SÃO COPIADOS PARA O SISTEMA DE ARQUIVOS
- APÓS A INSTALAÇÃO É NECESSÁRIO CONFIGURAR O SERVIÇO PARA ATENDER AS NECESSIDADES DO AMBIENTE, POIS CADA AMBIENTE É DIFERENTE
- A CONFIGURAÇÃO É REALIZADA ATRAVÉS DOS ARQUIVOS DE CONFIGURAÇÃO QUE NORMALMENTE ESTÃO NO FORMATO TEXTO E LOCALIZADOS NA PASTA “/etc”



■ SERVIÇOS DE REDE

□ SERVIÇOS DE REDE NO AMBIENTE LINUX

- APÓS A CONFIGURAÇÃO, O SERVIÇO PODERÁ SER INICIALIZADO, ISTO É, COLOCADO EM EXECUÇÃO
- DURANTE A INICIALIZAÇÃO DO SERVIÇO, O ARQUIVO DE CONFIGURAÇÃO É CARREGADO E É INICIADO O FORNECIMENTO DO SERVIÇO DESEJADO
- OS SERVIÇOS SÃO GERENCIADOS ATRAVÉS DE SCRIPTS QUE ESTÃO LOCALIZADOS NA PASTA “/etc/init.d/xxxxx”
- O NOME DO ARQUIVO DE SCRIPT NORMALMENTE É O MESMO QUE O NOME DO SERVIÇO
- O NOME DO ARQUIVO DE SCRIPT NORMALMENTE É O MESMO QUE O NOME DO SERVIÇO COMO POR EXEMPLO /etc/init.d/apache2”
- PARA INICIAR UM SERVIÇO: `service apache2 start`
- PARA ENCERRAR UM SERVIÇO: `service apache2 stop`
- PARA REINICIAR UM SERVIÇO: `service apache2 restart`



REDES PEER2PEER COM



■ CRIAÇÃO DE USUÁRIOS

- PARA CRIAR UM USUÁRIO ACESSAR O PAINEL DE CONTROLE → CONTAS DE USUÁRIO
- OU Iniciar → Executar → compmgmt.msc



■ CRIAÇÃO DE USUÁRIOS

- SELECIONAR A OPÇÃO “CRIAR UMA NOVA CONTA”



■ CRIAÇÃO DE USUÁRIOS

- INFORME O NOME DA CONTA E A SEGUIR O BOTÃO “Avançar”

Dê um nome para a nova conta

Digite um nome para a nova conta:

Este nome será mostrado na [tela de boas-vindas](#) e no [menu 'Iniciar'](#).

Avançar >

Cancelar



■ CRIAÇÃO DE USUÁRIOS

- SELECIONE O TIPO DE CONTA A SER CRIADO. O TIPO ADMINISTRADOR DEVE SER CRIADO APENAS PARA ADMINISTRAÇÃO DA MÁQUINA, DEVE SER EVITADO POIS COLOCA EM RISCO A INTEGRIDADE DA MÁQUINA
- E POR FIM CLICAR SOBRE O BOTÃO “Criar Conta”

Escolha um tipo de conta

☒ Administrador do computador ☐ Limitado

Com uma conta de administrador do computador, você pode:

- Criar, alterar e excluir contas
- Fazer alterações que abranjam todo o sistema
- Instalar programas e acessar todos os arquivos

< Voltar

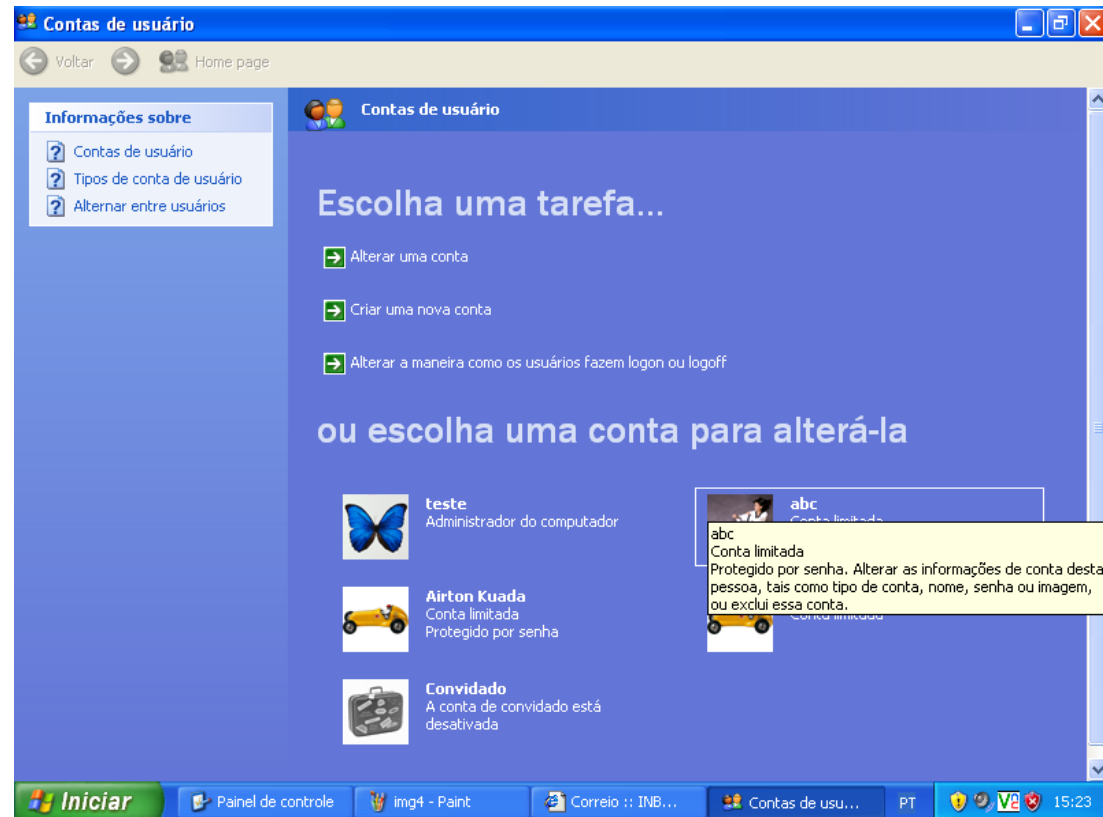
Criar conta

Cancelar



■ CRIAÇÃO DE USUÁRIOS

- PARA ALTERAR OU EXCLUIR UMA CONTA, CLIQUE SOBRE UMA DAS CONTAS QUE SÃO MOSTRADAS



■ CRIAÇÃO DE USUÁRIOS

- SELECIONE A OPERAÇÃO QUE SERÁ EFETUADA

O que você deseja alterar na conta de jose?

→ Alterar o nome

→ Criar uma senha

→ Alterar a imagem

→ Alterar o tipo de conta

→ Excluir a conta



■ CRIAÇÃO DE USUÁRIOS

- EM CASO DE EXCLUSÃO SERÁ NECESSÁRIO CONFIRMAR A EXCLUSÃO DOS ARQUIVOS DO USUÁRIO

Deseja manter os arquivos de jose?

Antes de você excluir a conta de jose, o Windows pode salvar automaticamente o conteúdo da área de trabalho e da pasta 'Meus documentos' de jose para uma nova pasta chamada "jose" na sua área de trabalho. No entanto, o Windows não pode salvar as mensagens de email, os favoritos da Internet e outras configurações de jose.

Manter arquivos

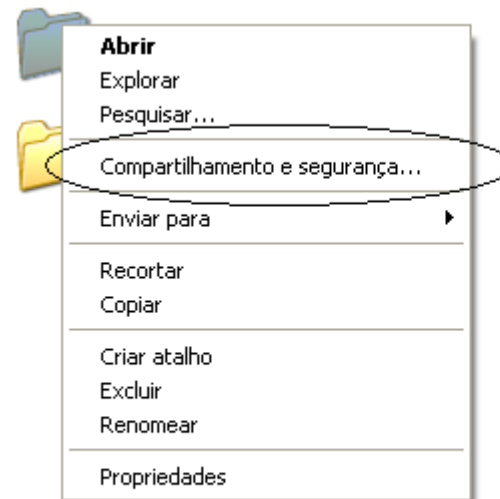
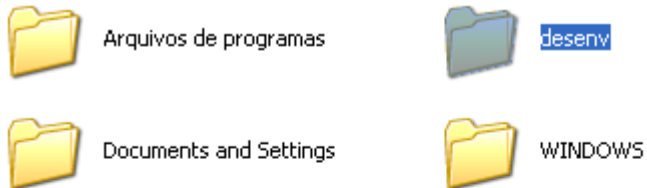
Excluir arquivos

Cancelar

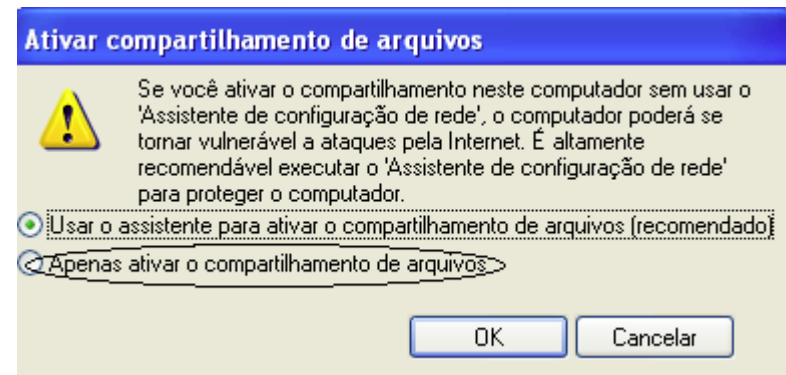
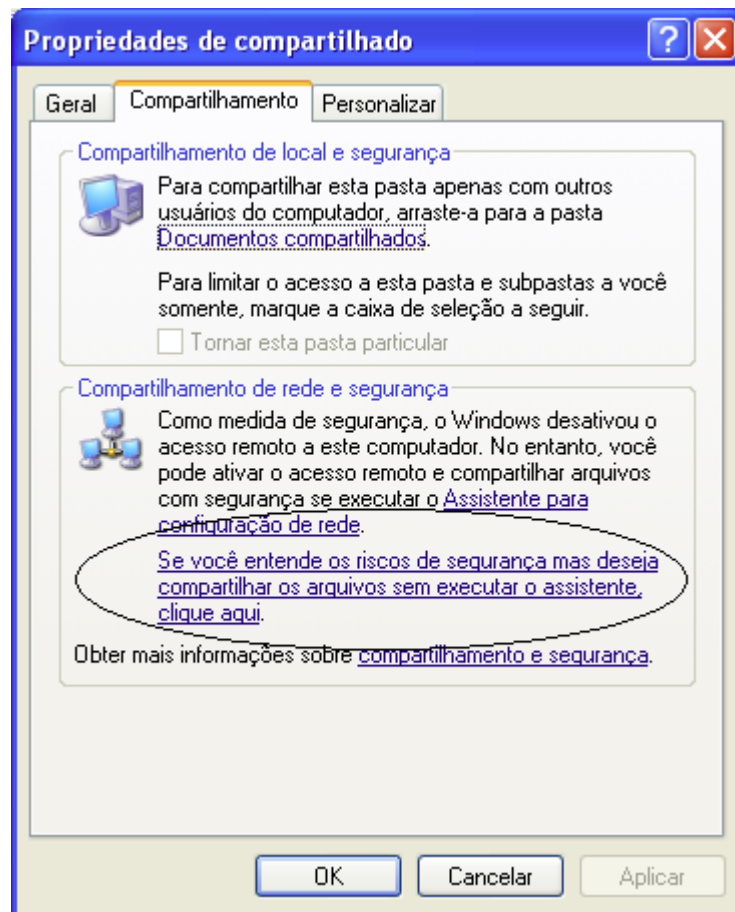


■ COMPARTILHAMENTO DE PASTAS

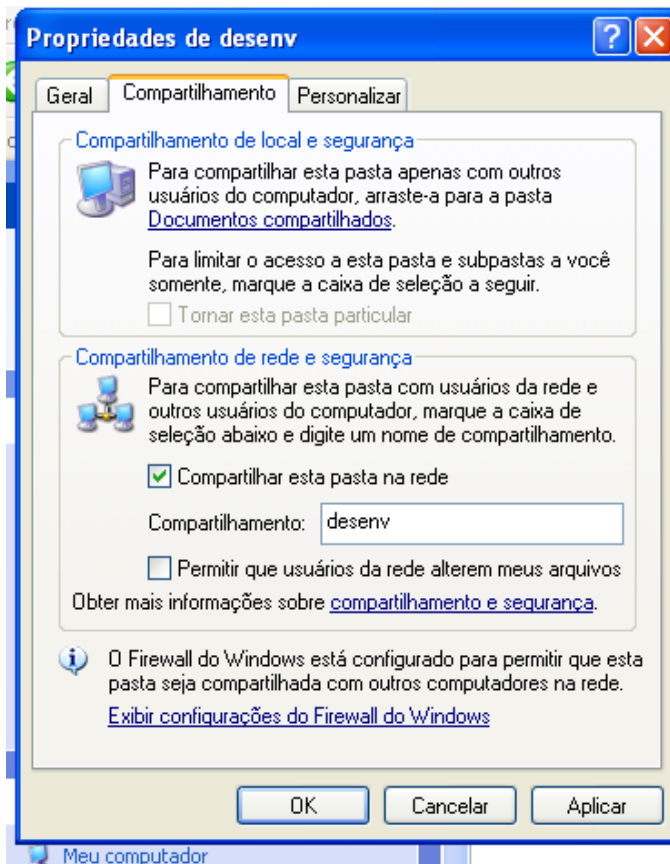
- SOBRE A PASTA QUE SERÁ COMPARTILHADA, CLICAR COM O BOTÃO DIREITO E SELECIONAR A OPÇÃO “Compartilhamento e Segurança”



- **COMPARTILHAMENTO DE PASTAS**
 - SE O COMPARTILHAMENTO NÃO ESTIVER ATIVADO É NECESSÁRIO ESCOLHER AS OPÇÕES ASSINALADAS ABAIXO

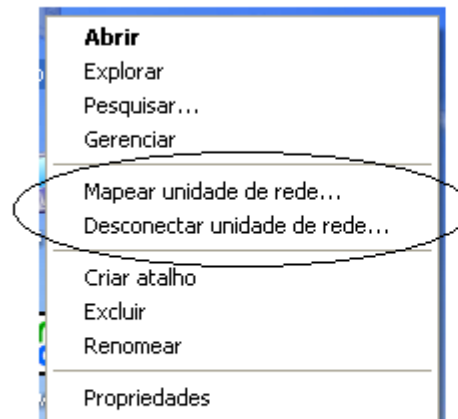


- **COMPARTILHAMENTO DE PASTAS**
 - INFORMAR O NOME DO COMPARTILHAMENTO E CLICAR SOBRE O BOTÃO “Aplicar” E DEPOIS “Ok”



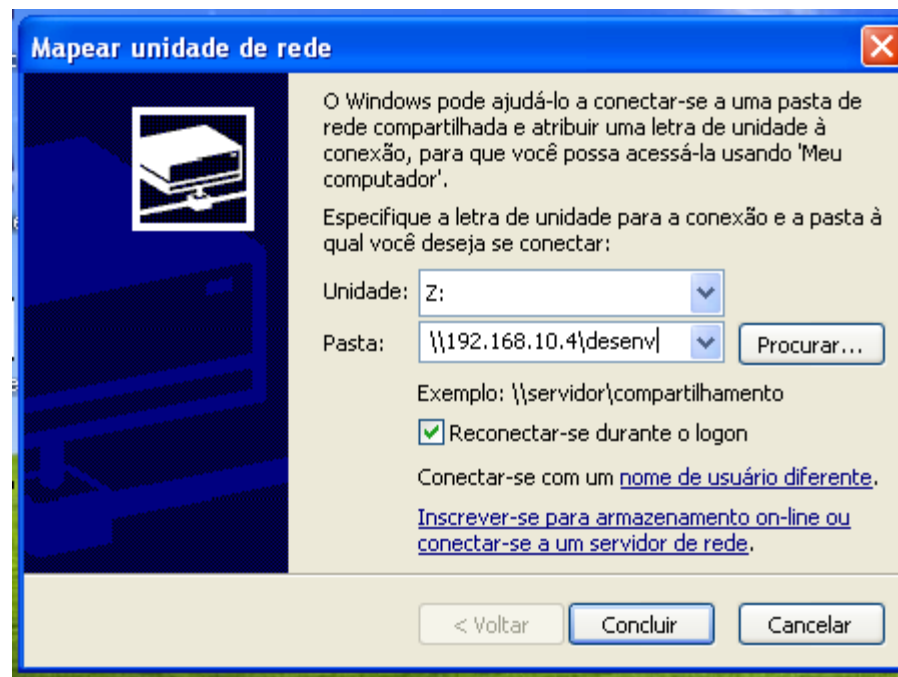
■ MAPEAMENTO DE UNIDADE DE REDE

- UMA VEZ QUE O COMPARTILHAMENTO FOI REALIZADO, OUTRAS ESTAÇÕES PODEM ACESSAR A PASTA COMPARTILHADA
- CLICAR SOBRE O ÍCONE “Meu Computador” NO DESKTOP COM O BOTÃO DIREITO DO MOUSE
- SELECIONAR A OPÇÃO “Mapear Unidade de Rede”



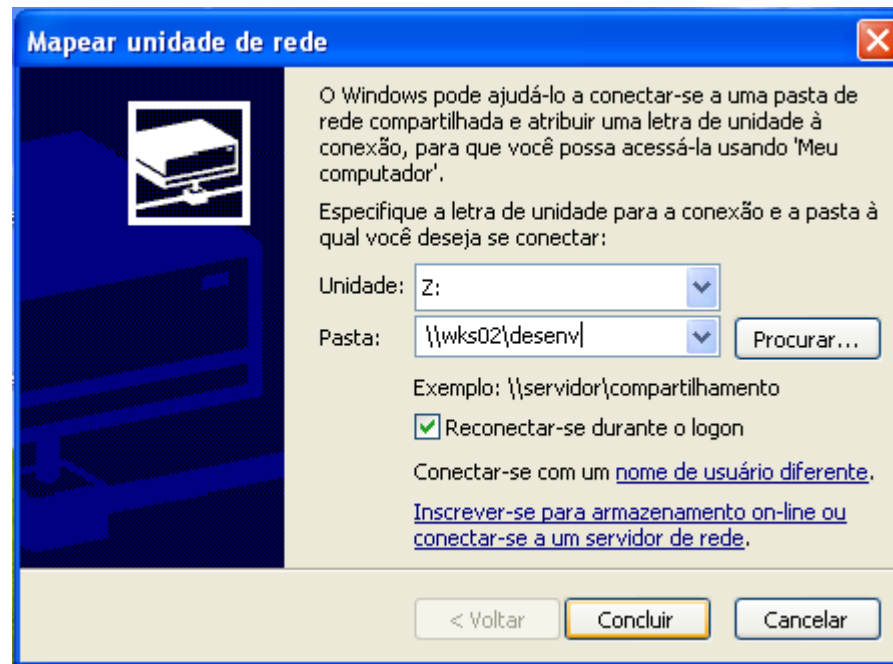
■ MAPEAMENTO DE UNIDADE DE REDE

- NA TELA SEGUINTE SELECIONE A IDENTIFICAÇÃO DA UNIDADE QUE SERÁ MAPEADA E INFORME O ENDEREÇO IP OU NOME DA MÁQUINA, SEGUIDO DO NOME DO COMPARTILHAMENTO



■ MAPEAMENTO DE UNIDADE DE REDE

- NA TELA SEGUINTE SELECIONE A IDENTIFICAÇÃO DA UNIDADE QUE SERÁ MAPEADA E INFORME O ENDEREÇO IP OU NOME DA MÁQUINA, SEGUIDO DO NOME DO COMPARTILHAMENTO



- **MAPEAMENTO DE UNIDADE DE REDE**
 - SE O MAPEAMENTO FOR REALIZADO COM SUCESSO, SERÁ MOSTRADO CONFORME FIGURA ABAIXO NO CONTEXTO “Unidades de rede”

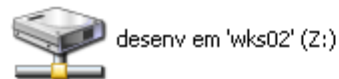
Unidades de disco rígido



Dispositivos com armazenamento removível



Unidades de rede



- **MAPEAMENTO DE UNIDADE DE REDE**
 - PARA INTERROMPER O MAPEAMENTO, CLIQUE COM O BOTÃO DIREITO SOBRE MAPEAMENTO REALIZADO E SELECIONE A OPÇÃO “Desconectar-se”



SAMBA



■ DESCRIÇÃO GERAL

- UTILIZADO PARA REALIZAR O COMPARTILHAMENTO DE ARQUIVOS
- UTILIZA O PROTOCOLO CIFS (COMMON INTERNET FILE SYSTEM)
- CIFS É A NOVA VERSÃO DO PROTOCOLO SMB (SERVER MESSAGE BLOCK)
- O PROTOCOLO SMB É UTILIZADO PELAS REDES MICROSOFT PARA REALIZAR O COMPARTILHAMENTO DE ARQUIVOS E IMPRESSORAS
- O PROTOCOLO SMB UTILIZA O PROTOCOLO NETBIOS PARA A TROCA DE MENSAGENS ENTRE HOSTS



■ DESCRIÇÃO GERAL

- O PROTOCOLO NETBIOS FOI DESENVOLVIDO PELA IBM EM 1984 E UTILIZA TRÊS PORTAS 137/138 (UDP) E 139 (TCP)
- O PROTOCOLO CIFS UTILIZA A PORTA 445 (TCP)
- SAMBA É IMPLEMENTADO EM DIVERSAS PLATAFORMAS
 - LINUX
 - BSD
 - SOLARIS
 - OUTROS
- CIFS É UTILIZADO PELA MICROSOFT A PARTIR DO WINDOWS 2000



■ INSTALAÇÃO, GERENCIAMENTO E DOCUMENTAÇÃO

- A INSTALAÇÃO DO SAMBA É FEITO A PARTIR DO COMANDO ABAIXO

apt-get install samba

- O SAMBA POSSUI APENAS UM ARQUIVO DE CONFIGURAÇÃO /etc/samba/smb.conf
- A ATIVAÇÃO/DESATIVAÇÃO DO SERVIÇO É FEITO ATRAVÉS DO COMANDO ABAIXO

service samba [start/stop/restart]

- A DOCUMENTAÇÃO SOBRE SAMBA PODE SER ENCONTRADO EM www.samba.org



CRIAÇÃO DE USUÁRIOS NO SAMBA



■ CRIAÇÃO DE USUÁRIOS

- PARA CRIAR USUÁRIOS NO SAMBA, O USUÁRIO OBRIGATORIAMENTE DEVE ESTAR CADASTRADO NO SISTEMA LINUX, OU SEJA, EXISTIR NO ARQUIVO `/etc/passwd`
 - `useradd -m -s /bin/bash usuario`
- PARA CADASTRAR UM USUÁRIO SEM UMA PASTA HOME UTILIZAR O COMANDO ABAIXO
 - `useradd -M usuario`
- UMA VEZ CADASTRADO O USUÁRIO NO LINUX, UTILIZAR O COMANDO `smbpasswd` PARA REALIZAR AS OPERAÇÕES BÁSICAS MOSTRADOS A SEGUIR
- OS USUÁRIOS SAMBA SÃO ARMAZENADOS NO ARQUIVO `“/var/lib/samba/passdb.tdb`



- **CRIAÇÃO DE USUÁRIOS**
 - CADASTRO DE CONTA
 - `smbpasswd -a usuario`
 - ALTERAÇÃO DE SENHA
 - `smbpasswd usuario`
 - EXCLUSÃO
 - `smbpasswd -x usuario`
 - DESABILITAR
 - `smbpasswd -d usuario`
 - HABILITAR
 - `smbpasswd -e usuario`



■ CRIAÇÃO DE USUÁRIOS

- PARA VERIFICAR OS USUÁRIOS QUE ESTÃO CADASTRADOS NO SAMBA, É NECESSÁRIO UTILIZAR O COMANDO “pdbedit “

- `pdbedit -Lw` → Lista todos os usuários
- `pdbedit -lv user` → Lista as propriedades de um usuário
- `pdbedit --pwd-must-change-time="2010-01-01" --time-format="%Y-%m-%d" nome_do_usuario`
- `pdbedit --pwd-must-change-time=0 nome_do_usuario`



CONFIGURAÇÕES GERAIS DO SAMBA



■ SWAT

- A CONFIGURAÇÃO DO SAMBA PODE SER REALIZADO ATRÁVES DE UMA INTERFACE WEB
- PACOTE QUE IMPLEMENTA ESTA FUNCIONALIDADE É INSTALADO ATRAVÉS DO COMANDO ABAIXO:

```
# apt-get install swat
```

- O SERVIÇO É INICIADO ATRAVÉS DO SUPER-SERVER “**inetd**”
- É NECESSÁRIO ADICIONAR OU DESCOMENTAR LINHA ABAIXO NO ARQUIVO “/etc/inetd.conf”

```
swat stream tcp nowait.400 root /usr/sbin/tcpd /usr/sbin/swat
```

- REINICIAR O SERVIÇO “**inetd**”

```
# killall inetd
```

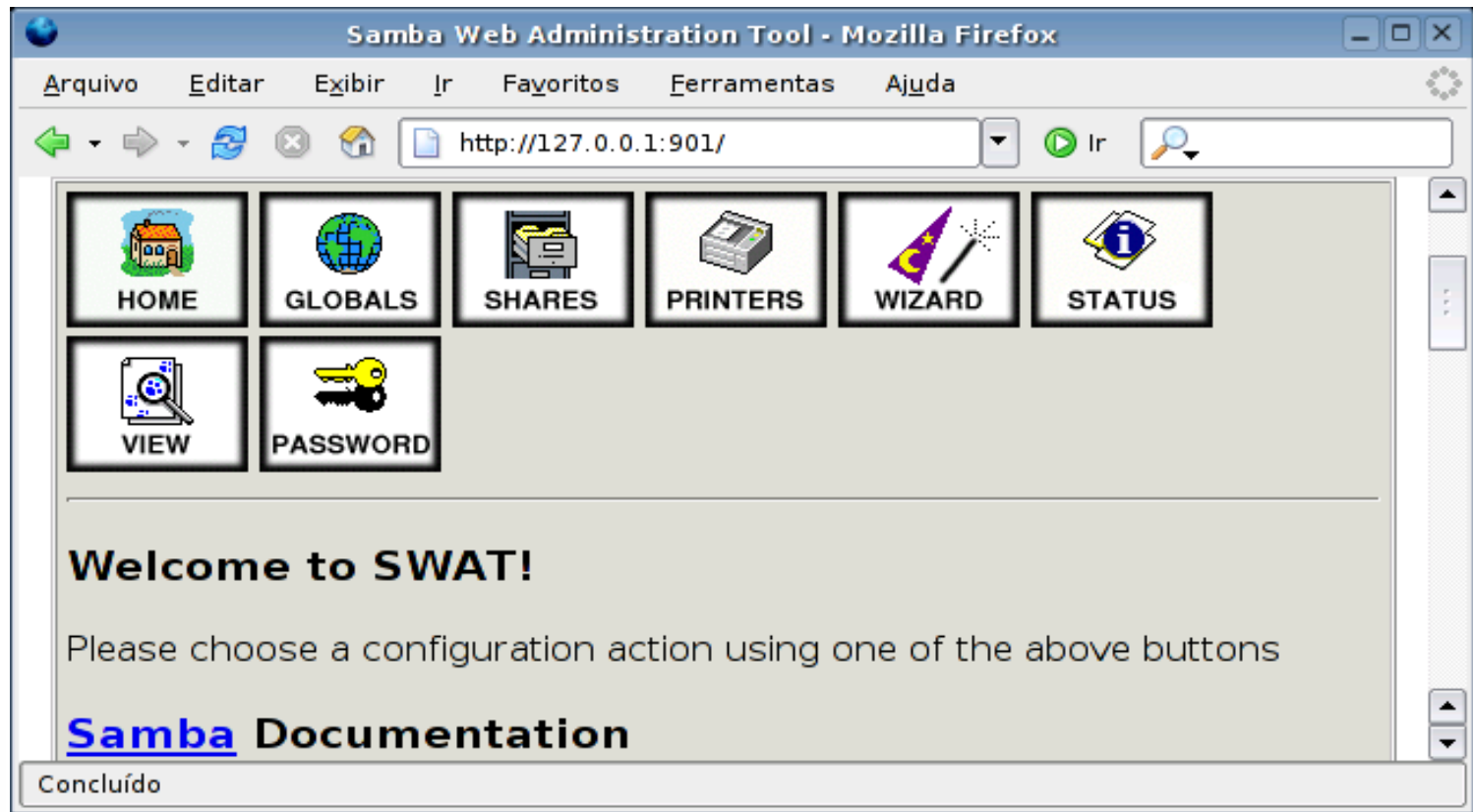
```
# inetd
```



■ SWAT

■ ACESSADO ATRAVÉS DO ENDEREÇO:

□ `http://endereço_IP:901 – root/teste123`



■ CONFIGURAÇÃO BÁSICA

■ CRIAÇÃO DE USUÁRIOS

□ PODEMOS CRIAR USUÁRIOS NO SAMBA, UTILIZAÇÃO A SEÇÃO “PASSWORD”. OS USUÁRIOS JÁ DEVEM ESTAR CRIADOS NO SISTEMA LINUX ATRAVÉS DO COMANDO ABAIXO:

□ `useradd user1 -m -s /bin/bash`



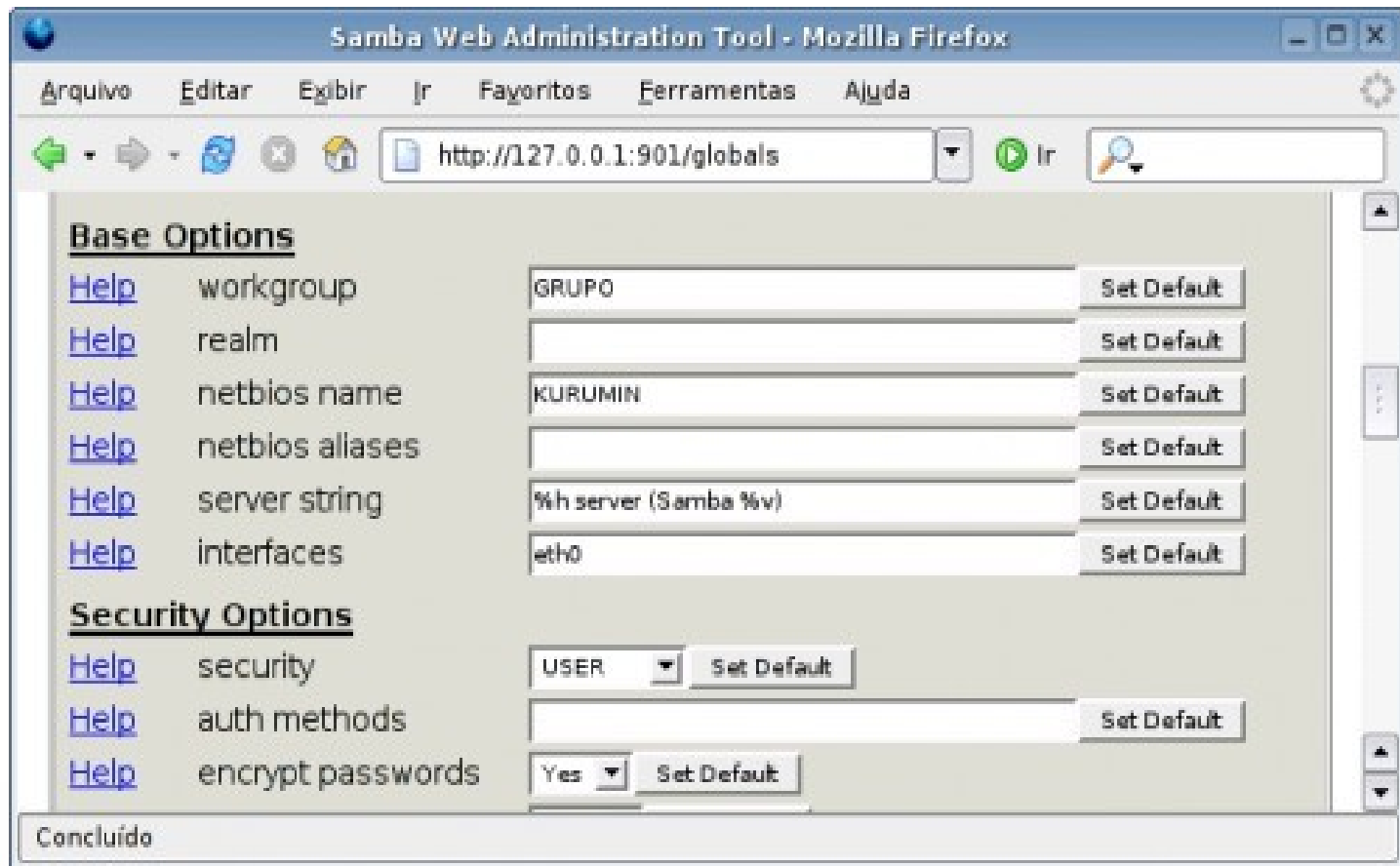
■ CONFIGURAÇÃO BÁSICA

- PARA INICIAR A CONFIGURAÇÃO, CLICK SOBRE A OPÇÃO “GLOBALS”
- O PARAMETRO “workgroup” INDICA O GRUPO DE TRABALHO AO QUAL O SERVIDOR PERTENCE
 - PODEM EXISTIR DIVERSOS GRUPOS DE TRABALHO DENTRO DE UMA MESMA REDE. COMO POR EXEMPLO: SUPORTE, VENDA, FINANCEIRO, ETC.
- NA SEÇÃO GLOBAL, O PARAMETRO “netbios name” INDICA O NOME DO SERVIDOR, ATRAVÉS DO QUAL SERÁ IDENTIFICADO EM UMA REDE WINDOWS
 - O NOME PODE TER ATÉ 15 CARACTERES E SER COMPOSTO POR LETRAS E NÚMEROS, ALÉM DE ESPAÇOS E DOS CARACTERES: ! @ # \$ % ^ & () - ' { } ~



■ CONFIGURAÇÃO BÁSICA

■ TELA DE CONFIGURAÇÃO GRUPO E NOME DE SERVIDOR



Samba Web Administration Tool - Mozilla Firefox

Arquivo Editar Exibir Ir Favoritos Ferramentas Ajuda

http://127.0.0.1:901/globals Ir

Base Options

Help	workgroup	GRUPO	Set Default
Help	realm		Set Default
Help	netbios name	KURUMIN	Set Default
Help	netbios aliases		Set Default
Help	server string	%h server (Samba %v)	Set Default
Help	interfaces	eth0	Set Default

Security Options

Help	security	USER	Set Default
Help	auth methods		Set Default
Help	encrypt passwords	Yes	Set Default

Concluído



■ CONFIGURAÇÃO BÁSICA

- NA SEÇÃO GLOBAL, O PARAMETRO “security” INDICA O MODO DE PROTEÇÃO A SER UTILIZADO
- AS PERMISSÕES DE ACESSO AOS COMPARTILHAMENTO DO SAMBA FICAM CONDICIONADAS ÀS PERMISSÕES DE ACESSO DO LINUX. POR EXEMPLO, SE VOCÊ COMPARTILHAR A PASTA /home/joaquim/arquivos, POR DEFAULT, APENAS O USUÁRIO “joaquim” TERÁ A PERMISSÃO DE MANIPULAR OS ARQUIVOS E PASTAS
- PARA QUE OUTROS USUÁRIOS TENHAM ACESSO A PASTA, VOCÊ DEVE DAR PERMISSÃO A ELES, CRIANDO UM NOVO GRUPO E DANDO PERMISSÃO DE ESCRITA PARA OS INTEGRANTES DO MESMO. OUTRA OPÇÃO É COLOCAR OS USUÁRIOS NO GRUPO “joaquim”



■ CONFIGURAÇÃO BÁSICA

- NA SEÇÃO GLOBAL, O PARAMETRO “Encrypt Password” DEVE FICAR SEMPRE “yes”
- MASTER BROWSER
 - EM UMA REDE WINDOWS, UMA DAS MÁQUINAS FICA RESPONSÁVEL EM MONTAR E ATUALIZAR UMA LISTA DE COMPARTILHAMENTO DISPONÍVEIS E ENVIÁ-LAS AOS DEMAIS
 - QUALQUER MÁQUINA WINDOWS PODE ATUAR COMO UM MASTER BROWSER E O CARGO PODE MUDAR DE DONO CONFORME AS MÁQUINAS VÃO SENDO DESLIGADAS
 - O CARGO DE MASTER BROWSER É DISPUTADO ATRAVÉS DE UM PROCESSO DE ELEIÇÃO



■ CONFIGURAÇÃO BÁSICA

■ ELEIÇÃO DO MASTER BROWSER

- TODOS OS COMPUTADORES ENVIAM PACOTES DE BROADCAST CONTENDO AS SEGUINTE INFORMações:
 - SISTEMA OPERACIONAL UTILIZADO
 - TEMPO DE UPTIME
 - OUTRAS INFORMações
- CADA MÁQUINA COMPARA SUAS CREDENCIAIS COM AS DO PACOTE RECEBIDO. SE SUAS CREDENCIAIS FOREM INFERIORES ELE DESISTE DA ELEIÇÃO, CASO CONTRÁRIO RESPONDE ENVIANDO O PACOTE COM SUAS CREDENCIAIS



■ CONFIGURAÇÃO BÁSICA

■ ELEIÇÃO DO MASTER BROWSER

- ESTE PROCESSO DE ELIMINAÇÃO CONTINUA ATÉ QUE SOBRE APENAS UMA MÁQUINA QUE PASSA A SER O MASTER BROWSER DA REDE, ATÉ QUE SEJA DESCONECTADA DA REDE OU PERCA A ELEIÇÃO PARA OUTRA MÁQUINA COM CREDENCIAIS SUPERIORES
- O PRINCIPAL CREDENCIAL É O “OS Level”
- PRINCIPAIS “OS Level” DA MICROSOFT
 - WINDOWS NT SERVER, 2000 SERVER, 2003 SERVER, 2008 SERVER POSSUEM “OS Level” 32
 - WINDOWS NT WORKSTATION, 2000 PROFESSIONAL, QUALQUER VERSÃO DOMÉSTICA DE XP, OU VISTA POSSUEM “OS Level” 16. VERSÕES ANTIGAS (3.11, 95, etc) POSSUEM “OS Level” 1



■ CONFIGURAÇÃO BÁSICA

■ AJUSTE DO “OS Level” NO LINUX

- NA SEÇÃO “Browse Options” O VALOR É AJUSTADO ATRAVÉS DA OPÇÃO “OS Level”
- COLOCANDO SEMPRE UM VALOR (0-255) ELEVADO (100) O LINUX SEMPRE GANHARÁ A ELEIÇÃO.
- O VALOR DEFAULT É 20 QUE FAZ COM QUE GANHE DE QUALQUER MÁQUINA WINDOWS, MENOS DAS VERSÕES SERVER



■ CONFIGURAÇÃO BÁSICA

■ AJUSTE DO “OS Level” NO LINUX

□ PARA COMPLETAR AJUSTAR AS OPÇÕES “Local Master” E “Preferred Master” COM “Yes”

□ Local Master – SERVIDOR SAMBA CONVOCA ELEIÇÃO SEMPRE QUE NECESSÁRIO

□ Preferred Master – POSSUI VANTAGEM QUANDO CONFRONTADO COM OUTRA MÁQUINA COM MESMO “OS Level”

□ NOTA IMPORTANTE

□ NUNCA COLOCAR DOIS SERVIDORES SAMBA COM O MESMO “OS Level” NA MESMA REDE, POIS INICIARÃO UMA DISPUTA INTERMINÁVEL PELO CARGO, O QUE FÁRA COM QUE A NAVEGAÇÃO FIQUE LENTA



■ CONFIGURAÇÃO BÁSICA

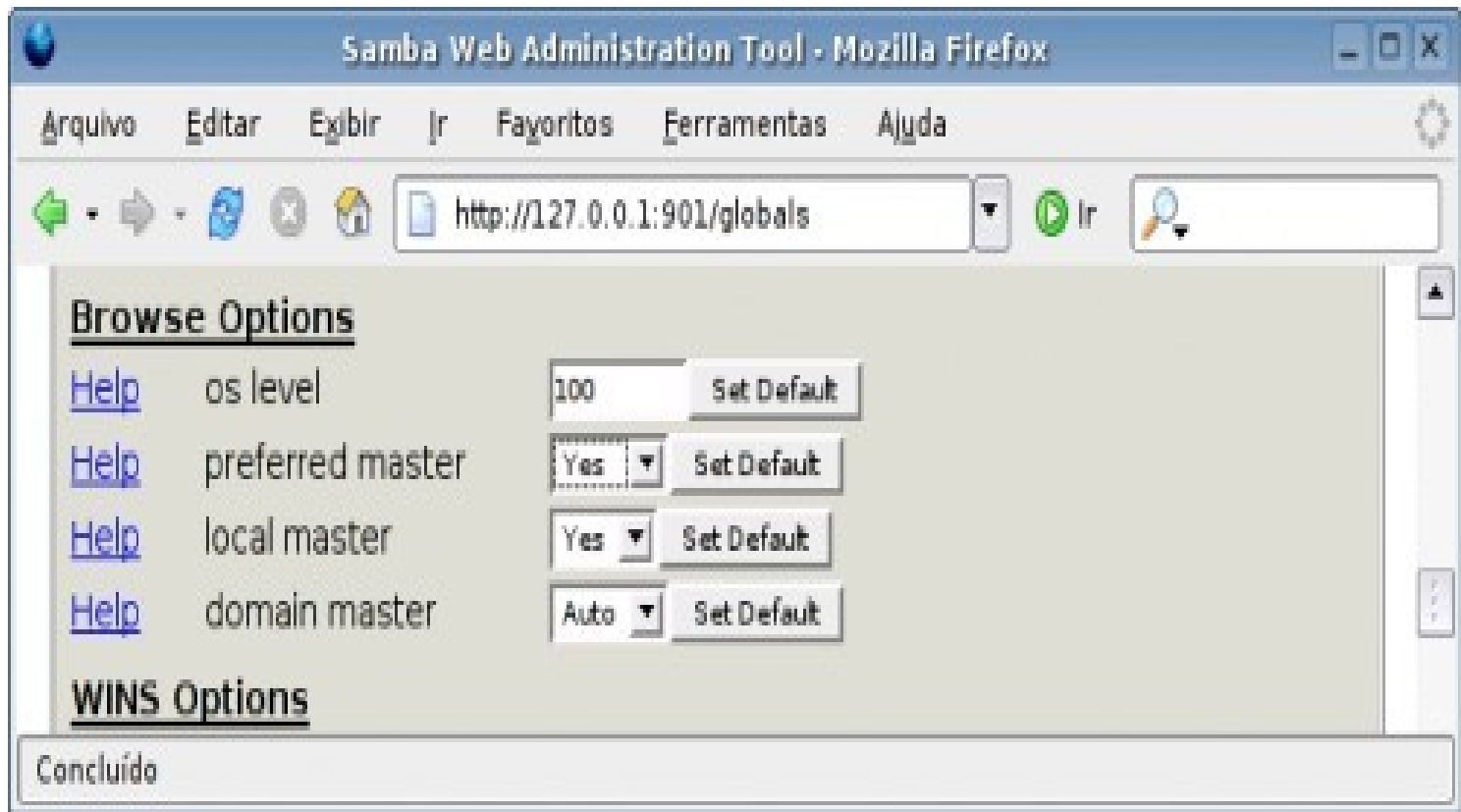
■ AJUSTE DO “OS Level” NO LINUX

□ NOTA IMPORTANTE

- SE HOUVER DIVERSOS SERVIDORES SAMBA NA MESMA REDE, DEVE SER UTILIZADO UMA HIERARQUIA UTILIZANDO DIFERENTES VALORES DE “OS Level”
- SE NÃO QUISE QUE O SERVIDOR SAMBA PARTICIPE DAS ELEIÇÕES, BASTA DEFINIR A OPÇÃO “Local Master” COM O VALOR “No”
- APÓS O TÉRMINO DO AJUSTE É NECESSÁRIO GRAVAR AS CONFIGURAÇÕES REALIZADAS, PRESSIONANDO O BOTÃO “Commit Changes” E DEPOIS REINICIANDO O SERVIÇO ATRAVÉS DO BOTÃO “STATUS” E “Restart All”



- CONFIGURAÇÃO BÁSICA
 - AJUSTE DO “OS Level” NO LINUX



■ CONFIGURAÇÃO BÁSICA

■ RESOLUÇÃO DE NOMES DE REDES WINDOWS

- A REDE MICROSOFT UTILIZA O CONCEITO DE NOMES DE HOST PARA IDENTIFICAR UM HOST NA REDE
- QUANDO UMA ESTAÇÃO ESTÁ ENTRANDO NA REDE, ELA DEVE VERIFICAR SE NÃO EXISTE UM NOME IGUAL. NO CASO DE EXISTIR UM NOME IGUAL, É FEITO UMA COMUNICAÇÃO A ESTAÇÃO QUE TERÁ DE ESCOLHER OUTRO, PARA REALIZAR ESTA DESCOBERTA, É ENVIADO UM PACOTE DE BROADCAST
- UMA VEZ QUE O NOME NÃO EXISTE NA REDE WINDOWS, ESTE NOME DEVE SER REGISTRADO EM UM SERVIDOR DE NOMES WINDOWS, DINAMICAMENTE



■ CONFIGURAÇÃO BÁSICA

■ RESOLUÇÃO DE NOMES DE REDES WINDOWS

- EM UMA REDE TCP/IP, ESTE NOME DEVE SER MAPEADO PARA UM ENDEREÇO IP
- O SERVIÇO QUE REALIZA ESTE MAPEAMENTO É O WINDOWS INTERNET NAME SERVICE (WINS)
- A UTILIZAÇÃO DESTES SERVIÇO FORNECE REDUÇÃO DE TRÁFEGO BROADCAST, POIS SE UMA ESTAÇÃO NÃO POSSUI UM SERVIDOR WINS CONFIGURADO, ENTÃO IRÁ UTILIZAR UM PACOTE BROADCAST PARA RESOLVER O NOME
- TODAS AS ESTAÇÕES DEVE TER CONFIGURADO PELO MENOS UM SERVIDOR DE WINS PARA EVITAR O TRÁFEGO BROADCAST



■ CONFIGURAÇÃO BÁSICA

■ CONFIGURANDO SUPORTE AO SERVIÇO WINS

- NA SEÇÃO WINS DEIXAR A OPÇÃO “wins support” ATIVADA (Yes). ESTA CONFIGURAÇÃO FARÁ COM QUE O SAMBA ATUE COMO UM SERVIDOR WINS PARA OS DEMAIS COMPUTADORES DA REDE
- A OPÇÃO “wins server” DEVE SER DEIXADA EM BRANCO, A NÃO SER QUE EXISTA UM OUTRO SERVIDOR WINS AO QUAL O SERVIDOR LINUX ESTEJA SUBORDINADO
- DEVE SER CONFIGURADO EM TODAS AS ESTAÇÕES WINDOWS O ENDEREÇO DO SERVIDOR WINS DA REDE



■ CONFIGURAÇÃO BÁSICA

■ FINALIZANDO A CONFIGURAÇÃO

- PARA EFETIVAR AS ALTERAÇÕES, PRESSIONE O BOTÃO “Commit Changes” NO TOPO DA TELA PARA QUE AS ALTERAÇÕES SEJAM SALVAS NO ARQUIVO “/etc/samba/smb.conf”
- PARA FAZER COM QUE AS ALTERAÇÕES TENHAM EFEITO, É NECESSÁRIO QUE O SERVIÇO SAMBA SEJA INICIADO. PARA ISSO , ENTRE NA SEÇÃO “STATUS” LOCALIZADO NO TOPO DA TELA E NA SEQUENCIA SELECIONE O BOTÃO “Restart All”



CRIANDO COMPARTILHAMENTOS NO SAMBA (GRUPO DE TRABALHO)



■ CRIANDO COMPARTILHAMENTOS

- APÓS CRIAR OS USUÁRIOS E CONFIGURAR A SEÇÃO “GLOBALS”, FALTA APENAS CONFIGURAR AS PASTAS QUE SERÃO COMPARTILHADAS COM AS ESTAÇÕES ATRAVÉS DA SEÇÃO “SHARE”
- DIRETÓRIO HOME
 - CADA USUÁRIO QUE É CADASTRADO NO SISTEMA LINUX, POSSUI UMA PASTA QUE FICA NO DIRETÓRIO “/home” E SÃO UTILIZADAS PARA GUARDAR ARQUIVOS PESSOAIS. NENHUM OUTRO USUÁRIO TERÁ ACESSO A ESTA PASTA, A NÃO SER QUE SEJA DADA PERMISSÃO
 - A PASTA HOME É AUTOMATICAMENTE ACESSÍVEL ATRAVÉS DO SAMBA QUANDO O USUÁRIO REALIZAR A AUTENTICAÇÃO ATRAVÉS DE UM CLIENTE SAMBA



■ CRIANDO COMPARTILHAMENTOS

■ DIRETÓRIO HOME

- POR PADRÃO O COMPARTILHAMENTO “HOME” ESTÁ HABILITADO SOMENTE PARA O MODO DE LEITURA, SENDO ASSIM, É NECESSÁRIO ALTERAR A FORMA DO COMPARTILHAMENTO
- PARA ALTERAR O COMPARTILHAMENTO PARA GRAVAÇÃO, NA INTERFACE DE COMPARTILHAMENTO (SHARE) DEVEMOS ALTERAR A OPÇÃO “read only” PARA “no”
- REINICIAR O SAMBA



■ CRIANDO COMPARTILHAMENTOS

■ CRIANDO UM COMPARTILHAMENTO

- PARA CRIAR UM COMPARTILHAMENTO, ACESSAMOS SEÇÃO “SHARE”
- PARA CRIAR O COMPARTILHAMENTO, BASTA ESCREVER O NOME DO COMPARTILHAMENTO NO CAMPO EM FRENTE AO BOTÃO “Create Share” E DEPOIS CLICAR SOBRE O BOTÃO “Create Share”



■ CRIANDO COMPARTILHAMENTOS

Samba Web Administration Tool - Mozilla Firefox

Arquivo Editar Exibir Ir Favoritos Ferramentas Ajuda

Base Options

Help	comment	Compartilhamento com arquivos de uso geral	Set Default
Help	path	/mnt/hda2/arquivos	Set Default

Security Options

Help	valid users	maria, joao, kurumin	Set Default
Help	admin users		Set Default
Help	read list		Set Default
Help	write list		Set Default
Help	read only	No ▾	Set Default
Help	guest ok	No ▾	Set Default
Help	hosts allow	192.168.0., 192.168.1., 10.0.0.	Set Default
Help	hosts deny	192.168.0.33, 192.168.1.33	Set Default

Filename Handling

Help	preserve case	No ▾	Set Default
Help	short preserve case	No ▾	Set Default

Browse Options

Help	browseable	Yes ▾	Set Default
----------------------	------------	-------	-----------------------------

Miscellaneous Options

Help	available	Yes ▾	Set Default
----------------------	-----------	-------	-----------------------------



■ CRIANDO COMPARTILHAMENTOS

■ PRINCIPAIS CAMPOS

☐ COMMENT

☐ DESCRIÇÃO GERAL DO COMPARTILHAMENTO

☐ PATH

☐ É O MAIS IMPORTANTE

☐ INDICA QUAL A PASTA SERÁ COMPARTILHADA

☐ READ ONLY

☐ DETERMINA SE A PASTA SERÁ DISPONÍVEL
SOMENTE PARA LEITURA (YES)

☐ USUÁRIOS TAMBÉM PODERÃO GRAVAR ARQUIVOS
(NO)



■ CRIANDO COMPARTILHAMENTOS

■ PRINCIPAIS CAMPOS

☐ BROWSEABLE

☐ PERMITE CONFIGURAR SE O COMPARTILHAMENTO APARECERÁ ENTRE OS OUTROS COMPARTILHAMENTOS DO SERVIDOR NO AMBIENTE DE REDES (YES)

☐ COMPARTILHAMENTO OCULTO QUE PODE SER ACESSADO SOMENTE SE SOUBER O NOME DO COMPARTILHAMENTO (NO)

☐ AVAILABLE

☐ ESPECIFICA SE O COMPARTILHAMENTO ESTÁ ATIVO (YES)

☐ TEMPORARIAMENTE DESATIVADO (NO)



■ CRIANDO COMPARTILHAMENTOS

■ NO LINUX

☐ # mkdir /vol3/temporario -p

■ NO SAMBA

☐ CRIAR O COMPARTILHAMENTO temp

☐ INFORMAR OS CAMPOS:

☐ COMMENT → Pasta para arquivos temporarios

☐ PATH → /vol3/temporario

☐ READ ONLY → Yes

☐ BROWSEABLE → Yes

☐ AVAILABLE → Yes

☐ SELECIONAR O BOTÃO “Commit Changes”

☐ RESTART DO SAMBA VIA STATUS



CONFIGURAÇÃO MANUAL DO SAMBA



■ ALTERAÇÃO MANUAL

■ ALTERAÇÃO MANUAL DO ARQUIVO DE CONFIGURAÇÃO

- O ARQUIVO DE CONFIGURAÇÃO (/etc/samba/smb.conf) PODE SER ALTERADO MANUALMENTE ATRAVÉS DE UM EDITOR DE TEXTO, PARA VERIFICAR SE A CONFIGURAÇÃO ESTÁ CORRETA, É NECESSÁRIO UTILIZAR O PROGRAMA “testparm”

```
# testparm
```

```
Load smb config files from /etc/samba/smb.conf
```

```
Processing section "[arquivos]"
```

```
Loaded services file OK.
```

```
Server role: ROLE_STANDALONE
```

- O "ROLE_STANDALONE" SIGNIFICA QUE O SERVIDOR FOI CONFIGURADO COM MEMBRO NORMAL DE GRUPO DE TRABALHO



■ ALTERAÇÃO MANUAL

- O SAMBA NÃO DIFERENCIA MAÍUSCULA DE MINÚSCULAS, MAS MUITAS VEZES OS PARAMETROS SÃO REPASSADOS PARA O SISTEMA OPERACIONAL POR EXEMPLO:
 - PATH=/mnt/Arquivos e PATH=/mnt/arquivos
- CARACTERES UTILIZADOS QUE INDICAM COMENTÁRIOS SÃO “#” E “;”
- NÃO INSERIR COMENTÁRIOS EM LINHAS VÁLIDAS, MESMO QUE NO FINAL DA LINHA, POIS AO FAZER ISTO, TODA A LINHA SERÁ IGNORADA PELO SAMBA
- ALTERAÇÕES NO ARQUIVO DE CONFIGURAÇÃO DO LIDOS A CADA 3 MINUTOS E APLICADAS AUTOMATICAMENTE



■ ALTERAÇÃO MANUAL

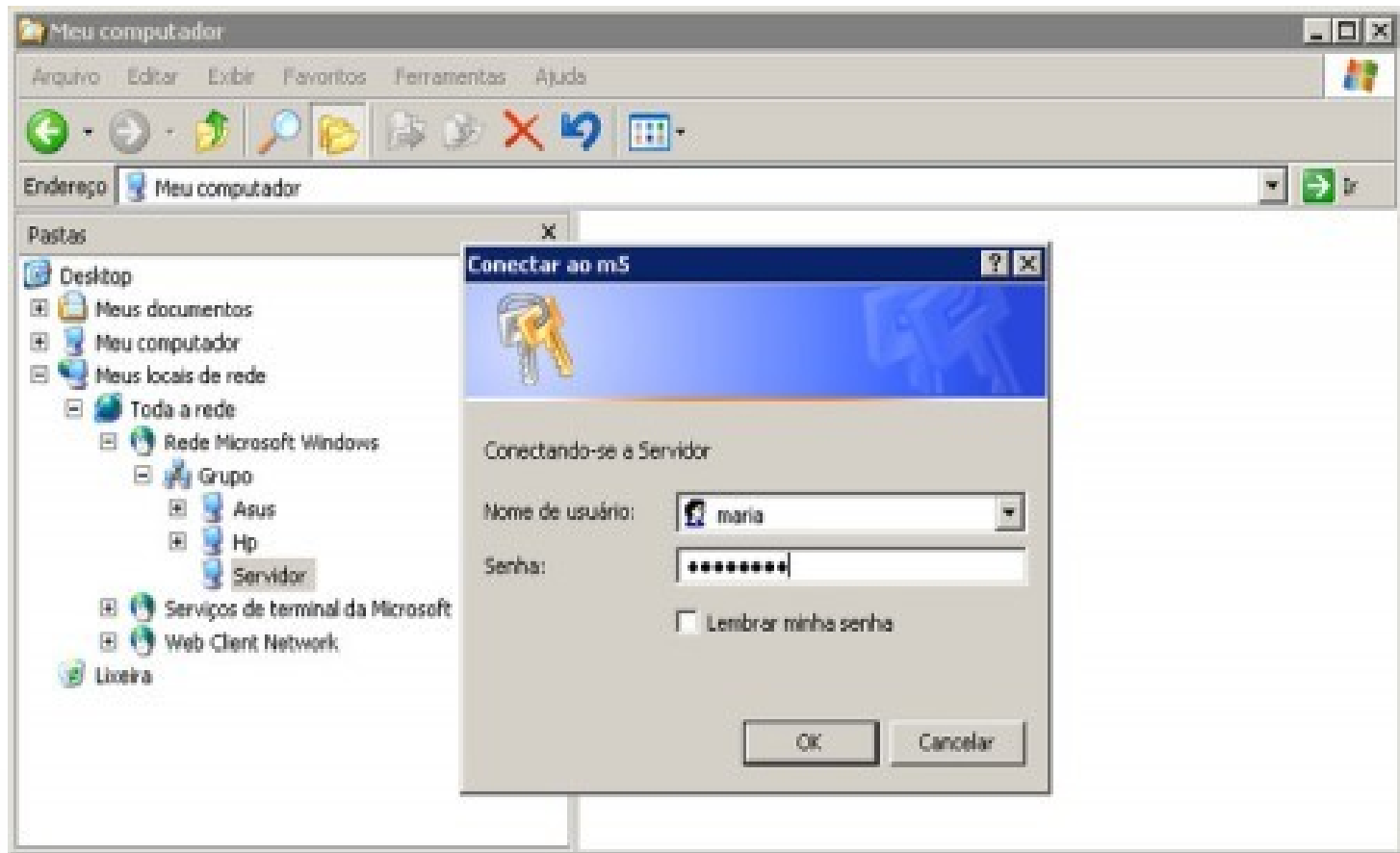
- PARA FAZER COM QUE AS ALTERAÇÕES ENTREM EM VIGOR IMEDIATAMENTE, REINICIAR O SERVIÇO DO SAMBA COM MOSTRADO ABAIXO

service samba restart

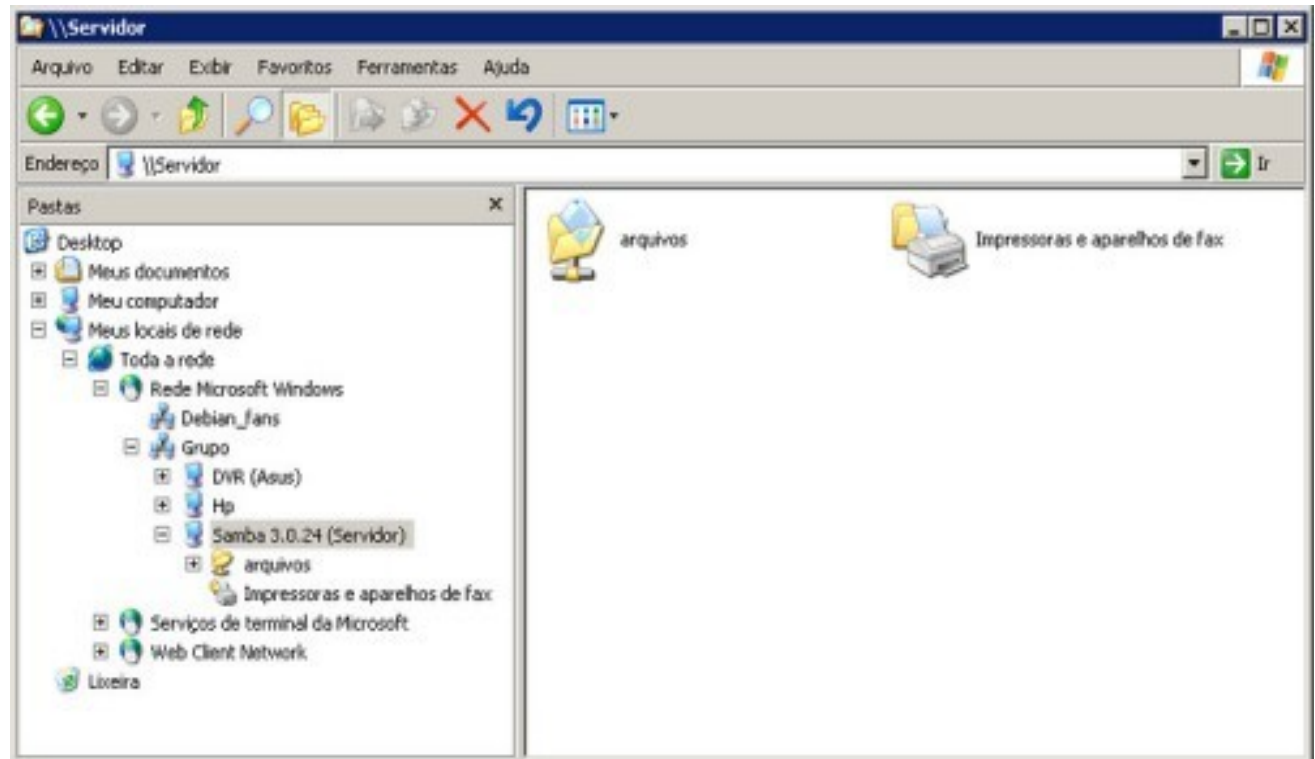
- A PARTIR DAÍ, O COMPARTILHAMENTO ESTARÁ DISPONÍVEL
- PARA ACESSAR OS COMPARTILHAMENTOS ACESSAR ATRAVÉS DO “Meus Locais de Rede” NO CLIENTE WINDOWS, VOCÊ RECEBERÁ UM PROMPT DE SENHA, ONDE VOCÊ PRECISA FORNECER UM DOS LOGIN CADASTRADO NO SERVIDOR UTILIZANDO O COMANDOS “smbpasswd -a”



■ ACESSO AO COMPARTILHAMENTO NO WINDOWS



- **ACESSO AO COMPARTILHAMENTO NO WINDOWS**
 - DEPOIS QUE O USUÁRIO FOI AUTENTICADO, O CLIENTE PODE VISUALIZAR OS COMPARTILHAMENTOS DO SERVIDOR



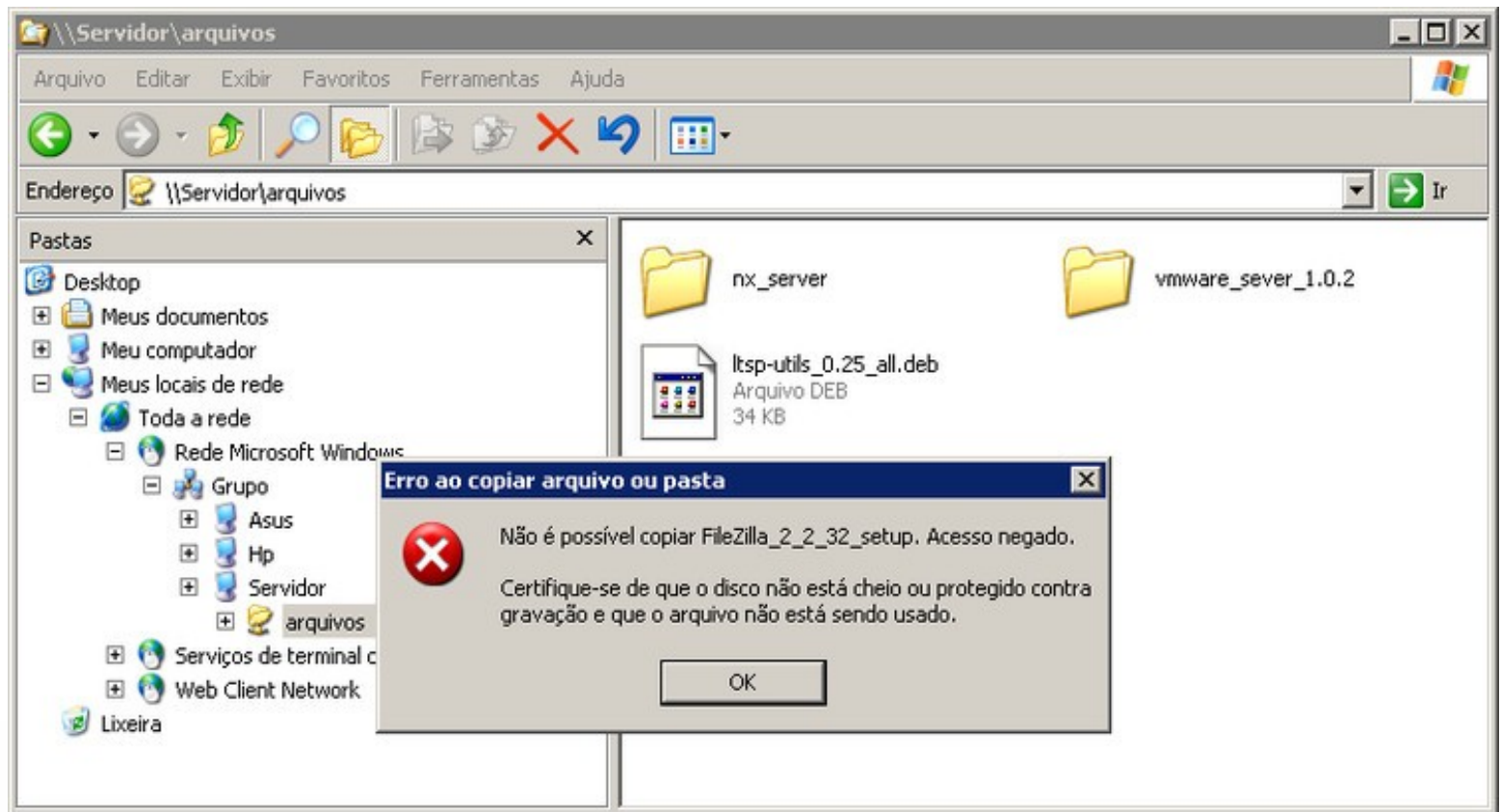
CONTROLE DE ACESSO NO SAMBA



- **CONTROLE DE ACESSO AO COMPARTILHAMENTO**
 - COM AS CONFIGURAÇÕES REALIZADAS ANTERIORMENTE, JÁ É POSSÍVEL VISUALIZAR OS ARQUIVOS DA PASTA, MAS AINDA NÃO É POSSÍVEL GRAVAR NOS ARQUIVOS OU CRIAR OUTRAS ARQUIVOS OU PASTAS
 - AO TENTAR SALVAR ARQUIVOS OU CRIAR PASTAS, IRÁ RECEBER UMA MENSAGEM DE ACESSO NEGADO



- **CONTROLE DE ACESSO AO COMPARTILHAMENTO**
 - MENSAGEM DE CONTROLE DE ACESSO: ACESSO NEGADO



- **CONTROLE DE ACESSO AO COMPARTILHAMENTO**
 - PARA QUE O COMPARTILHAMENTO FIQUE DISPONÍVEL PARA COM PERMISSÃO DE LEITURA E ESCRITA, É NECESSÁRIO ADICIONAR A OPÇÃO “read only=no” DENTRO DO ARQUIVO DE CONFIGURAÇÃO DO COMPARTILHAMENTO
 - MESMO COM AS ALTERAÇÕES ACIMA, AINDA É POSSÍVEL QUE RECEBAMOS MENSAGENS DE ACESSO NEGADO, PORÉM, AGORA, É O SISTEMA DE PROTEÇÃO DO LINUX QUE ESTÁ IMPEDINDO O ACESSO AO SISTEMA DE ARQUIVO



- **CONTROLE DE ACESSO AO COMPARTILHAMENTO**
 - O MODO MAIS FÁCIL PARA CONTORNAR ESTE PROBLEMA É ABRIR TODAS AS PERMISSÕES DE ACESSO, UTILIZANDO O COMANDO
 - `chmod 777 /vol3/temporario`
 - O GRANDE PROBLEMA É QUE AS PERMISSÕES FICARIAM ABERTAS PARA QUE QUALQUER UM TENHA ACESSO AO SERVIDOR PARA LER O CONTEÚDO DOS ARQUIVOS DENTRO DA PASTA, O QUE NÃO É NADA BOM DO PONTO DE VISTA DA SEGURANÇA



- **CONTROLE DE ACESSO AO COMPARTILHAMENTO**
 - PARA REALIZAR O COMPARTILHAMENTO DE ARQUIVOS ENTRE UM GRUPO DE USUÁRIOS, O IDEAL É QUE TODOS USUÁRIO PERTENÇAM A UM GRUPO DE TRABALHO. SOMENTE ESTE GRUPO TERÁ ACESSO A PASTA OU ARQUIVOS
 - O PRIMEIRO PASSO É CRIAR UM GRUPO PARA OS USUÁRIOS QUE PODERÃO FAZER ALTERAÇÕES NA PASTA OU NOS ARQUIVOS
 - A CRIAÇÃO DE UM GRUPO É REALIZADO ATRAVÉS DO COMANDO
 - # groupadd grupo
 - OS GRUPO ESTÃO ARMAZENADOS NO ARQUIVO /etc/group



■ CONTROLE DE ACESSO AO COMPARTILHAMENTO

■ CRIANDO OS GRUPOS E USUÁRIOS DO GRUPO

□ # groupadd desenvolvimento

□ # useradd -m -s /bin/bash -g desenvolvimento user11

□ # useradd -m -s /bin/bash -g desenvolvimento user12

□ # useradd -m -s /bin/bash -g desenvolvimento user13

■ O GRUPO desenvolvimento É O GRUPO PRIMÁRIO DOS USUÁRIOS user11, user12 E user13

■ TROCAR O DONO E O GRUPO DA PASTA

□ # chgrp desenvolvimento /vol2/temporario

■ AJUSTAR PERMISSÕES DE ACESSO DA PASTA

□ # chmod 775 /vol2/temporario



- **CONTROLE DE ACESSO AO COMPARTILHAMENTO**
 - ADICIONANDO UM USUÁRIO A OUTROS GRUPOS SECUNDÁRIOS
 - `usermod -G grupo usuário`
 - ALTERAR PARAMETROS DO COMPARTILHAMENTO “temp” PARA PERMITIR QUE OS TODOS USUÁRIOS DO GRUPO desenvolvimento TENHAM ACESSO SOBRE OS ARQUIVOS
 - `create mask = 770`
 - `directory mask = 770`



- **CONTROLE DE ACESSO AO COMPARTILHAMENTO**
 - CONTROLE DE ACESSO POR GRUPO E USUÁRIOS
 - SE QUISERMOS QUE O COMPARTILHAMENTO FIQUE DISPONÍVEL APENAS PARA OS USUÁRIOS QUE PERTENÇAM AO GRUPO, ADICIONAMOS A OPÇÃO:
 - valid users = +desenvolvimento
 - AINDA PODEMOS ESPECIFICAR UMA LISTA DE USUÁRIOS ISOLADOS, SEPARADOS POR VÍRGULA OU POR ESPAÇOS
 - valid users = mario, carlos, maria, batista
 - AINDA PODEMOS COMBINAR AS DUAS OPÇÕES ACIMA
 - valid users = +desenvolvimento, mario, carlos, maria, batista



- **CONTROLE DE ACESSO AO COMPARTILHAMENTO**
 - CONTROLE DE ACESSO POR GRUPO E USUÁRIOS
 - SE QUISERMOS QUE O COMPARTILHAMENTO FIQUE DISPONÍVEL PARA TODOS E BLOQUEAR O ACESSO AOS USUÁRIOS: manoel e joaquin
 - invalid users = manoel, joaquin
 - AINDA PODEMOS ESPECIFICAR UMA EXCESSÃO DENTRO DE UM GRUPO SEM REMOVÊ-LOS DO GRUPO
 - valid users = +desenvolvimento
 - invalid users = carlos, maria, batista



- **CONTROLE DE ACESSO AO COMPARTILHAMENTO**
 - CONTROLE DE ACESSO POR GRUPO E USUÁRIOS
 - OUTRA FORMA DE CONTROLAR O ACESSO A PASTA É CRIAR UMA LISTA COM PERMISSÃO DE ESCRITA NA PASTA
 - read only = no ← **Remover esta linha**
 - writable=no
 - write list=carlos
 - CASO UM USUÁRIO NÃO PERTENÇA AO GRUPO MAS MESMO ASSIM NECESSITA ACESSAR A PASTA COMPARTILHADA
 - valid users = +desenvolvimento, antonio



■ CONTROLE DE ACESSO AO COMPARTILHAMENTO

■ CONTROLE DE ACESSO POR GRUPO E USUÁRIOS

- PODEMOS PERMITIR QUE TODOS OS MEMBROS DO GRUPO TENHA ACESSO TOTAL AO COMPARTILHAMENTO, PORÉM OS USUÁRIOS manael e joaquim TEM SOMENTE ACESSO A LEITURA
 - writable=Yes
 - readlist list=manael, joaquim
- OUTRA FORMA DE CONTROLAR O ACESSO A PASTA É A OPÇÃO “read only” QUE ACEITA AS OPÇÕES “Yes/No”. POSSUI A FUNÇÃO INVERSA A OPÇÃO “writable”
- DIZER “read only=yes” É O MESMO QUE “writable=no”
- EM GERAL UTILIZAMOS “read only” OU “writable”



■ CONTROLE DE ACESSO AO COMPARTILHAMENTO

■ PODEMOS VERIFICAR O STATUS DO SERVIDOR

□ O STATUS DOS COMPARTILHAMENTOS PODE SER OBTIDO ATRAVÉS DO COMANDO “smbstatus”

□ Samba version 3.5.6

□ PID Username Group Machine

□ -----

□ 3463 user10 economia wks01 (::ffff:192.168.10.14)

□ Service pid machine Connected at

□ -----

□ temp 3463 wks01 Tue Jul 26 04:29:04 2011

□ IPC\$ 3463 wks01 Tue Jul 26 04:29:18 2011

□



LIXEIRA NO SAMBA



■ LIXEIRA NO SAMBA

- MUITAS VEZES O USUÁRIO PODE APAGAR ACIDENTALMENTE UM ARQUIVO IMPORTANTE.
- O SAMBA OFERECE A OPÇÃO DE UTILIZAR UMA LIXEIRA EM CADA PASTA COMPARTILHADA
- A OPÇÃO QUE OFERECE ESTE RECURSO É ([global]):
 - vfs object = recycle
 - recycle:repository = lixeira
 - recycle:keeptree = yes
- OUTRA OPÇÃO ÚTIL QUE MANTÉM DIVERSAS VERSÕES DE UM MESMO ARQUIVO É “recycle:versions = yes”
- OS ARQUIVOS REPETIDOS SÃO RENOMEADOS PARA "Copy #1 of abc.txt", "Copy #2 of abc.txt" E ASSIM CONTINUAMENTE



■ LIXEIRA NO SAMBA

- É IMPORTANTE LEMBRAR QUE DE VEZ EM QUANDO É NECESSÁRIO LIMPAR A PASTA UTILIZADO COMO LIXEIRA
- UMA OPÇÃO PARA FACILITAR O GERENCIAMENTO DE ESPAÇO É CONCENTRAR TODAS AS LIXEIRAS EM UMA ÚNICA PASTA, UTILIZANDO A OPÇÃO
 - `recycle:repository = /var/samba/lixreira/%U`
- O PARAMETRO %U INDICA UMA PASTA PARA CADA USUÁRIO, COM O OBJETIVO DE NÃO MISTURAR OS ARQUIVOS APAGADOS E TAMBÉM FACILITAR A BUSCA POR UM ARQUIVO
- A PASTA DEVERÁ SER CRIADO ATRAVÉS DOS COMANDOS ABAIXO: `mkdir -p /var/samba/lixreira/user10`
 - `chown -R user10:user10 /var/samba/lixreira/user10`



■ LIXEIRA NO SAMBA

- NEM TODOS OS ARQUIVOS NECESSITAM SER MANTIDOS COMO BACKUP NA LIXEIRA E PODEM SER REMOVIDOS DIRETAMENTE, COMO POR EXEMPLOS, ARQUIVOS TEMPORÁRIOS (tmp), ARQUIVOS DE MÚSICA (mp3), IMAGEM (iso), LOG (log), ETC
- AS EXTENSÕES DOS ARQUIVOS SÃO ESPECIFICADAS ATRAVÉS DA OPÇÃO “recycle:exclude” E NOMES DE PASTAS ATRAVÉS DA OPÇÃO “recycle:exclude_dir”
 - recycle:exclude = *.tmp, *.log, *.obj, ~*.*, *.bak, *.iso
 - recycle:exclude_dir = tmp, cache



DOMAIN CONTROLLER NO SAMBA



■ REDES WINDOWS – CONCEITOS BÁSICOS

■ DOMÍNIO

- UM DOMÍNIO É UM CONCEITO INTRODUZIDO NO WINDOWS NA QUAL UM USUÁRIO PODE TER ACESSO A UMA SÉRIE DE RECURSOS DE REDE COM O USO DE UM NOME DE USUÁRIO E UMA SENHA
- O USUÁRIO NECESSITA FAZER LOGIN NO DOMÍNIO PARA GANHAR ACESSO AOS RECURSOS QUE ESTÃO LIGADOS NA REDE
- OS RECURSOS DE REDES PODEM SER:
 - ARQUIVOS, IMPRESSORAS, APLICAÇÕES, ETC



■ REDES WINDOWS – CONCEITOS BÁSICOS

■ CONTROLADOR DE DOMÍNIO

- É UM SERVIDOR QUE RESPONDE A REQUISIÇÕES DE AUTENTICAÇÃO (LOGIN, VERIFICAÇÃO DE PERMISSÕES, AUTORIZAÇÃO DE ACESSO, ETC) DENTRO DO DOMÍNIO WINDOWS
- UM SERVIDOR É CONHECIDO COMO PRIMARY DOMAIN CONTROLLER (PDC) E ARMAZENA A BASE DE DADOS PARA O DOMÍNIO
- UM OU MAIS SERVIDORES SÃO DESIGNADOS COMO BACKUP DOMAIN CONTROLLER (BDC)
- PERIODICAMENTE O PDC ENVIA UMA CÓPIA DA BASE DE DADOS DO DOMÍNIO PARA OS BDC



■ REDES WINDOWS – CONCEITOS BÁSICOS

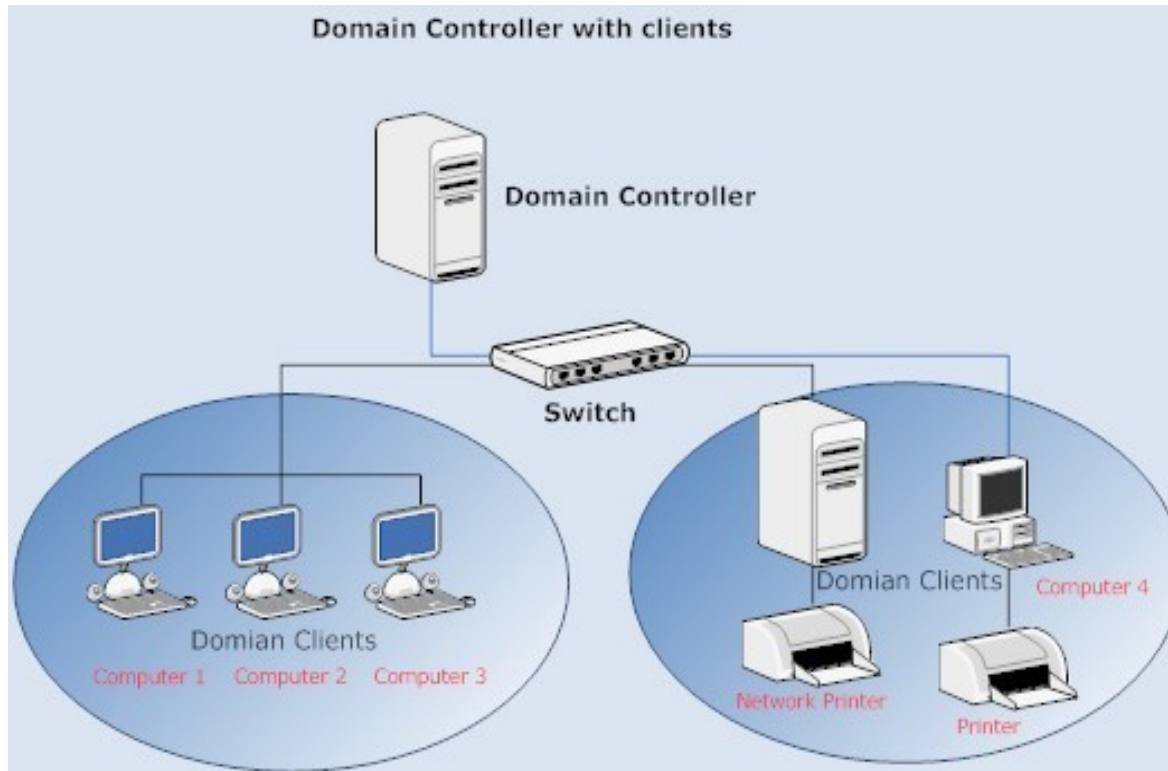
■ CONTROLADOR DE DOMÍNIO

- UM BDC PODE SER PROMOVIDO A CONTROLADOR DE DOMÍNIO PRIMÁRIO (PDC) SE O SERVIDOR PDC FALHAR E TAMBÉM PODE AJUDAR A EQUILIBRAR A CARGA DE TRABALHO DO PDC

□



■ REDES WINDOWS – CONCEITOS BÁSICOS



■ REDES WINDOWS – CONCEITOS BÁSICOS

■ CONTROLADOR DE DOMÍNIO

- UM BDC PODE SER PROMOVIDO A CONTROLADOR DE DOMÍNIO PRIMÁRIO (PDC) SE O SERVIDOR PDC FALHAR E TAMBÉM PODE AJUDAR A EQUILIBRAR A CARGA DE TRABALHO DO PDC

□



SAMBA COMO PDC



- **SAMBA PRIMARY DOMAIN CONTROLLER**
 - O SAMBA É UTILIZADO COMO UM SERVIDOR DE AUTENTICAÇÃO PARA CLIENTES WINDOWS E OPCIONALMENTE ARMAZENAR OS PERFIS DE USUÁRIOS, PERMITINDO QUE ELE TENHA ACESSO A SEUS ARQUIVOS E CONFIGURAÇÕES A PARTIR DE QUALQUER MÁQUINA QUE ELE FAÇA LOGIN
 - AO CADASTRAR UM USUÁRIO NO SERVIDOR SAMBA, ELE É CAPAZ DE FAZER LOGIN EM QUALQUER UMA DAS ESTAÇÕES CONFIGURADAS
 - AO REMOVER OU BLOQUEAR UM CONTA DE ACESSO, O USUÁRIO É AUTOMÁTICAMENTE BLOQUEADO EM QUALQUER ESTAÇÃO



■ SAMBA PRIMARY DOMAIN CONTROLLER

■ PASSOS PARA CONFIGURAR O SAMBA PDC

- NA SEÇÃO [global] ADICIONAR AS OPÇÕES
 - domain master = yes"
 - domain logons = yes
 - logon script = netlogon.bat
 - invalid users = root ← não pode haver esta linha
 - security = user ← já é default
 - encrypt passwords = yes ← já é default
 - passdb backend = tdbsam ← já é default



■ SAMBA PRIMARY DOMAIN CONTROLLER

■ PASSOS PARA CONFIGURAR O SAMBA PDC

□ CRIAR O COMPARTILHAMENTO “netlogon”

[netlogon]

comment = Servico de Logon

path = /var/samba/netlogon

read only = yes

browseable = no

□ CADASTRAR O USUÁRIO ROOT NO SAMBA

smbpasswd -a root

□ CRIAR A PASTA /var/samba/netlogon

mkdir -p /var/samba/netlogon

chmod 775 /var/samba/netlogon



■ SAMBA PRIMARY DOMAIN CONTROLLER

- CRIAR A PASTA profile.pds DENTRO DA PASTA HOME DE CADA USUÁRIO
 - # mkdir profile.pds /home/usuario/profile.pds
 - # chown usuario.usuario /home/usuario/profile.pds
 - # mkdir /etc/skel/profile.pds
- CADASTRAR CONTA BLOQUEADA PARA CADA MÁQUINA DA REDE
 - # groupadd maquinas
 - # useradd -g maquinas -d /dev/null -s /bin/false wks01\$
 - # passwd -l wks01\$
 - # smbpasswd -a -m wks01



■ SAMBA PRIMARY DOMAIN CONTROLLER

■ OBSERVAÇÕES

- NOTE O DOLAR (\$) NA FRENTE DO NOME DA MÁQUINA
- CONTA DE MÁQUINA
 - DEVE PERTENCER AO GRUPO `maquinas` (opcional)
 - NÃO TEM PASTA HOME (`-d /dev/null`)
 - NÃO TEM SHELL VÁLIDO (`-s /bin/false`)
 - ESTÁ TRAVADA (`passwd -l`)
 - A CONTA É VÁLIDA APENAS NO SAMBA ONDE É CADASTRADO COM A COM A OPÇÃO `-m` (`machine`)
 - SÃO CHAMADAS DE “TRUSTED ACCOUNTS”



■ SAMBA PRIMARY DOMAIN CONTROLLER

- CRIAR O ARQUIVO “/var/samba/netlogon/netlogon.bat” QUE É UM SCRIPT QUE É LIDO E EXECUTADO PELO CLIENTE WINDOWS AO FAZER LOGIN NO DOMÍNIO
- ESTE ARQUIVO DEVE SER CRIAR DENTRO DO AMBIENTE WINDOWS DEVIDO AOS FINAIS DE CONTROLE DE LINHA QUE SÃO ADICIONADOS AO ARQUIVO (cr/lf)
- ALTERAR A PERMISSÃO PARA 777
- EXEMPLO DE ARQUIVO netlogon.bat
 - net use h: /HOME ← mapeia a pasta home como h:
 - net use x: \\srv001\temp /yes ← mapeia o compart temp como x:



■ SAMBA PRIMARY DOMAIN CONTROLLER

■ ROAMING PROFILES – PERFIS MÓVEIS

- O ARQUIVOS E CONFIGURAÇÕES DE USUÁRIO SÃO ARMAZENADOS NO SERVIDOR, ISTO PERMITE QUE O USUÁRIO POSSA TRABALHAR EM QUALQUER MÁQUINA DA REDE, REDUZINDO A POSSIBILIDADE DE PERDA DE DADOS
- NO MOMENTO QUE O USUÁRIO FAZ LOGIN NO DOMÍNIO, O SERVIDOR ENVIA OS ARQUIVOS E AS CONFIGURAÇÕES PARA A ESTAÇÃO.
- ESTA MOBILIDADE AUMENTA O CONSUMO DE ESPAÇO NO SERVIDOR E O TRÁFEGO DE REDE



■ SAMBA PRIMARY DOMAIN CONTROLLER

■ ROAMING PROFILES – PERFIS MÓVEIS

□ O SERVIDOR ARMAZENA OS SEGUINTE ARQUIVOS DE USUÁRIO:

□ CONFIGURAÇÃO DE APLICATIVOS

□ ENTRADAS DO MENU INICIAR

□ COOKIES

□ BOOKMARKS

□ ARQUIVOS TEMPORÁRIOS

□ CONTEÚDOS DAS PASTAS:

□ DESKTOP

□ MODELOS

□ MEUS DOCUMENTOS



■ SAMBA PRIMARY DOMAIN CONTROLLER

■ ROAMING PROFILES – PERFIS MÓVEIS

- POR DEFAULT ESTES ARQUIVOS FICAM ARMAZENADOS DENTRO DA PASTA HOME DO USUÁRIO, NA PASTA “profile”
- PODEMOS ALTERAR ESTE DIRECIONAMENTO, ADICIONANDO AS SEGUINTE OPÇÕES LOGO ABAIXO DA OPÇÃO “logon script=netlogon.bat”
 - logon home = \\%L\%U
 - logon path = \\%L\profiles\%U
 - logon drive = m:
- ONDE
 - %L ← NOME NETBIOS DO SERVIDOR
 - %U ← NOME DE USUÁRIO QUE FAZ LOGIN



■ SAMBA PRIMARY DOMAIN CONTROLLER

■ ROAMING PROFILES – PERFIS MÓVEIS

□ CRIAR O COMPARTILHAMENTO “[profiles]”

[profiles]

path = /var/profiles

writable = yes

browseable = no

create mask = 0600

directory mask = 0700

□ CRIAR A PASTA /var/profiles

mkdir /var/profiles

chmod 1777 /var/profiles



■ SAMBA PRIMARY DOMAIN CONTROLLER

■ LOGANDO OS CLIENTES WINDOWS NO SAMBA

□ PARA LOGAR O CLIENTES WINDOWS EM UM DOMÍNIO, É NECESSÁRIO SEGUIR OS PASSOS ABAIXO:

□ UTILIZANDO O USUÁRIO ADMINISTRADOR DA MÁQUINA

□ Painel de Controle → Desempenho e Manutenção → Sistema → Nome do Computador

□ SELECIONAR O BOTÃO “Alterar”

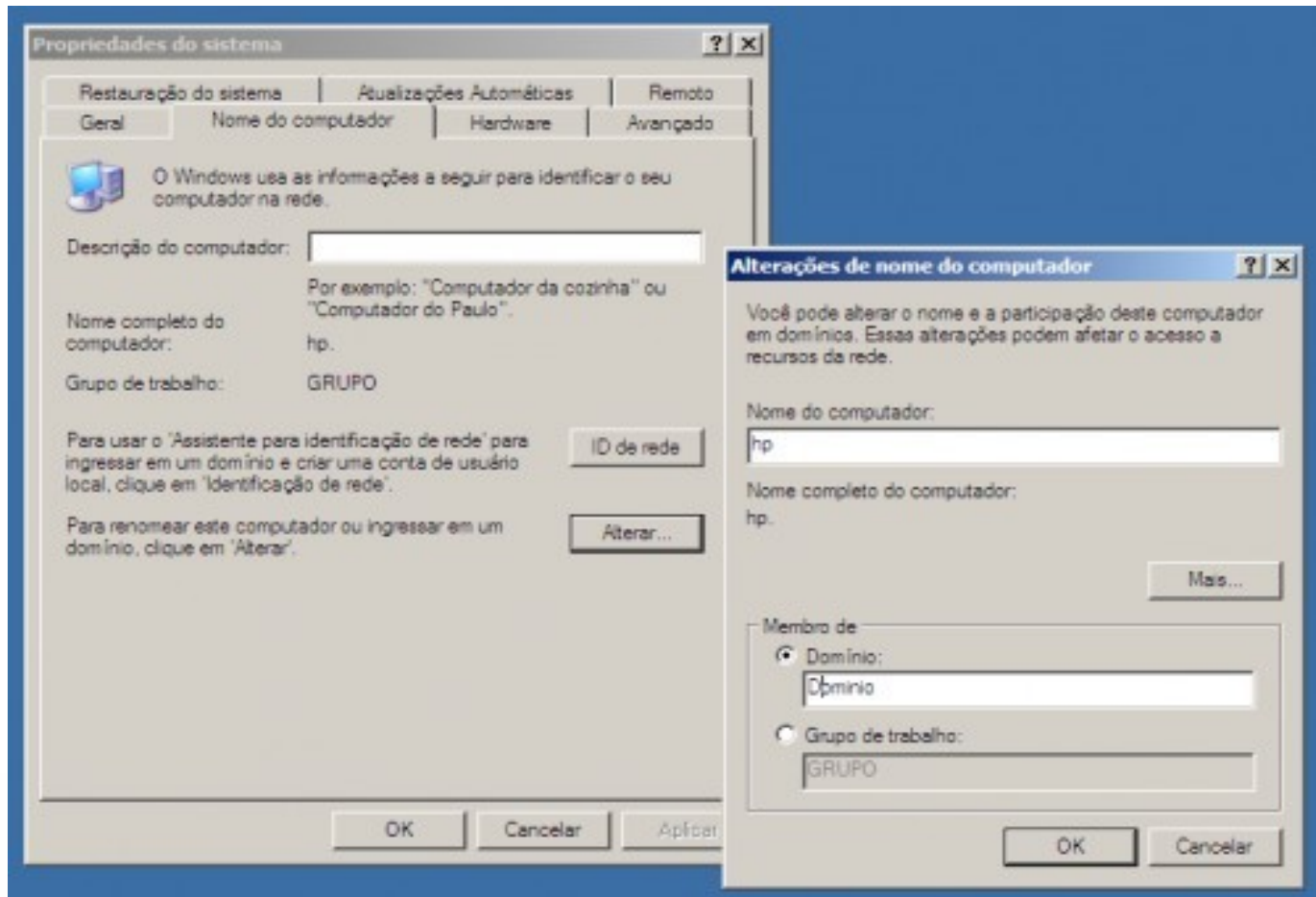
□ INFORMAR O NOME DO COMPUTADOR QUE ESTÁ CADASTRADO NO SAMBA

□ SELECIONE O BOTÃO “Dominio”

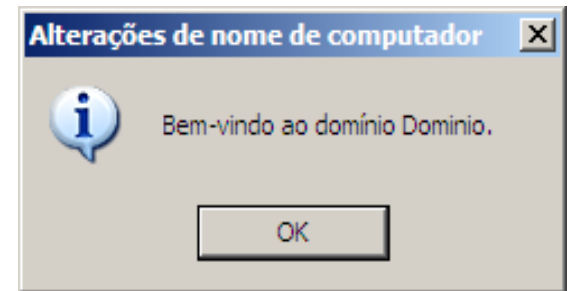
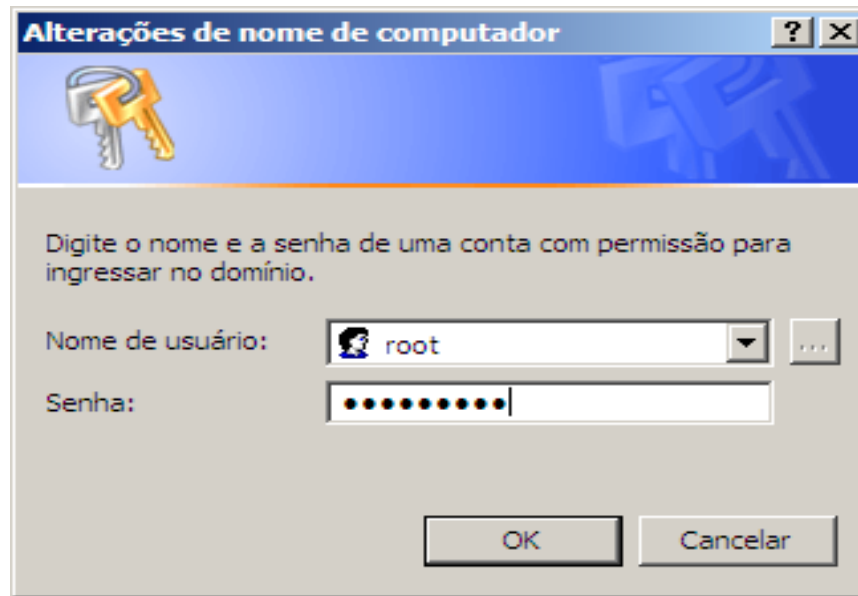
□ INFORMAR O NOME DO DOMINIO QUE É DEFINIDO NA OPÇÃO “Workgroup” DO SAMBA



- **SAMBA PRIMARY DOMAIN CONTROLLER**
 - LOGANDO OS CLIENTES WINDOWS NO SAMBA



- **SAMBA PRIMARY DOMAIN CONTROLLER**
 - LOGANDO OS CLIENTES WINDOWS NO SAMBA
 - SERÁ SOLICITADO UM USUÁRIO COM PERMISSÃO DE INGRESSO NO DOMÍNIO, RESPONDA COM O USUÁRIO “root” E SENHA QUE FOI CADASTRADO NO SAMBA



- **SAMBA PRIMARY DOMAIN CONTROLLER**
 - LOGANDO OS CLIENTES WINDOWS NO SAMBA
 - APÓS REINICIAR A MÁQUINA, APARECERÁ A OPÇÃO PARA REALIZAR O LOGON NO DOMINIO, PERMITINDO QUE O USUÁRIO FAÇA O LOGIN EM QUALQUER UMA DAS CONTAS CADASTRADAS NO SERVIDOR



■ SAMBA PRIMARY DOMAIN CONTROLLER

■ LOGANDO OS CLIENTES WINDOWS NO SAMBA

- APÓS O LOGON NO DOMÍNIO, O USUÁRIO PODE RECEBER UMA TELA COM O NOTEPAD ABERTO COM O CONTEÚDO ABAIXO, É NECESSÁRIO REMOVER O ARQUIVO “desktop.ini” DA PASTA DE PERFIS MÓVEIS PARA RESOLVER ESTA SITUAÇÃO

```
[.ShellClassInfo]
```

```
LocalizedResourceName=@ SystemRoot  
%\system32\shell32.dll,-21787
```

- COMANDO PARA REMOVER OS ARQUIVOS

```
# cd /var/profile/usuario
```

```
# find . -name desktop.ini -exec rm {} \;
```



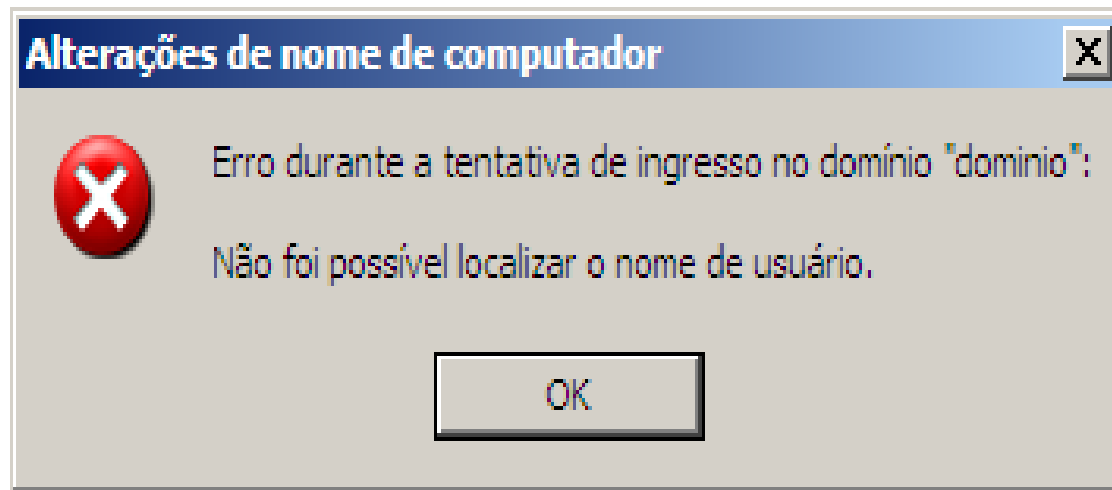
- **SAMBA PRIMARY DOMAIN CONTROLLER**
 - LOGANDO OS CLIENTES WINDOWS NO SAMBA
 - PARA REMOVER A MÁQUINA DO DOMÍNIO, É PRECISO ACESSAR A MESMA OPÇÃO E MUDAR A OPÇÃO DE “MEMBRO DE DOMINIO” PARA “MEMBRO DE GRUPO DE TRABALHO”
 - SERÁ SOLICITADO UM USUÁRIO AUTORIZADO PARA REALIZAR AS CONFIGURAÇÕES, PARA ISSO, UTILIZE A O USUÁRIO ADMINISTRADOR LOCAL



■ SAMBA PRIMARY DOMAIN CONTROLLER

■ PROBLEMAS MAIS COMUNS

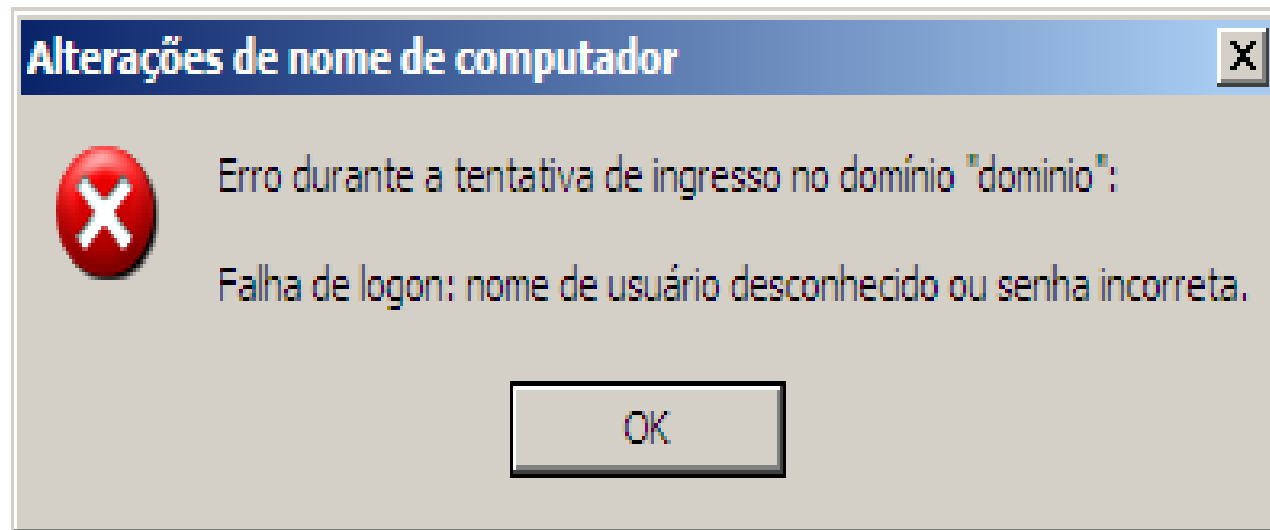
- A MÁQUINA NÃO FOI CADASTRADA NO SERVIDOR SAMBA COMO UMA CONTA DE MÁQUINA. O NOME DO USUÁRIO REFERE-SE A CONTA DA MÁQUINA



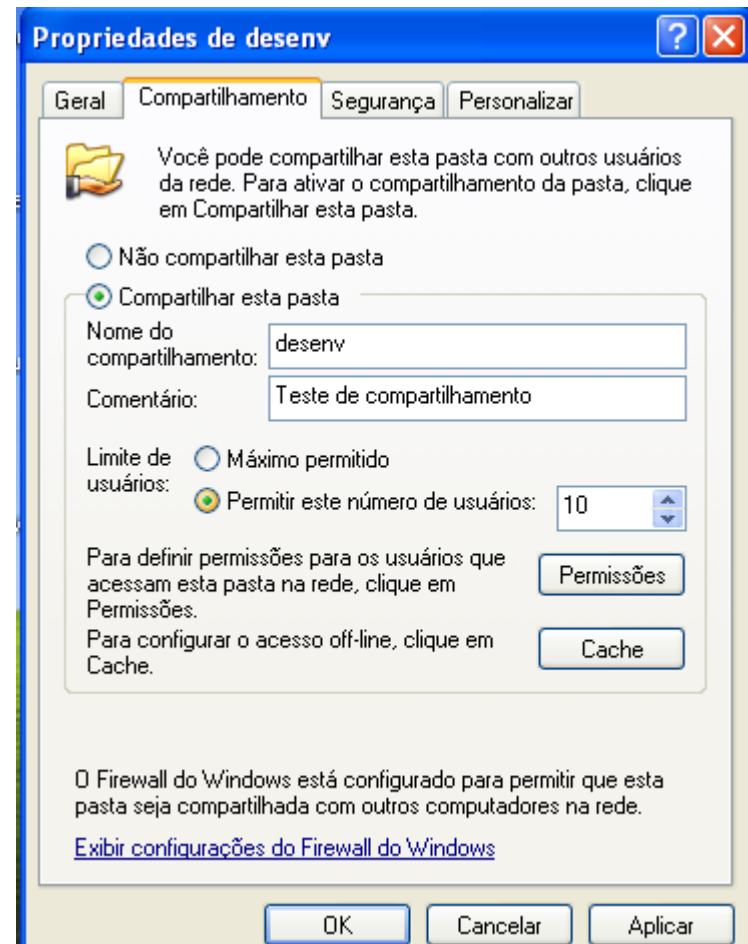
■ SAMBA PRIMARY DOMAIN CONTROLLER

■ PROBLEMAS MAIS COMUNS

- ☐ A CONTA DE root NÃO FOI CADASTRADA NO SAMBA (smbpasswd -a root)
- ☐ A SENHA DE root ESTÁ ERRADA
- ☐ A OPÇÃO "invalid users = root" ESTÁ PRESENTE NO ARQUIVO DE CONFIGURAÇÃO smb.conf

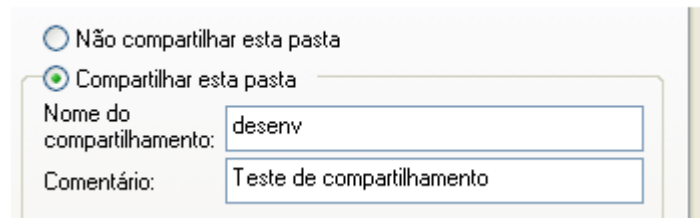


- **COMPARTILHAMENTO DE PASTAS**
 - SOBRE A PASTA QUE SERÁ COMPARTILHADA, CLICAR COM O BOTÃO DIREITO



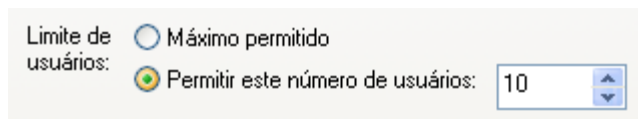
■ COMPARTILHAMENTO DE PASTAS

- SELECIONAR O BOTÃO “Compartilhar esta pasta” E NA SEQUENCIA INFORMAR O NOME DO COMPARTILHAMENTO. UM COMENTÁRIO É OPCIONAL



The screenshot shows the 'Compartilhamento e Segurança' (Sharing and Security) window for a folder. Under the 'Compartilhamento' (Sharing) tab, the 'Compartilhar esta pasta' (Share this folder) radio button is selected. Below it, the 'Nome do compartilhamento' (Share name) text box contains the text 'desenv'. The 'Comentário' (Comment) text box contains the text 'Teste de compartilhamento'.

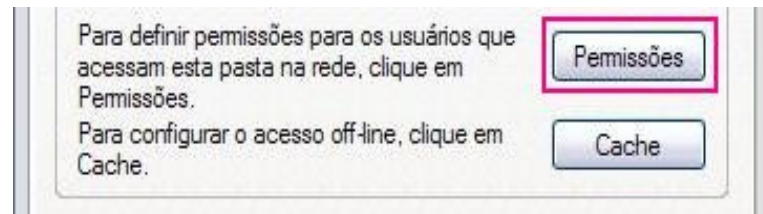
- INFORMAR O NÚMERO LIMITE DE COMPARTILHAMENTO, ONDE O VALOR MÁXIMO É 10



The screenshot shows the 'Limites de compartilhamento' (Sharing limits) section of the 'Compartilhamento e Segurança' (Sharing and Security) window. The 'Limite de usuários' (User limit) section has two radio buttons: 'Máximo permitido' (Maximum allowed) and 'Permitir este número de usuários' (Allow this number of users). The 'Permitir este número de usuários' option is selected, and the adjacent spin box is set to the value '10'.

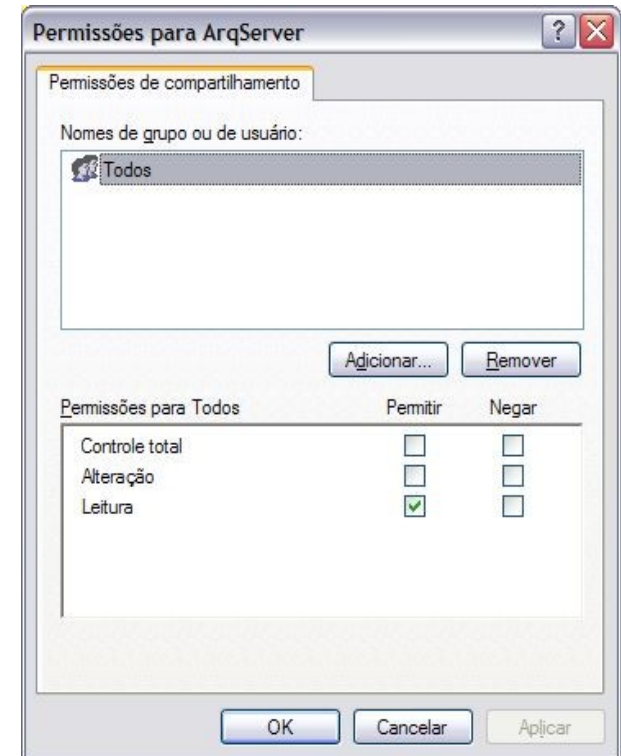


- **COMPARTILHAMENTO DE PASTAS**
 - PARA GARANTIR O ACESSO A PASTA PODEMOS ADICIONAR O CONTROLE POR USUÁRIO NA DEFINIÇÃO DO COMPARTILHAMENTO, CLICANDO SOBRE O BOTÃO “Permissões”

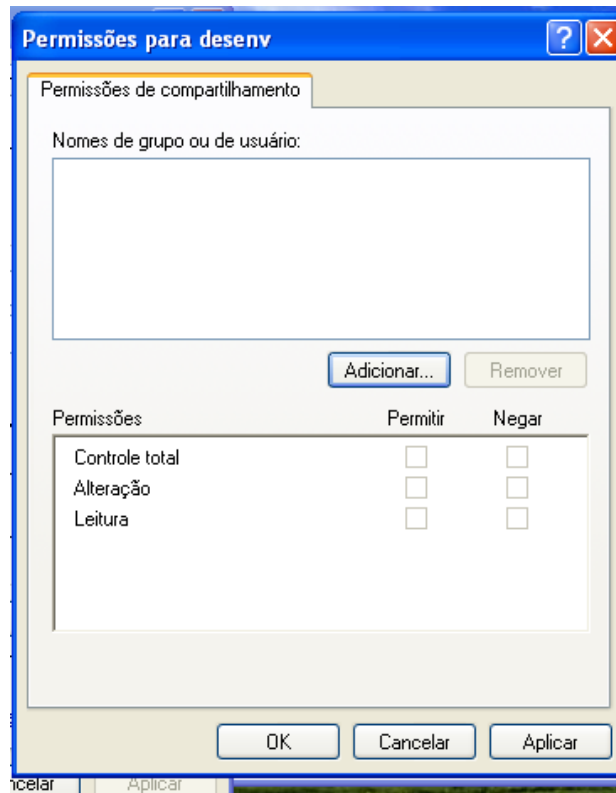


■ COMPARTILHAMENTO DE PASTAS

- POR PADRÃO, TODOS OS USUÁRIOS TEM ACESSO A PASTA, COM O DIREITO DE LEITURA SOMENTE, PODEMOS REMOVER ESTA PERMISSÃO, CLICANDO SOBRE O GRUPO “Todos” E DEPOIS SOBRE O BOTÃO “Remover”

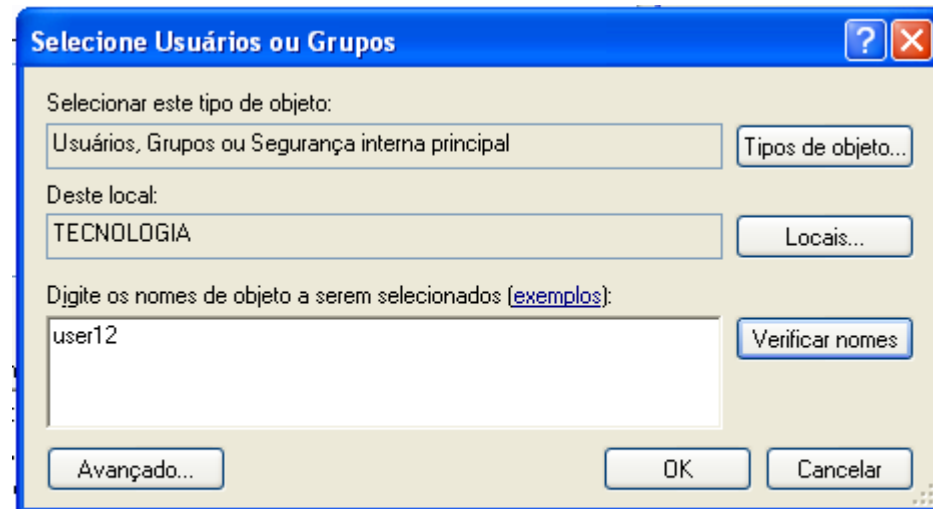
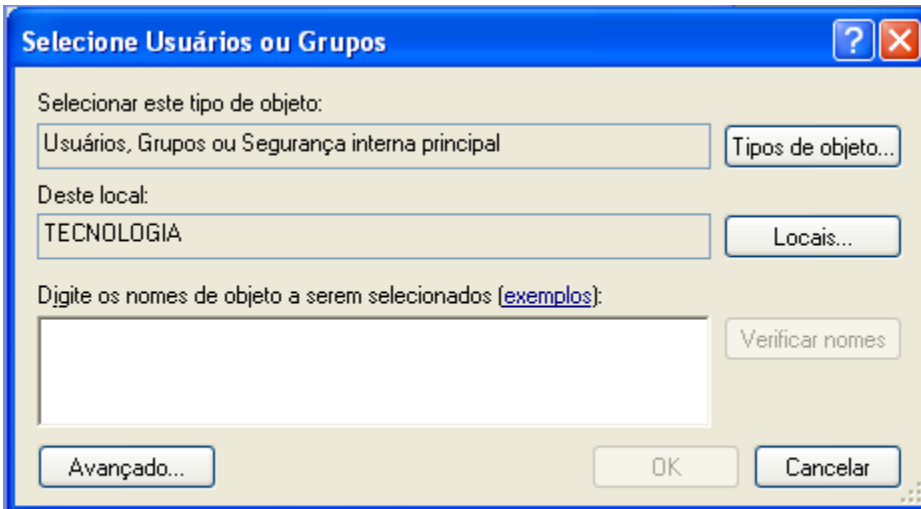


- **COMPARTILHAMENTO DE PASTAS**
 - PARA ADICIONAR QUAIS USUÁRIOS TERÃO A PASTA, CLICAR NO BOTÃO “Adicionar”

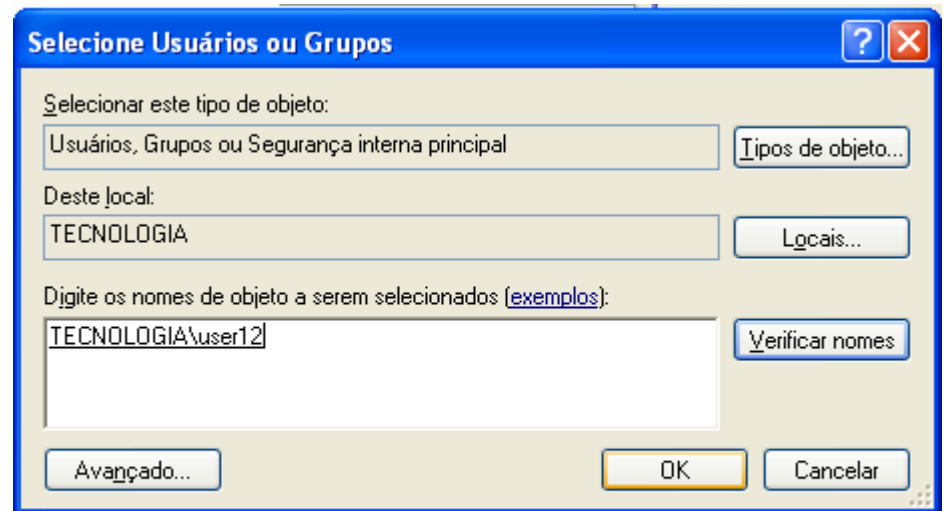
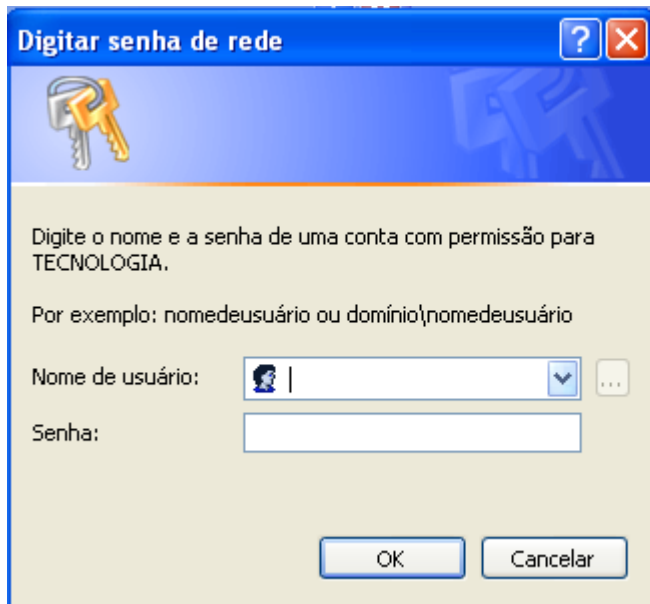


■ COMPARTILHAMENTO DE PASTAS

- AO CADASTRAR UM USUÁRIO O BOTÃO “Verificar Nomes” É HABILITADO E PODEMOS VERIFICAR SE O USUÁRIO É VALIDO

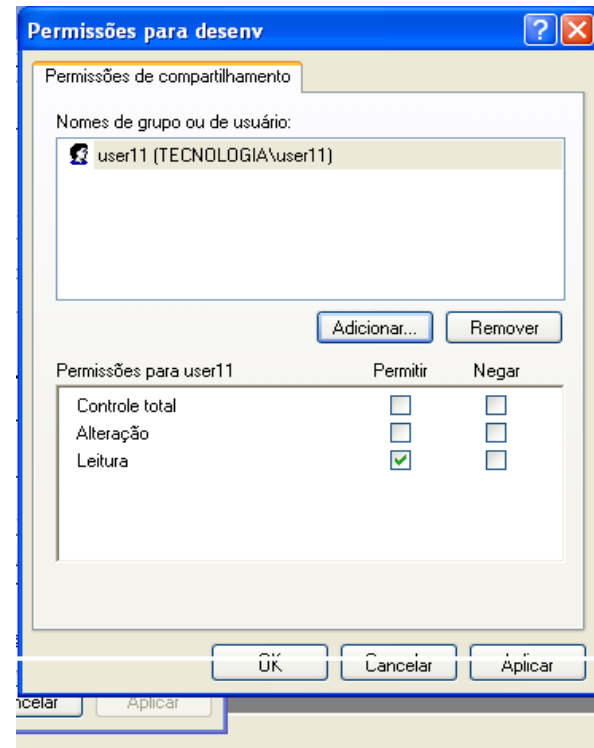


- **COMPARTILHAMENTO DE PASTAS**
 - A VERIFICAÇÃO NECESSITA DE LOGIN NO DOMINIO

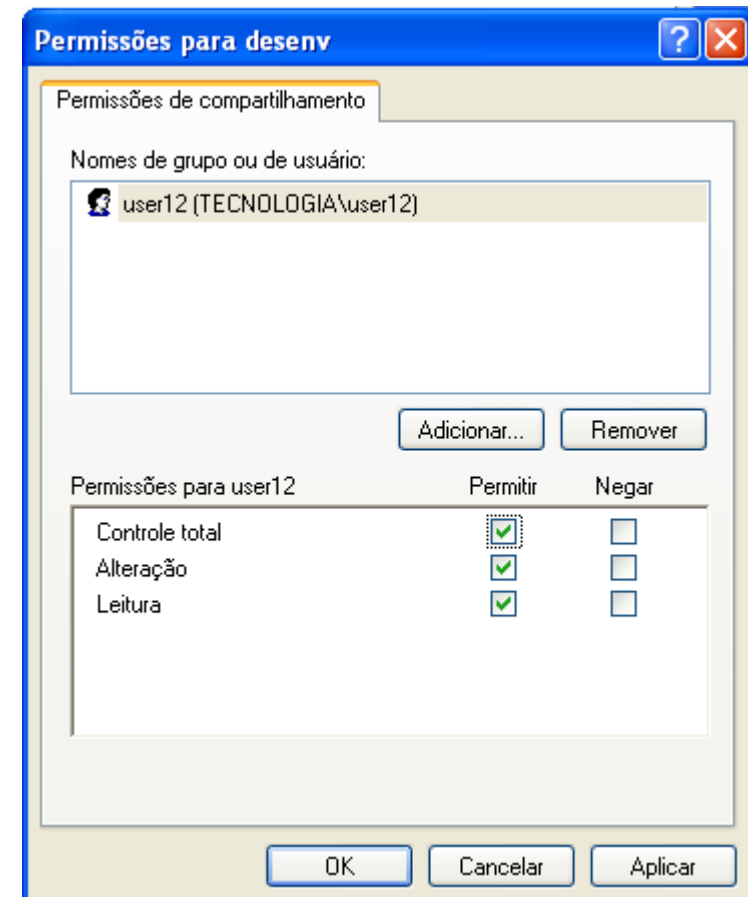


■ COMPARTILHAMENTO DE PASTAS

- APÓS SELECIONAR OS USUÁRIOS E AS PERMISSÕES DE ACESSO, CLICAR SOBRE O BOTÃO OK. SE HOUVER NECESSIDADE DE ADICIONAR NOVOS USUÁRIOS, OS PASSO ANTERIORES DEVEM SER REPETIDOS, CLICANDO SOBRE O BOTÃO “Adicionar”

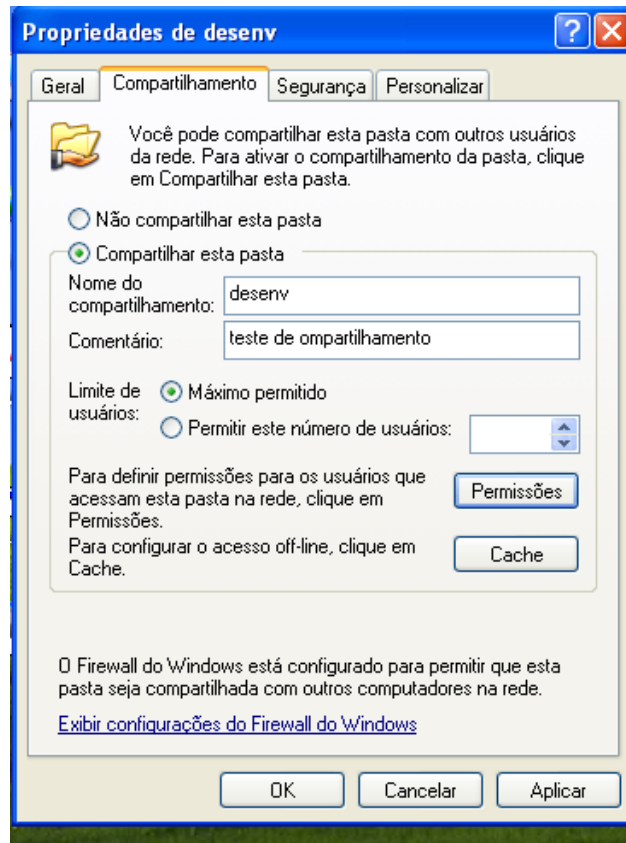


- **COMPARTILHAMENTO DE PASTAS**
 - PARA FINALIZAR, SELECIONAMOS AS PERMISSÕES DE ACESSO E CLICAR SOBRE O BOTÃO OK



■ COMPARTILHAMENTO DE PASTAS

- PARA FINALIZAR, CLICAR SOBRE O BOTÃO OK DA TELA ABAIXO E NA SEQUENCIA SER Á MOSTRADO O COMPARTILHAMENTO:



■ COMPARTILHAMENTO DE PASTAS

■ DIFERENÇAS ENTRE AS PERMISSÕES:

□ LEITURA

- LISTAR NOMES DE ARQUIVOS E SUBPASTAS
- ABRIR ARQUIVOS PARA LEITURA
- EXECUÇÃO DE ARQUIVOS DE PROGRAMAS (.EXE, .COM)

□ ALTERAÇÃO

- CRIAÇÃO DE SUBPASTAS E ARQUIVOS
- ALTERAÇÃO DE DADOS NOS ARQUIVOS
- EXCLUSÃO DE SUBPASTAS E ARQUIVOS



■ COMPARTILHAMENTO DE PASTAS

■ DIFERENÇAS ENTRE AS PERMISSÕES:

□ CONTROLE TOTAL

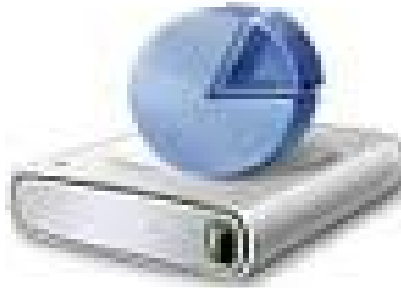
□ TODAS AS OPÇÕES ANTERIORMENTE MENCIONADAS

□ ALTERAÇÃO DAS PERMISSÕES

□ APROPRIAÇÃO



DISK QUOTA



■ CONTROLE DE ESPAÇO EM DISCO (QUOTA)

- OS SERVIDORES DE ARQUIVOS PERMITEM QUE OS USUÁRIOS DA REDE CENTRALIZEM EM UM ÚNICO LOCAL OS SEUS ARQUIVOS, PORÉM É NECESSÁRIO QUE O ESPAÇO DISPONÍVEL SEJA CONTROLADO PARA EVITAR QUE OS USUÁRIOS MAIS “FOME” UTILIZEM TODO O ESPAÇO EM DISCO DO SERVIDOR
- ATRAVÉS DO SISTEMA DE QUOTA, É POSSÍVEL LIMITAR A QUANTIDADE DE ESPAÇO EM DISCO DISPONÍVEL PARA CADA USUÁRIO DA REDE, COMO POR EXEMPLO, 50MB PARA CADA UM
- O USO MAIS COMUM É UTILIZAR UMA PARTIÇÃO SEPARADA ONDE OS USUÁRIOS ESTARÃO ARMAZENANDO AS INFORMAÇÕES E ATIVAR A QUOTA NESTA PARTIÇÃO



■ CONTROLE DE ESPAÇO EM DISCO (QUOTA)

- O SISTEMA DE QUOTA UTILIZA UMA BASE DE DADOS QUE POSSUI INFORMAÇÕES SOBRE A UTILIZAÇÃO DE ESPAÇO EM DISCO DE TODOS USUÁRIOS NA PARTIÇÃO
- AO SER ATIVADO, O SISTEMA DE QUOTA PROCURA TODOS OS ARQUIVOS DE CADA USUÁRIO DENTRO DA PARTIÇÃO
- OS ARQUIVOS PODEM ESTAR ESPALHADOS NO SISTEMA DE ARQUIVOS ONDE O SISTEMA DE QUOTA ESTÁ ATIVADO
- O SISTEMA DE QUOTA PODE TRABALHAR SOBRE OS SISTEMAS DE ARQUIVO EXT2, EXT3 E REISERFS



■ CONTROLE DE ESPAÇO EM DISCO (QUOTA)

- O CONTROLE DE ESPAÇO É FEITO COM BASE EM DOIS LIMITES

- HARD LIMIT

- É O LIMITE DE DADOS PROPRIAMENTE DITO, POR EXEMPLO 100MB

- O SISTEMA NÃO PERMITIRÁ A GRAVAÇÃO DE UM BYTE ACIMA DESTE LIMITE

- SOFT LIMIT

- É UM LIMITE DE ADVERTÊNCIA, POR EXEMPLO 80MB

- SEMPRE QUE SUPERAR O “SOFT LIMITE” O USUÁRIO RECEBERÁ UMA MENSAGEM DE ALERTA, MAS PODERÁ CONTINUAR A GRAVAÇÃO, ATÉ ATINGIR O “HARD LIMIT”



■ CONTROLE DE ESPAÇO EM DISCO (QUOTA)

- O CONTROLE DE ESPAÇO É FEITO COM BASE EM DOIS LIMITES

- GRACE PERIOD

- É UM LIMITE DE TEMPO QUE O USUÁRIO PODE PERMANECER DENTRO DO “SOFT LIMIT”

- PASSADO ESTE TEMPO, O USUÁRIO DEVERÁ APAGAR ALGUNS ARQUIVOS PARA VOLTAR A FICAR ABAIXO DO LIMITE ESTABELECIDO POR “SOFT LIMIT” PARA PODER VOLTAR A GRAVAR NO SISTEMA DE ARQUIVOS

- O CONTROLE DE ESPAÇO TAMBÉM PODE SER REALIZADO ATRAVÉS DE GRUPOS DE USUÁRIOS, OU A COMBINAÇÃO DE AMBOS (USUÁRIO + GRUPO)



■ CONTROLE DE ESPAÇO EM DISCO (QUOTA)

■ INSTALAÇÃO E CONFIGURAÇÃO

□ PARA INSTALAR O SISTEMA DE QUOTA EXECUTAR OS COMANDOS ABAIXO:

```
# apt-get install quota quotatool
```

□ NA PARTIÇÃO ONDE SERÁ IMPLEMENTAÇÃO O CONTROLE DE QUOTAS, ALTERAR O ARQUIVO “/etc/fstab”

□ POR EXEMPLO, A PARTIÇÃO “/dev/hdb1” MONTADO A PARTIR DA PASTA “/media/hd1” DEVE POSSUIR A ENTRADA ABAIXO, PARA CONTROLAR O ESPAÇO EM DISCO

```
□ /dev/hdb1 /media/hd1 usrquota=aquota.user,grpquota=aquota.group,jqfmt=vfsv0 0 2
```



■ CONTROLE DE ESPAÇO EM DISCO (QUOTA)

■ INSTALAÇÃO E CONFIGURAÇÃO

□ CRIAR OS ARQUIVOS NA PASTA /media/hd1

```
# mount /dev/hdb1 /media/hd1
```

```
# cd /media/hd1
```

```
#touch /media/hd1/aquota.group
```

```
# touch /media/hd1/aquota.user
```

```
# chmod 0600 /media/hd1/aquota.*
```

```
# mount -o remount /media/hd1
```



■ CONTROLE DE ESPAÇO EM DISCO (QUOTA)

■ INSTALAÇÃO E CONFIGURAÇÃO

□ APLICAÇÕES QUE SERÃO UTILIZADOS:

□ quotacheck

□ FAZ A VARREDURA NO SISTEMA DE ARQUIVO
PARA MONTAR A BASE DE DADOS

□ edquota

□ EDITA QUOTA PARA USUÁRIOS

□ repquota

□ EMITE RELATÓRIO DO SISTEMA DE QUOTA

□ quotaon/quotaoff

□ ATIVA/DESATIVA O SISTEMA DE QUOTA

□ quota

□ MOSTRA A UTILIZAÇÃO DE QUOTAS NO DISCO



■ CONTROLE DE ESPAÇO EM DISCO (QUOTA)

■ GERAÇÃO DA BASE DE DADOS

- A BASE DE DADOS É UM DOS PRINCIPAIS COMPONENTES DO CONTROLE DE ESPAÇO E DEVE ESTAR SEMPRE ATUALIZADA
- A ATUALIZAÇÃO É REALIZADA ATRAVÉS DO COMANDO ABAIXO
 - # quotacheck -avug



■ CONTROLE DE ESPAÇO EM DISCO (QUOTA)

■ GERAÇÃO DA BASE DE DADOS

□ ANOTAÇÕES IMPORTANTES

□ DURANTE O MOMENTO QUE O SISTEMA DE QUOTA ESTEJA ATUALIZANDO A BASE DE DADOS, NENHUMA ALTERAÇÃO PODE OCORRER NO SISTEMA DE ARQUIVO, PARA EVITAR INFORMAÇÕES INCONSISTENTES NESTA BASE DE DADOS, SE POSSÍVEL ALTERAR TROCAR O NÍVEL DE EXECUÇÃO DO SISTEMA OPERACIONAL PARA MODO DE MANUTENÇÃO, ISTO É NÍVEL 1

□ O SISTEMA DE QUOTA DEVE ESTAR DESABILITADOS

quotaoff -a



■ CONTROLE DE ESPAÇO EM DISCO (QUOTA)

- ADICIONAR QUOTA PARA O USUÁRIO
- PARA CONTROLAR O ESPAÇO DE UM É NECESSÁRIO SEGUIR OS PASSOS ABAIXO:
- # edquota -u usuário
- # edquota -u user20

192.168.10.80 - PuTTY
GNU nano 2.0.7 Arquivo: /tmp//EdP.a9TtlpI

Disk quotas for user user20 (uid 1001):

Filesystem	blocks	soft	hard	inodes	soft	hard
/dev/hdb1	1000	500	1000	1	0	0

Número máximo de I-Nodes (1 I-Node = 1 arquivo ou Pasta)

Alerta de Número de I-Nodes

Número de I-Nodes em uso

Espaço máximo em disco (blocos de 1K = 1024 bytes)

Alerta de espaço em disco (blocos de 1K = 1024 bytes)

Espaço em disco em uso atualmente (blocos de 1K = 1024 bytes)

Sistema de arquivo em que ocorre o controle



■ CONTROLE DE ESPAÇO EM DISCO (QUOTA)

■ ADICIONAR QUOTA PARA UM GRUPO

□ `edquota -g faturamento`

■ ALTERAR O GRACE PERIOD

`# edquota -u -t`

`# edquota -g -t`

■ MOSTRANDO DE UM USUÁRIO

`# quota -v -u user20`

Disk quotas for user user20 (uid 1001):

Filesystem	blocks	quota	limit	grace	files	quota	limit	grace
/dev/hdb1	1000*	500	1000	6days	1	0	0	



■ CONTROLE DE ESPAÇO EM DISCO (QUOTA)

- MOSTRANDO RELATÓRIO DE QUOTA

- # repquota /media/hd1

- *** Report for user quotas on device /dev/hdb1

- Block grace time: 7days; Inode grace time: 7days

- Block limits File limits

- User used soft hard grace used soft hard grace

- -----

- root -- 5663 0 0 4 0 0

- user20 +- 1000 500 1000 6days 1 0 0

-



■ CONTROLE DE ESPAÇO EM DISCO (QUOTA)

■ ADIÇÃO DE QUOTA NÃO INTERATIVA

□ # setquota -a -u user20 5000 7000 150 250

-u, Define a quota para usuário

-g, Define a quota para um grupo de usuários

-a, Todos os sistemas de arquivos com quotas

5000 – soft limit para blocos

7000 – hard limit para blocos

150 – soft limit para I-Nodes

250 – hard limit para I-Nodes



DHCP



■ DHCP – CONCEITOS BÁSICOS

- O PROTOCOLO DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL) PERMITE QUE AS ESTAÇÕES DE TRABALHO RECEBAM AS CONFIGURAÇÕES DE REDE DE FORMA AUTOMÁTICA A PARTIR DE UM SERVIDOR CENTRAL

■ FUNCIONAMENTO BÁSICO

- A ESTAÇÃO ENVIA UM PACOTE DE BROADCAST (UDP) SOLICITANDO UM ENDEREÇO IP (REQUEST)
- O SERVIDOR RECEBE ESTE PEDIDO E ALOCA UM ENDEREÇO IP. DEVOLVE UM PACOTE UNICAST CONTENDO AS INFORMAÇÕES PARA A ESTAÇÃO (RESPONSE)
- DENTRO DO PACOTE DE RESPOSTA ESTÃO: ENDEREÇO IP, MÁSCARA DE REDE, GATEWAY E SERVIDOR DE DNS QUE SERÃO UTILIZADOS PELA ESTAÇÃO



- DHCP – CONCEITOS BÁSICOS
 - FUNCIONAMENTO



■ DHCP – CONCEITOS BÁSICOS

■ FUNCIONAMENTO BÁSICO

- PERIODICAMENTE A ESTAÇÃO DEVE SOLICITAR A RENOVAÇÃO DE ALUGUEL (LEASE TIME) DO ENDEREÇO IP QUE FOI ALOCADO
- ESTE PROCEDIMENTO GARANTE QUE OS ENDEREÇOS IP SEJAM ALOCADOS SOMENTE PARA A ESTAÇÃO QUE ESTÁ ONLINE, EVITANDO QUE OS ENDEREÇOS DISPONÍVEIS SE ESGOTEM



■ DHCP – CONCEITOS BÁSICOS

■ FORMAS DE DISTRIBUIÇÃO

□ MANUAL

□ EXISTE UMA ASSOCIAÇÃO ENTRE UM ENDEREÇO MAC E UM ENDEREÇO IP NO BANCO DE DADOS DO SERVIDOR

□ AUTOMÁTICA

□ A ESTAÇÃO OBTÉM UM ENDEREÇO DE UM ESPAÇO DE ENDEREÇOS POSSÍVEIS, ESPECIFICADO PELO ADMINISTRADOR, POR TEMPO INDETERMINADO



■ DHCP – CONCEITOS BÁSICOS

■ FORMAS DE DISTRIBUIÇÃO

□ DINÂMICA

- A ESTAÇÃO OBTÉM UM ENDEREÇO IP POR UM PERÍODO DE TEMPO LIMITADO
- PERIODICAMENTE É NECESSÁRIO A ATUALIZAÇÃO DA LOCAÇÃO.
- DIFERENTES EQUIPAMENTOS PODEM UTILIZAR O MESMO ENDEREÇO IP EM MOMENTOS DIFERENTES



■ DHCP – CONCEITOS BÁSICOS

- ESTADOS DE AQUISIÇÃO DE ENDEREÇO IP
- UM CLIENTE DHCP PODE PASSAR POR SEIS ESTADOS DE AQUISIÇÃO
 - INICIALIZA
 - SELECIONA
 - SOLICITA
 - LIMITE
 - RENOVA
 - VINCULA NOVAMENTE
- O QUE DEFINE O ESTADO É A MENSAGEM QUE O CLIENTE ENVIA PARA UM SERVIDOR DHCP NA REDE



■ DHCP – CONCEITOS BÁSICOS

■ ESTADOS DE AQUISIÇÃO DE ENDEREÇO IP

■ INICIALIZA (INITIALIZE)

- QUANDO O CLIENTE É INICIALIZADO
- ENVIA UMA MENSAGEM PARA DESCOBRIR A SUA CONFIGURAÇÃO DE REDE
- MENSAGEM “DHCPDISCOVER”
- UTILIZA ENDEREÇO DE BROADCAST
- APÓS O ENVIA DESTA MENSAGEM, O CLIENTE PASSA PARA O ESTADO “SELECIONA”



■ DHCP – CONCEITOS BÁSICOS

■ ESTADOS DE AQUISIÇÃO DE ENDEREÇO IP

■ SELECIONA(SELECT)

- PERMANECE NESTE ESTADO AGUARDANDO RESPOSTA DOS SERVIDORES DHCP QUE RECEBERAM A MENSAGEM “DHCPDISCOVER”
- OS SERVIDORES DHCP CONFIGURADOS NA REDE ENVIAM MENSAGEM “DHCPOFFER” CONTENDO AS INFORMAÇÕES NECESSÁRIAS PARA A CONFIGURAÇÃO DO CLIENTE
- O CLIENTE IRÁ OPTAR POR UM SERVIDOR DE DHCP E ENTRARÁ EM UMA NEGOCIAÇÃO DE LOCAÇÃO COM O SERVIDOR OFERTANTE
- PARA INICIAR A NEGOCIAÇÃO O SERVIDOR ENVIA UMA MENSAGEM “DHCPREQUEST” E ENTRA NO ESTADO “SOLICITA”



■ DHCP – CONCEITOS BÁSICOS

■ ESTADOS DE AQUISIÇÃO DE ENDEREÇO IP

■ SOLICITA (REQUEST)

- O CLIENTE AGUARDA UMA RESPOSTA DE CONFIRMAÇÃO DO SERVIDOR DHCP QUE ELE ENTROU EM NEGOCIAÇÃO
- A CONFIRMAÇÃO É REMETIDA ATRAVÉS DA MENSAGEM “DHCPACK”
- COM O RECEBIMENTO DA CONFIRMAÇÃO, O CLIENTE UTILIZADO O ENDEREÇO LOCADO, E TAMBÉM OUTRAS INFORMAÇÕES ENVIADOS PELO SERVIDOR DHCP
- O CLIENTE ENTRA NO ESTADO “LIMITE”



■ DHCP – CONCEITOS BÁSICOS

■ ESTADOS DE AQUISIÇÃO DE ENDEREÇO IP

■ LIMITE (BOUND)

- ESTE É O ESTADO EM QUE PERMANECE O CLIENTE DURANTE A UTILIZAÇÃO DO ENDEREÇO IP ATÉ QUE ATINJA O PERÍODO DE RENOVAÇÃO OU O CLIENTE DECIDA NÃO UTILIZAR MAIS O ENDEREÇO LOCADO
- PARA ESTE CASO, O CLIENTE NÃO ESPERA O TÉRMINO DO PRAZO DE LOCAÇÃO E ELE ENVIA UMA MENSAGEM “DHCPRELEASE” PARA O SERVIDOR, A FIM DE PROVOCAR A LIBERAÇÃO DO ENDEREÇO IP E PASSA PARA O ESTADO “INICIALIZA”



■ DHCP – CONCEITOS BÁSICOS

■ ESTADOS DE AQUISIÇÃO DE ENDEREÇO IP

■ RENOVA (RENEW)

- AO RECEBER UMA MENSAGEM “DHCPACK” O CLIENTE ADQUIRI O TEMPO DO PERÍODO DE LOCAÇÃO DO ENDEREÇO (ESTADO LIMITE/BOUND)
- DE POSSE DESTA INFORMAÇÃO ELE UTILIZA TRÊS TEMPORIZADORES QUE SÃO UTILIZADO PARA CONTROLAR
 - PERÍODOS DE RENOVAÇÃO (T1)
 - PERÍODO DE REVINCULAÇÃO (T2)
 - FIM DA LOCAÇÃO (T3)
- O SERVIDOR PODE ESPECIFICAR O VALOR DE CADA TEMPORIZADOR. NA FALTA DESTES VALORES, SÃO UTILIZADO: 50%(T1), 85% (T2) E 100% (T3) RESPECTIVAMENTE DO VALOR LIMITE



■ DHCP – CONCEITOS BÁSICOS

- ESTADOS DE AQUISIÇÃO DE ENDEREÇO IP
- RENOVA (RENEW)

- QUANDO O TEMPORIZADOR ULTRAPASSA O VALOR DA RENOVAÇÃO, (T1) O CLIENTE TENTARÁ RENOVAR A LOCAÇÃO, ENVIANDO UMA MENSAGEM UNICAST “DHCPREQUEST” AO SERVIDOR
- ASSIM ELE PASSA PARA O ESTADO “RENOVA” E AGUARDA RESPOSTA
- NA MENSAGEM “DHCPREQUEST” SEGUE O ENDEREÇO IP ATUAL E UMA EXTENSÃO DE LOCAÇÃO DO ENDEREÇO IP
- O SERVIDOR PODERÁ RESPONDER POSITIVAMENTE, NEGATIVAMENTE OU NÃO RESPONDER



■ DHCP – CONCEITOS BÁSICOS

■ ESTADOS DE AQUISIÇÃO DE ENDEREÇO IP

■ RENOVA (RENEW)

- SE A RESPOSTA FOR POSITIVA, ENTÃO O SERVIDOR IRÁ ENVIAR UMA MENSAGEM “DHCPACK” AO CLIENTE QUE NOVAMENTE ENTRARÁ NO ESTADO “LIMITE”
- SE RESPOSTA FOR NEGATIVA, ENTÃO O SERVIDOR IRÁ ENVIAR UMA MENSAGEM “DHCPNACK” AO CLIENTE QUE FAZ COM QUE O CLIENTE INTERROMPA A UTILIZAÇÃO DO ENDEREÇO IP PASSE PARA O ESTADO “INICIALIZA”



■ DHCP – CONCEITOS BÁSICOS

- ESTADOS DE AQUISIÇÃO DE ENDEREÇO IP
- RENOVA (RENEW)

- AO ENTRAR NO ESTADO “RENOVA”, O CLIENTE FICA AGUARDANDO A RESPOSTA DO SERVIDOR. CASO ESTA RESPOSTA NÃO CHEGUE (O SERVIDOR FOI DESLIGADO OU DESCONECTADO DA REDE) O CLIENTE PERMANECE NESTE ESTADO E COMUNICADO-SE NORMALMENTE ATÉ QUE SEJA ULTRAPASSADO O SEGUNDO TEMPORIZADOR (T2) (PERÍODO DE REVINCULAÇÃO)
- APÓS ULTRAPASSADO O SEGUNDO TEMPORIZADOR (T2), O CLIENTE PASSA PARA O ESTADO “VINCULA NOVAMENTE”



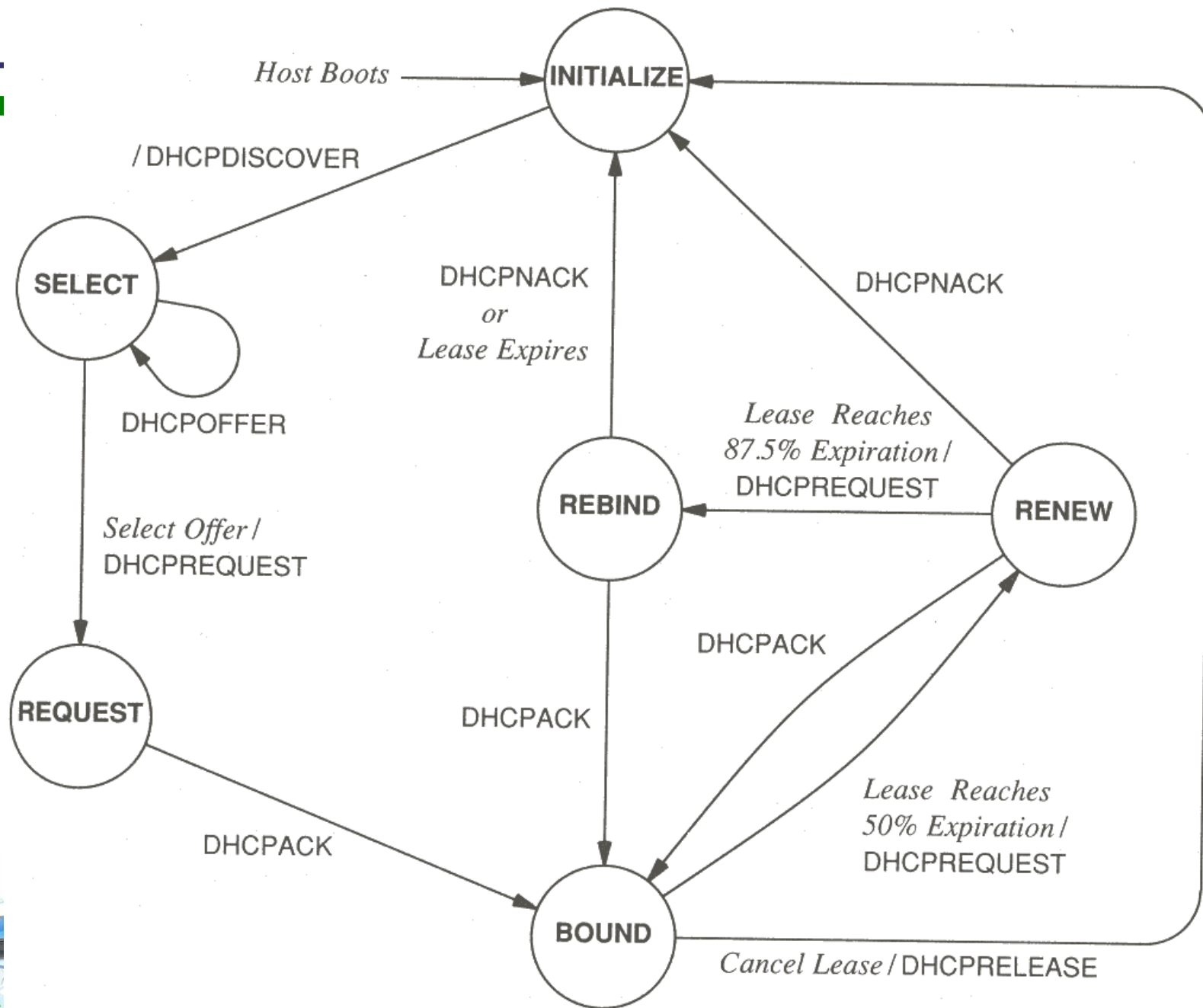
■ DHCP – CONCEITOS BÁSICOS

■ ESTADOS DE AQUISIÇÃO DE ENDEREÇO IP

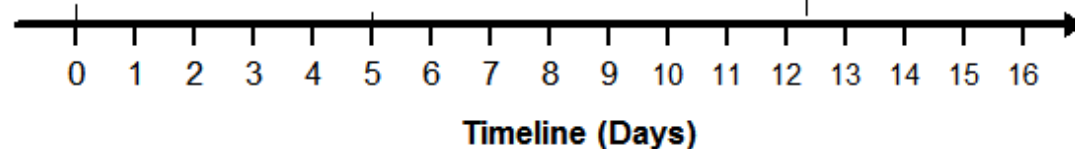
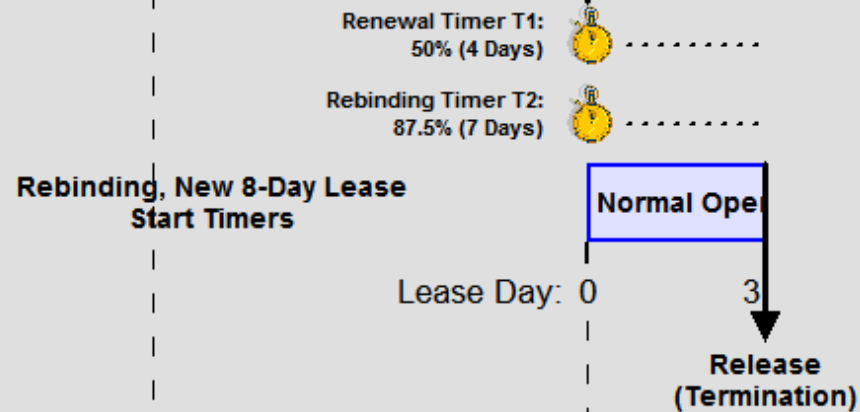
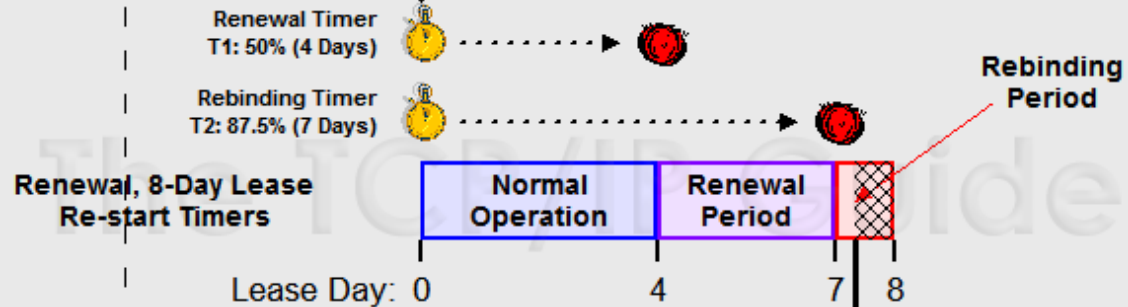
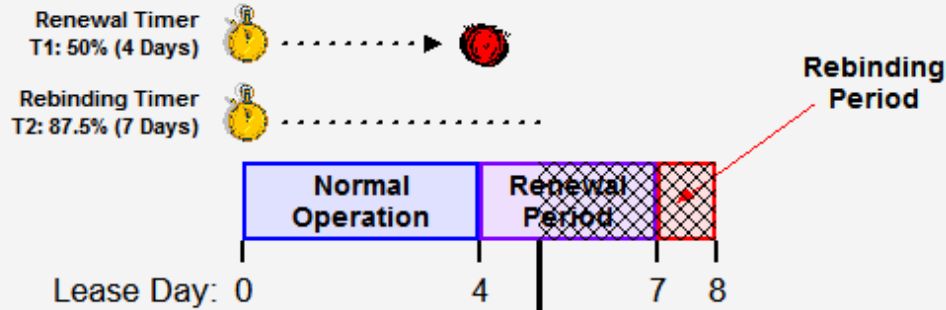
■ VINCULA NOVAMENTE (REBIND)

- A PARTIR DAÍ, O CLIENTE PRESSUPÕE QUE O SERVIDOR NÃO ESTÁ MAIS DISPONÍVEL E TENTA OBTER RENOVAÇÃO COM QUALQUER OUTRO SERVIDOR DHCP ATRAVÉS DA DIFUSÃO DA MENSAGEM “DHCPREQUEST”
- SE O CLIENTE RECEBER UMA MENSAGEM “DHCPACK”, ELE RETORNA PARA O ESTADO “LIMITE”
- EM RECEBENDO UMA MENSAGEM “DHCPNACK” ELE PASSARÁ PARA O ESTADO “INICIALIZA”
- NO CASO DE NÃO RECEBER NENHUMA RESPOSTA, ELE CONTINUARÁ A UTILIZAR O ENDEREÇO IP ATÉ QUE O TERCEIRO TEMPORIZADOR (T3) ATINJA O SEU LIMITE, FAZENDO RETORNO PARA O ESTADO “INICIALIZA”





Allocation, 8-Day Lease Start Timers



■ DHCP – CONCEITOS BÁSICOS

■ INSTALAÇÃO DO PACOTE NO DEBIAN

```
# apt-get install isc-dhcp-server
```

■ INICIALIZAÇÃO DO SERVIÇO

```
# service isc-dhcp-server [start/stop/restart]
```

■ ARQUIVO DE CONFIGURAÇÃO

□ O ARQUIVO DE CONFIGURAÇÃO ESTÁ LOCALIZADO EM /etc/dhcp/dhcpd.conf



■ DHCP – ARQUIVO DE CONFIGURAÇÃO

■ EXEMPLO DE ARQUIVO DE CONFIGURAÇÃO

```
default-lease-time 600;  
max-lease-time 7200;  
option subnet-mask 255.255.255.0;  
option routers 192.168.1.1;  
option domain-name-servers 200.106.80.11, 200.106.1.5;  
option domain-name "example.com.br";  
subnet 192.168.1.0 netmask 255.255.255.0 {  
    range 192.168.1.10 192.168.1.100;  
}
```



■ DHCP – CONCEITOS BÁSICOS

■ DESCRIÇÃO DOS REGISTROS

□ default-lease-time

□ O CLIENTE PODE REQUISITAR UM ENDEREÇO POR UM DETERMINADO PERÍODO DE TEMPO, CASO NÃO SEJA ESPECIFICADO O TEMPO, O SERVIDOR UTILIZARÁ ESTE VALOR.

□ POR PADRÃO 10 MINUTOS (600 seg)

□ max-lease-time

□ TEMPO MÁXIMO QUE UMA ESTAÇÃO PODE REQUISITAR UM ENDEREÇO IP PARA O SERVIDOR

□ POR PADRÃO 2 HORAS (7200 seg)

□ option subnet-mask

□ MÁSCARA DE SUB-REDE A SER FORNECIDA AOS CLIENTES



■ DHCP – CONCEITOS BÁSICOS

■ DESCRIÇÃO DOS REGISTROS

- option routers

 - ENDEREÇO DO GATEWAY DA REDE

- option domain-name-servers

 - LISTA DE SERVIDORES DE NOMES

- option domain-name

 - NOME DO DOMINIO

- subnet

 - ESPECIFICA O ENDEREÇO DE REDE QUE SERÁ OFERECIDO OS ENDEREÇOS IP

- range

 - DETERMINA A FAIXA DE ENDEREÇOS IP QUE SERÁ UTILIZADA PELO SERVIDOR PARA ATRIBUIR AOS CLIENTES



■ DHCP – CONCEITOS BÁSICOS

■ RESULTADO DE CLIENTES WINDOWS

> ipconfig /all

Descrição : AMD PCNET Family PCI Ethernet Adapter

Endereço físico : 00-0C-29-EF-98-D9

DHCP ativado. : Sim

Configuração automática ativada . . : Sim

Endereço IP : 192.168.10.42

Máscara de sub-rede : 255.255.255.0

Gateway padrão. : 192.168.10.1

Servidor DHCP : 192.168.10.1

Servidores DNS. : 192.168.10.1

Servidor WINS primário. : 192.168.10.13

Concessão obtida. : segunda-feira, 11 de julho de 2011 14:47:32

Concessão expira. : segunda-feira, 11 de julho de 2011 16:47:32



■ DHCP – ARQUIVO DE CONFIGURAÇÃO

■ EXEMPLO DE ARQUIVO DE CONFIGURAÇÃO UTILIZANDO COM SALTOS NO ENDEREÇAMENTO IP – 2 RANGES

default-lease-time 600;

max-lease-time 7200;

option subnet-mask 255.255.255.0;

option routers 192.168.1.1;

option domain-name-servers 200.106.80.11, 200.106.1.5;

option domain-name "example.com.br";

subnet 192.168.1.0 netmask 255.255.255.0 {

 range 192.168.1.10 192.168.1.100;

 # A faixa de endereço que foi pulado pode ser utilizado
 para endereçar servidores de aplicação

 range 192.168.1.150 192.168.1.200;

}



- DHCP – ARQUIVO DE CONFIGURAÇÃO
 - ATRIBUINDO ENDEREÇO SOMENTE PARA HOSTS CONHECIDOS

```
subnet 172.16.10.0 netmask 255.255.255.0 {  
    option routers 172.16.10.1;  
    option subnet-mask 255.255.255.0;  
    range 172.16.10.1 172.16.10.50;  
    # Não fornece IP para clientes desconhecidos (não cadastrados)  
    deny unknown-clients;  
    host wks01 { # ← HOST CONHECIDO  
        hardware ethernet 00:0b:82:14:b3:2a;  
    }  
    host wks02 { # ← HOST CONHECIDO  
        hardware ethernet 68:b5:99:4d:45:18;  
    }  
}
```



- DHCP – ARQUIVO DE CONFIGURAÇÃO
 - ATRIBUINDO ENDEREÇOS FIXOS PARA HOSTS CONHECIDOS

```
subnet 172.16.10.0 netmask 255.255.255.0 {  
    option routers 172.16.10.1;  
    option subnet-mask 255.255.255.0;  
    # Outros clientes receberão a faixa de endereçamento abaixo  
    range 172.16.10.1 172.16.10.50;  
    host wks01 { # ← HOST CONHECIDO  
        hardware ethernet 00:0b:82:14:b3:2a;  
        fixed-address 172.16.10.100; # ← ENDEREÇO IP FIXO  
    }  
    host wks02 { # ← HOST CONHECIDO  
        hardware ethernet 68:b5:99:4d:45:18;  
        fixed-address 172.16.10.101; # ← ENDEREÇO IP FIXO  
    }  
}
```



■ DHCP – ARQUIVO DE CONFIGURAÇÃO

- EM ALGUMAS SITUAÇÕES É NECESSÁRIO ATRIBUIR ENDEREÇOS ips COM PARAMETROS DIFERENCIADOS DOS DEMAIS ENDEREÇOS, COMO POR EXEMPLO UM PERÍODO MAIOR DE UTILIZAÇÃO DO ENDEREÇAMENTO IP
- A CLAUSULA “pool” OFERECE A POSSIBILIDADE DE COLOCAR AS INFORMAÇÕES DIFERENCIAIS PARA ESTAS CLASSES



- DHCP – ARQUIVO DE CONFIGURAÇÃO
 - ATRIBUINDO ENDEREÇO COM “pool”

```
subnet 172.16.10.0 netmask 255.255.255.0 {  
    option routers 172.16.10.1;  
    option subnet-mask 255.255.255.0;  
    pool { # ← pool geral  
        range 172.16.10.1 172.16.10.50;  
    }  
    pool { # ← pool diferenciado para hosts conhecidos  
        range 172.16.10.51 172.16.10.60;  
        option domain-name-servers abc.com.br;  
        default-leases-time 1200;  
        max-leases-time 3600;  
        deny unknown-clients;  
    }  
    host wks01 { # ← HOST CONHECIDO  
        hardware ethernet 00:0b:82:14:b3:2a;  
    }  
}
```



- **DHCP – CONFIGURAÇÃO DO CLIENTE DHCP NO WINDOWS XP**
 - CLICAR COM O BOTÃO DIREITO DO MOUSE SOBRE O ÍCONE “Meus Locais de Rede”
 - SELECIONAR “Propriedades”
 - CLICAR COM O BOTÃO DIREITO DO MOUSE SOBRE O ÍCONE “Conexão Local”
 - SELECIONAR “Propriedades”
 - SELECIONAR “Protocolo TCP/IP” → “Propriedades”
 - NA ABA “Geral”, SELECIONAR O BOTÃO “Obter um endereço IP automaticamente” E TAMBÉM “Obter o endereço dos servidores DNS automaticamente”
 - SELECIONAR O BOTÃO “Ok”



- **DHCP – CONFIGURAÇÃO DO CLIENTE DHCP NO WINDOWS XP**
 - PARA RENOVAR MANUALMENTE O ENDEREÇAMENTO IP NO
 - CLICAR NO BOTÃO “Iniciar” → “Executar” → “cmd”
 - NO PROMPT DE COMANDO, EXECUTAR O COMANDO ABAIXO
 - `ipconfig /renew`
 - O ENDEREÇO MAC PODE SER OBTIDO ATRAVÉS DO COMANDO COMANDO ABAIXO
 - CLICAR NO BOTÃO “Iniciar” → “Executar” → “cmd”
 - NO PROMPT DE COMANDO, EXECUTAR O COMANDO ABAIXO
 - `ipconfig /all | more`



■ BANCO DE DADOS DE ALUGUEL

- O ARQUIVO “/var/lib/dhcp/dhcpd.leases” ARMAZENAM AS INFORMAÇÕES DE TODOS OS ENDEREÇOS Ips QUE ESTÃO ALOCADOS
- ESTE ARQUIVO NÃO DEVE SER ALTERADO MANUALMENTE
- AS INFORMAÇÕES QUE ESTÃO ARMAZENADOS SÃO:
 - ENDEREÇO MAC
 - hardware ethernet
 - INFORMAÇÕES DO ALUGUEL
 - start
 - end
 - tstp (Time Sent To Peer)
 - IDENTIFICAÇÃO DO CLIENTE
 - uid



■ BANCO DE DADOS DE ALUGUEL

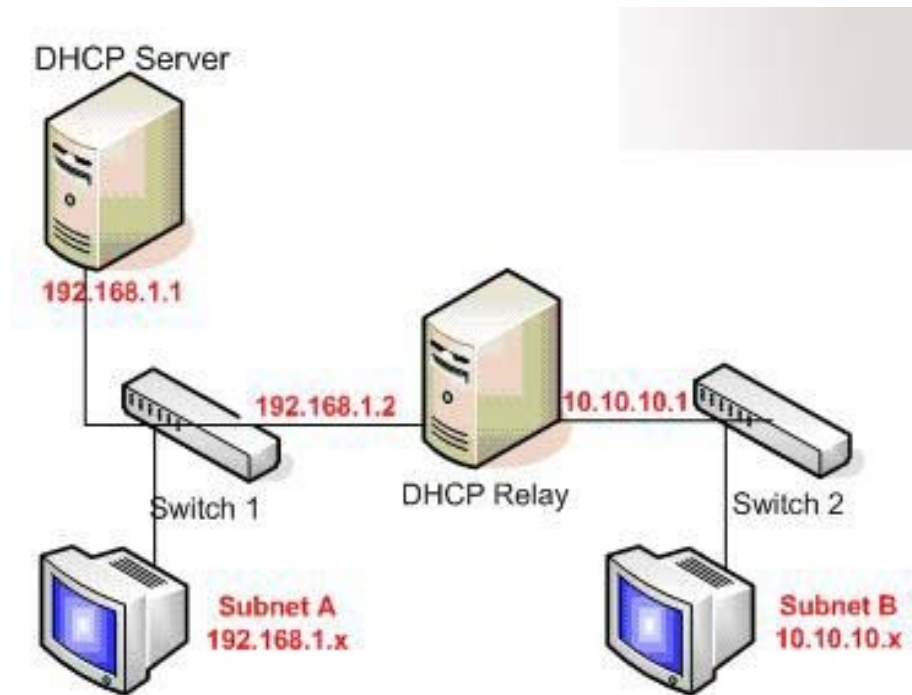
■ EXEMPLO DE BANCO DE DADOS

lease 192.168.0.220

```
[ {  
[   starts 0 2008/03/16 17:25:09;  
[   ends 0 2008/03/16 17:35:09;  
[   tstp 0 2008/03/16 17:35:09;  
[   binding state free;  
[   hardware ethernet 00:18:f3:03:f4:5b;  
[   uid "\001\000\030\363\003\364[";  
[   }  
[ lease 192.168.0.219  
[ {  
[   starts 0 2008/03/16 19:22:01;  
[   ends 0 2008/03/16 19:32:01;  
[   binding state active;  
[   next binding state free;  
[   hardware ethernet 00:a0:d1:3d:00:dd;  
[   uid "\001\000\240\321=\000\335";  
[   client-hostname "pixel";  
[   }  
[ ]
```



- **DHCP AGENT RELAY (DHCP-HELPER)**
 - CENTRALIZAÇÃO DE SERVIDOR DE DHCP



■ DHCP-HELPER

■ INSTALAÇÃO DE SERVIÇO DHCP-HELPER

- APT-GET INSTALL DHCP-HELPER
- ALTERAR O ARQUIVO `"/etc/default/dhcp-helper"`
- `DHCPHELPER_OPTS="" -b eth0 -s 172.16.10.1"`
 - -b INTERFACE ONDE O DHCP-SERVER ESTÁ CONECTADO
 - -s ENDEREÇO IP DO SERVIDOR DHCP
 -
 -



DNS



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - O SERVIÇO DNS CONVERTE NOME DE MÁQUINAS PARA SEUS RESPECTIVOS ENDEREÇO IP E VICE-VERSA
 - A CORRESPONDENCIA ENTRE O NOME E O ENDEREÇO IP É CHAMADO DE MAPEAMENTO E É ORGANIZADO DE FORMA HIERARQUICA
 - EXEMPLO DE MAPEAMENTO

wks01.atm.com.br ↔ 172.16.1.10

□ wks01.atm.com.br É O NOME DO HOST

□ 172.16.1.10 É O ENDEREÇO DO HOST



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - PARA UM HOST SER ENCONTRADO NA REDE, É NECESSÁRIO QUE ELA TENHA UMA IDENTIFICAÇÃO ÚNICA NESTA REDE
 - UM NOME DE HOST É COMPOSTO PELAS SEGUINTE PARTES:
 - EXEMPLO: `www.abc.com.br`
 - `br` – É O DOMÍNIO DE TOPO
 - `com` – É O O DOMÍNIO SECUNDÁRIO
 - `abc` – NOME DO DOMÍNIO LOCAL
 - `www` – NOME DO HOST
 - UM DOMÍNIO É UM NOME QUE É UTILIZADO PARA LOCALIZAR E IDENTIFICAR CONJUNTOS DE COMPUTADORES NA INTERNET. NO EXEMPLO ACIMA, “`abc.com.br`” CORRESPONDE A UM DOMÍNIO E “`www`” É UM HOST DO DOMÍNIO “`abc.com.br`”



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - EXISTEM DIVERSOS DOMÍNIOS CADASTRADOS NA INTERNET
 - CADA SERVIDOR NA INTERNET É RESPONSÁVEL POR MANTER INFORMAÇÕES POR UM OU MAIS DOMÍNIOS
 - SE O SERVIDOR DE DOMÍNIO ESTIVER INDISPONÍVEL, ENTÃO TODOS OS HOSTS ABAIXO DAQUELE DOMÍNIO ESTARÃO INACESSÍVEIS
 - FAQ: <http://registro.br/suporte/faq/faq1.html>



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - OS SERVIDORES DE DNS NA INTERNET FORMAM UMA GRANDE BASE DE DADOS DISTRIBUÍDA E TEM FUNÇÃO CRÍTICA NO FUNCIONAMENTO DA REDE
 - OS SERVIDORES DE DNS ESTÃO ORGANIZADOS DE FORMA HIERÁRQUICA
 - EXISTEM 13 SERVIDORES DE DOMÍNIOS (ROOT SERVER) ESPALHADOS PELO MUNDO QUE TEM A FUNÇÃO DE RESPONDER A TODAS AS REQUISIÇÕES DE RESOLUÇÃO DE DOMÍNIO (public-root.com)
 - ESTES SERVIDORES NÃO RESPONDEM A NENHUMA REQUISIÇÃO, APENAS DELEGAM O TRABALHO A SERVIDORES RESPONSÁVEIS PELOS DOMÍNIOS
 - UM NOME DE DOMÍNIO É LIDO DA DIREITA PARA A ESQUERDA COMO POR EXEMPLO “atm.com.br” LÊ-SE “.br” “.com” “.atm”



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - O NOME “.br” (PONTO br) É CONSIDERADO UM DOMÍNIO PRIMÁRIO (TOP LEVEL DOMAIN - TLD)
 - OUTROS DOMÍNIOS PRIMÁRIOS SÃO:
 - “.net”
 - “.com”
 - “.org”
 - “.edu”
 - “.jp”
 - “.ar”
 - “.py”
 - etc



■ DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS

- O SEGUNDO NOME “.com” CORRESPONDE AO DOMÍNIO SECUNDÁRIO (COUNTRY CODE TLD) QUE RECEBEM PREFIXOS DE CADA PAÍS COMO POR EXEMPLO:

- “.com.br”

- “.net.br”

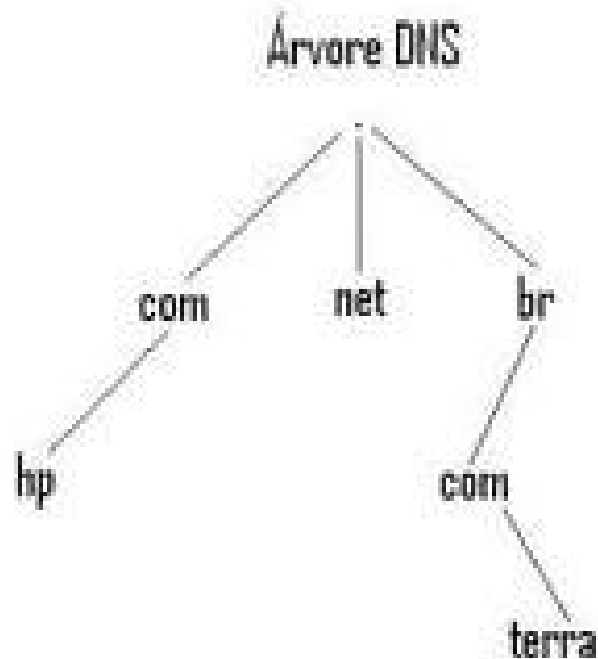
- “.org.br”

- “.edu.br”

- OS DOMÍNIOS “.com”, “.net”, “.org” e “.edu” SÃO SUB-DOMÍNIOS DO DOMÍNIO “br”
- A INTERNIC (EUA) CUIDA DOS REGISTROS DOS DOMÍNIOS RAIZ (“.br”, “.com”, “.org”, “.net”, “.jp”, “.py”, “.ar”)
- O “registro.br” CUIDA DOS REGISTROS DOS DOMÍNIOS COM A EXTENSÃO “.br” (“.com.br”, “.edu.br”, “.org.br”, etc)



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - ÁVORE DE DOMÍNIOS



■ DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS

- O REGISTRO DE DOMÍNIO É FEITO PELO “registro.br” . É NECESSÁRIO POSSUIR DOIS ENDEREÇOS DE DNS PARA ONDE SERÃO ENVIADOS AS CONSULTAS REFERENTES AO SEU DOMÍNIO, ALÉM DE DOCUMENTO DE CNPJ
- O SERVIDOR DE DNS É A AUTORIDADE RESPONSÁVEL PELAS INFORMAÇÕES QUE SÃO PRESTADAS SOBRE O DOMÍNIO, COMO POR EXEMPLO:
 - ☐ ENDEREÇO DE HOST (TYPE A)
 - ☐ SERVIDORES DE EMAIL (TYPE MX)
 - ☐ SERVIDORES DE NOMES (TYPE NS)
 - ☐ REGISTRO DE PONTEIRO (TYPE PTR)
 - ☐ DESCRIÇÃO DO HW E SO DO HOST (TYPE HINFO)
 - ☐ FUNCIONALIDADES DO HOST (TYPE TXT)
 - ☐ APELIDOS (TYPE CNAME)
 - ☐ AUTORIDADE (TYPE SOA)



■ DOMAIN NAME SYSTEM (DNS)

■ INSTALAÇÃO

- apt-get install bind9

■ INICIALIZAÇÃO

- service bind9 [start/stop/restart]

■ ARQUIVOS DE CONFIGURAÇÃO

- OS ARQUIVOS DE CONFIGURAÇÃO ESTÃO LOCALIZADOS NA PASTA /etc/bind

- ARQUIVO DE CONFIGURAÇÃO PRINCIPAL

 - /etc/bind/named.conf

 - include “/etc/bind/named.conf.options”

 - include “/etc/bind/named.conf.local”

 - include “/etc/bind/named.conf.default-zone”



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - UM SERVIDOR DE DNS PODE SER:
 - PRIMÁRIO, AUTORIDADE POR UM DOMÍNIO ONDE AS INCLUSÕES, ALTERAÇÕES E EXCLUSÃO DE REGISTROS DO DOMÍNIO SÃO REALIZADAS
 - SECUNDÁRIO, FUNCIONA COMO BACKUP DO SERVIDOR PRIMÁRIO ATUALIZA SEUS REGISTRO A PARTIR DO SERVIDOR PRIMÁRIO, PODE RESPONDER A REQUISIÇÕES
 - CACHING-ONLY, NÃO É RESPONSÁVEL POR NENHUM DOMÍNIO, APENAS EFETUA CONSULTA E RETORNA OS RESULTADOS, MANTENDO UM CACHE LOCAL PARA MELHORAR O DESEMPENHO DA RESOLUÇÃO DE NOMES PARA OS CLIENTES LOCAIS UTILIZANDO O SEU CACHE



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - SE O ARQUIVO DE CONFIGURAÇÃO `named.conf.local` ESTIVER EM BRANCO, ENTÃO O SERVIDOR ESTARÁ ATUANDO COMO UM SERVIDOR DNS CACHE ONLY
 - SE O SERVIDOR LOCAL É RESPONSÁVEL POR ALGUMA ZONA, ENTÃO DEVERÁ CONTER A DEFINIÇÃO DA ZONA CONFORME DESCRITO NO PRÓXIMO SLIDE



■ DOMAIN NAME SYSTEM (DNS)

■ ARQUIVOS DE CONFIGURAÇÃO DE UMA ZONA

□ /etc/bind/named.conf.local

#definição da zona atm.org.br

zone "atm.org.br" {

type master;

file "/etc/bind/db.atm.org.br";

};

#definição do reverso da zona atm.org.br

zone "10.168.192.in-addr.arpa" in {

type master;

file "/etc/bind/db.reverse.atm.org.br";

};

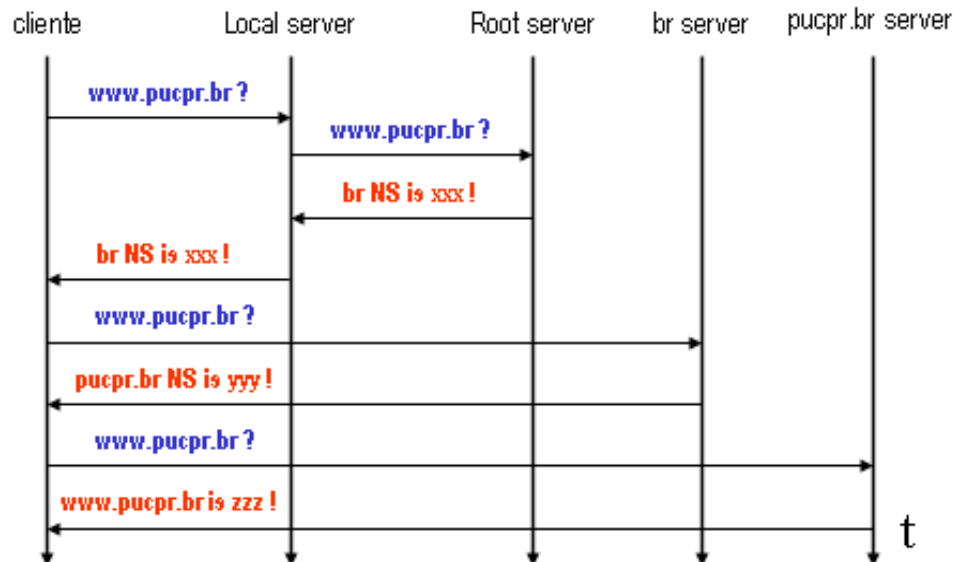


■ DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS

■ CONSULTAS DNS

□ CONSULTA ITERATIVA

O CLIENTE DNS PODE RECEBER DO SERVIDOR LOCAL UMA RESPOSTA PARCIAL, ASSIM ELE TERÁ DE CONTACTAR SUCESSIVAMENTE OUTROS SERVIDORES DNS PARA CONSEGUIR RESOLVER O NOME DESEJADO

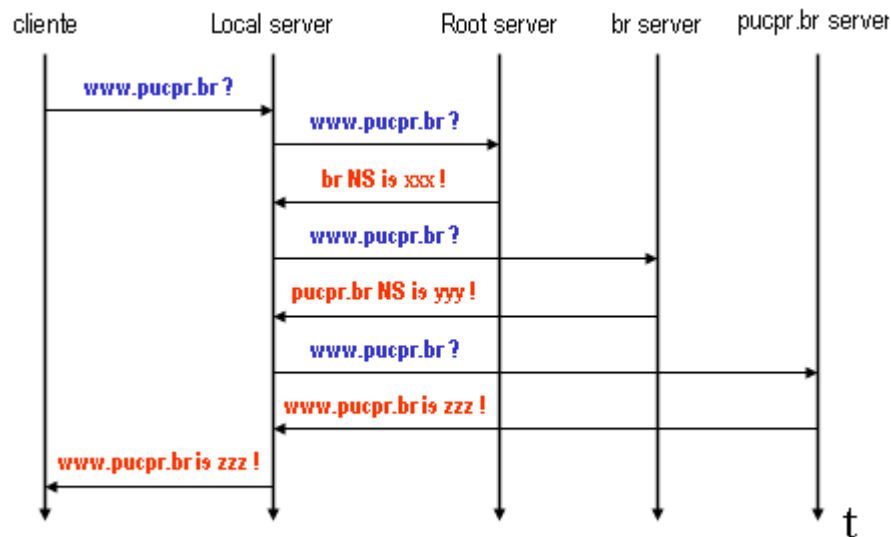


■ DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS

■ CONSULTAS DNS

□ CONSULTA RECURSIVA

O SERVIDOR LOCAL SE ENCARREGA DE ENCAMINHAR A CONSULTA DO CLIENTE A TODOS OS SERVIDORES DNS NECESSÁRIOS, ATÉ QUE A CONSULTA SEJA RESOLVIDA, DEVOLVENDO AO CLIENTE SOMENTE A RESPOSTA FINAL



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - ARQUIVOS DE ZONA
 - CADA DOMÍNIO INTERNET SOB RESPONSABILIDADE DE UM SERVIDOR DNS POSSUI UM ARQUIVO DE CONFIGURAÇÃO QUE MANTÉM INFORMAÇÕES SOBRE O GRUPO DE MÁQUINAS E OS SEUS ENDEREÇOS IP
 - O ARQUIVO DE CONFIGURAÇÃO TAMBÉM É CONHECIDO COMO “**ARQUIVO DE ZONA**” (**ZONE FILE**)
 - CADA DOMÍNIO DEVE POSSUIR TAMBÉM UM “**ARQUIVO DE ZONA REVERSA**” QUE RELACIONA OS ENDEREÇOS IP AOS NOMES EXISTENTES NO DOMÍNIO



■ DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS

■ EXEMPLO DE ARQUIVO DE ZONA

\$TTL 43200 ; 12 hours

atm.org.br. IN SOA ns1.atm.org.br. postmaster@atm.org.br. (

1 ; Serial number (increase it after edit)

10800 ; Refresh after 3 hours (3 x 3600 sec)

3600 ; Retry after 1 hour (1 x 3600 sec)

604800 ; Expire after 1 week (7 x 24 x 3600 sec)

86400) ; Minimum TTL of 1 day (24 x 2600 sec)

; Name server for this domain

atm.org.br. IN NS ns1.atm.org.br.

; Mail server for this domain

atm.org.br. IN MX 10 alfa.atm.org.br.

; Addresses for local names

localhost.atm.org.br IN A 127.0.0.1

ns1.atm.org.br. IN A 192.168.10.80

TXT "Servidor de nomes primario"

HINFO "PC P4" "Linux Slackware 8"

alfa.atm.org.br. IN A 192.168.10.50

; Aliases

mailer1.atm.org.br. IN CNAME alfa.atm.org.br.



■ DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS

■ EXEMPLO DE ARQUIVO DE ZONA REVERSA

\$TTL 43200 ; 12 hours

10.168.192.in-addr.arpa. IN SOA ns1.atm.org.br. postmaster@atm.org.br.(

1 ; Serial number (increase it after edit)

10800 ; Refresh after 3 hours (3 x 3600 sec)

3600 ; Retry after 1 hour (1 x 3600 sec)

604800 ; Expire after 1 week (7 x 24 x 3600 sec)

86400) ; Minimum TTL of 1 day (24 x 3600 sec)

; Name servers

10.168.192.in-addr.arpa. IN NS ns1.atm.org.br.

; Addresses point to canonical name

80.10.168.192.in-addr.arpa. IN PTR ns1.atm.org.br.

1.10.168.192.in-addr.arpa. IN PTR alfa.atm.org.br.



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - TIPOS DE REGISTROS
 - SOA
 - INDICA QUE É O RESPONSÁVEL POR ESTA ZONA, ISTO É A AUTORIDADE
 - NS
 - INDICA UM SERVIDOR DE NOMES PARA ESTA ZONA
 - MX
 - INDICA UM SERVIDOR DE E-MAIL PARA ESTA ZONA
 - A
 - INDICA O ENDEREÇO IP DE UM DADO NOME DO DOMÍNIO (RESOLUÇÃO DIRETA)



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - **DESCRIÇÃO DOS REGISTROS**
 - TXT
 - DESCRIÇÃO DO HOST
 - HINFO
 - INDICA DADOS DE SOFTWARE E HARDWARE DO HOST
 - CNAME
 - INDICA UM APELIDO (SINÔNIMO) DE NOME DE DOMÍNIO
 - PTR
 - INDICA O NOME DE DOMÍNIO RELATIVO A UM DADO ENDEREÇO IP (RESOLUÇÃO REVERSA)



■ EXERCÍCIO

■ CADASTRAR TODOS OS ELEMENTOS DE REDE NOS ARQUIVOS PRINCIPAL E REVERSO

■ PRINCIPAL

jose-prado.atm.org.br.	IN	A	192.168.10.50
carlos.atm.org.br.	IN	A	192.168.10.51
wks-01.atm.org.br.	IN	A	192.168.10.52



■ REVERSO

50.10.168.192.in-addr.arpa.	IN	PTR	jose-prado.atm.org.br.
51.10.168.192.in-addr.arpa.	IN	PTR	carlos.atm.org.br.
52.10.168.192.in-addr.arpa.	IN	PTR	wks-01.atm.org.br.



■ EXERCÍCIO

■ CADASTRAR A DESCRIÇÃO DOS HOSTS

■ PRINCIPAL

jose-prado.atm.org.br.	IN	A	192.168.10.50	TXT	“Host do Jose Prado”	HINFO	“Pentium II 90 mhz” “mac os”
carlos.atm.org.br.	IN	A	192.168.10.51	TXT	“Host do Carlos Alberto - Contab”	HINFO	“core II DUO” “Linux”
wks-01.atm.org.br.	IN	A	192.168.10.52	TXT	“Host do Trabalho – Folha pgto”	HINFO	“Pentium IV 2.4 Ghz” “Windows”



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - UTILITÁRIOS DE CONSULTA
 - AO INSERIR UM NOME NO BROWSER, ESTE FAZ UMA CONSULTA AO SERVIDOR DNS LOCAL. SE O SERVIDOR NÃO CONSEGUIR UMA RESPOSTA, INICIA UM PROCESSO DE PESQUISA, ENQUANTO ISSO O BROWSER PERMANECE AGUARDANDO UMA RESPOSTA
 - A RESOLUÇÃO DE NOMES TAMBÉM PODE SER REALIZADA ATRAVÉS DE APLICAÇÕES ESPECÍFICAS COMO “dig” e “nslookup”. ESTE ÚLTIMO ESTÁ OBSOLETO SENDO SUBSTITUÍDO PELO “dig”



- DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS
 - UTILITÁRIOS DE CONSULTA

```
# dig alfa.atm.org.br
```

Linha de comando

```
; <<>> DiG 9.6-ESV-R3 <<>> alfa.atm.org.br  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50075  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
```

Cabeçalho da resposta

```
;; QUESTION SECTION:  
;alfa.atm.org.br.      IN      A
```

Pergunta que foi realizada

```
;; ANSWER SECTION:  
alfa.atm.org.br.      43200 IN      A      192.168.10.50
```

Resposta recebida

```
;; AUTHORITY SECTION:  
atm.org.br.           43200 IN      NS      ns1.atm.org.br.
```

Autoridade que respondeu a pergunta

```
;; ADDITIONAL SECTION:  
ns1.atm.org.br.       43200 IN      A      192.168.10.80
```

Informações sobre a autoridade

```
;; Query time: 1 msec  
;; SERVER: 127.0.0.1#53(127.0.0.1)  
;; WHEN: Mon Jul 4 22:48:12 2011  
;; MSG SIZE rcvd: 83
```

Relatório de encerramento



■ DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS

■ UTILITÁRIOS DE CONSULTA

□ COMANDO DIG

□ dig [opção] [@servidor] nome [tipo de registro]

□ DESCRIÇÃO DOS PARÂMETROS

□ @127.0.0.1 ESPECIFICA QUE O SERVIDOR COM IP 127.0.0.1 SERÁ UTILIZADO COMO SERVIDOR DE DNS EM VEZ DE UTILIZAR O SERVIDOR APONTADO PELOS ARQUIVO DE CONFIGURAÇÃO /etc/resolv.conf

□ Nome CORRESPONDE AO NOME A SER RESOLVIDO

□ TIPO DE REGISTRO CORRESPONDE A

□ ns – Servidor de nomes do dominio

□ mx – Servidores de correio do dominio



■ DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS

■ UTILITÁRIOS DE CONSULTA

□ COMANDO DIG

□ dig [opção] [@servidor] nome [tipo de registro]

□ DESCRIÇÃO DOS PARÂMETROS

□ TIPO DE REGISTRO CORRESPONDE A

□ txt – Descreve a função do Servidor

□ hinfo – Informação de Hardware e Sistema Operacional

□ soa – Autoridade do dominio



■ DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS

■ UTILITÁRIOS DE CONSULTA

□ COMANDO DIG

□ `dig [opção] [@servidor] nome [tipo de registro]`

□ Exemplos

□ `dig alfa.atm.org.br`

□ `dig @127.0.0.1 atm.org.br mx`

□ `dig atm.org.br ns`

□ `dig alfa.atm.org.br any`

□ `dig alfa.atm.org.br hinfo`

□ `dig alfa.atm.org.br txt`

□ `dig atm.org.br soa`

□ `dig -x 192.168.10.80 ; resolução reversa`



■ DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS

■ UTILITÁRIOS DE CONSULTA

□ COMANDO NSLOOKUP

□ ACESSO A CONSOLE

□ nslookup

□ ALTERANDO O TIPO DE REGISTRO

□ set type=MX

□ ALTERANDO O SERVIDOR DE DNS DEFAULT

□ Server 127.0.0.1

□ REALIZANDO PESQUISA

□ > uol.com.br

□ ATIVANDO DEBUG

□ set debug/nodebug

□ SAINDO DO PROMPT

□ exit



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - SE O SERVIDOR DNS LOCAL NÃO TIVER ACESSO AOS SERVIDORES “root” MAS POSSA ACESSAR OUTRO SERVIDOR DNS, ENTÃO PODEMOS UTILIZAR UMA CONFIGURAÇÃO DE “forwarding” QUE CONSISTE EM ENCAMINHAR A SOLICITAÇÃO PARA OUTRO SERVIDOR DNS E GUARDAR O RESULTADO EM UM CACHE LOCAL
 - A CONFIGURAÇÃO DE “forwarding” É REALIZADA ADICIONANDO A ENTRADA ABAIXO NO ARQUIVO `named.conf`

```
options {  
    forward only ;  
    forwarders { a.b.c.d; e.f.g.h;};  
};  
};
```



■ DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS

- PARA LIMITAR O ACESSO AO SERVIDOR DE DNS, UTILIZADO A CLAUSULA “allow-query” DENTRO DO ARQUIVO named.conf

```
options {  
    forward only ;  
    forwarders { a.b.c.d; e.f.g.h;};  
    allow-query {127.0.0.1;192.168.10.0/24;};  
};
```



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - PARA AUMENTAR A DISPONIBILIDADE DO SERVIÇO, PODEMOS MONTAR DIVERSOS SERVIDORES SECUNDÁRIOS
 - APÓS A DEFINIÇÃO DE UM DOMÍNIO, CINCO PARAMETROS SÃO DECLARADOS PARA CONTROLAR A SINCRONIZAÇÃO ENTRE OS SERVIDORES PRIMÁRIO E O SECUNDÁRIO

atm.org.br. IN SOA ns1.atm.org.br. postmaster@atm.org.br. (
1 ; Serial number (increase it after edit)
10800 ; Refresh after 3 hours (3 x 3600 sec)
3600 ; Retry after 1 hour (1 x 3600 sec)
604800 ; Expire after 1 week (7 x 24 x 3600 sec)
86400) ; Minimum TTL of 1 day (24 x 2600 sec)



■ DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS

■ EXPLANAÇÃO DOS PARAMETROS

□ SERIAL NUMBER

□ ESTE NÚMERO DETERMINA A SINCRONIZAÇÃO ENTRE O PRIMÁRIO E O SECUNDÁRIO

□ EM CADA ALTERAÇÃO NO PRIMÁRIO ESTE NÚMERO DEVE SER INCREMENTADO E O SERVIÇO DEVE SER REINICIADO

□ REFRESH TIME

□ PERÍODO TEMPO QUE O SECUNDÁRIO DEVE AGUARDAR ENTRE ATUALIZAÇÕES NORMAIS

□ RETRY TIME

□ SE O SERVIDOR PRIMÁRIO NÃO RESPONDER A TENTATIVA DE TRANSFÊNCIA DE ZONA, O SECUNDÁRIO IRÁ AGUARDAR ESTE INTERVALOR DE TEMPO PARA TENTAR NOVAMENTE



■ DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS

■ EXPLANAÇÃO DOS PARAMETROS

□ EXPIRE TIME

□ PERÍODO MÁXIMO DE TEMPO QUE O SECUNDÁRIO PODE ASSUMIR A FUNÇÃO DE PRIMÁRIO DEVIDO A AUSENCIA DO SERVIDOR PRIMÁRIO

□ APÓS EXPIRADO ESTE TEMPO, O DOMÍNIO DEIXARÁ DE SER VISTO NA INTERNET

□ TTL MÍNIMO

□ TEMPO MÍNIMO ANTES DE DEVOLVER O DOMÍNIO PARA O SERVIDOR PRIMÁRIO QUANDO ELE RETORNAR



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - OS SERVIDORES PRIMARIO E SECUNDÁRIO DEVEM SER CONFIGURADOS CORRETAMENTE PARA TRABALHAREM COM FUNÇÃO QUE FOI ATRIBUÍDA.
 - O SERVIDOR MASTER DEVE POSSUIR A SEGUINTE CONFIGURAÇÃO

```
zone "atm.org.br" {  
    type master;  
    file "/etc/bind/db.atm.org.br";  
    allow-transfer { 192.168.10.10; };  
};  
zone "10.168.192.in-addr.arpa" in {  
    type master;  
    file "/etc/bind/db.reverse.atm.org.br";  
    allow-transfer { 192.168.10.10; };  
};
```



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - PARA AUMENTAR A DISPONIBILIDADE DO SERVIÇO, PODEMOS MONTAR DIVERSOS SERVIDORES SECUNDÁRIOS
 - O SERVIDOR SLAVE DEVE POSSUIR A SEGUINTE CONFIGURAÇÃO

```
zone "atm.org.br" {  
    type slave;  
    file "/etc/bind/db.atm.org.br";  
    masters { 192.168.10.1; };  
};  
zone "10.168.192.in-addr.arpa" in {  
    type master;  
    file "/etc/bind/db.reverse.atm.org.br";  
    masters { 192.168.10.1; };  
};
```



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - PARA AUMENTAR A DISPONIBILIDADE DO SERVIÇO, PODEMOS MONTAR DIVERSOS SERVIDORES SECUNDÁRIOS
 - O SERVIDOR SLAVE DEVE POSSUIR A SEGUINTE CONFIGURAÇÃO

```
zone "atm.org.br" {  
    type slave;  
    file "/etc/bind/db.atm.org.br";  
    masters { 192.168.10.1; };  
};  
zone "10.168.192.in-addr.arpa" in {  
    type master;  
    file "/etc/bind/db.reverse.atm.org.br";  
    masters { 192.168.10.1; };  
};
```



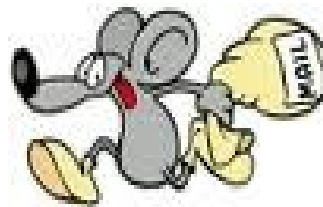
- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - UMA VEZ QUE OS ARQUIVOS FORAM MODIFICADOS, PODEMOS REINICIAR O SERVIÇO NO PRIMÁRIO
 - NO SERVIDOR SECUNDÁRIO IREMOS REMOVER OS ARQUIVOS DE CONFIGURAÇÃO DOS DOMÍNIOS, POIS, QUANDO O SERVIÇO FOR INICIADO, SERÃO TRAZIDOS DO SERVIDOR PRIMÁRIO (SINCRONIZADOS)
 - ALTERAR AS PERMISSÕES DA PASTA /etc/bind UTILIZANDO O COMANDO ABAIXO
 - `chmod 775 /etc/bind`
 - INICIAR O SERVIÇO DO SECUNDÁRIO. DURANTE A INICIALIZAÇÃO, OS ARQUIVOS DE DOMÍNIOS E REVERSO SERÃO SINCRONIZADOS. AS MENSAGENS DE SINCRONIZAÇÃO PODEM SER LIDAS NO ARQUIVO /var/log/syslog



- **DOMAIN NAME SYSTEM (DNS) – CONCEITOS BÁSICOS**
 - TODAS ALTERAÇÕES DEVEM SER REALIZADAS NO SERVIDOR PRIMÁRIO
 - PERIODICAMENTE O SERVIDOR SECUNDÁRIO IRÁ VERIFICAR O “SERIAL NUMBER” DO PRIMÁRIO, CASO ESTE NÚMERO SEJA SUPERIOR AO SEU, ENTÃO SERÁ REALIZADA A TRANSFERENCIA DE ZONA.
 - PARA ACELERAR A TRANSFERENCIA DE ZONA, PODEMOS DIGITAR O COMANDO ABAIXO NO SERVIDOR SECUNDÁRIO
 - # rndc retransfer “nome da zona”
 - # rndc retransfer atm.org.br



POSTFIX



POSTFIX



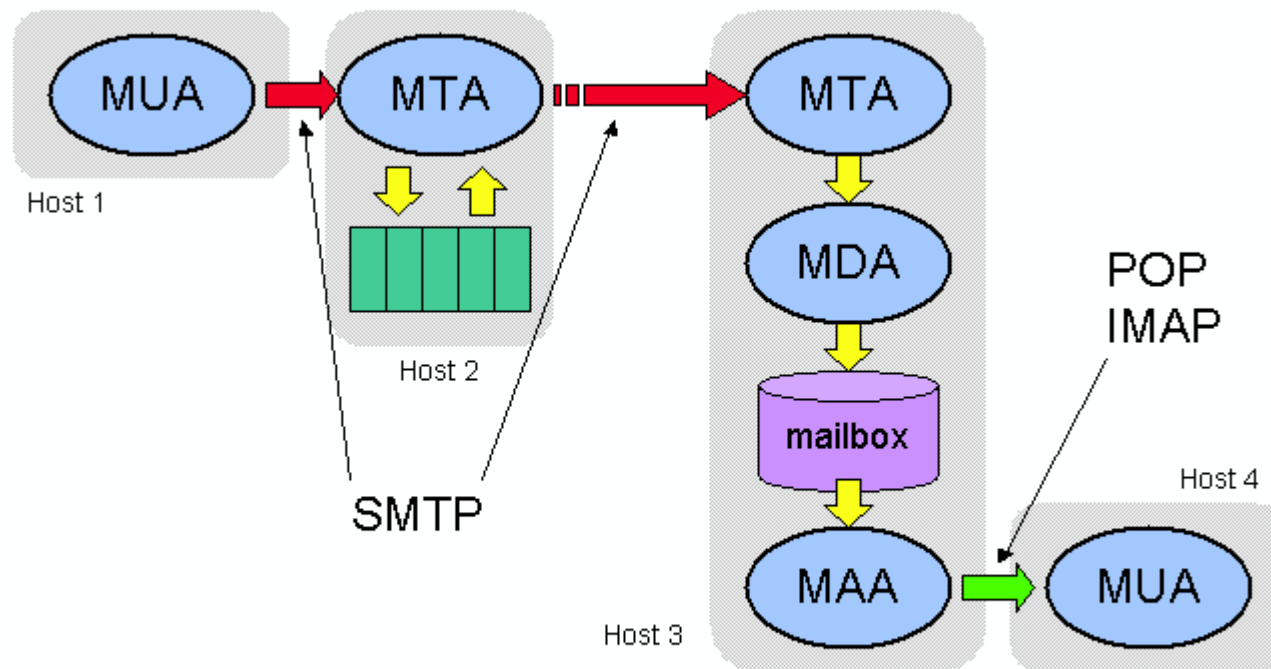
■ CORREIO ELETRÔNICO

■ CARACTERÍSTICAS GERAIS

- UTILIZA O PROTOCOLO SMTP (SIMPLE MAIL TRANSFER PROTOCOL) PARA TRANSFERÊNCIA DE MENSAGENS ATRAVÉS DA INTERNET
- UTILIZA O PROTOCOLO TCP COM PORTA 25
- EXISTEM DIVERSOS SERVIDORES DE EMAIL:
 - SENDMAIL (MAIS ANTIGO)
 - EXIM
 - POSTFIX
 - QMAIL
 - MICROSOFT EXCHANGE SERVER



- CORREIO ELETRÔNICO
- COMPONENTES DE CORREIO ELETRÔNICO



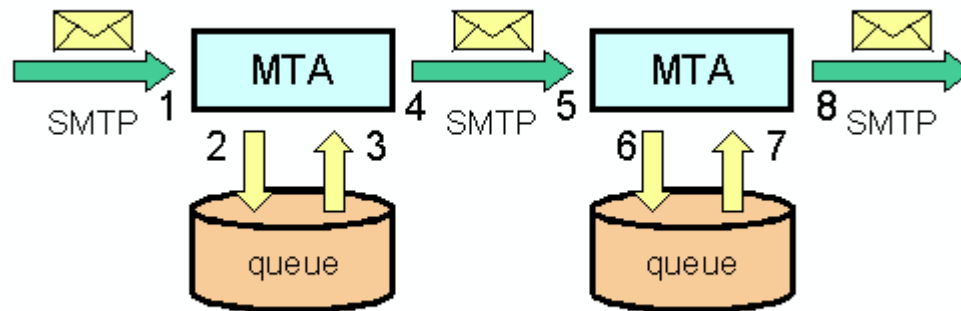
http://www.ppgia.pucpr.br/~maziero/doku.php/espec:servico_de_e-mail



- **CORREIO ELETRÔNICO**
- **DESCRIÇÃO DOS COMPONENTES**
- **MUA – MAIL USER AGENT**
 - PROGRAMA UTILIZADO PELO USUÁRIO PARA COMPOR O EMAIL – NETSCAPE, OUTLOOK, EUDORA, ETC
- **MTA – MAIL TRANSPORT AGENT**
 - RECEBE O EMAIL DO MUA E ENVIA PARA OUTROS MTA PARA QUE SEJA ENTREGUE AO DESTINATÁRIO – SENDMAIL, QMAIL, POSTFIX
- **MDA – MAIL DELIVERY AGENT**
 - RECEBE O EMAIL DO MTA E DEPOSITA NA CAIXA DE CORREIO DO USUÁRIO – NO LINUX É O PROCMAIL
- **MAA – MAIL ACCESS AGENT**
 - PERMITE AO MUA O ACESSO A CAIXA POSTAL DO USUÁRIO – POP3 E IMAP



- **CORREIO ELETRÔNICO**
- **FUNCIONAMENTO STORE AND FORWARD**
- O MTA RECEBE A MENSAGEM INTEGRALMENTE E ARMAZENA TEMPORARIAMENTE EM UMA PASTA, PARA ENTÃO REPASSÁ-LA ADIANTE PARA UMA OUTRO MTA OU PARA O MDA CASO O DESTINO SEJA LOCAL
- ESTE PROCEDIMENTO GARANTE A ENTREGA AO DESTINATÁRIO, SEM POSSIBILIDADE DE PERDA NA TRANSMISSÃO



http://www.ppgia.pucpr.br/~maziero/doku.php/espec:servico_de_e-mail



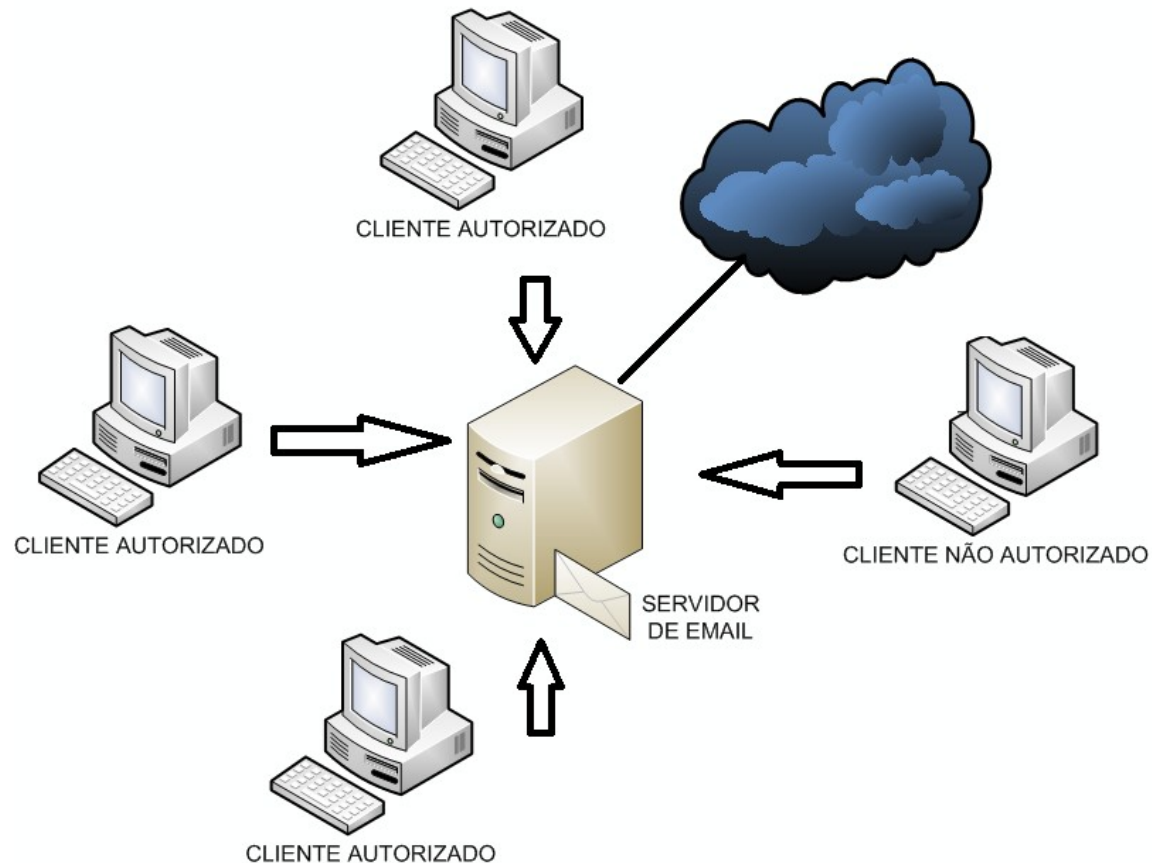
■ CORREIO ELETRÔNICO

■ RELAY DE MENSAGENS

- AS MENSAGENS SÃO ELABORADAS E ENVIADAS AO SERVIDOR EMAIL DE UM DOMÍNIO UTILIZANDO UM MUA (OUTLOOK, WEBMAIL, ETC)
- OS SERVIDORES DE EMAIL SÃO UTILIZADOS PARA MANDAR MENSAGENS PARA FORA DE UM DOMÍNIO
- SOMENTE CLIENTES AUTORIZADOS PODEM SOLICITAR AO SERVIDOR DE EMAIL DO DOMÍNIO LOCAL PARA ENCAMINHAR MENSAGENS PARA OUTRO DOMÍNIO
- QUANDO CLIENTES NÃO AUTORIZADOS TENTAM ENVIAR ENVIAR MENSAGENS ATRAVÉS DO SERVIDOR DE EMAIL LOCAL, EXISTE UM PROBLEMA DE SEGURANÇA.



- CORREIO ELETRÔNICO
- RELAY DE MENSAGENS



- **CORREIO ELETRÔNICO**
- O PROTOCOLO SMTP (SIMPLE MAIL TRANSPORT PROTOCOL) É O RESPONSÁVEL PELA TRANSPORTE DA MENSAGENS ENTRE MUA E MTA LOCAL E DESTE ATÉ O DESTINO FINAL

```
#[root@arara postfix]# telnet localhost 25 -----> Usuário digita o comando
Trying 127.0.0.1... -----> Mensagem do LINUX
Connected to localhost (127.0.0.1).-----> Mensagem do LINUX
Escape character is '^]'. -----> Mensagem do LINUX
220 arara.intranet.empresa ESMTP Postfix (2.3.3) (Mandriva Linux) -----> Mensagem de boas vindas do POSTFIX
mail from: bill@microsoft.com -----> Usuário digita o comando
250 2.1.0 Ok -----> Mensagem do POSTFIX
rcpt to: puc -----> Usuário digita o comando
250 2.1.5 Ok -----> Mensagem do POSTFIX
data -----> Usuário digita o comando
354 End data with <CR><LF>.<CR><LF> -----> Mensagem do POSTFIX
subject: primeira mensagem -----> Usuário digita o comando
Esta e a primeira mensagem enviada atraves do correio eletrónico.-----> Usuário digita o comando
.-----> Usuário digita o comando
250 2.0.0 Ok: queued as 77AEB3E0DE -----> Mensagem do POSTFIX
quit -----> Usuário digita o comando
221 2.0.0 Bye -----> Mensagem do POSTFIX
Connection closed by foreign host -----> Mensagem do LINUX
```



- **CORREIO ELETRÔNICO**

- mail from: bill@microsoft

- EMISSOR DA MENSAGEM

- rcpt to: puc@localhost

- RECEPTOR DA MENSAGEM

- data

- INICIO DA MENSAGEM

- subject: primeira mensagem

- TÍTULO DA MENSAGEM

- Corpo do Texto

- . (ponto)FINALIZADOR DO CORPO DA MENSAGEM

- quit

- FINALIZADOR DE PROTOCOLO



- **CORREIO ELETRÔNICO - POSTFIX**
- PARA INSTALAR O POSTFIX, É NECESSÁRIO SEGUIR O ROTEIRO ABAIXO
- EXECUTAR O COMANDO ABAIXO
apt-get install postfix
- UM GUIA DE CONFIGURAÇÃO PODE SER ENCONTRADO EM:
http://www.postfix.org/STANDARD_CONFIGURATION_README.html
<http://www.postfix.org/postconf.5.html>



- **CORREIO ELETRÔNICO**
- QUANDO APRESENTADO A TELA ABAIXO, SELECIONAR A OPÇÃO “Site Internet” E DEPOIS “OK”

```
Por favor escolha o tipo de configura  o do servidor de mail que melhor se adequa   s suas necessidades

Sem configura  o:
  Deve ser escolhido para deixar a configura  o actual inalterada.
Site Internet:
  O mail   enviado e recebido directamente utilizando SMTP.
Internet utilizando smarthost:
  O mail   recebido directamente utilizando SMTP ou correndo um utilit rio
  como o fetchmail. O mail que sai   enviado utilizando um smarthost.
Sistema sat lite
  Todo o mail   enviado para outra m quina, chamada "smarthost".
Apenas entrega local:
  O  nico mail entregue   o mail para os utilizadores locais. N o existe rede.

Tipo geral de configura  o de mail:

Sem configura  o
Site Internet
Internet com smarthost
Sistema sat lite
Apenas local

<Ok>                                <Cancelar>
```



- **CORREIO ELETRÔNICO**

- **DESCRIÇÃO DOS TIPOS DE SERVIDORES**

- Internet Site

- SERVIDOR QUE ENVIA E RECEBE MENSAGENS DE CORREIO DIRETAMENTE

- Com smarthost

- APENAS RECEBE MENSAGENS DE CORREIO, FICANDO A CARGO DE OUTRO SERVIDOR ENVIAR A MENSAGENS DE CORREIO

- Sistema Satélite

- MAIS LIMITA, ENVIA MENSAGENS ATRAVÉS DE OUTRA MÁQUINA E NÃO RECEBE

- Apenas Local

- PERMITE QUE APENAS USUÁRIOS LOCAIS TROQUEM MENSAGENS



- **CORREIO ELETRÔNICO - POSTFIX**
- QUANDO SOLICITADO O NOME DO SERVIDOR, INFORMAR O NOME DO DOMÍNIO AO QUAL O SERVIDOR SERÁ RESPONSÁVEL

O "nome de mail" é o nome do domínio utilizado para "qualificar" _TODOS_ os endereços de mail sem um nome de domínio. Isto inclui mail de e para <root>: favor não fazer a sua máquina enviar mail de root@exemplo.org a menos que root@exemplo.org lhe tenha dito para o fazer.

Este nome será também utilizado por outros programas. Deve ser o único, nome de domínio completo (FQDN).

Por isso, se um endereço de mail numa máquina local for foo@exemplo.org, o valor correcto para esta opção deve ser exemplo.org.

Nome de mail do sistema:

servidor-debian.atm.com.br

<Ok>

<Cancelar>



- **CORREIO ELETRÔNICO - POSTFIX**
- COM BASE NAS INFORMAÇÕES OBTIDAS ANTERIORMENTE, SERÁ GERADO O ARQUIVO DE CONFIGURAÇÃO “/etc/postfix/main.cf”
- DEPOIS DE CONCLUÍDO A INSTALAÇÃO DO SERVIDOR, PODEMOS ENVIAR UMA MENSAGEM PARA QUALQUER USUÁRIO LOCAL, UTILIZANDO O COMANDO ABAIXO:

mail user1@localhost

Subject: teste com mensagem

Corpo da mensagem

Corpo da mensagem

. (ponto na primeira coluna + enter) → encerramento da mensagem



■ CORREIO ELETRÔNICO - POSTFIX

■ DESCRIÇÃO DO ARQUIVO MAIN.CF

myhostname = servidor-debian.atm.com.br

alias_maps = hash:/etc/aliases

alias_database = hash:/etc/aliases

myorigin = atm.com.br

mydestination = atm.com.br, localhost.atm.com.br, , localhost

mynetworks = 127.0.0.0/8

mailbox_command = procmail -a "\$EXTENSION"

mailbox_size_limit = 0

recipient_delimiter = +

inet_interfaces = all



- **CORREIO ELETRÔNICO - POSTFIX**

- **DESCRIÇÃO DO ARQUIVO MAIN.CF**

- myhostname

- NOME DA MÁQUINA QUE ESTÁ EXECUTANDO O POSTFIX, POR EXEMPLO - aguia.atm.com.br

- myorigin

- DEFINE O DOMÍNIO QUE APARECE NAS MENSAGENS QUE SÃO ENVIADAS, POR EXEMPLO - atm.com.br

- mydestination

- DEFINIE O DOMÍNIO QUE O POSTFIX ESTÁ HABILITADO A RECEBER MENSAGENS POR EXEMPLO: localhost, aguia.atm.com.br, atm.com.br, localhost.atm.com.br



- **CORREIO ELETRÔNICO - POSTFIX**

- **DESCRIÇÃO DO ARQUIVO MAIN.CF**

- mynetworks

- DEFINE AS REDES QUE PODEM UTILIZAR O POSTFIX PARA ENVIAR MENSAGENS, POR EXEMPLO: 127.0.0.0/8 172.20.0.0/16 10.0.0.0/24

- inet_interfaces

- DEFINE OS ENDEREÇOS DAS INTERFACES NA QUAL O POSTFIX ESTARÁ ESPERANDO MENSGENS, POR EXEMPLO: 127.0.0.1 172.16.10.1

- O DEFAULT É “all”



- **CORREIO ELETRÔNICO - POSTFIX**
- ENVIANDO MENSAGENS
- PARA ENVIAR UMA MENSAGEM, PODEMOS UTILIZAR A APLICAÇÃO “mail” (MUA), CONFORME MOSTRADO ABAIXO

```
# mail usuario_destino@localhost -s “titulo da mensagem”
```

```
Bom dia camada
```

```
Esta é uma mensagem de teste
```

```
.
```

```
Cc:
```

- PARA LER UM EMAIL

```
# mail -u user1 (quando root)
```

```
$ mail (ler as mensagens atuais pelo proprio usuário)
```



- **CORREIO ELETRÔNICO - POSTFIX**
- **ARMAZENAMENTO DE MENSAGEM**
 - O MDA IRÁ DEPOSITAR AS MENSAGENS NA PASTA /var/mail/
 - CADA USUÁRIO POSSUI UM ARQUIVO ONDE AS MENSAGENS SÃO ADICIONADAS AO FINAL DESTE ARQUIVO, COMO POR EXEMPLO: /var/mail/airton
 - SOMENTE O DONO DO ARQUIVO E O “root” TEM ACESSO AOS ARQUIVOS DA PASTA /var/mail, GARANTINDO ASSIM A PRIVACIDADE
 - ATRAVÉS DE UM MUA AS MENSAGENS PODEM SER REMOVIDAS DESTE ARQUIVO
 - OUTRAS FORMAS DE UTILIZAR O PROGRAMA MAIL É DESCRITO NO SITE “<http://www.devin.com.br/mail-linha-de-comando/>”



- **CORREIO ELETRÔNICO - POSTFIX**
- COMANDOS DE CONTROLE DO POSTFIX
 - # postfix start
 - INICIALIZA O POSTFIX
 - # postfix stop
 - FINALIZA O POSTFIX
 - # postfix reload
 - RECARREGA OS ARQUIVOS DE CONFIGURÇÃ
 - # postfix check
 - REALIZA A VERIFICAÇÃO DO ARQUIVO DE CONFIGURAÇÃO
 - # postfix flush
 - FORÇA A ENTREGA DE MENSAGENS PENDENTES



- **CORREIO ELETRÔNICO - POSTFIX**
- COMANDOS DE GERENCIAMENTO DE FILA DE CORREIO
- `postqueue` - MOSTRA AS FILAS DE MENSAGENS DO SISTEMA OPERACIONAL

`postqueue -p`

`postqueue: warning: Mail system is down -- accessing queue directly`

-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-----

D4F8F2EA03 137 Mon Jul 18 20:56:50 root

user1@atm.com.br



- **CORREIO ELETRÔNICO - POSTFIX**
- COMANDOS DE GERENCIAMENTO DE FILA DE CORREIO
- postsuper – REMOVE MENSAGENS DA FILA

postsuper -d D4F8F2EA03 → (valor obtido em postqueue -p)

postsuper: D4F8F2EA03: removed

postsuper: Deleted: 1 message

postsuper -d all (remove todas as mensagens da fila)



- **CORREIO ELETRÔNICO - POSTFIX**

- **MAPA DE APELIDOS**

- EM ALGUMAS SITUAÇÕES, O DESTINATÁRIO DE UMA MENSAGEM NÃO É UMA CONTA QUE ESTEJA CADASTRADA, MAS UM APELIDO PARA UMA CONTA, COMO POR EXEMPLO: webmaster@atm.org.br
- ONDE O DESTINATÁRIO “webmaster” PODE SER UM “APELIDO” PARA UMA GRUPO DE USUÁRIOS, ASSIM TODOS OS INTEGRANTES DESTE GRUPO RECEBEM A MENSAGEM
- O ARQUIVO QUE IRÁ POSSUIR AS INFORMAÇÕES DE “APELIDOS” ESTÁ EM /etc/aliases



- **CORREIO ELETRÔNICO - POSTFIX**

- **MAPA DE APELIDOS**

- A ESTRUTURA DO ARQUIVO `/etc/aliases` É DESCRITO ABAIXO:

- apelido: destino

- EXEMPLO:

- webmaster: root, user1, user2, user3

- root: user5

- O POSTFIX CONSULTA O ARQUIVO `/etc/aliases.db` QUE É GERADO A PARTIR DO ARQUIVO `/etc/aliases` ATRAVÉS DA APLICAÇÃO “`postalias /etc/aliases`”

- UMA VEZ QUE FOI GERADO O ARQUIVO, PODEMOS ENVIAR UMA MENSAGEM PARA O USUÁRIO webmaster QUE SERÁ ENTREGUE PARA OS QUATRO USUÁRIOS DESCRITOS ACIMA



■ POST OFFICE PROTOCOL - POP3



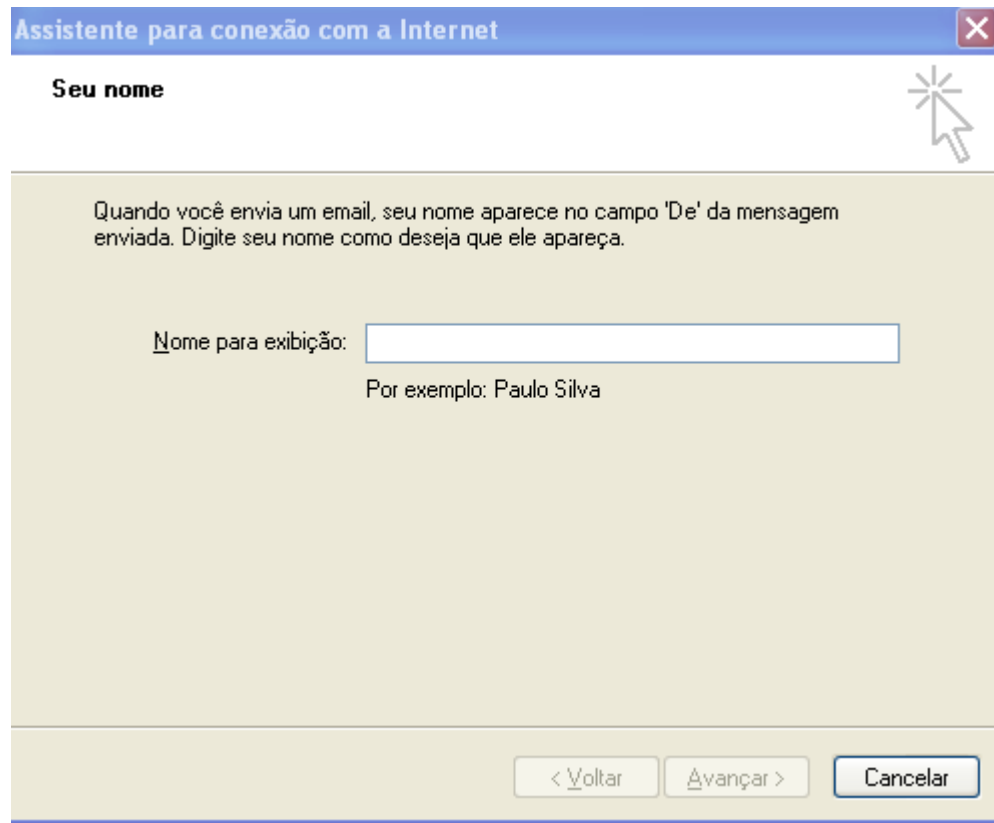
- **CORREIO ELETRÔNICO - POP3**
- PROCEDIMENTO DE INSTALAÇÃO
 - apt-get install courier-pop
- ADICIONAR A ENTRADA ABAIXO AO ARQUIVO main.cf
 - home_mailbox = Maildir/
- COMENTAR A ENTRADA ABAIXO NO ARQUIVO main.cf
 - mailbox_command =
- REINICIAR O POSTFIX
 - invoke postfix restart



- **CORREIO ELETRÔNICO - POP3**
- **PROCEDIMENTO DE CONFIGURAÇÃO – MS OUTLOOK**
- **CLICAR SOBRE O ÍCONE DO OUTLOOK EXPRESS**



- **CORREIO ELETRÔNICO - POP3**
- **PROCEDIMENTO DE CONFIGURAÇÃO – MS OUTLOOK**
- **INFORMAR O NOME DO DONO DA CONTA**



Assistente para conexão com a Internet

Seu nome

Quando você envia um email, seu nome aparece no campo 'De' da mensagem enviada. Digite seu nome como deseja que ele apareça.

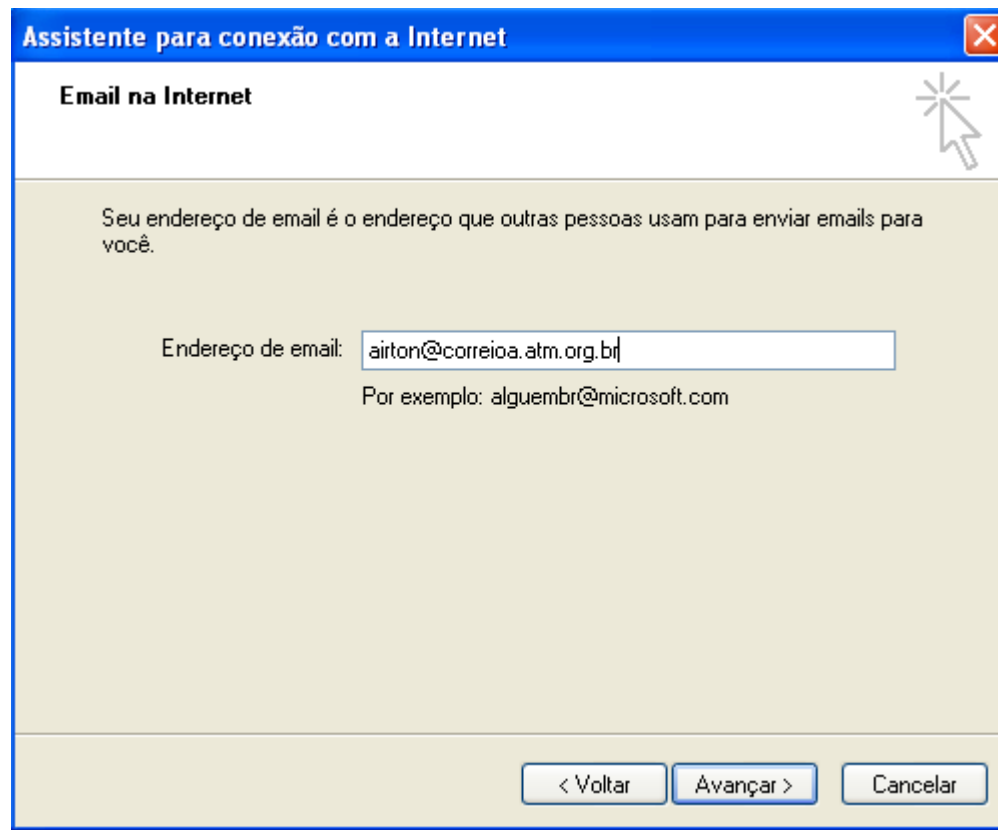
Nome para exibição:

Por exemplo: Paulo Silva

< Voltar Avançar > Cancelar



- **CORREIO ELETRÔNICO - POP3**
- **PROCEDIMENTO DE CONFIGURAÇÃO – MS OUTLOOK**
- **INFORMAR A CONTA DE CORREIO**



Assistente para conexão com a Internet

Email na Internet

Seu endereço de email é o endereço que outras pessoas usam para enviar emails para você.

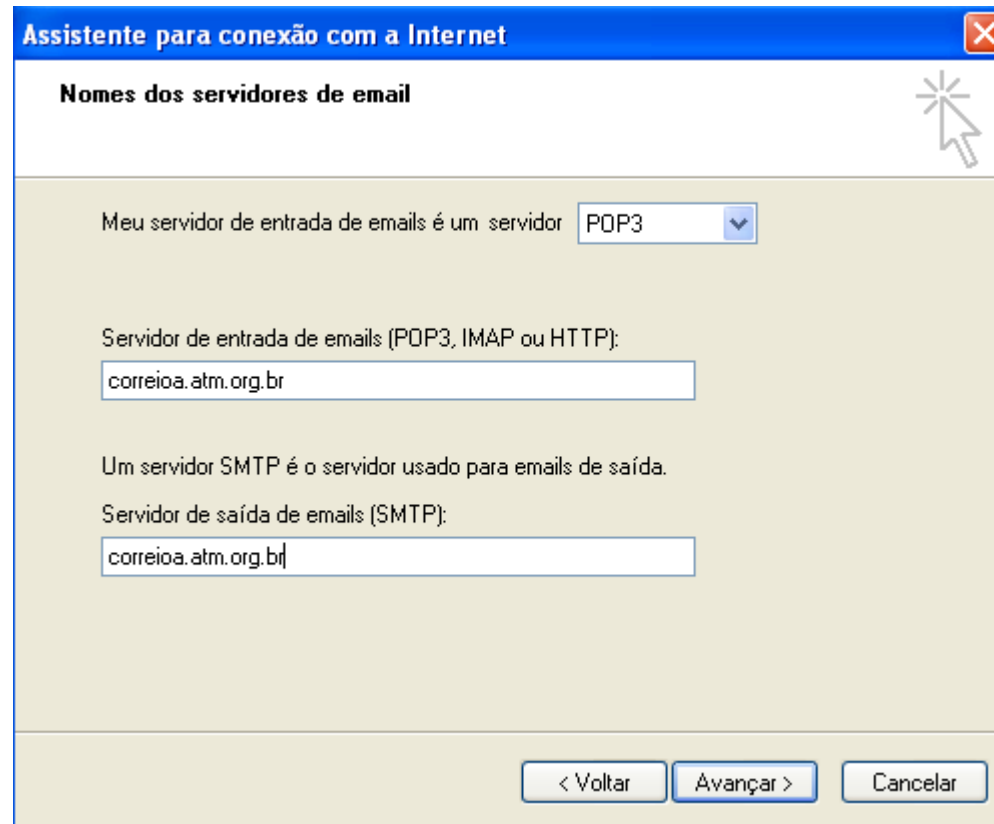
Endereço de email:

Por exemplo: alguembr@microsoft.com

< Voltar Avançar > Cancelar



- **CORREIO ELETRÔNICO - POP3**
- PROCEDIMENTO DE CONFIGURAÇÃO – MS OUTLOOK
- INFORMAR O NOME OU ENDEREÇO IP DO SERVIDOR POP3
- INFORMAR O NOME OU ENDEREÇO IP DO SERVIDOR SMTP



Assistente para conexão com a Internet

Nomes dos servidores de email

Meu servidor de entrada de emails é um servidor

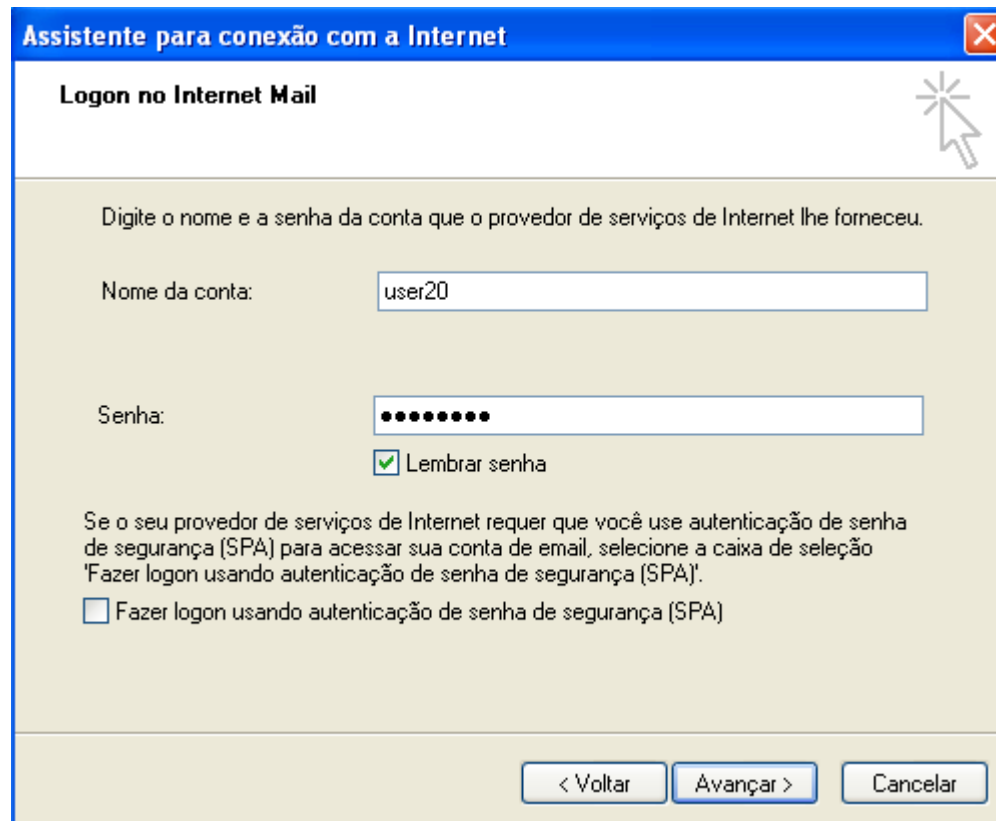
Servidor de entrada de emails (POP3, IMAP ou HTTP):

Um servidor SMTP é o servidor usado para emails de saída.
Servidor de saída de emails (SMTP):

< Voltar Avançar > Cancelar



- **CORREIO ELETRÔNICO - POP3**
- **PROCEDIMENTO DE CONFIGURAÇÃO – MS OUTLOOK**
- **INFORMAR O NOME E A SENHA DE ACESSO AO SERVIDOR POP3**



Assistente para conexão com a Internet

Logon no Internet Mail

Digite o nome e a senha da conta que o provedor de serviços de Internet lhe forneceu.

Nome da conta:

Senha:

☒ Lembrar senha

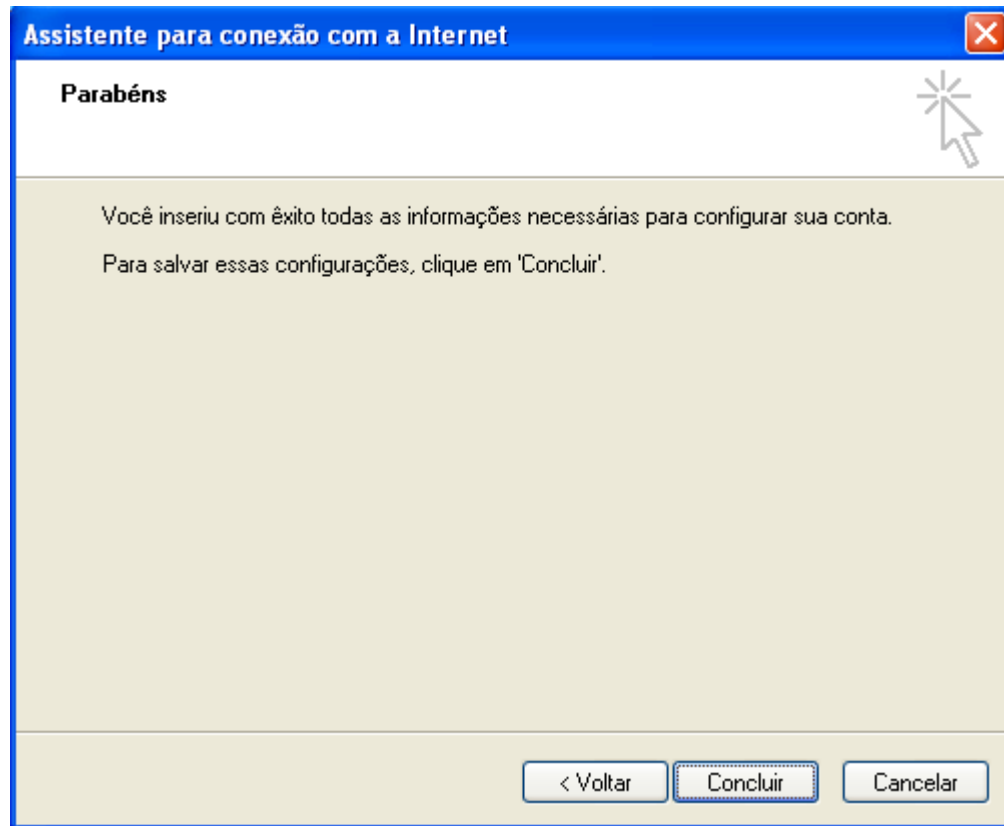
Se o seu provedor de serviços de Internet requer que você use autenticação de senha de segurança (SPA) para acessar sua conta de email, selecione a caixa de seleção 'Fazer logon usando autenticação de senha de segurança (SPA)'.

☐ Fazer logon usando autenticação de senha de segurança (SPA)

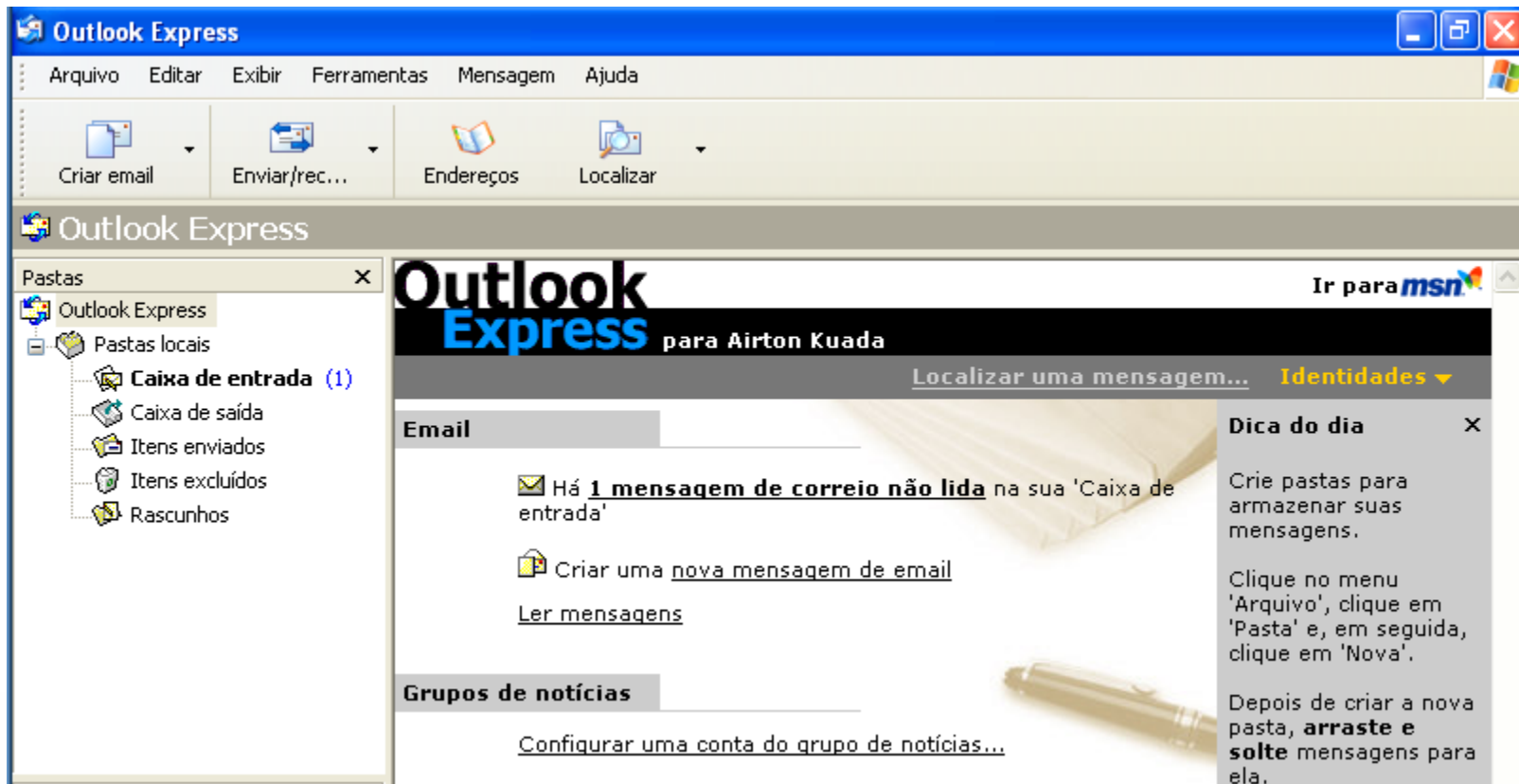
< Voltar Avançar > Cancelar



- **CORREIO ELETRÔNICO - POP3**
- **PROCEDIMENTO DE CONFIGURAÇÃO – MS OUTLOOK**
- **A CONFIGURAÇÃO DO OUTLOOK FOI FINALIZADA**



- CORREIO ELETRÔNICO - POP3
- PROCEDIMENTO DE CONFIGURAÇÃO – MS OUTLOOK
- O OUTLOOK ESTÁ PRONTO PARA ENVIAR E RECEBER MENSAGENS



- **CORREIO ELETRÔNICO - POSTFIX**

- **CONTROLE DE ACESSO**

- MUITAS VEZES O SERVIDOR DE CORREIO ELETRÔNICO RECEBE VARIAS MENSAGENS INDEVIDAS, COMO POR EXEMPLO:

- DOMÍNIO DE REDE NÃO CONHECIDO ATRAVÉS DE DNS

- ENDEREÇO DE REDE NÃO CONHECIDO ATRAVÉS DE DNS REVERSO

- DOMÍNIO DE REDE SUSPEITO DE PROBLEMAS DE SPAM

- QUANDO CHEGAM MENSAGENS PROVENIENTES DE SITES COM ALGUMA CARACTERÍSTICA INDESEJÁVEL, ALGUMA AÇÃO DEVE SER TOMADA



- **CORREIO ELETRÔNICO - POSTFIX**

- **CONTROLE DE ACESSO**

- **AÇÕES QUE PODEM SER TOMADAS**

- **REJECT – REJEITAR A MENSAGEM QUE ESTÁ CHEGANDO, AVISANDO O EMISSOR**
 - **DISCARD – REJEITAR A MENSAGEM QUE ESTÁ CHEGANDO, SEM AVISAR O EMISSOR**
 - **IGNORE – A MENSAGEM SERÁ TRATADO NORMALMENTE, EMBORA TENHA INDÍCIOS DE PROBLEMAS**
 - **WARN – A MENSAGEM IRÁ GERAR UM ALERTA NO SISTEMA DE LOG, MAS SERÁ TRATADA NORMALMENTE**
 - **HOLD – A MENSAGEM SERÁ MANTIDA EM UMA FILA DE ESPERA PARA SER ANALISADA POSTERIORMENTE**



- **CORREIO ELETRÔNICO - POSTFIX**

- **CONTROLE DE ACESSO**

- **MAPAS DE CONTROLE DE ACESSO**

- UM MAPA É UM ARQUIVO QUE CONTÉM DUAS COLUNAS NO FORMATO ABAIXO:

- chave ação

- ONDE:

- chave É UMA EXPRESSÃO REGULAR EM UMA FORMATO COMO 10.1.0.0/24, 10.1.1.1/32, @uol.com.br, tucano@xyz.com

- ação CORRESPONDE A UMA DAS AÇÕES DESCRITAS ANTERIORMENTE QUE SÃO EXECUTADAS PELO SERVIDOR DE CORREIO QUANDO UMA MENSAGEM É RECEBIDA



- **CORREIO ELETRÔNICO - POSTFIX**

- **CONTROLE DE ACESSO**

- **MAPAS DE CONTROLE DE ACESSO**

- **EXEMPLO DE MAPA**

- 192.167.10.0/24 OK

- 192.168.10.5 DISCARD “MSG DISCARD”

- microsoft.com REJECT

- user1@ REJECT

- user1@abc.com OK

- desconhecido.com HOLD “MSG DESCONHECIDA”

- O POSTFIX UTILIZA UM ARQUIVO BINÁRIO COM EXTENSÃO “.db” DESTE MAPA QUE É GERADO ATRAVÉS DO COMANDO `postmap`, CONFORME MOSTRADO ABAIXO

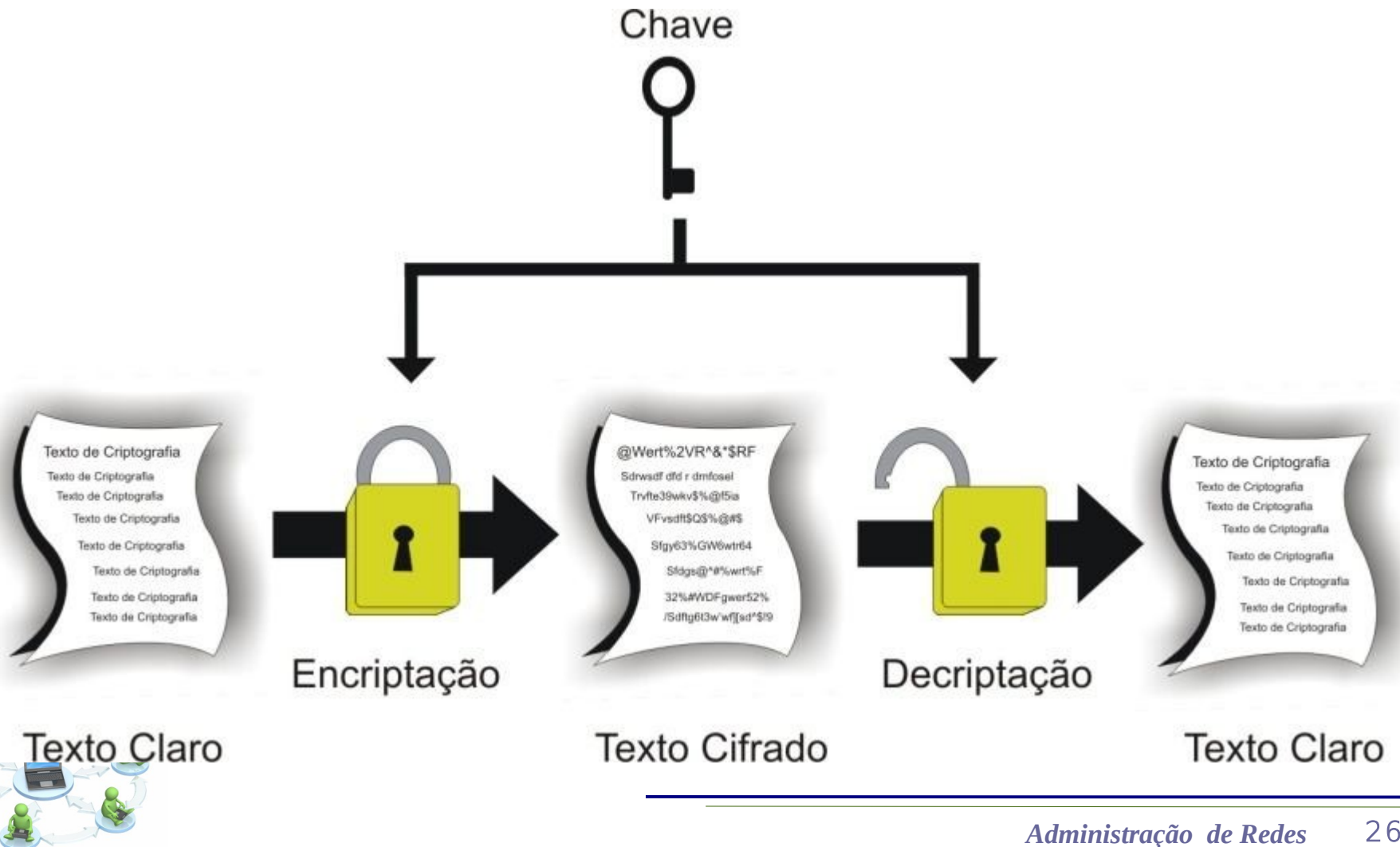
- `# postmap arquivo_de_mapa`



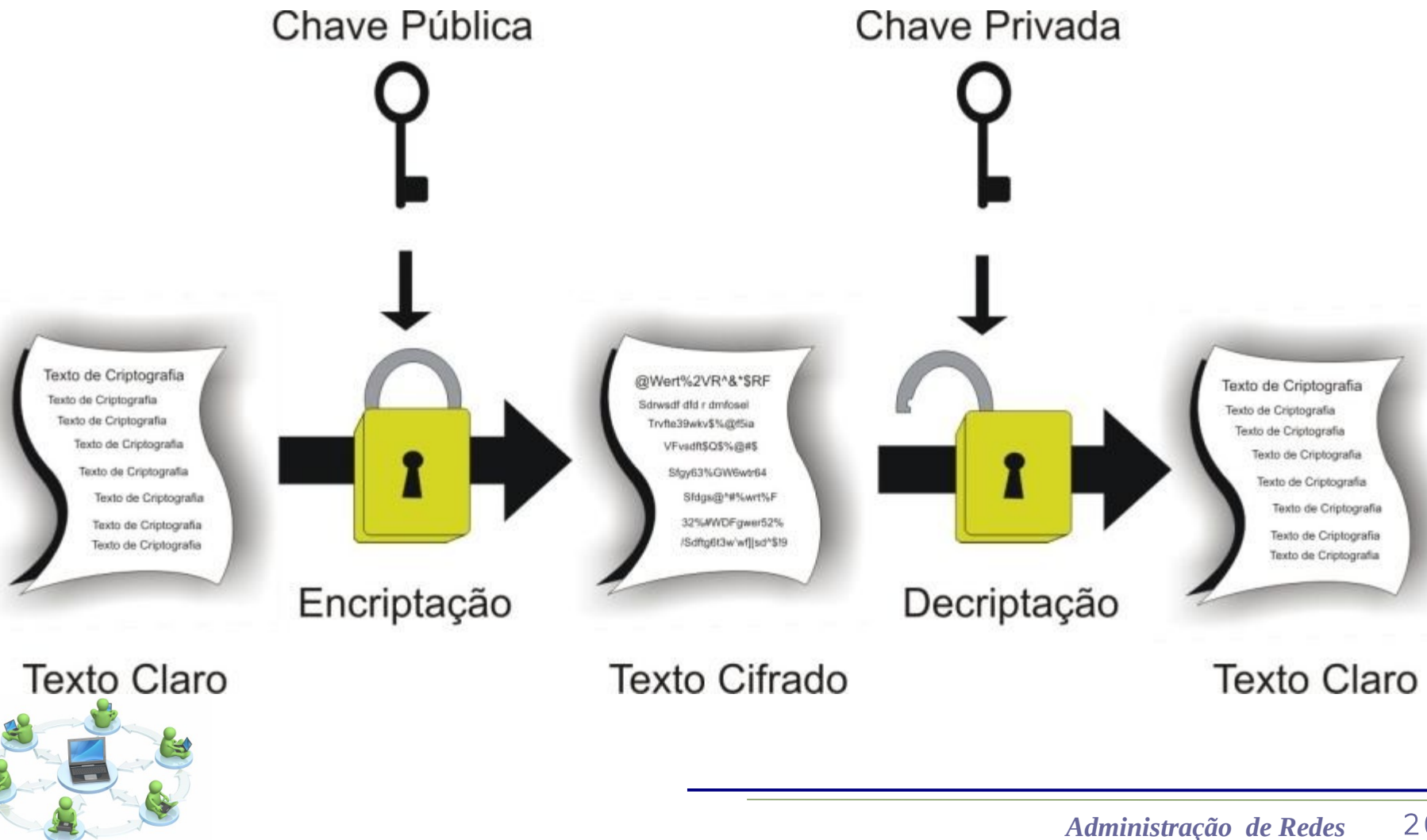
SSH



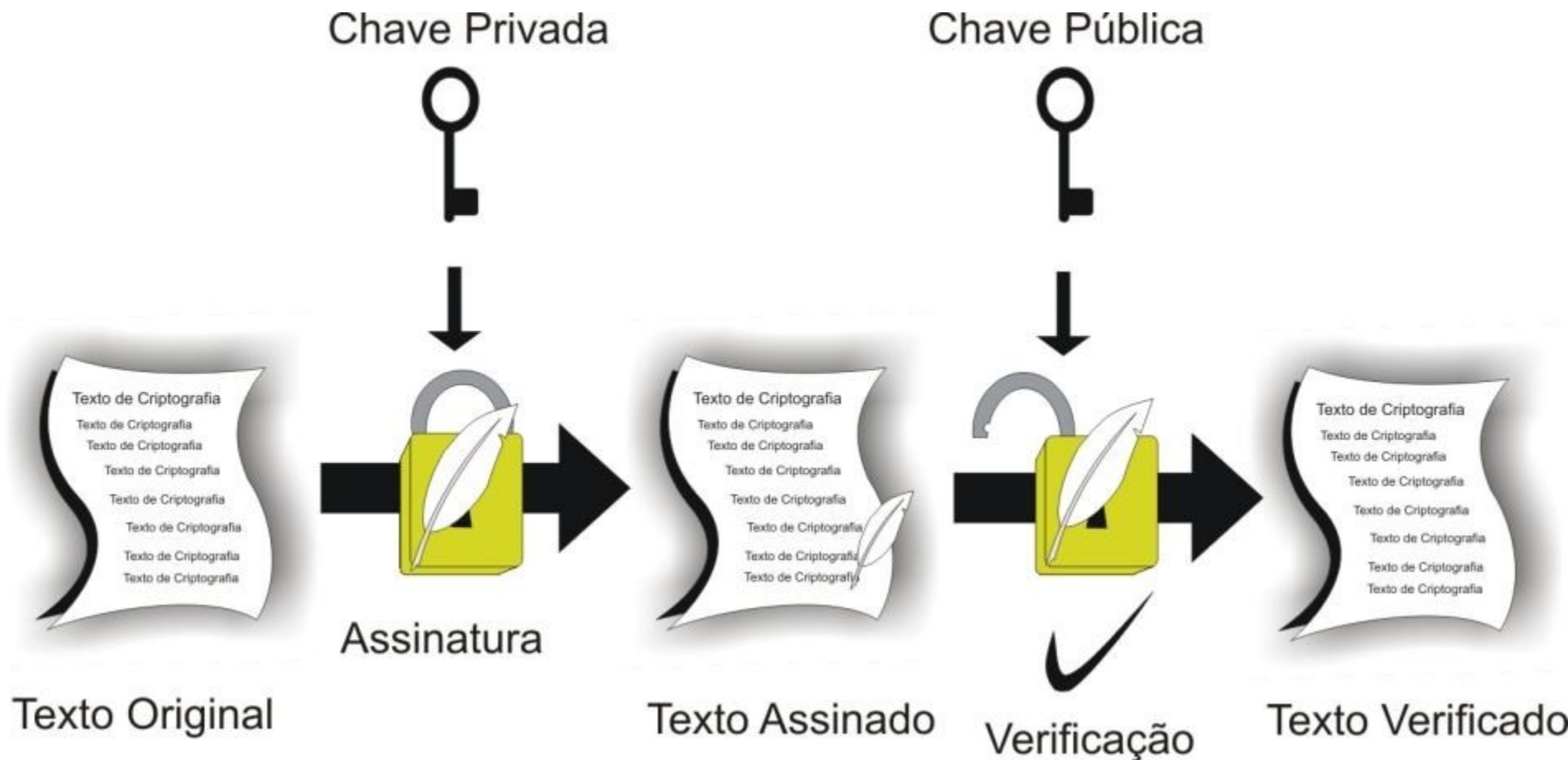
- SSH
- CRIPTOGRAFIA COM CHAVE SIMÉTRICA



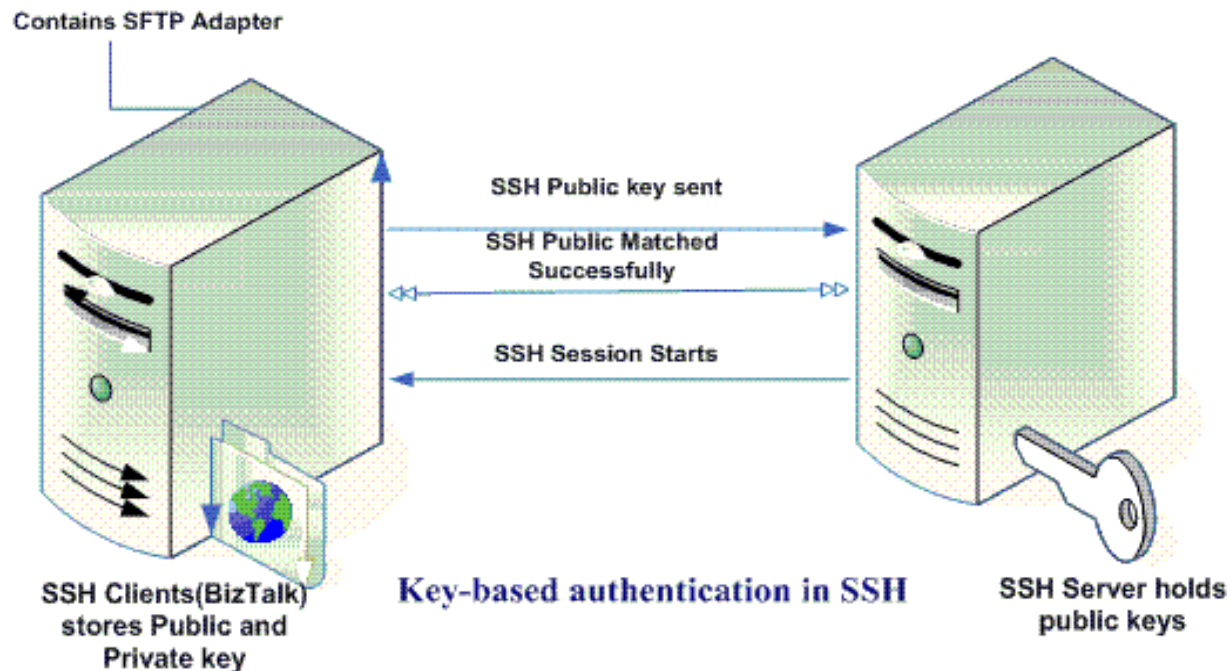
- SSH
- CRIPTOGRAFIA COM CHAVE ASSIMÉTRICA



- SSH
- ASSINATURA DIGITAL



- SSH
- CRIPTOGRAFIA COM CHAVE SIMÉTRICA



- **SSH**
- É UM PROTOCOLO DE COMUNICAÇÃO SEGURO
- É UTILIZADO PARA IMPLEMENTAR UMA COMUNICAÇÃO SEGURA ENTRE DOIS HOSTS QUE ESTÃO INTERLIGADOS ATRAVÉS DA INTERNET
- EXEMPLO DE APLICAÇÕES
 - EMULAÇÃO DE TERMINAL
 - TRANSFERÊNCIA DE ARQUIVOS
 - CRIAÇÃO DE TÚNEIS
- É DIVIDIDO EM DUAS PARTES
 - CLIENTE SSH
 - SERVER SSH
- UTILIZA CHAVE ASSIMÉTRICA PARA AUTENTICAÇÃO E CHAVE SIMÉTRICA PARA TROCA DE INFORMAÇÃO



■ SSH

□ INICIALIZAÇÃO DA SESSÃO

- HOST CLIENTE E SERVIDOR TROCAM CHAVES PÚBLICAS
- CLIENTE ENVIA USUÁRIO E SENHA CIFRADO COM A CHAVE PUBLICA DO SERVIDOR
- APÓS A AUTENTICAÇÃO DO USUÁRIO, UMA CHAVE DE CRIPTOGRAFIA SIMÉTRICA E UM ALGORITMO DE CRIPTOGRAFIA SIMETRICA É NEGOCIADA, NORMALMENTE UTILIZANDO (NORMALMENTE 3DES OU BLOWFISH)
- INICIA A TROCA DE INFORMAÇÃO ENTRE O CLIENTE E SERVIDOR UTILIZANDO O CANAL SEGURO



■ SSH

- INSTALANDO PACOTE SSH
 - `apt-get install openssh-server`
- PARA UTILIZAR O SSH É NECESSÁRIO POSSUIR APENAS O PACOTE `openssh-client`
- A PORTA DE ACESSO É TCP/22
- O ARQUIVO DE CONFIGURAÇÃO DO SERVIDOR ESTÁ EM `/etc/ssh/sshd_config`
- O ARQUIVO DE CONFIGURAÇÃO DO SERVIDOR ESTÁ EM `/etc/ssh/ssh_config`
- GERENCIAMENTO DO SERVIDOR
 - `service ssh stop/start/restart`



■ SSH

□ UTILIZAÇÃO DO SSH

- `ssh usuário@servidor`
- SE O USUÁRIO NÃO FOR INFORMADO, SERÁ UTILIZADO O USUÁRIO COM O QUAL ESTÁ LOGADO – `ssh servidor`



■ SSH

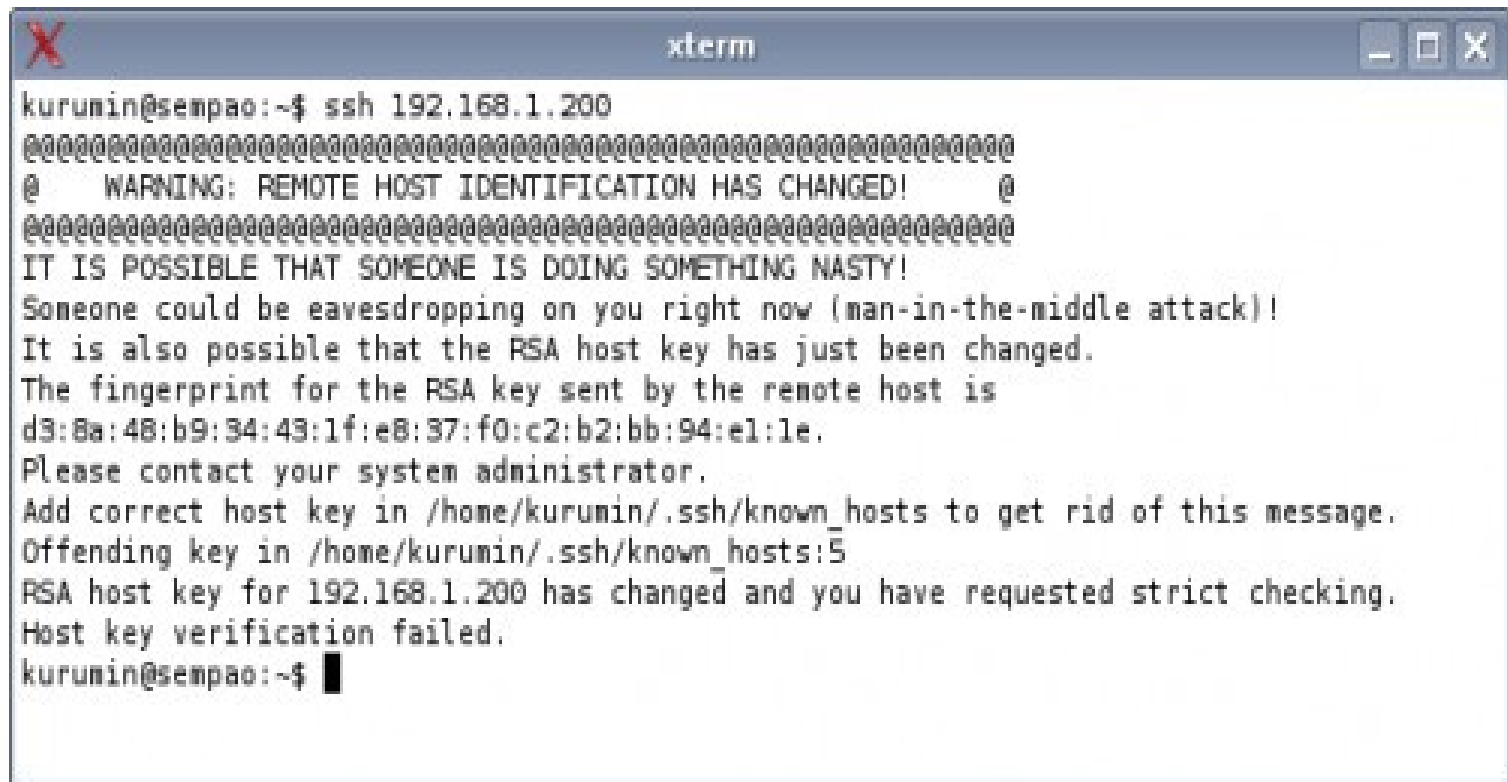
□ AUTENTICAÇÃO DO SERVIDOR

- NA PRIMEIRA CONEXÃO COM O SERVIDOR, ESTE ENVIA A CHAVE PÚBLICA QUE FICA ARMAZENADO NO CLIENTE EM /home/usuário/.ssh/known_hosts
- TODA VEZ QUE O CLIENTE IRÁ SE CONECTAR COM UM SERVIDOR CONHECIDO, INICIALMENTE SERÁ ENVIADO UM DESAFIO PARA O SERVIDOR QUE É UMA FRASE CIFRADA COM A CHAVE PÚBLICA (DO SERVIDOR) QUE SÓ PODE SER DESCOBERTO COM A CHAVE PRIVADA. O SERVIDOR DEVERÁ ENVIAR DE VOLTA ESTE DESAFIO. SE A RESPOSTA ESTIVER CORRETA, ENTÃO O SERVIDOR ESTÁ AUTENTICADO PELO CLIENTE E A CONVERSA PODE TER INICIO
- ESTE PROCEDIMENTO É UTILIZADO PARA EVITAR QUE UM IMPOSTOR RESPONDA – ALTERAÇÃO DE IP



■ SSH

□ MENSAGEM DE ERRO



```
kurumin@sempao:~$ ssh 192.168.1.200
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
d3:8a:48:b9:34:43:1f:e8:37:f0:c2:b2:bb:94:e1:1e.
Please contact your system administrator.
Add correct host key in /home/kurumin/.ssh/known_hosts to get rid of this message.
Offending key in /home/kurumin/.ssh/known_hosts:5
RSA host key for 192.168.1.200 has changed and you have requested strict checking.
Host key verification failed.
kurumin@sempao:~$ █
```



■ SSH

□ AUTENTICAÇÃO DO SERVIDOR

- SE A SUBSTITUIÇÃO FOI REALIZADA DE FORMA VERDADEIRA, É NECESSÁRIO REMOVER A LINHA QUE CONTÉM A CHAVE PÚBLICA ATUAL DO SERVIDOR SUBSTITUÍDO ATRAVÉS DO COMANDO ABAIXO

ssh-keygen -R endereço_IP

- AO INICIAR UMA NOVA CONEXÃO TEREMOS A MENSAGEM ABAIXO, PERMITINDO ADICIONAR A NOVA CHAVE PÚBLICA NO ARQUIVO DE CONFIGURAÇÃO “know_hosts”

The authenticity of host '192.168.1.200 (192.168.1.200)'
can't be established.

RSA key fingerprint is

f1:0f:ae:c6:01:d3:23:37:34:e9:29:20:f2:74:a4:2a.

Are you sure you want to continue connecting (yes/no)?



■ SSH

□ AUTENTICAÇÃO DO SERVIDOR

- AS CHAVE DE IDENTIFICAÇÃO SÃO GERADAS DURANTE A INSTALAÇÃO DO SSH
- AS CHAVES DO CLIENTE ESTÃO ARMAZENADAS EM `"/etc/ssh/ssh_host_rsa_key"` E DO SERVIDOR EM `"/etc/ssh/ssh_host_dsa_key"`
- QUANDO A SUBSTITUIÇÃO DE MÁQUINA FOR REALIZADO É RECOMENDADO QUE SE TIRE BACKUP DESTES ARQUIVO



■ SSH

□ AUTENTICAÇÃO DO CLIENTE

- APÓS A AUTENTICAÇÃO DO SERVIDOR PELO CLIENTE, É A VEZ DO SERVIDOR AUTENTICAR O CLIENTE
- O CLIENTE DEVE FORNECER A SENHA DO USUÁRIO QUE ESTÁ SENDO UTILIZADO PARA CONEXÃO COM O SERVIDOR
- ESTA SENHA PODE SER QUEBRADA DE ALGUMA FORMA POR UM HACKER
- PARA CONTORNAR ESTE PROBLEMA, PODEMOS UTILIZAR UM PAR DE CHAVES PARA AUTENTICAR O USUÁRIO QUE ESTÁ FAZENDO LOGIN
- A CHAVE PÚBLICA É INSTALADA NOS SERVIDORES QUE ESTÃO SENDO ACESSADOS E A CHAVE PRIVADA NÃO SAI É MANTIDA NO CLIENTE



■ SSH

□ AUTENTICAÇÃO DO CLIENTE

□ GERAÇÃO DA CHAVE PÚBLICO/PRIVADO

```
$ ssh-keygen -t rsa
```

Generating public/private rsa key pair.

Enter file in which to save the key (/home/abc123/.ssh/id_rsa):

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /home/abc123/.ssh/id_rsa.

Your public key has been saved in /home/abc123/.ssh/id_rsa.pub.

The key fingerprint is:

```
1f:bd:2e:9a:26:98:20:fe:38:41:6d:1c:65:8b:9e:75
```

```
abc123@ecelepar16812
```

□ A “PASSPHRASE” PODE SER UMA SENHA DE 8 OU 12 CARACTERES, ATÉ UMA FRASE SEM LIMITE DE TAMANHO



■ SSH

□ AUTENTICAÇÃO DO CLIENTE

- O COMANDO ANTERIOR IRÁ GERAR OS ARQUIVOS
 - `~usuário/.ssh/id_rsa` – CHAVE PRIVADA
 - `~usuário/.ssh/id_rsa.pub` – CHAVE PÚBLICA
- MODIFICAR A PERMISSÃO DO ARQUIVO `id_rsa` COM O COMANDO: `chmod 600 id_rsa`
- COPIAR A CHAVE PÚBLICA PARA O SERVIDOR REMOTO
`ssh-copy-id -i ~/.ssh/id_rsa.pub login@servidor`
- SERÁ CRIADO UMA ENTRADA NO ARQUIVO `~login/.ssh/authorized_keys` NO SERVIDOR REMOTO
- SE A “PASSPHRASE” ESTIVER EM BRANCO, O LOGIN SERÁ REALIZADO AUTOMATICAMENTE, ISTO É, SEM A SOLICITAÇÃO DE SENHA
- VEJA A SEGUIR O EXEMPLO PRÁTICO



■ SSH

□ AUTENTICAÇÃO DO CLIENTE – EXEMPLO PRÁTICO

□ DESCRIÇÃO DO AMBIENTE

□ USUÁRIO JOSÉ CADASTRADO NA MÁQUINA
TICO

□ USUÁRIO SILVA CADASTRADO NA MÁQUINA
TECO

□ USUÁRIO JOSE REALIZA LOGIN NA MAQUINA
TECO UTILIZANDO O USUÁRIO SILVA COM
ATENTICAÇÃO COM CHAVE PUBLICO/PRIVADO

□ AÇÕES DO USUÁRIO JOSE

□ `ssh-keygen -t rsa`

□ `cd .ssh`

□ `chmod 600 id_rsa`

□ `ssh-copy-id -i ~/.ssh/id_rsa.pub silva@teco`

□ Informar a senha do usuário silva



■ SSH

□ AUTENTICAÇÃO DO CLIENTE – EXEMPLO PRÁTICO

□ AÇÕES DO USUÁRIO JOSE

□ ssh silva@teco

□ INFORMAR A “PASSPHRASE” SE NECESSÁRIO

□ SE TUDO OCORREU CORRETAMENTE, VOCÊ
ESTÁ COM O PROMPT DA MÁQUINA TECO

□ FAÇA O MESMO PARA O USUÁRIO SILVA ACESSAR
A MÁQUINA TICO, UTILIZANDO O USUÁRIO “jose”



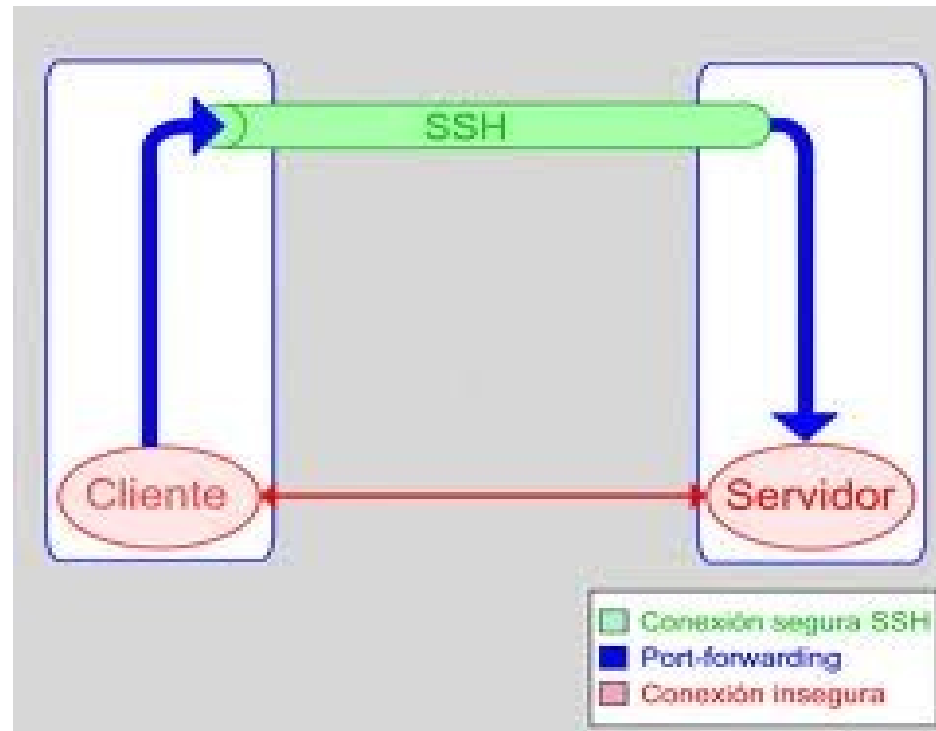
■ SSH

- OUTRA FUNCIONALIDADE IMPORTANTE QUE PODE SER EXECUTADO ATRAVÉS DO SSH É A TRANSFERÊNCIA DE ARQUIVO ENTRE HOSTS
- O COMANDO QUE TRANSFERE ARQUIVO É
 - `scp origem destino`
- EXEMPLO: (OS COMANDOS SÃO EXECUTADOS EM TICO)
 - TRANSFERINDO ARQUIVO ENTRE TICO E TECO
 - `scp /etc/hosts silva@teco:/tmp`
 - TRANSFERINDO ARQUIVO ENTRE TECO E TICO
 - `scp silva@teco:/tmp/hosts /tmp`
- SE A CONFIGURAÇÃO DE CHAVES ESTIVER REALIZADA A TRANSFERÊNCIA É REALIZADA AUTOMÁTICAMENTE, ISTO É, SEM SOLICITAR A SENHA



■ SSH

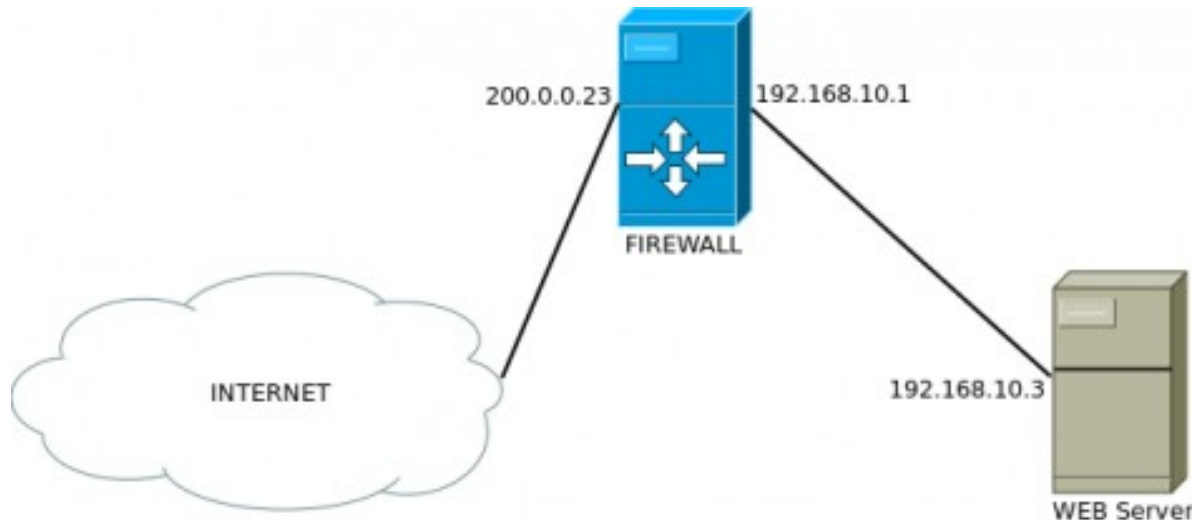
- OUTRA FUNCIONALIDADE IMPORTANTE QUE PODE SER EXECUTADO ATRAVÉS DO SSH É A CRIAÇÃO DE TÚNEIS, CONFORME MOSTRADO NA FIGURA ABAIXO:



■ SSH

□ REDIRECIONAMENTO DE PORTAS

- PARA ENTENDER O CONCEITO UTILIZADO QUANDO UTILIZAMOS O TÚNEL SSH, DEVEMOS ENTENDER O CONCEITO DE REDIRECIONAMENTO DE PORTA
- QUANDO UMA REQUISIÇÃO CHEGA PARA O IP/PORTA A REQUISIÇÃO É REDIRECIONADA PARA OUTRO IP/PORTA



■ SSH

□ CONFIGURAÇÃO SSH NO LINUX

- `$ ssh -f -N -L10.15.17.20:8080:10.15.151.50:80 -l root 10.15.151.50`
 - -L – PERMITE O REDIRECIONAMENTO DA PORTA LOCAL (8080) PARA O ENDEREÇO 10.15.151.50 E PORTA 80
 - -f – FAZ COM QUE O COMANDO SEJA EXECUTADO EM BACKGROUND
 - -N – FAZ COM QUE O SSH CRIE APENAS O REDIRECIONAMENTO DE PORTAS SEM ABRIR UM TERMINAL NO SERVIDOR REMOTO
 - -l – ESPECIFICA O USUÁRIO COM O QUAL QUEREMOS CONECTAR NA MÁQUINA REMOTA
- APÓS A EXECUÇÃO DO COMANDO, SERÁ SOLICITADO A SENHA DE ACESSO NA MÁQUINA REMOTA



■ SSH

□ CONFIGURAÇÃO SSH NO LINUX

□ DESCRIÇÃO DA CONFIGURAÇÃO ANTERIOR

- A MÁQUINA LOCAL QUE POSSUI O ENDEREÇO IP 10.15.17.20 E PORTA 8080 ESTÁ REDIRECIONANDO TODAS AS CONEXÕES PARA O ENDEREÇO IP DE DESTINO 10.15.151.50 E PORTA 80
- A PORTA 8080 NÃO PODE ESTAR SENDO UTILIZADO POR NENHUMA OUTRA APLICAÇÃO, CASO CONTRÁRIO, IRÁ OCORRER ERRO NA INICIALIZAÇÃO DO TÚNEL
- O TÚNEL SERÁ ABERTO E QUALQUER SOLICITAÇÃO QUE CHEGUE AO ENDEREÇO IP 10.15.17.20 E PORTA 8080 SERÁ ENCAMINHADO PARA O DESTINO 10.15.151.50 E PORTA 80 DE FORMA CRIPTOGRAFA ATRAVÉS DO SSH



SSH



■ SSH – CONCEITOS BÁSICOS

- EMULAÇÃO DE TERMINAL (SSH CLIENTE)
- EXECUÇÃO DE COMANDOS REMOTOS (SSH CLIENTE)
- TRANSFERÊNCIA DE ARQUIVO (SCP/SFTP)
- TUNEL
- SISTEMA DE ARQUIVO REMOTO (SSHFS)
- <http://tychoish.com/rhizome/9-awesome-ssh-tricks/>



- **SSH – CONCEITOS BÁSICOS**
 - **INSTALAÇÃO DO PACOTE**
 - apt-get install sshfs
 - **ADICIONAR O “root” AO GRUPO “fuse”**
 - adduser root fuse
 - **CRIANDO A PASTA NO COMPUTADOR LOCAL**
 - # mkdir /backup
 - **CRIANDO A PASTA NO COMPUTADOR REMOTO**
 - # mkdir /home/airton/backup
 - Fonte: <http://www.howtoforge.com/mounting-remote-directories-with-sshfs-on-debian-squeeze>



■ SSH – CONCEITOS BÁSICOS

■ MONTANDO O FILE SYSTEM REMOTO

- CAMINHO COMPLETO DE MAPEAMENTO

- `sshfs -o idmap=user
airton@10.15.151.101:/home/airton/backup /backup`

- CAMINHO RELATIVO DE MAPEAMENTO

- `sshfs -o idmap=user root@10.15.151.101:backup /backup`

- CAMINHO DEFAULT DE MAPEAMENTO

- `sshfs -o idmap=user root@10.15.151.101: /backup`

■ TODOS OS CAMINHOS FORNECIDOS DIZEM RESPEITO A PASTA HOME DO USUÁRIO “airton” QUE ESTÁ SENDO UTILIZANDO NO ACESSO DA MÁQUINA REMOTA



■ SSH – CONCEITOS BÁSICOS

■ VERIFICANDO A MONTAGEM

■ # mount

```
airton@10.15.151.101:/home/airton/backup on /backup type  
fuse.sshfs (rw,nosuid,nodev,max_read=65536)
```

■ VERIFICANDO ESPAÇO EM DISCO

■ # df -h

```
airton@10.15.151.101:/home/airton/backup  
4,8G 2,1G 2,7G 45% /backup
```

■ DESMONTANDO O SISTEMA DE ARQUIVOS

☐ # fusermount -u /media/cd

☐ OU

☐ # umount /media/cd



■ SSH – CONCEITOS BÁSICOS

■ CRIANDO AS CHAVES PUBLICO/PRIVADO EM HOSTA

□ # ssh-keygen

Generating public/private rsa key pair.

Enter file in which to save the key (/root/.ssh/id_rsa): <-- ENTER

Enter passphrase (empty for no passphrase): <-- ENTER

Enter same passphrase again: <-- ENTER

Your identification has been saved in /root/.ssh/id_rsa.

Your public key has been saved in /root/.ssh/id_rsa.pub.

The key fingerprint is:

b4:22:48:21:99:72:65:3e:1d:93:6f:9a:5c:5f:70:61 root@server1.example.com

- É importante não adicionar uma senha de acesso na “passphrase” senão no momento da montagem será solicitado esta senha. No caso de montagem automática não irá funcionar devido a necessidade de intervenção humana, portanto somente tecle ENTER!



■ SSH – CONCEITOS BÁSICOS

■ COPIANDOS AS CHAVES PARA A MÁQUINA REMOTA

```
# cd ~root/.ssh
```

```
#scp id_rsa.pub  
root@192.168.0.101:/~airton/.ssh/authorized_keys
```

■ VERIFICANDO O CONTEUDO DA MÁQUINA REMOTA

```
# cat /home/airton.ssh/authorized_keys
```

■ VERIFICANDO A MONTAGEM SEM SENHA

```
# sshfs -o idmap=user airton@10.15.151.101:backup /backup  
(Note que não haverá a solicitação de senha)
```

■ MONTAGEM AUTOMÁTICA NA INICIALIZAÇÃO

```
# vi /etc/rc.local
```

```
#!/usr/bin/sshfs -o idmap=user airton@10.15.151.101:backup  
/backup
```



APACHE



■ HTTP – HYPERTEXT TRANSFER PROTOCOL

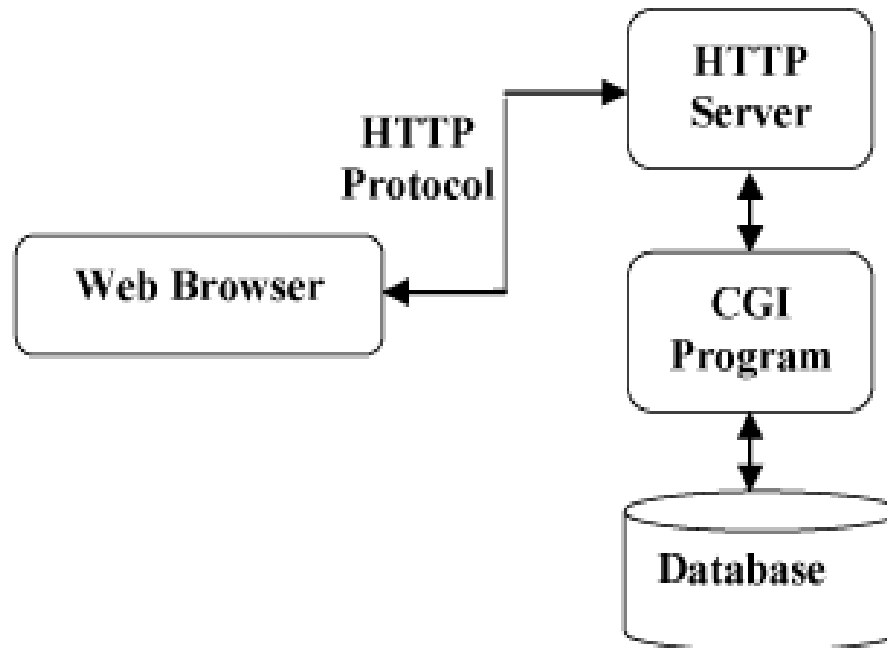
■ CONCEITOS BÁSICOS

- É UM PROTOCOLO DE COMUNICAÇÃO UTILIZADO PARA ENTREGAR INFORMAÇÕES QUE PODEM ESTAR NO FORMATO TEXTO, IMAGEM, BANCO DE DADOS E ETC, QUE SÃO CONHECIDOS COMO RECURSOS
- O BROWSER É UM CLIENTE HTTP QUE ENVIA REQUISIÇÕES A UM HTTP SERVER, CONHECIDO COMO WEB SERVER
- O WEB SERVER RESPONDE AS REQUISIÇÕES PARA BROWSER
- UTILIZA O PROTOCOLO TCP (PORTA 80) QUE OFERECE GARANTIA DE ENTREGA E CONFIABILIDADE DA COMUNICAÇÃO

□



- **HTTP – HYPERTEXT TRANSFER PROTOCOL**
- **CONCEITOS BÁSICOS**
 - **ESQUEMA DE FUNCIONAMENTO DO PROTOCOLO HTTP**



■ HTTP – HYPERTEXT TRANSFER PROTOCOL

■ CONCEITOS BÁSICOS

- EXEMPLO DE REQUISIÇÃO HTTP DO CLIENTE

- `www.uol.com.br [:8080]`

- MENSAGEM HTTP

- CADA REQUISIÇÃO HTTP É DIVIDIDA EM TRÊS PARTES

- O NOME DO MÉTODO HTTP UTILIZADO

- O CAMINHO DE CADA RECURSO REQUISITADO

- A VERSÃO DO PROTOCOLO HTTP QUE É UTILIZADO

- EXEMPLO: *GET /path/to/file/index.html HTTP/1.0*

- GET É O MÉTODO UTILIZADO

- `/path/to/file/index.html` É O OBJETO REQUISITADO

- HTTP/1.0 É A VERSÃO DO PROTOCOLO HTTP



■ HTTP – HYPERTEXT TRANSFER PROTOCOL

■ CONCEITOS BÁSICOS

☐ PRINCIPAIS MÉTODOS UTILIZADOS

☐ GET

☐ AS INFORMAÇÕES ENVIADAS PARA O SERVIDOR WEB SÃO MOSTRADOS NA TELA DO BROWSER DURANTE O ENVIO DA REQUISIÇÃO

☐ MÉTODO DEFAULT

☐ POST

☐ AS INFORMAÇÕES QUE SÃO ENVIDADAS PARA O SERVIDOR WEB NÃO SÃO MOSTRADAS NA TELA DO BROWSER DURANTE O ENVIO DA REQUISIÇÃO

☐ UTILIZADO PARA O ENVIO DE INFORMAÇÕES COLETADAS EM FORMULÁRIOS

☐ VEJA OS EXEMPLOS (SENHA.HTML)



■ HTTP – HYPERTEXT TRANSFER PROTOCOL

■ CONCEITOS BÁSICOS

- MENSAGEM HTTP

- A PRIMEIRA RESPOSTA É CHAMADA “STATUS LINE” E TAMBÉM DIVIDIDA EM TRÊS PARTES

- VERSÃO DO PROTOCOLO HTTP UTILIZADO

- O CÓDIGO DE STATUS (STATUS CODE) DO RESULTADO DA REQUISIÇÃO

- UMA FRASE EM INGLÊS DESCREVENDO O CÓDIGO DE STATUS

- EXEMPLO DE RESPOSTA

- *HTTP/1.0 200 OK*

- *ou*

- *HTTP/1.0 404 Not Found*



■ HTTP – HYPERTEXT TRANSFER PROTOCOL

■ CONCEITOS BÁSICOS

- 1xx: INFORMAÇÃO – UTILIZADO PARA ENVIAR INFORMAÇÕES PARA O CLIENTE DE QUE SUA REQUISIÇÃO FOI RECEBIDA E ESTÁ SENDO PROCESSADA;
- 2xx: SUCESSO – INDICA QUE A REQUISIÇÃO DO CLIENTE FOI BEM SUCEDIDA;
- 3xx: REDIRECIONAMENTO – INFORMA A AÇÃO ADICIONAL QUE DEVE SER TOMADA PARA COMPLEMENTAR A REQUISIÇÃO;
- 4xx: ERRO NO CLIENTE – AVISA QUE O CLIENTE QUE FEZ UMA REQUISIÇÃO QUE NÃO PODE SER ATENDIDA;
- 5xx: ERRO NO SERVIDOR – OCORREU UM ERRO NO SERVIDOR AO ATENDER UMA REQUISIÇÃO



- **INSTALAÇÃO APACHE2**
- **PROCEDIMENTO PARA INSTALAÇÃO**
 - apt-get install apache2
 - apt-get install libapache2-mod-php5
- **PASTA PRINCIPAL DE CONFIGURAÇÃO**
 - /etc/apache2
- **ARQUIVO PRINCIPAL**
 - apache2.conf
- **DESCRIÇÃO DO ARQUIVO PRINCIPAL**
 - CONFIGURAÇÕES GERAIS
 - CONFIGURAÇÕES ESPECÍFICAS



- **INSTALAÇÃO APACHE2**
- **PASTA DE INSTALAÇÃO**
 - A PASTA ONDE SE ENCONTRA OS ARQUIVOS DE CONFIGURAÇÃO
 - /etc/apache2
 - ARQUIVO PRINCIPAL DE CONFIGURAÇÃO
 - apache2.conf
- **O ARQUIVO PRINCIPAL É DIVIDIDO EM DUAS PARTES**
 - PARÂMETROS GLOBAIS
 - DEFINE COM O SERVIDOR APACHE IRÁ TRABALHAR
 - PARÂMETROS ESPECÍFICOS
 - POSSUI INFORMAÇÕES DE OBJETOS QUE SÃO OFERECIDOS PELO SERVIDOR



■ INSTALAÇÃO APACHE2

■ PARAMETROS GLOBAIS (apache2.conf)

- ☐ ServerRoot – DIRETÓRIO DE CONFIGURAÇÃO DO APACHE
- ☐ Timeout - NÚMERO DE SEGUNDOS PASSADOS, APÓS RECEBER UMA SOLICITAÇÃO E NÃO OCORRER UMA RESPOSTA
- ☐ StartServers – NÚMERO DE PROCESSOS SERVIDORES A SEREM INICIADOS (5) (7 MB POR PROCESSO)
- ☐ MinSpareServers – NÚMERO MÍNIMO DE PROCESSOS SERVIDORES A SEREM MANTIDOS EM ESPERA (5)
- ☐ MaxSpareServers – NÚMERO MÁXIMO DE PROCESSOS SERVIDORES A SEREM MANTIDOS EM ESPERA (10)
- ☐ MaxClients – NÚMERO MÁXIMO DE PROCESSOS SERVIDORES QUE PODEM SER CRIADOS (150) INDEPENDENTE DA DEMANDA



■ INSTALAÇÃO APACHE2

■ PARAMETROS GLOBAIS (apache2.conf)

□ Include – ADICIONA UM ARQUIVO QUALQUER NA CONFIGURAÇÃO

■ VERIFICANDO O NÚMERO DE PROCESSOS

```
#ps -ylC apache2 --sort:rss
```

S	UID	PID	PPID	C	PRI	NI	RSS	SZ	WCHAN	TTY	TIME	CMD
S	33	11621	3996	0	80	0	6748	41861	schedu ?		00:00:00	apache2
S	33	9269	3996	0	80	0	6756	41861	schedu ?		00:00:00	apache2
S	33	10451	3996	0	80	0	6756	41861	schedu ?		00:00:00	apache2
S	33	10630	3996	0	80	0	6756	41861	schedu ?		00:00:00	apache2
S	33	11738	3996	0	80	0	6756	41861	schedu ?		00:00:00	apache2
S	33	12148	3996	0	80	0	6760	41863	schedu ?		00:00:00	apache2
S	33	4928	3996	0	80	0	6856	41863	schedu ?		00:00:00	apache2
S	33	6803	3996	0	80	0	6856	41863	schedu ?		00:00:00	apache2



- **GERENCIAMENTO DO SERVIÇO -APACHE2**

- PARA INICIAR O SERVIÇO

- `service apache2 start`

- PARA ENCERRAR O SERVIÇO

- `service apache2 stop`

- PARA REINICIAR O SERVIÇO

- `service apache2 reload`

- PASTA DE DISPONIBILIZAÇÃO DE PÁGINAS

- `/var/www`

- ARQUIVO DE PÁGINA DEFAULT

- `/var/www/index.html`

- ACESSO AO SERVIDOR DE PÁGINA

- `http://nome Ou IP`

- `http://nome Ou IP/pasta`



- **EXERCÍCIO**
- ACESSAR O SERVIDOR DE PÁGINAS ATRAVÉS DO BROWSER DA VM DO WINDOWS
- ALTERAR A PÁGINA ORIGINAL E ADICIONAR O SEU NOME NO ARQUIVO index.html. ACESSAR NOVAMENTE A PÁGINA E VERIFICAR A ALTERAÇÃO REALIZADA
- RENOMEAR O ARQUIVO index.html para inicio.html.old E ACESSAR NOVAMENTE E VERIFICAR O RESULTADO DO ACESSO



- **CONFIGURAÇÃO DO SERVIÇO**
- O PARAMETRO QUE DEFINE A PASTA ONDE OS DOCUMENTOS ESTÃO ARMAZENADOS É “DocumentRoot” ESTÁ DEFINIDO NO ARQUIVO /etc/apache2/sites-available/default,
- POR PADRÃO A PASTA BASE É “/var/www” E É CONSIDERADO O INÍCIO DO SISTEMA DE ARQUIVOS (“/”) QUE SÃO REFERENCIADOS PELOS BROWSER
- QUANDO O CLIENTE NÃO INFORMADO NENHUM NOME DE ARQUIVO A SER BUSCADO NO SERVIDOR (www.site.com), O SERVIDOR IRÁ BUSCAR POR UMA LISTA DE **ARQUIVOS DE INDICE** (index.html, index.php, etc) QUE É DIRIGIDA PELA DIRETIVA “DirectoryIndex” QUE ESTÁ CONTIDO EM /etc/apache2/mods-available/dir.conf. O ARQUIVO ESTARÁ NA PASTA DEFINIDO PELA DIRETIVA “DocumentRoot”



- **CONFIGURAÇÃO DO SERVIÇO**
- SE O BROWSER INDICAR UM SITE E UMA DETERMINADA PASTA COMO POR EXEMPLO `www.site1.com/restrito`, O SERVIDOR IRÁ BUSCAR EM “`/var/www/restrito`” OS ARQUIVOS APONTADOS PELA DIRETIVA `DirectoryIndex`
- SE O BROWSER INDICAR UM SITE E UMA DETERMINADA PASTA E UM ARQUIVO COMO POR EXEMPLO `www.site1.com/restrito/site1.html`, O SERVIDOR IRÁ BUSCAR EM “`/var/www/restrito`” OS ARQUIVOS `site1.html`
- SE O ARQUIVO OU A PASTA PROCURADA NÃO EXISTIR, SERÁ DEVOLVIDO O STATUS 404 – NOT FOUND PARA O BROWSER DO CLIENTE



- **CONFIGURAÇÃO DO SERVIÇO**
- NO EXERCÍCIO ANTERIOR, QUANDO O ARQUIVO DE ÍNDICE index.html NÃO É ENCONTRADO, SERÁ MOSTRADO O CONTEÚDO DA PASTA, PORÉM NEM SEMPRE ISTO É INTERESSANTE E SEGURO
- O SERVIDOR APACHE CONTROLA O ACESSO A UMA PASTA ATRAVÉS DAS DIRETIVAS
 - <Directory nome da pasta>
 - </Directory>
- TODAS AS PASTAS QUE SÃO ACESSADAS PELO SERVIÇO APACHE NECESSITA DE UMA DECLARAÇÃO ACIMA



- **CONFIGURAÇÃO DO SERVIÇO**
- AS PRINCIPAIS DIRETIVAS QUE CONTRAL O ACESSO AS PASTAS SÃO:
 - ExecCGI – PERMITE A EXECUÇÃO DE SCRIPTS CGI DENTRO DA PASTA
 - FollowSynLinks - PERMITE SEGUIR LINKS SIMBOLICOS INCLUSIVE PARA FORA DO “DocumentRoot”
 - Indexes – PERMITE A LISTAGEM DO CONTEÚDO DE UM DIRETÓRIO DESDE QUE NÃO EXISTA UM ARQUIVO DE INDICE (index)
 - MultiViews – PERMITE A NEGOCIAÇÃO DE CONTEÚDO



- CONFIGURAÇÃO DO SERVIÇO
- EXEMPLO DE CONTROLE

<Directory /var/www/>

Options Indexes FollowSymLinks MultiViews

Order allow,deny

allow from all

</Directory>

- SE REMOVERMOS A CLAUSULA “Indexes” E NÃO HOUVER NENHUM ARQUIVO DE ÍNDICE, SERÁ MOSTRADO UMA MENSAGEM DE ERRO(FORBIDDEN)
- EXERCÍCIO
 - REMOVER O CLAUSULA “Indexes” E REINICIAR O APACHE
 - RENOMEAR O ARQUIVO DE ÍNDICE index.html PARA inicio.html, E ACESSAR NOVAMENTE COM BROWSER



- **CONFIGURAÇÃO DO SERVIÇO**

- **EXEMPLO DE CONTROLE**

<Directory /var/www/>

Options Indexes FollowSymLinks MultiViews

Order allow,deny

allow from all

</Directory>

- SE O SERVIDOR TIVER QUE SEGUIR UM LINK SIMBÓLICO, A CLAUSULA “FollowSymLinks” DEVE ESTAR PRESENTE
- **EXERCÍCIO**

- EXECUTAR OS COMANDOS:

- `man ls > /tmp/ls.txt`

- `cd /var/www`

- `ln -sf /tmp/ls.txt arquivo.txt`



- CONFIGURAÇÃO DO SERVIÇO

- EXERCÍCIO

- ACESSAR O ENDEREÇO ATRAVÉS DO BROWSER. EMBORA O ARQUIVO NÃO ESTEJA NA PASTA “/var/www”, EXISTE O LINK SIMBÓLICO QUE SEGUE O ARQUIVO
- REMOVER A CLAUSULA “FollowSymLinks” DO ARQUIVO DE CONFIGURAÇÃO E REINICIAR O SERVIÇO. ACESSAR NOVAMENTE A PÁGINA
- VERIFICAREMOS QUE O NÃO SERÁ POSSÍVEL ACESSAR O CONTEÚDO DEVIDO A RESTRIÇÃO DE SEGURANÇA



■ CONFIGURAÇÃO DO SERVIÇO

■ EXERCÍCIO (MULTIVIEWS)

- ☐ SE O SERVIDOR RECEBE A REQUISIÇÃO “localhost/abc/foo”, SE A PASTA abc POSSUIR A OPÇÃO MULTIVIEW HABILITADA E O ARQUIVO “abc/foo” NÃO EXISTE, ENTÃO IRÁ PROCURAR NA PASTA “abc”, TODOS OS ARQUIVOS “foo.*” E IRÁ APRESENTAR O SEU CONTEÚDO NA ORDEM “html,php,jpeg,jpg,png,etc”
- ☐ EXECUTAR OS COMANDOS:
 - ☐ `cd /var/www`
 - ☐ `mkdir abc`
 - ☐ `cd abc`
 - ☐ `cp ../index.html foo.html`
- ☐ ACESSAR ATRAVÉS DO BROWSER O CAMINHO “localhost/abc/foo”



- **CONFIGURAÇÃO DO SERVIÇO**
- A DIRETIVA “allow/deny” CONTROLAM O ACESSO AO SERVIDOR
- EXEMPLOS:
 - Allow from 192.168.0.0/16
 - Deny from 192.168.1.1



- CONFIGURAÇÃO DO SERVIÇO
-
- A DIRETIVA “Order” ESPECIFICA A ORDEM DE AVALIAÇÃO DO CONTROLE DE ACESSO AO SERVIDOR
- OS VALORES POSSÍVEIS SÃO:
 - Order allow,deny
 - Order deny,allow
 - OBSERVAÇÃO IMPORTANTE: NÃO PODE HAVER ESPAÇO NA ESCRITA ENTRE “deny,allow” ou “allow,deny”
- NA PRIMEIRA ANÁLISE, É APLICADO AS REGRAS DE PERMISSÃO E NA SEQUENCIA AS REGRAS DE NEGAÇÃO
- NA SEGUNDA ANÁLISE, É APLICADO AS REGRAS DE NEGAÇÃO E NA SEQUENCIA AS REGRAS DE PERMISSÃO



- **CONFIGURAÇÃO DO SERVIÇO**

- **CONSIDERE A CONFIGURAÇÃO ABAIXO:**

allow from 10.1.0.0/16

deny from 10.1.1.1

order deny allow

- **COMENTÁRIOS**

- UTILIZANDO A SEQUENCÊNCIA DEFINIDO PELA CLÁUSULA “order”, INICIALMENTE BLOQUEAMOS A ENTRADA DA FONTE COM IP “10.1.1.1” E DEPOIS LIBERADOS O ACESSO PARA TODA A REDE “10.1.0.0/16”. COMO RESULTADO FINAL, A MÁQUINA COM IP 10.1.1.1 TAMBÉM TERÁ ACESSO AO SERVIDOR POIS A CLAUSULA “allow” IRÁ SOBREPÔR SOBRE A CLAUSULA “deny”

- PARA CORRIGIR O ERRO, A ORDEM CORRETA SERIA
order allow deny



- **CONFIGURAÇÃO DO SERVIÇO**
- **CONSIDERE A CONFIGURAÇÃO ABAIXO:**
 - allow from 10.1.0.0/16
 - deny all
 - order deny,allow
- **COMENTÁRIOS**
 - UTILIZANDO A SEQUENCÊNCIA DEFINIDO PELA CLÁUSULA “order”, INICIALMENTE BLOQUEAMOS A ENTRADA DE QUALQUER ORIGEM E NA SEQUENCIA, LIBERAMOS O ACESSO A REDE “10.1.0.0/16”. QUALQUER OUTRA REDE TERÁ O ACESSO NEGADO
 - SE HOVER INVERSÃO DA CLAUSULA “order” NENHUMA REDE TERÁ ACESSO AO SERVIDOR



- CONFIGURAÇÃO DO SERVIÇO
- CONTROLANDO O ACESSO
 - UMA VEZ QUE OS ARQUIVOS FORAM COLOCADOS NA INTERNET, ESTARÁ DISPONÍVEL PARA QUALQUER UM
 - SE QUIERMOS, PODEMOS LIMITAR O ACESSO A UMA DETERMINADA PASTA UTILIZANDO O PARAMETRO “AuthType”, CONFORME MOSTRADO ABAIXO:

```
<Directory "/var/www/restrito">  
    AuthType Basic  
    AuthUserFile /var/www/senha.pwd  
    Authname "Area Restrita, Identifique-se"  
    Require valid-user  
</Directory>
```



- CONFIGURAÇÃO DO SERVIÇO

- CONTROLANDO O ACESSO

- DESCRIÇÃO DOS PARAMETROS

- Directory `"/var/www/restrito"` – DECLARA A PASTA QUE ESTÁ SENDO PROTEGIDO
 - AuthType Basic – TIPO DE AUTENTICAÇÃO BÁSICA
 - AuthUserFile `/var/www/senha.pwd` – ARQUIVO DE AUTENTICAÇÃO QUE CONTÉM OS PARAMETROS DE AUTENTICAÇÃO
 - Authname `"Area Restrita, Identifique-se"` – MENSAGEM QUE SERÁ MOSTRADO NA CAIXA DE AUTENTICAÇÃO
 - Require valid-user – QUALQUER USUÁRIO CADASTRADO NO ARQUIVO DE AUTENTICAÇÃO SERÁ ACEITO



- **CONFIGURAÇÃO DO SERVIÇO**
- **CONTROLANDO O ACESSO**
 - CRIAÇÃO DO ARQUIVO DE SENHAS
 - `htpasswd -c /var/www/senha.pwd aluno`
 - ALTERAÇÃO DE SENHA DO USUÁRIO
 - `htpasswd /var/www/senha.pwd aluno`
 - REMOVER USUÁRIO
 - `htpasswd /var/www/senha.pwd aluno`



■ CONFIGURAÇÃO DO SERVIÇO

■ EXERCÍCIO

- CRIAR A PASTA /var/www/restrito
- COPIAR O ARQUIVO index.html PARA A PASTA CRIADA ANTERIORMENTE
- ADICIONAR A CONFIGURAÇÃO ABAIXO NO ARQUIVO /etc/apache2/sites-available/default LOGO ABAIXO DA DEFINIÇÃO DA PASTA “/var/www”

```
<Directory "/var/www/restrito">
```

```
    AuthType Basic
```

```
    AuthUserFile /var/www/senha.pwd
```

```
    Authname "Area Restrita, Identifique-se"
```

```
    Require valid-user
```

```
</Directory>
```



- CONFIGURAÇÃO DO SERVIÇO
- EXERCÍCIO
 - ☐ REINICIAR O SERVIÇO APACHE2
 - ☐ CRIAR O ARQUIVO DE AUTENTICAÇÃO DE USUÁRIO (senha.pwd)
 - ☐ ACESSAR ATRAVÉS DO BROWSER (X.X.X.X/restrito)
 - ☐ INFORMAR USUÁRIO E SENHA
 - ☐ VERIFICAR A PÁGINA QUE ESTÁ PRESENTE NA PASTA “restrito”



- CONFIGURAÇÃO DO SERVIÇO
- CRIAÇÃO DE SERVIDORES VIRTUAIS
 - O SERVIDOR APACHE FORNECE O RECURSO DE SERVIDORES VIRTUAIS, ONDE UM ÚNICO SERVIDOR APACHE PODE FORNECER PÁGINAS PARA DIFERENTES DOMÍNIOS
 - ESTE RECURSO É MUITO UTILIZADO POR PROVEDORES DE SERVIÇOS INTERNET, POIS PERMITE QUE UM ÚNICO SERVIDOR SEJA UTILIZADO PARA HOSPEDAR SITES DE DIFERENTES CLIENTES



- **CONFIGURAÇÃO DO SERVIÇO**
- PASSOS PARA CRIAÇÃO DE SERVIDORES VIRTUAIS
 - ADICIONAR UM ARQUIVO COM O CONTEÚDO ABAIXO, NA PASTA “/etc/apache2/sites-available”. O NOME DO ARQUIVO PODE SER O DOMÍNIO DO CLIENTE, POR EXEMPLO “alfa.atm.org.br”

```
<VirtualHost *:80>
```

```
    ServerName alfa.atm.org.br
```

```
    DocumentRoot /var/www/alfa
```

```
    DirectoryIndex /index.html
```

```
</VirtualHost>
```



- **CONFIGURAÇÃO DO SERVIÇO**
- **PASSOS PARA CRIAÇÃO DE SERVIDORES VIRTUAIS**
 - **DESCRIÇÃO**
 - VirtualHost *:80
 - DIRETIVA DE ABERTURA DE SESSÃO
 - ServerName alfa.atm.org.br
 - NOME DE ACESSO AO SERVIDOR VIRTUAL
 - DocumentRoot /var/www/alfa
 - PASTA ONDE OS ARQUIVOS DO DOMINIO ESTARÃO DISPONÍVEIS
 - DirectoryIndex /index.html
 - ARQUIVO DE INDICE QUE SERÁ PROCURADO
 - /VirtualHost
 - DIRETIVA DE ENCERRAMENTO DE SESSÃO



- **CONFIGURAÇÃO DO SERVIÇO**
- PASSOS PARA CRIAÇÃO DE SERVIDORES VIRTUAIS
 - HABILITAR O SITE VIRTUAL ATRAVÉS DO COMANDO ABAIXO:

a2ensite alfa.atm.org.br

- PARA DESABILITAR O ACESSO AO SITE VIRTUAL:

a2dissite alfa.atm.org.br



- **CONFIGURAÇÃO DO SERVIÇO**
- **PASSOS PARA CRIAÇÃO DE SERVIDORES VIRTUAIS**
 - **HABILITAR/DESABILITAR O SITE VIRTUAL ATRAVÉS DO COMANDO ABAIXO:**
 - # a2ensite alfa.atm.org.br (habilitar)
 - # service apache2 restart
 - # a2dissite alfa.atm.org.br (desabilitar)
 - # service apache2 restart
 - **ADICIONAR ENTRADA NO DNS DO NOME DE ACESSO DO SITE VIRTUAL**



- **ATIVAÇÃO DO SERVIÇO HTTPS**
- **PASSOS PARA NECESSÁRIOS**
 - **HABILITAR/DESABILITAR O RECURSO HTTPS:**
 - # a2enmod ssl (habilitar)
 - # service apache2 restart
 - # a2dismod alfa.atm.org.br (desabilitar)
 - # service apache2 restart

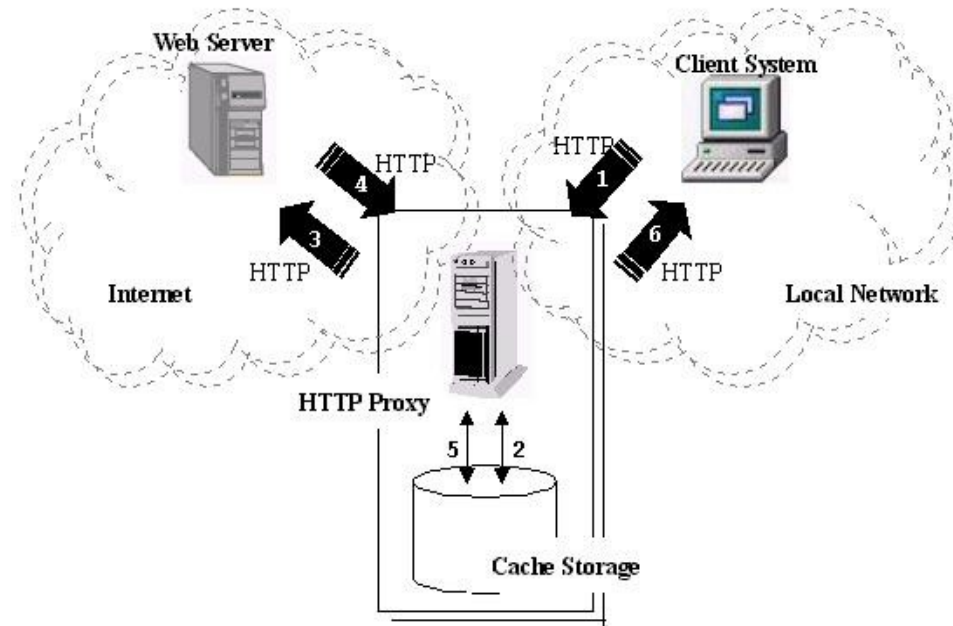


PROXY SQUID



■ PROXY

- UM SERVIDOR PROXY ATENDE AS REQUISIÇÕES DE SERVIÇO DE UM CLIENTE E REPASSA PARA O SERVIDOR FINAL
- A REQUISIÇÃO DO CLIENTE PODE SER UMA ACESSO A UM ARQUIVO, PÁGINA WEB, OU OUTRO RECURSO DISPONÍVEL EM UM SERVIDOR



■ PROXY

■ FUNCIONALIDADES DO SERVIDOR PROXY

- ☐ ALTERAR A SOLICITAÇÃO DO CLIENTE OU A RESPOSTA DO SERVIDOR
- ☐ ARMAZENAR INFORMAÇÕES EM FORMA DE CACHE
- ☐ AUTENTICAÇÃO DE USUÁRIOS
- ☐ FILTRAR CONTEÚDO
- ☐ REDUZIR O CONSUMO DE BANDA

- UM PROXY CACHE PERMITE QUE A REQUISIÇÃO DE UM CLIENTE SEJA ATENDIDA SEM A NECESSIDADE DE CONTACTAR UM SERVIDOR ESPECIFICO, POIS O SERVIDOR PROXY CACHE PODE ARMAZENAR LOCALMENTE OS ARQUIVOS ACESSADOS ANTERIORMENTE, QUANDO ESTES ARQUIVOS FOREM ACESSADOS POSTERIORMENTE OS ARQUIVOS JÁ ESTARÃO DISPONÍVEIS NO CACHE



■ SQUID

■ INSTALAÇÃO

- # apt-get install squid

■ CONFIGURAÇÃO

- A CONFIGURAÇÃO DO SQUID É TOTALMENTE REALIZADA NO ARQUIVO /etc/squid/squid.conf
- O ARQUIVO DE CONFIGURAÇÃO ORIGINAL POSSUI DIVERSAS OPÇÕES COMENTADAS
- NO CURSO IREMOS CRIAR UM ARQUIVO DE CONFIGURAÇÃO SOMENTE COM AS OPÇÕES NECESSÁRIAS
- CRIAR O ARQUIVO CONFORME O CONTEÚDO DO PRÓXIMO SLIDE



■ SQUID

■ CONFIGURAÇÃO BÁSICA

#Porta TCP onde o squid recebe requisições

http_port 3128

Nome do Servidor

visible_hostname curso_proxy_squid

#Cria uma politica (classificação) chamada “all”

#que inclui qualquer origem

acl all src 0.0.0.0/0.0.0.0

#Executa uma ação sobre a politica politica “all”

http_access allow all



- **SQUID**
- **GERENCIAMENTO**
 - # service squid stop/start/restart
 - # /etc/init.d/squid stop/start/restart
- **VERIFICAÇÃO DO PROCESSO SQUID**
 - # ps aux | grep squid
- **VERIFICAÇÃO DA PORTA DE COMUNICAÇÃO**
 - # netstat -an | grep 3128
- **QUANDO O SQUID EM EXECUÇÃO PODEMOS**
 - **ENCERRAR A EXECUÇÃO**
 - squid -k shutdown
 - **RECARREGAR O SQUID**
 - squid -k reconfigure



- **SQUID**
- CONFIGURAÇÃO DO BROWSER IE
- CONFIGURAÇÃO DO BROWSER FIREFOX
- ACESSANDO O SERVIDOR ATRAVÉS DO BROWSER



■ SQUID

■ CONFIGURAÇÃO BÁSICA

- TODA CONFIGURAÇÃO DO SQUID, RESUME-SE AO COMANDO “acl” e “http_access”
- UMA “acl” FAZ A CLASSIFICAÇÃO DE UMA SOLICITAÇÃO,
- AS “acl” DESCREVEM UMA CARACTERÍSTICA DE UMA SOLICITAÇÃO
- SE SOLICITAÇÃO POSSUI A CARACTERÍSTICA, ENTÃO ELA SERÁ CLASSIFICADA COM O NOME DA ACL



■ SQUID

■ CONFIGURAÇÃO BÁSICA

- UTILIZANDO O PARÂMETRO “src” É VERIFICADO O ENDEREÇO DE ORIGEM DA SOLICITAÇÃO.
- EXEMPLO DE ESCRITA COM “src”
 - QUALQUER ENDEREÇO DE ORIGEM
 - 0.0.0.0/0.0.0.0
 - ENDEREÇO DE ORIGEM PERTENCE A REDE
 - 10.1.12.0/255.255.255.0
 - ENDEREÇO DE ORIGEM É UM HOST ESPECIFICO
 - 10.1.12.10/255.255.255.255



■ SQUID

■ CONFIGURAÇÃO BÁSICA

□ CONSIDERE A CONFIGURAÇÃO ABAIXO

```
acl origem_a src 10.1.1.0/255.255.255.0
```

```
acl origem_a src 10.1.2.0/255.255.255.0
```

```
acl origem_b src 20.1.1.0/255.255.255.0
```

```
acl origem_host_a src 10.1.1.1/255.255.255.255
```

```
acl qualquer_outro src 0.0.0.0/0.0.0.0
```

□ UMA SOLICITAÇÃO PROVENIENTE DO ENDEREÇO DE 10.1.1.10 SERÁ CLASSIFICADO COMO “origem_a”

□ UMA SOLICITAÇÃO PROVENIENTE DO ENDEREÇO DE 10.1.2.10 SERÁ CLASSIFICADO COMO “origem_a”

□ UMA SOLICITAÇÃO PROVENIENTE DO ENDEREÇO DE 10.1.1.1 SERÁ CLASSIFICADO COMO “acl origem_a” e “origem_host_a”



- **SQUID**

- CONFIGURAÇÃO BÁSICA

- CONSIDERE A CONFIGURAÇÃO ABAIXO

- `acl origem_a src 10.1.1.0/255.255.255.0`

- `acl origem_a src 10.1.2.0/24`

- `acl origem_b src 20.1.1.0/255.255.255.0`

- `acl origem_host_a src 10.1.1.1/255.255.255.255`

- `acl qualquer_outro src 0.0.0.0/0.0.0.0`

- UMA SOLICITAÇÃO PROVENIENTE DO ENDEREÇO DE 30.1.1.10 SERÁ CLASSIFICADO COMO “qualquer_outro”



- **SQUID**

- CONFIGURAÇÃO BÁSICA

- CONTROLANDO O ACESSO

- UMA VEZ QUE FOI ESPECIFICADO AS “acl”, O PRÓXIMO PASSO É CONTROLAR O ACESSO AO PROXY ATRAVÉS DO COMANDO “http_access” COMO MOSTRADO ABAIXO:

- ACEITA A SOLITAÇÃO

- http_access allow nome_acl

- http_access allow all

- REJEITA A SOLICITAÇÃO

- http_access deny nome_acl

- http_access allow all



■ SQUID

■ CONFIGURAÇÃO BÁSICA

□ PROCESSAMENTO DAS REGRAS

```
acl origem_a src 10.1.1.0/255.255.255.0
acl origem_a src 10.1.2.0/255.255.255.0
acl origem_b src 20.1.1.0/255.255.255.0
acl origem_host_a src 10.1.1.1/255.255.255.255
acl qualquer_outro src 0.0.0.0/0.0.0.0
http_access allow origem_a # regra 1
http_access allow origem_b # regra 2
http_access deny orig_host_a # regra 3
http_access deny qualquer_outro # regra 4
```

□ O PROCESSAMENTO DAS REGRAS É SEQUENCIAL, INICIANDO PELA REGRA 1, PASSANDO POR 2,3 E 4

□ APÓS O PROCESSAMENTO DE UMA REGRA O PROCESSAMENTO É INTERROMPIDO E OUTRAS REGRAS ABAIXO SÃO IGNORADAS



■ SQUID

■ CONFIGURAÇÃO BÁSICA

□ PROCESSAMENTO DAS REGRAS

```
acl origem_a src 10.1.1.0/255.255.255.0
acl origem_a src 10.1.2.0/255.255.255.0
acl origem_b src 20.1.1.0/255.255.255.0
acl origem_host_a src 10.1.1.1/255.255.255.255
acl qualquer_outro src 0.0.0.0/0.0.0.0
http_access allow origem_a # regra 1
http_access allow origem_b # regra 2
http_access deny orig_host_a # regra 3
http_access deny qualquer_outro # regra 4
```

□ EXEMPLO 1.

- UMA SOLICITAÇÃO PROVENIENTE DO ENDEREÇO 10.1.1.30, SERÁ PROCESSADO ATRAVÉS DA REGRA 1, PERMITINDO O ACESSO AO PROXY



■ SQUID

■ CONFIGURAÇÃO BÁSICA

□ PROCESSAMENTO DAS REGRAS

```
acl origem_a src 10.1.1.0/255.255.255.0
acl origem_a src 10.1.2.0/255.255.255.0
acl origem_b src 20.1.1.0/255.255.255.0
acl origem_host_a src 10.1.1.1/255.255.255.255
acl qualquer_outro src 0.0.0.0/0.0.0.0
http_access allow origem_a # regra 1
http_access allow origem_b # regra 2
http_access deny orig_host_a # regra 3
http_access deny qualquer_outro # regra 4
```

□ EXEMPLO 2.

□ UMA SOLICITAÇÃO PROVENIENTE DO ENDEREÇO 10.1.1.1, SERÁ PROCESSADO ATRAVÉS DA REGRA 1, PERMITINDO O ACESSO AO PROXY



■ SQUID

■ CONFIGURAÇÃO BÁSICA

□ PROCESSAMENTO DAS REGRAS

```
acl origem_a src 10.1.1.0/255.255.255.0
acl origem_a src 10.1.2.0/255.255.255.0
acl origem_b src 20.1.1.0/255.255.255.0
acl origem_host_a src 10.1.1.1/255.255.255.255
acl qualquer_outro src 0.0.0.0/0.0.0.0
http_access allow origem_a # regra 1
http_access allow origem_b # regra 2
http_access deny orig_host_a # regra 3
http_access deny qualquer_outro # regra 4
```

□ EXEMPLO 3.

□ UMA SOLICITAÇÃO PROVENIENTE DO ENDEREÇO 20.1.1.1, SERÁ PROCESSADO ATRAVÉS DA REGRA 2, PERMITINDO O ACESSO AO PROXY



■ SQUID

■ CONFIGURAÇÃO BÁSICA

□ PROCESSAMENTO DAS REGRAS

```
acl origem_a src 10.1.1.0/255.255.255.0
acl origem_a src 10.1.2.0/255.255.255.0
acl origem_b src 20.1.1.0/255.255.255.0
acl origem_host_a src 10.1.1.1/255.255.255.255
acl qualquer_outro src 0.0.0.0/0.0.0.0
http_access allow origem_a # regra 1
http_access allow origem_b # regra 2
http_access deny orig_host_a # regra 3
http_access deny qualquer_outro # regra 4
```

□ EXEMPLO 4.

□ UMA SOLICITAÇÃO PROVENIENTE DO ENDEREÇO 30.1.1.1 SERÁ CLASSIFICADA COMO “qualquer_outro” E SERÁ PROCESSADO ATRAVÉS DA REGRA 4, BLOQUEANDO O ACESSO AO PROXY



■ SQUID

■ CONFIGURAÇÃO BÁSICA

□ PROCESSAMENTO DAS REGRAS

```
acl origem_a src 10.1.1.0/255.255.255.0
acl origem_a src 10.1.2.0/255.255.255.0
acl origem_b src 20.1.1.0/255.255.255.0
acl origem_host_a src 10.1.1.1/255.255.255.255
acl qualquer_outro src 0.0.0.0/0.0.0.0
http_access deny orig_host_a # regra 3
http_access allow origem_a # regra 1
http_access allow origem_b # regra 2
http_access deny qualquer_outro # regra 4
```

□ EXEMPLO 5.

□ PARA BLOQUEAR O ACESSO DO HOST 10.1.1.1 (origem_host_a) DEVEMOS ALTERAR A SEQUENCIA DO PROCESSAMENTO DAS REGRAS, COLOCANDO A REGRA 3 EM PRIMEIRO LUGAR



■ SQUID

■ CONFIGURAÇÃO BÁSICA

□ PROCESSAMENTO DAS REGRAS

```
acl origem_a src 10.1.1.0/255.255.255.0
acl origem_a src 10.1.2.0/255.255.255.0
acl origem_b src 20.1.1.0/255.255.255.0
acl origem_host_a src 10.1.1.1/255.255.255.255
acl qualquer_outro src 0.0.0.0/0.0.0.0
http_access deny orig_host_a # regra 3
http_access allow origem_a # regra 1
http_access allow origem_b # regra 2
http_access deny qualquer_outro # regra 4
```

□ OBSERVAÇÃO

- A REGRA 4 DEVE SER SEMPRE A ÚLTIMA DA LISTA E PREVINI QUE QUALQUER OUTRA SITUAÇÃO QUE NÃO FOI PREVISTA, SERÁ BLOQUEADO



■ SQUID

■ CONFIGURAÇÃO BÁSICA

□ VERIFICANDO A PORTA DE COMUNICAÇÃO

```
acl ssl_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https, snews
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl Safe_ports port 901 # SWAT
acl Safe_ports port 1025-65535 # portas altas
```



■ SQUID

■ SITES COM PROBLEMAS DE ACESSO

□ ALGUNS SITES NÃO FUNCIONAM MUITO BEM QUANDO SÃO ACESSADOS ATRAVÉS DE PROXY E PARA SOLUCIONAR ESTE PROBLEMA, UTILIZAMOS A OPÇÃO “always_direct” ATRAVÉS DA SEGUINTE FORMA:

```
□ acl site_problema dstdomain .abc.com.br  
always_direct allow site_problema
```

*** note o ponto na frete do nome do domínio ****

□

□ ESTA CONTRUÇÃO FARÁ COM QUE SERVIDOR PROXY REPASSE OS ACESSOS DIRETAMENTE PARA AO “site_problema”

□ ESTA REGRA DEVE VIR ANTES DE QUALQUER OUTRA



- **SQUID**

- CONFIGURAÇÃO DE CACHE

- O SERVIDOR PROXY ARMAZENA AS PÁGINAS LOCALMENTE (CACHE) PARA OFERECER AOS CLIENTES DE FORMA RÁPIDA
- PARA AUMENTAR O DESEMPENHO, O SQUID TRABALHA COM DOIS TIPOS DE CACHE
 - CACHE RÁPIDO E PEQUENO ARMAZENADO EM MEMÓRIA RAM
 - PEQUENAS PÁGINAS E IMAGENS SERÃO ENTREGUES INSTANTANEAMENTE
 - CACHE LENTO E MAIOR ARMAZENADO EM HD
 - ARMAZENA ARQUIVOS MAIORES COMO ATUALIZAÇÃO DO WINDOWS UPDATE



■ SQUID

■ CONFIGURAÇÃO DE CACHE

- TAMANHO DA MEMÓRIA RAM DISPONÍVEL PARA CACHE

cache_mem 64 MB

- NORMALMENTE O TAMANHO DA MEMÓRIA DISPONÍVEL PARA CACHE EM UM SERVIDOR NÃO DEDICADO É DE 32 A 64 MB

- PARA UMA SERVIDOR DEDICADO, NORMALMENTE 1/3 DA MEMÓRIA RAM

- POR EXEMPLO: UM SERVIDOR PROXY DEDICADO COM UM 1GB DE MEMÓRIA PODEMOS ALOCAR 350MB DE MEMÓRIA RAM

cache_mem 350 MB

- SE FOR ALOCADO MUITO ESPAÇO EM MEMÓRIA PARA O CACHE RÁPIDO PODE SER QUE FALTE MEMÓRIA PARA OUTRAS APLICAÇÕES



■ SQUID

■ CONFIGURAÇÃO DE CACHE

- APÓS DEFINIR O TAMANHO DO CACHE RÁPIDO, IREMOS DEFINIR O TAMANHO MÁXIMO DOS ARQUIVOS QUE SERÃO ARMAZENADOS NESTE CACHE ATRAVÉS DA DIRETIVA

`maximum_object_size_in_memory 64 KB`

- OS ARQUIVOS QUE ULTRAPASSAREM ESTE TAMANHO, (64 KB) IRÃO DIRETAMENTE PARA O CACHE EM HD
- PARA DEFINIR O TAMANHO DOS ARQUIVOS QUE SERÃO ARMAZENADOS EM HD (A MAIORIA) UTILIZAMOS DUAS DIRETIVAS QUE DETERMINAM O TAMANHO MÁXIMO E MÍNIMO

- `maximum_object_size 512 MB`

- `minimum_object_size 0 KB`



■ SQUID

■ CONFIGURAÇÃO DE CACHE

- O CACHE EM DISCO IRÁ CONSUMIR NO MÁXIMO UM ESPAÇO PRÉ-DEFINIDO, SENDO ASSIM É NECESSÁRIO QUE OS ARQUIVOS MAIS ANTIGOS SEJAM DESCARTADOS PARA QUE NOVOS ARQUIVOS SEJAM ARMAZENADOS
- PARA INICIAR O DESCARTE DE ARQUIVOS ANTIGOS, IREMOS DETERMINAR UM PERCENTUAL DE UTILIZAÇÃO DO CACHE EM HD. POR PADRÃO, SEMPRE QUE O CACHE ATINGIR 95% DE USO, OS ARQUIVOS MAIS ANTIGOS SERÃO DESCARTADOS ATÉ QUE A PERCENTAGEM VOLTE PARA UM NÚMERO ABAIXO DE 90%
- AS DIRETIVAS QUE CONTROLAM ESTE ESPAÇO SÃO:
cache_swap_low 90
cache_swap_high 95



■ SQUID

■ CONFIGURAÇÃO DE CACHE

- O CACHE EM HD É ARMAZENADO NO SISTEMA DE ARQUIVOS DO LINUX O LOCAL É INDICADO ATRAVÉS DA DIRETIVA
- `cache_dir ufs /var/spool/squid 2048 16 256`
- Ufs INDICA O TIPO DE SISTEMA DE ARQUIVO
- `/var/spool/squid` INDICA A PASTA ONDE OS ARQUIVOS DE CACHE SERÃO ARMAZENADOS
- 2048 (MB) INDICA O ESPAÇO MÁXIMO QUE SERÁ UTILIZADO PARA ARMAZENAR OS ARQUIVOS DE CACHE, O DEFAULT É 100 MB
- 16 QUANTIDADE DE PASTAS QUE SERÃO CRIADAS ABAIXO DE `“/var/spool/squid`
- 256 QUANTIDADE DE SUBPASTAS QUE SERÃO CRIADAS DENTRO DE CADA PASTA (16)



- **SQUID**
- CONFIGURAÇÃO DE CACHE
 - PODEMOS ARMAZENAR OS LOGS DE ACESSO AO SQUID. O PADRÃO É USAR O DIRETÓRIO “/var/log/squid/access.log” MAS PODEMOS ALTERAR O DIRECIONAMENTO ATRAVÉS DA DIRETIVA ABAIXO

`cache_access_log /var/log/squid/access.log`



■ SQUID

■ CONFIGURAÇÃO DE CACHE

- OUTRA DIRETIVA QUE AFETA O DESEMPENHO DO PROXY É A ATUALIZAÇÃO DAS PÁGINAS QUE ESTÃO EM CACHE AS TRÊS LINHAS ABAIXO NECESSITAM ESTAR PRESENTES. ELIMINANDO UMA OS SQUID IGNORA AS OUTRAS DUAS

`refresh_pattern ^ftp: 15 20% 2280`

`refresh_pattern ^gopher: 15 0% 2280`

`refresh_pattern . 15 20% 2280`

- OS TRÊS NÚMEROS INDICAM O INTERVALO EM MINUTOS QUE O SQUID IRÁ AGUARDAR ANTES DE VERIFICAR SE UM ÍTEM DO CACHE (UMA PÁGINA) FOI ATUALIZADO PARA CADA UM DOS PROTOCOLOS

□



■ SQUID

■ CONFIGURAÇÃO DE CACHE

refresh_pattern ^ftp: 15 20% 2280

refresh_pattern ^gopher: 15 0% 2280

refresh_pattern . 15 20% 2280

- O PRIMEIRO NÚMERO (15) INDICA QUE O SQUID VERIFICARÁ (A CADA ACESSO) SE A PÁGINA OU ARQUIVOS COM MAIS DE 15 MINUTOS FORAM ATUALIZADOS (VERIFICA O TAMANHO DO ARQUIVO)
- SE NÃO HOUE ALTERAÇÃO, O PROXY CONTINUA FORNECENDO O ARQUIVO PARA OS CLIENTES, DESTA FORMA, ECONOMIZANDO BANDA
- SE HOUE A ALTERAÇÃO, O PROXY IRÁ ATUALIZAR O CACHE, ISTO É, CONSULTAR A FONTE DA PÁGINA E GRAVAR EM DISCO E FINALMENTE FORNECER A PÁGINA PARA O CLIENTE



■ SQUID

■ CONFIGURAÇÃO DE CACHE

refresh_pattern ^ftp: 15 20% 2280

refresh_pattern ^gopher: 15 0% 2280

refresh_pattern . 15 20% 2280

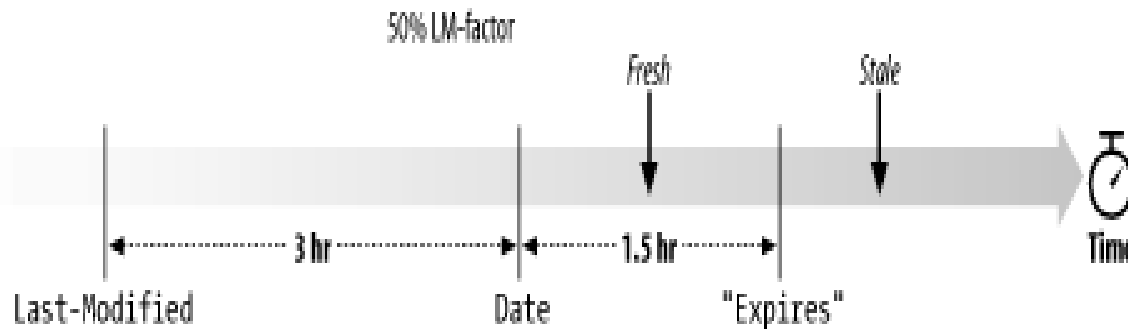
- O TERCEIRO NÚMERO (2280, EQUIVALENTE A DOIS DIAS) INDICA O TEMPO MÁXIMO, DEPOIS DO QUAL QUE O OBJETO É SEMPRE VERIFICADO
- NESTE CASO, O SQUID FAZ UMA VARREDURA EM SEU CACHE E DETECTAM AS PÁGINAS QUE POSSUI TEMPO DE VALIDADE ACIMA DO TEMPO MÁXIMO (2280) E REALIZA A ATUALIZAÇÃO DA PAGINA OU ARQUIVO
- OS PROTOCOLOS RELEVANTES SÃO FTP E HTTP, O GOPHER PERDEU A RELEVANCIA, MAS NECESSITA ESTAR PRESENTE



■ SQUID

■ CONFIGURAÇÃO DE CACHE

- O SEGUNDO NÚMERO (20%) É CONHECIDO COMO FATOR LM (LAST MODIFIED FACTOR)
-
- ESTE FATOR É UMA CORRESPONDE AO TEMPO QUE UM OBJETO POSSUI E QUE ESTÁ ACIMA DO TEMPO MÍNIMO E ABAIXO DO TEMPO MÁXIMO DE EXPIRAÇÃO DO CACHE



- **SQUID**
- **CONFIGURAÇÃO DE CACHE**

```
http_port 3128
visible_hostname curso_proxy_squid
cache_mem 64 MB
maximum_object_size_in_memory 64 KB
maximum_object_size 512 MB
minimum_object_size 0 KB
cache_dir ufs /var/spool/squid 2048 16 256
cache_swap_low 90
cache_swap_high 95
acl origem_a src 10.1.1.0/255.255.255.0
acl origem_a src 10.1.2.0/255.255.255.0
acl origem_b src 20.1.1.0/255.255.255.0
acl origem_host_a src 10.1.1.1/255.255.255.255
acl qualquer_outro src 0.0.0.0/0.0.0.0
http_access deny orig_host_a # regra 3
http_access allow origem_a # regra 1
http_access allow origem_b # regra 2
http_access deny qualquer_outro # regra 4
```



■ SQUID

- PARA BLOQUEAR O ACESSO A SITES INDESEJADOS QUE CONTENHAM PORNOGRAFIA OU OUTROS DE CONTEÚDO DUVIDOSO, UTILIZAMOS O PARÂMETRO “dstdomain” NA CLASSIFICAÇÃO DA SOLICITAÇÃO
- EXEMPLO:
 - `acl sites_bloqueados dstdomain .orkut.com .sex.com nave.py`
 - `acl site_jogos dstdomain .playstation.com.br .gameover.com`
 - `http_access deny site_bloqueados`
 - `http_access deny site_jogos`
- ANOTE O PONTO NA FRENTE DO NOME DO DOMÍNIO, SEM O PONTO OCORRERÁ MATCH EXATO
- PODEMOS UTILIZAR UM ARQUIVO QUANDO A QUANTIDADE DE SITES TORNA-SE MUITO GRANDE PARA SER ESCRITO DENTRO DO ARQUIVO DE CONFIGURAÇÃO DO SQUID



- **SQUID**
- BLOQUEANDO O ACESSO A SITES OU PALAVRAS
 - ESCRREVEMOS OS SITES DENTRO DE UM ARQUIVO (/etc/squid/site_bloqueados) COMO O EXEMPLO ABAIXO:

orkut.com

www.orkut.com

playboy.abril.com.br

www.myspace.com

```
acl sites_bloqueados url_regex -i "/etc/squid/sites_bloqueados"  
http_access deny sites_bloqueados
```



- **SQUID**
- BLOQUEANDO O ACESSO A SITES OU PALAVRAS
 - TAMBÉM PODEMOS BLOQUEAR O ACESSO DIRETAMENTE ATRAVÉS DO ENDEREÇO IP DE DESTINO UTILIZANDO O PARÂMETRO “dst” NA CLASSIFICAÇÃO DA SOLICITAÇÃO
 - EXEMPLO:

```
acl ip_bloqueados dst 10.1.1.1 20.1.1.1 30.1.1.1  
http_access deny ip_bloqueados
```



■ SQUID

■ BLOQUEANDO O ACESSO A SITES OU PALAVRAS

- OUTRA FORMA DE BLOQUEAR O ACESSO A SITES É UTILIZAR O PARAMETRO “dstdom_regex” QUE UTILIZA AS PALAVRAS INCLUÍDAS NA URL DE ACESSO, COMO POR EXEMPLO:

URL = `http://www.sexototal.com.br`

- ADICIONAMOS AS PALAVRAS DENTRO DE UM ARQUIVO (`/etc/squid/palavras_proibidas.txt`)

`xxx`

`sexo`

`teens`

```
acl palavras dstdom_regex "/etc/squid/palavrasproibidas"
```

```
http_access deny palavras
```



■ SQUID

■ BLOQUEANDO O ACESSO POR HORÁRIO

- OUTRA FORMA DE BLOQUEAR ACESSOS É ATRAVÉS DE HORÁRIO UTILIZANDO O PARAMETRO “time” CONFORME MOSTRADO ABAIXO

```
acl madrugada time 00:00-06:00
```

```
http_access deny madrugada
```

```
acl almoco time 12:00-14:00
```

```
http_access deny almoco
```

- PODEMOS LIBERAR O ACESSO A ALGUNS AO SITE ORKUT NO HORÁRIO DO ALMOÇO SOMENTE COMBINAMOS DUAS “acl” MOSTRADO ABAIXO

```
acl almoco time 12:00-14:00
```

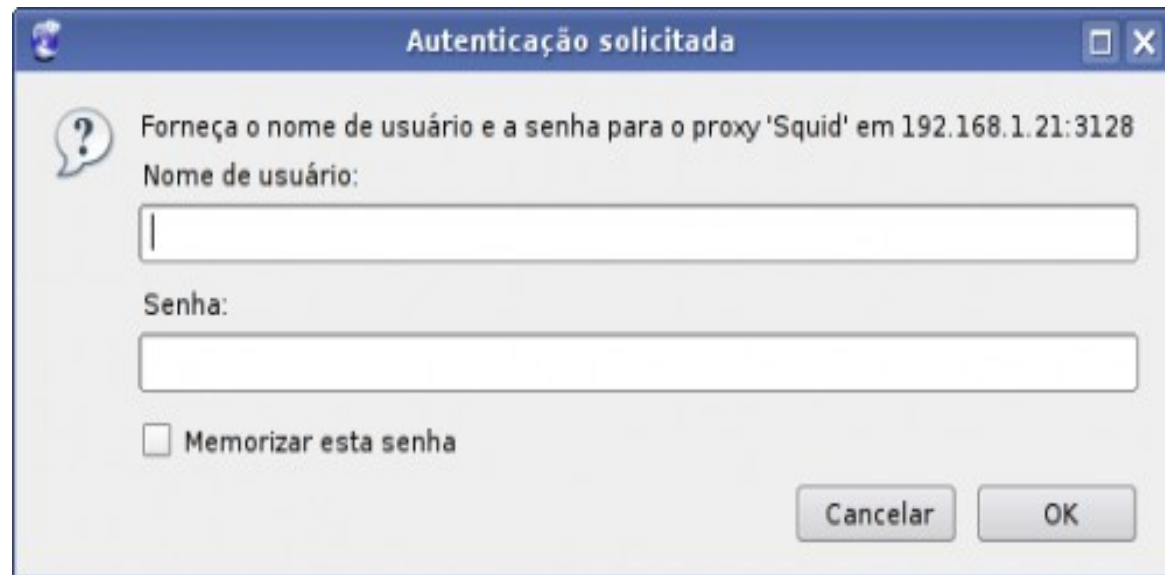
```
acl orkut dstdomain orkut.com www.orkut.com
```

```
http_access allow orkut almoco
```

```
http_access deny orkut
```



- SQUID
- PROXY COM AUTENTICAÇÃO
 - PODEMOS AUMENTAR A SEGURANÇA DO PROXY, EXIGINDO QUE O CLIENTE UTILIZE UMA USUÁRIO/SENHA PARA NAVEGAR NA INTERNET
 - ESTE RECURSO PODE SER UTILIZADO PARA REALIZAR AUDITORIA DE ACESSO EM CASO DE NECESSIDADE



■ SQUID

■ PROXY COM AUTENTICAÇÃO

- PARA ATIVAR A AUTENTICAÇÃO É NECESSÁRIO ADICIONAR AS LINHAS ABAIXO

auth_param basic realm Squid

auth_param basic program /usr/lib/squid/ncsa_auth
/etc/squid/squid_passwd

acl autenticados proxy_auth REQUIRED

http_access allow autenticados

- QUANDO O CLIENTE ENVIAR UMA SOLICITAÇÃO PARA O PROXY, SERÁ ENVIADO UMA TELA COM SOLICITAÇÃO DE AUTENTICAÇÃO, CONFORME MOSTRADO ANTERIORMENTE
- UMA VEZ QUE O USUÁRIO ESTEJA AUTENTICADO, É LIBERADO O ACESSO AO PROXY



■ SQUID

■ PROXY COM AUTENTICAÇÃO

- O PARAMETRO “auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/squid_passwd” ATIVA A AUTENTICAÇÃO DO USUÁRIO
- O PROGRAMA ncsa_auth É O PROGRAMA QUE REALIZA A AUTENTICAÇÃO. ESTE PROGRAMA ESTÁ PRESENTE NO PACOTE DE INSTALAÇÃO DO APACHE2
- O ARQUIVO “squid_passwd” CONTÉM AS CONTAS DE ACESSO AO PROXY E DEVE SER CRIADO ATRAVÉS DA APLICAÇÃO “htpasswd” TAMBÉM PRESENTE NO PACOTE DE INSTALAÇÃO DO APACHE2



■ SQUID

■ PROXY COM AUTENTICAÇÃO

- PARA CRIAR O ARQUIVO DE AUTENTICAÇÃO, SIGA OS PASSOS ABAIXO:

```
# htpasswd -c /etc/squid/squid_passwd aluno1
```

New password:

Re-type new password:

Adding password for user aluno1

- PARA ALTERAR A SENHA DE UM USUÁRIO, SIGA OS PASSOS ABAIXO:

```
# htpasswd /etc/squid/squid_passwd aluno1
```

- PARA REMOVER UM USUÁRIO DA BASE DE DADOS, SIGA OS PASSOS ABAIXO:

```
#htpasswd -D /etc/squid/squid_passwd aluno1
```



- **SQUID**

- PROXY COM AUTENTICAÇÃO

- PARA PERMITIR QUE DOIS USUÁRIOS (aluno1 e aluno2) TENHA ACESSO IRRESTRITO AO PROXY E OS DEMAIS USUÁRIOS, APENAS NO HORÁRIO DO ALMOÇO

```
auth_param basic program /usr/lib/squid/nsc_auth  
/etc/squid/squid_passwd
```

```
acl autenticados proxy_auth REQUIRED
```

```
acl permitidos proxy_auth aluno1 aluno2
```

```
acl almoco time 12:00-13:00
```

```
http_access allow permitidos
```

```
http_access allow autenticados almoco
```



- **SQUID**
- CONFIGURAÇÃO AUTOMÁTICA DO PROXY
 - PARA EVITAR O TRABALHO ADMINISTRATIVO DE CONFIGURAÇÃO DAS ESTAÇÕES COM O ENDEREÇO DO PROXY, UTILIZAMOS UM SCRIPT PAC (PROXY AUTO-CONFIGURATION), QUE É UM ARQUIVO DISPONIBILIZADO ATRAVÉS DO SERVIDOR WEB
 - O SERVIDOR APACHE2 DEVE ESTAR INSTALADO
 - O ARQUIVO ABAIXO DEVE SER CRIADO NO PASTA /var/www/proxy.dat

```
function FindProxyForURL(url, host)
{
return "PROXY 192.168.1.1:3128";
}
```



- **SQUID**

- CONFIGURAÇÃO AUTOMÁTICA DO PROXY

- CONFIGURAÇÃO NO FIREFOX

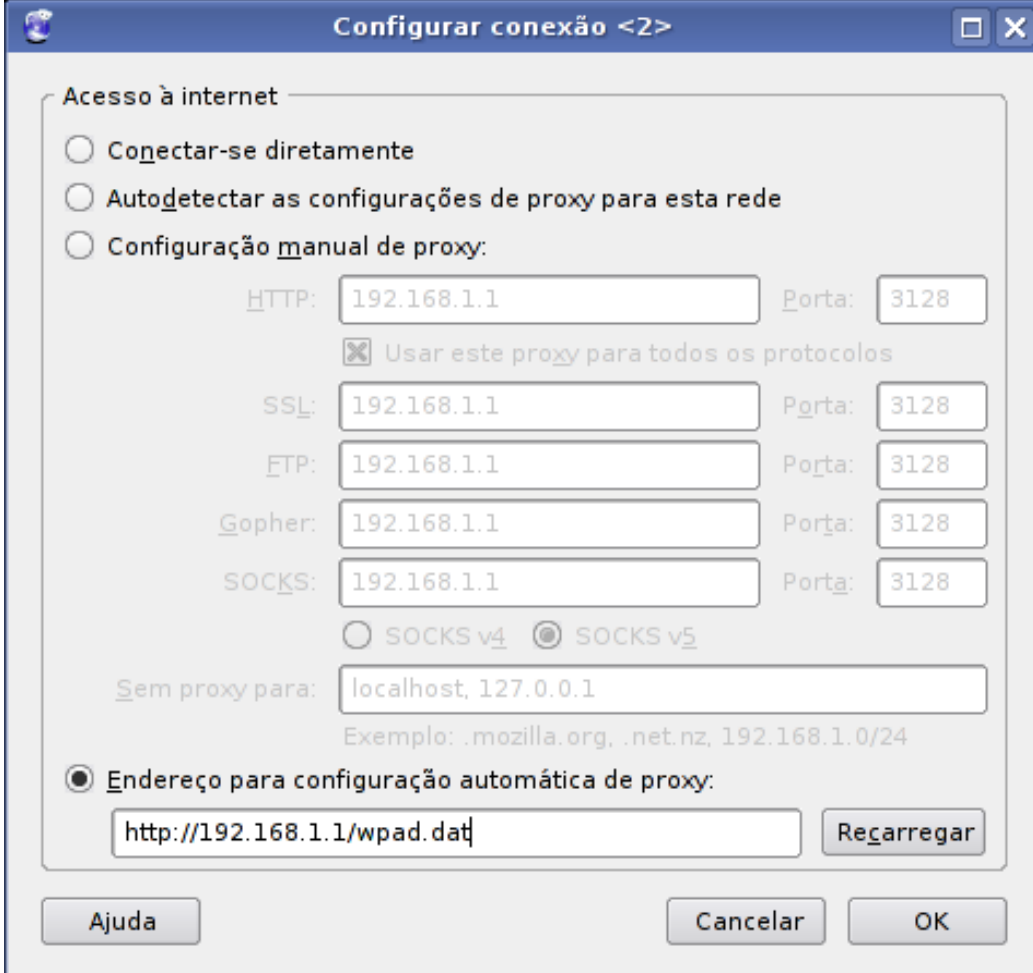
- EDITAR → PREFERÊNCIAS → AVANÇADO → REDE → CONFIGURAÇÕES → ENDEREÇO PARA CONFIGURAÇÃO AUTOMÁTICA DE PROXY → PREENCHER O QUADRO COM O CONTEÚDO “http://endereço ip do servidor/nome do arquivo”

- CONFIGURAÇÃO NO WINDOWS EXPLORER

- FERRAMENTAS → OPÇÕES DE INTERNET → CONEXÕES → CONFIGURAÇÕES DE LAN → MARCAR A OPÇÃO “usar script de configuração automática” → PREENCHER O QUADRO “Endereço” COM O CONTEÚDO “http://endereço ip do servidor/nome do arquivo”



- SQUID
- CONFIGURAÇÃO AUTOMÁTICA DO PROXY - FIREFOX



Configurar conexão <2>

Acesso à internet

☐ Conectar-se diretamente

☐ Autodetectar as configurações de proxy para esta rede

☐ Configuração manual de proxy:

HTTP: 192.168.1.1 Porta: 3128

☒ Usar este proxy para todos os protocolos

SSL: 192.168.1.1 Porta: 3128

FTP: 192.168.1.1 Porta: 3128

Gopher: 192.168.1.1 Porta: 3128

SOCKS: 192.168.1.1 Porta: 3128

☐ SOCKS v4 ☒ SOCKS v5

Sem proxy para: localhost, 127.0.0.1

Exemplo: .mozilla.org, .net.nz, 192.168.1.0/24

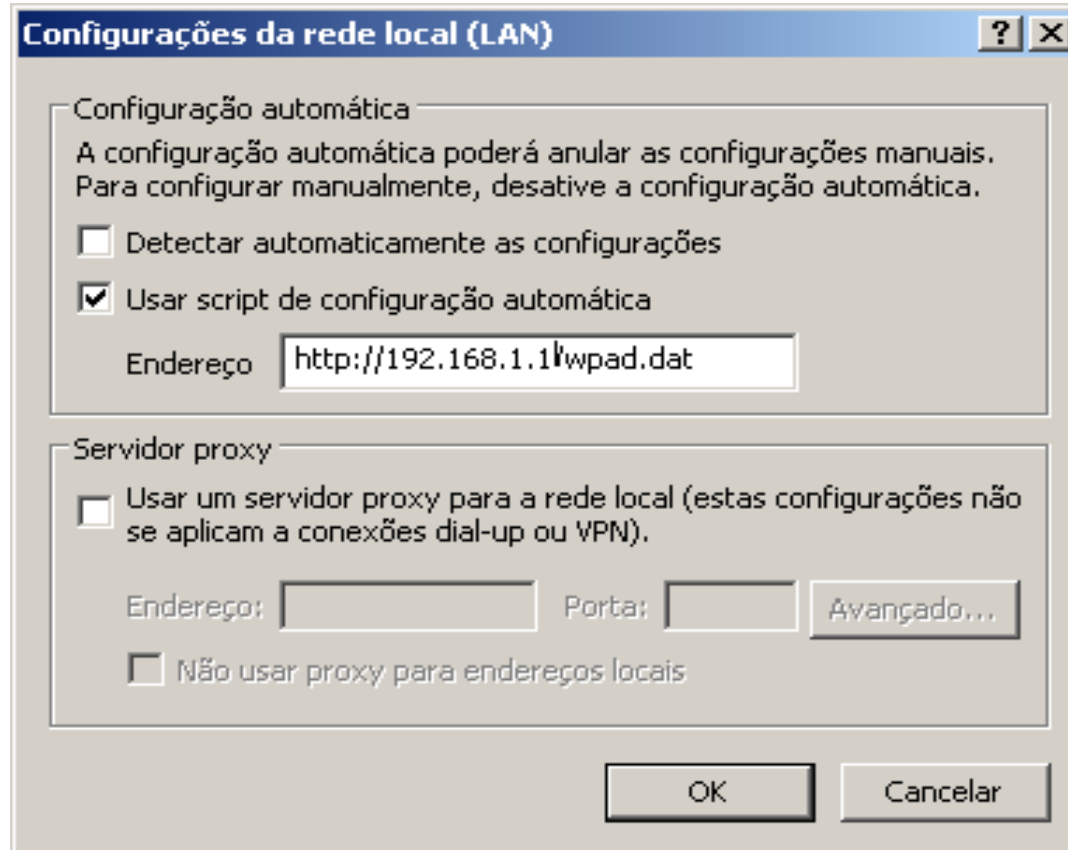
☒ Endereço para configuração automática de proxy:

http://192.168.1.1/wpad.dat

Ajuda Cancelar OK



- SQUID
- CONFIGURAÇÃO AUTOMÁTICA DO PROXY - IE



- **SQUID**

- CONFIGURAÇÃO AUTOMÁTICA DO PROXY – VIA DHCP

ddns-update-style none;

default-lease-time 600;

max-lease-time 7200;

authoritative;

option wpad-url code 252 = text;

subnet 192.168.1.0 netmask 255.255.255.0 {

range 192.168.1.100 192.168.1.199;

option routers 192.168.1.1;

option domain-name-servers 208.67.222.222;

option broadcast-address 192.168.1.255;

option wpad-url "http://192.168.1.1/wpad.dat\n";

}



■ SQUID

■ CONSTRUÇÃO DO CACHE

□ COMO VISTO ANTERIORMENTE, O PARAMETRO ABAIXO DETERMINA A CRIAÇÃO DO CACHE

□ `cache_dir ufs /var/spool/squid 2048 16 256`

□ A ESTRUTURA DE DIRETÓRIOS DO CACHE EM DISCO É CONSTRUÍDO ATRAVÉS DO COMANDO ABAIXO

□ `squid -z`

□ PARA AUMENTAR O TAMANHO DO CACHE EM DISCO, É NECESSÁRIO ADICIONAR UMA NOVA ENTRADA NO ARQUIVO DE CONFIGURAÇÃO E REPETIR O COMANDO DE CRIAÇÃO DO CACHE

□



- **SQUID**
- **CONSTRUÇÃO DO CACHE**

□ EXEMPLO

```
http_port 3128
visible_hostname curso_squid
acl all src 0.0.0.0/0.0.0.0
http_access allow all

#-----

#   cache aumentado

#-----

cache_dir ufs /var/spool/squid 100 16 256
cache_dir ufs /vol2/spool/squid1 100 16 256
```



- **SQUID**
- **CONSTRUÇÃO DO CACHE**
 - **EXEMPLO**

```
# chown proxy.proxy /vol2/spool/squid1
```

```
# su - proxy
```

```
# squid -z
```

```
2011/12/20 16:56:11| Creating Swap Directories
```

```
# ls -la /vol2/squid/squid1
```

```
□
```

```
□ VEREMOS A ESTRUTURA DO CACHE QUE FOI CRIADA
```

```
□ O CACHE INICIAL EXISTENTE NÃO É AFETADO PELO COMANDO
```

