

Sistema Operacional

Unidade 12 – Comandos de Rede e Acesso
Remoto

Ubuntu 12.04 LTS
Precise Pangolin



QI ESCOLAS E FACULDADES
Curso Técnico em Informática

SUMÁRIO

INTRODUÇÃO	3
Protocolo de rede	3
Protocolo TCP/IP	3
Máscara de sub-rede.....	3
Hostname	3
COMANDOS BÁSICOS DE REDE LINUX	4
ip addr show.....	4
ifconfig.....	4
ping	5
ACESSO REMOTO VIA SSH	5
SSH	5
SSH no Windows?.....	5
Porta padrão	5
Como funciona?.....	5
Instalação	6
Acessando um computador remoto	6
Atributo -X.....	6
TRANSFERINDO ARQUIVOS COM SCP	6
TRANSFERINDO ARQUIVOS VIA SFTP (COM NAUTILUS)	7
ACESSANDO LINUX VIA SSH ATRAVÉS DO SISTEMA WINDOWS (COM PUTTY)	8
Efetuando download do software PuTTY.	8

INTRODUÇÃO

Uma rede é um conjunto de computadores interligados permitindo que se comuniquem entre si.

Para conseguirmos acessar um computador remotamente precisamos entender alguns conceitos básicos de rede, são eles:

Protocolo de rede

Um protocolo de rede é utilizado pelos computadores para estabelecer a comunicação entre si, ou seja, os computadores só conseguirão se comunicar se estiverem utilizando os mesmos protocolos.

Protocolo TCP/IP

Esse sem dúvida é o protocolo de rede mais conhecido e utilizado. Na verdade o TCP/IP é um conjunto de protocolos utilizados na comunicação entre computadores dentro de uma rede seja ela local ou global (no caso a internet). Todos os sistemas operacionais atuais trabalham com o protocolo TCP/IP.

Além do protocolo TCP/IP os computadores necessitam de um número para serem identificados. Para isso cada placa de rede tem um número físico (gravado de fábrica) chamado de endereço **Mac Address**. Também podemos definir um número lógico para a placa de rede, este chamamos de **endereço de IP**. O endereço de IP nada mais é que um endereço lógico (número), assim como o nosso CPF, que nos identifica na sociedade. O IP identifica um computador na rede de computadores.

Máscara de sub-rede

A máscara de sub-rede é um endereço composto por 4 bytes (como o IP) usada para mascarar uma parte do endereço IP para se poder distinguir a qual rede um dispositivo pertence.

Hostname

É um nome dado a um dispositivo que faz parte de uma rede. O dispositivo pode ser um computador, um celular, um servidor de rede e assim por diante.

Ex: Computador1

COMANDOS BÁSICOS DE REDE LINUX

ip addr show

Mostra o endereço IP da placa.

```
ip addr show
```

Digitando o comando, o endereço de IP será mostrado no campo "inet".

ifconfig

O comando **ifconfig** serve para visualizar e/ou alterar as configurações de IP, máscara, *Mac Address* de uma interface de rede(placa de rede). As interfaces de rede no Linux são reconhecidas como:

- **eth0** – *ethernet* 0 (zero).
- **wlan0** – *wireless* LAN 0 (zero).

LAN = Rede local

Eth significa que você tem uma placa de rede física seja ela *onboard* ou *offboard*, enquanto **wlan** significa que você está utilizando uma placa de rede física *wireless*.

Se tivéssemos no computador três placas de rede e duas placas *wireless*, teríamos:

- eth0, eth1 e eth2
- wlan0, wlan1

Podemos ativar ou desativar a nossa placa de rede, com o seguinte comando:

```
#ifconfig eth0 up
#ifconfig eth0 down
```

- *up* – significa levantar(ativar) o adaptador eth0
- *down* – significa baixar(desativar) o adaptador eth0

Configurando IP e máscara manualmente para a placa de rede:

```
ifconfig 192.168.0.171 netmask 255.255.255.0 up
```

ping

Com o comando **ping** podemos testar se há conexão entre um computador e outro dentro de uma mesma rede.

```
ping 192.168.0.10
```

ACESSO REMOTO VIA SSH

SSH

O SSH significa Security Shell (*shell* seguro). Ele é uma ferramenta de acesso remoto, ou seja, ele permite acessar computadores remotamente para realizar diversas tarefas, como por exemplo:

- Instalação e remoção de *softwares*;
- Alteração de *scripts* de servidor;
- Transferência de arquivos;
- Execução de aplicativos gráficos;

SSH no Windows?

Apesar de SSH ser uma ferramenta nativa do sistema operacional UNIX, assim como a maioria das ferramentas do Linux ele também pode ser utilizado no Windows. Desta forma, podemos através de um sistema Windows administrar via SSH um Sistema Operacional Linux.

Porta padrão

Por padrão o SSH utiliza a porta 22, então se por ventura houver um servidor de *firewall* na rede, não esqueça de manter a porta 22 liberada no *firewall*.

FIREWALL: Controla a entrada e saída de dados do computador, seu principal objetivo é proteger o computador

Como funciona?

O SSH é dividido em dois módulos, são eles: O **ssh client** e o **ssh server**. Por padrão nas distribuições Ubuntu o *ssh client* já vem instalado.

- ssh client = Utilitário que utilizamos para acessar uma máquina.
- ssh server (openssh-server) = Utilitário que permite que outras máquinas acessem a máquina local, ou seja, módulo que fica na máquina que será acessada.

Instalação

Para instalar no Ubuntu 12.04 o *openssh-server* utilizamos o gerenciador de pacotes *apt-get*:

```
sudo apt-get install ssh
```

Ao instalar o pacote ssh automaticamente o pacote openssh-server será instalado.

Acessando um computador remoto

Para acessar via SSH, precisamos apenas de três informações:

- Nome da conta de usuário que será acessada;
- Senha da conta;
- Host (pode ser nome do computador ou número de IP).

Atributo -X

O atributo X serve para permitir o acesso aos programas gráficos do computador remoto.

Exemplos:

```
ssh thiagocury@192.168.0.171
ssh -X thiagocury@192.168.0.171
```

TRANSFERINDO ARQUIVOS COM SCP

O comando **scp** permite a transferência de arquivos por rede. Para isso basta especificar em uma única linha o *login* e endereço do servidor, junto com o arquivo que será transferido.

A sintaxe do *scp* é: "scp arquivo_local login@servidor:pasta_remota"

Nesse exemplo, o comando scp passará o arquivo currículo para a pasta docs dentro de /home/aluno

```
scp currículo aluno@192.168.0.10:/home/aluno/docs
```

TRANSFERINDO ARQUIVOS VIA SFTP (COM NAUTILUS)

Vamos utilizar o Nautilus para transferir arquivos via SFTP. **SFTP** significa *Secure File Transfer Protocol*, ou seja, é o protocolo de transferência de arquivos sendo utilizado em conjunto com o protocolo SSH. Mas qual é a diferença de utilizar o SSH comum e o SFTP (SSH com FTP)? O SFTP transfere arquivos entre computadores criptografando os mesmos, ou seja, os arquivos são “embaralhados” de um ponto até outro. Ao chegar ao computador de destino o computador descriptografa a informação para poder ler.

No **Nautilus**, clique em **Arquivo > Conectar ao servidor**. Na janela seguinte, escolha "SSH" na opção "Tipo de serviço" e forneça o endereço do servidor e o *login* que será usado, no campo "Nome do Usuário". O campo com a pasta permite especificar qual pasta será acessada por padrão ao efetuar a conexão, mas ela é opcional. Se você não especificar nenhuma pasta, o *Nautilus* conectará na pasta raiz, ou seja, no "/" (barra).

A figura 1 mostra a caixa de diálogo de “Conectar ao servidor”. Neste exemplo será conectado no servidor cujo IP é 192.168.0.15 via SSH. O diretório que será acessado será o “barra”(/), com o usuário “thiagocury”.

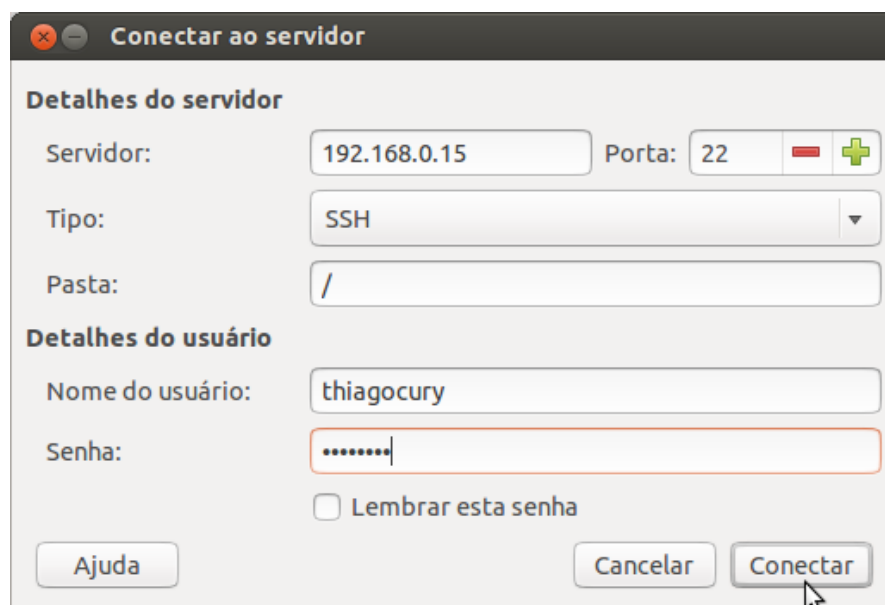


Figura 1

Após clicar no botão “**Conectar**”, aparecerá uma nova janela do *Nautilus* (Gerenciador de arquivos) com os arquivos do computador remoto. Note a barra de localização indicando a conexão via SFTP no usuário **thiagocury**. A Figura 2 mostra a conexão remota.

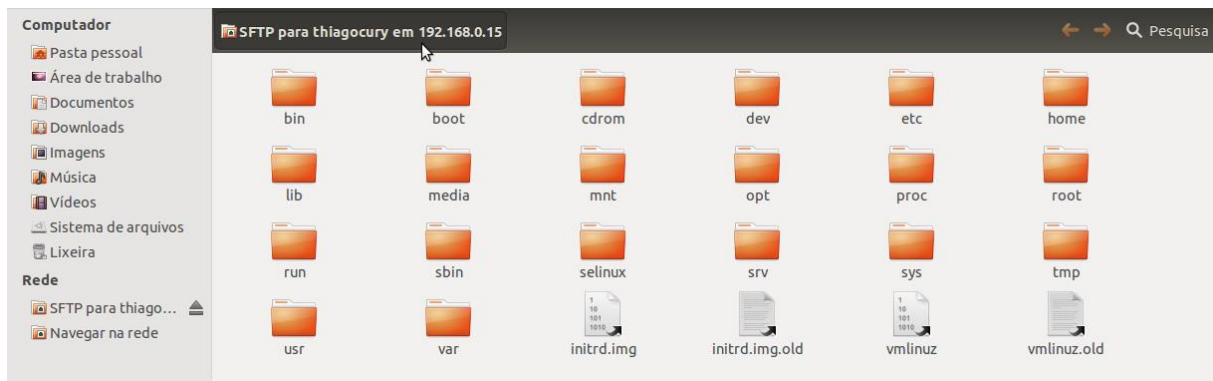


Figura 2

Obs: Podemos modificar a visualização da barra de localização do Nautilus pressionando as teclas: CTRL + L.

Se modificar a barra de visualização o Nautilus mostrará a conexão SFTP conforme a Figura 3.

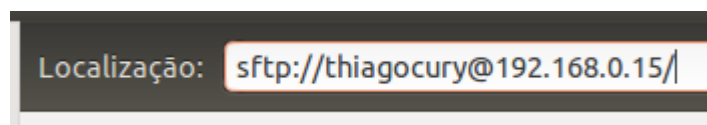


Figura 3

ACESSANDO LINUX VIA SSH ATRAVÉS DO SISTEMA WINDOWS (COM PUTTY)

Algumas redes são híbridas, ou seja, temos sistemas operacionais Linux, Windows, MacOS, entre outros. Podemos acessar, por exemplo, um sistema Linux via protocolo SSH através de um sistema operacional Windows. Para fazer isso podemos utilizar um *software* chamado PuTTY.

Efetuando download do software PuTTY.

Para efetuar download podemos acessar o site: <http://www.putty.org/>

No site terá uma opção dizendo: “*download here*”, onde se clicada redirecionará para o *link* que efetuará o download do software:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

Para efetuar o *download* do *software* para o sistema operacional Windows, escolha a opção: **PuTTY: putty.exe** conforme a figura 4.

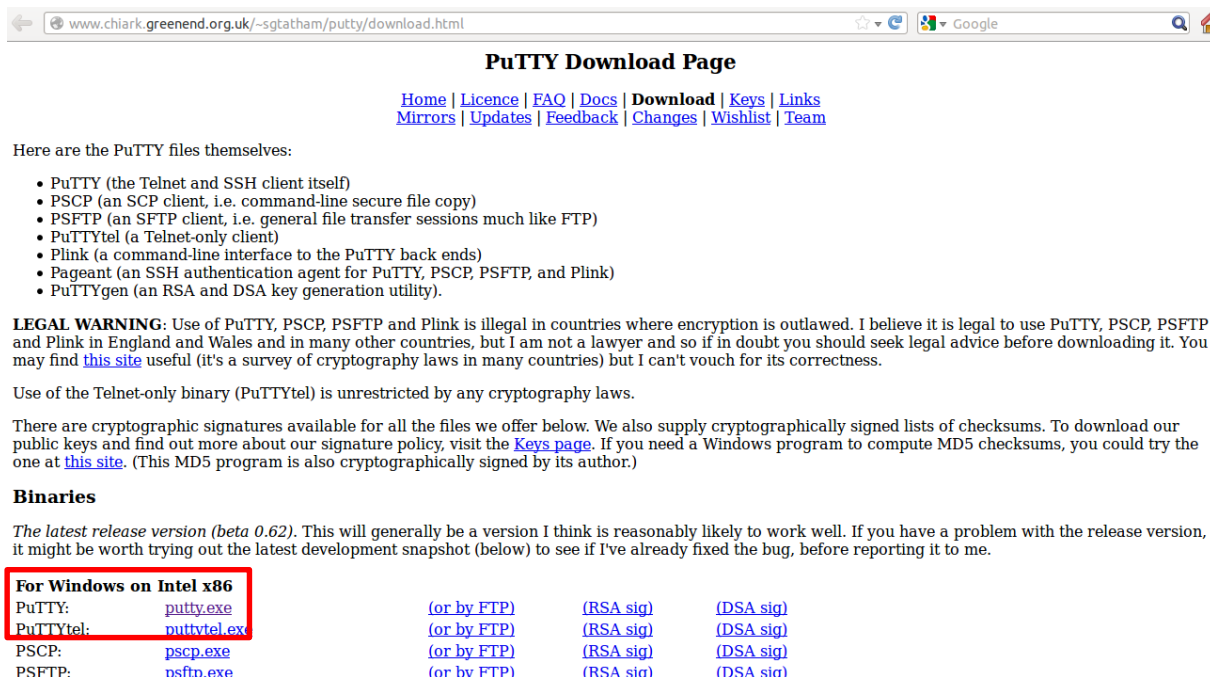


Figura 4

O PuTTY é um *software* executável que não necessita de instalação, ou seja, podemos abrir o *software* e conectar em outro computador. Para isso precisamos escolher o tipo de protocolo que desejamos utilizar, no caso SSH, informar em qual porta lógica será efetuada a conexão (porta 22) e o *hostname* do computador que será conectado através do número de IP.

A Figura 5 mostra como seria a configuração necessária para efetuar a conexão via SSH no IP de número 192.168.0.10, por exemplo.

Após configurar qual será o *hostname*, porta lógica e protocolo é só clicar no botão “open”. Em seguida será aberta outra tela com fundo preto solicitando o nome do usuário (*login as*) e a senha do usuário (*password*). Depois de digitar essas informações, estaremos acessando o Linux através do sistema Windows, mais precisamente através do *software* PuTTY.

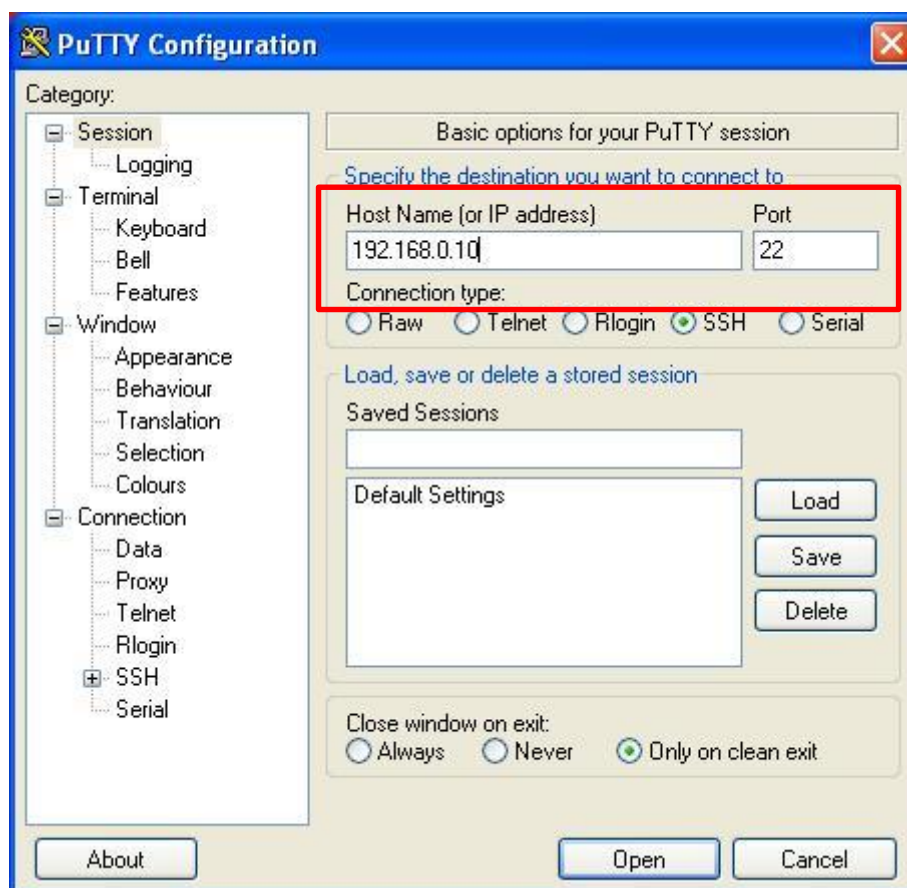


Figura 5