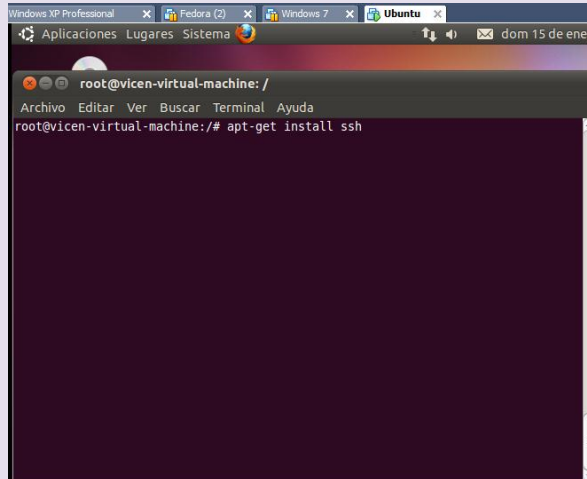


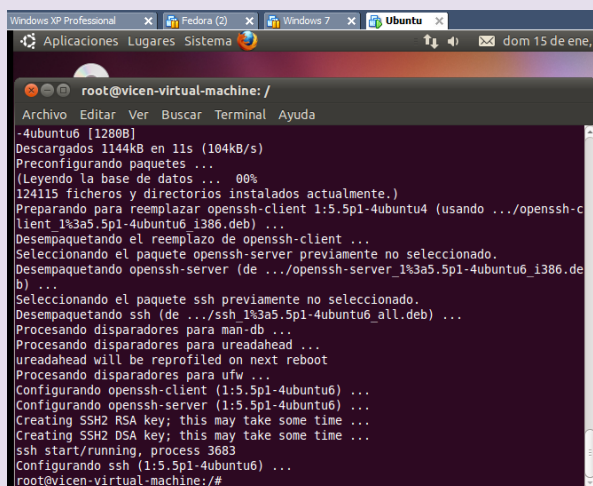
TECNICAS DE CIFRADO: COMUNICACIONES SEGURAS**7. SSH****a) Instalación del servidor SSH en GNU/Linux****En Ubuntu**

Lo instalamos apt-get install ssh



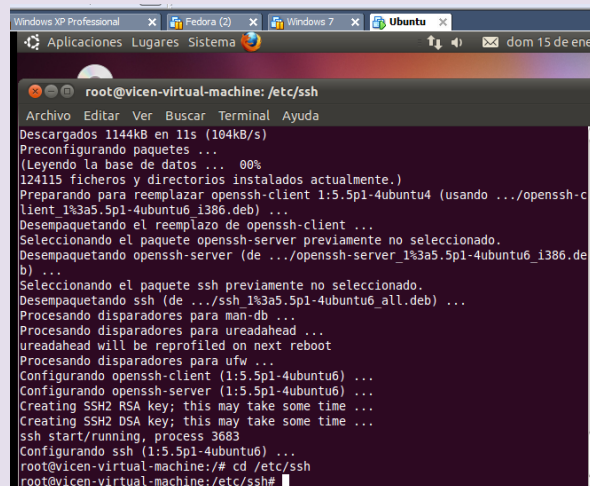
```
root@vicen-virtual-machine: /
Archivo Editar Ver Buscar Terminal Ayuda
root@vicen-virtual-machine:~# apt-get install ssh
```

Se ha terminado su instalación



```
root@vicen-virtual-machine: /
Archivo Editar Ver Buscar Terminal Ayuda
-4ubuntu6 [1280B]
Descargados 1144kB en 11s (104kB/s)
Preconfigurando paquetes ...
(Leyendo la base de datos ... 00%
124115 ficheros y directorios instalados actualmente.)
Preparando para reemplazar openssh-client 1:5.5p1-4ubuntu4 (usando .../openssh-c
lient_1%3a5.5p1-4ubuntu6_i386.deb) ...
Desempaquetando el reemplazo de openssh-client ...
Seleccionando el paquete openssh-server previamente no seleccionado.
Desempaquetando openssh-server (de .../openssh-server_1%3a5.5p1-4ubuntu6_i386.de
b) ...
Seleccionando el paquete ssh previamente no seleccionado.
Desempaquetando ssh (de .../ssh_1%3a5.5p1-4ubuntu6_all.deb) ...
Procesando disparadores para man-db ...
Procesando disparadores para ureadahead ...
ureadahead will be reprofiled on next reboot
Procesando disparadores para ufw ...
Configurando openssh-client (1:5.5p1-4ubuntu6) ...
Configurando openssh-server (1:5.5p1-4ubuntu6) ...
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
ssh start/running, process 3683
Configurando ssh (1:5.5p1-4ubuntu6) ...
root@vicen-virtual-machine:~#
```

Nos movemos al directorio /etc/ssh



```
root@vicen-virtual-machine: /etc/ssh
Archivo Editar Ver Buscar Terminal Ayuda
Descargados 1144kB en 11s (104kB/s)
Preconfigurando paquetes ...
(Leyendo la base de datos ... 00%
124115 ficheros y directorios instalados actualmente.)
Preparando para reemplazar openssh-client 1:5.5p1-4ubuntu4 (usando .../openssh-c
lient_1%3a5.5p1-4ubuntu6_i386.deb) ...
Desempaquetando el reemplazo de openssh-client ...
Seleccionando el paquete openssh-server previamente no seleccionado.
Desempaquetando openssh-server (de .../openssh-server_1%3a5.5p1-4ubuntu6_i386.de
b) ...
Seleccionando el paquete ssh previamente no seleccionado.
Desempaquetando ssh (de .../ssh_1%3a5.5p1-4ubuntu6_all.deb) ...
Procesando disparadores para man-db ...
Procesando disparadores para ureadahead ...
ureadahead will be reprofiled on next reboot
Procesando disparadores para ufw ...
Configurando openssh-client (1:5.5p1-4ubuntu6) ...
Configurando openssh-server (1:5.5p1-4ubuntu6) ...
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
ssh start/running, process 3683
Configurando ssh (1:5.5p1-4ubuntu6) ...
root@vicen-virtual-machine:~# cd /etc/ssh
root@vicen-virtual-machine: /etc/ssh#
```

Comprobamos que se ha instalado bien todos los paquetes

```

root@vican-virtual-machine: /etc/ssh
124115 ficheros y directorios instalados actualmente.)
Preparando para reemplazar openssh-client 1:5.5p1-4ubuntu4 (usando .../openssh-c
lient_1%3a5.5p1-4ubuntu6_i386.deb) ...
Desempaquetando el reemplazo de openssh-client ...
Seleccionando el paquete openssh-server previamente no seleccionado.
Desempaquetando openssh-server (de .../openssh-server_1%3a5.5p1-4ubuntu6_i386.de
b) ...
Seleccionando el paquete ssh previamente no seleccionado.
Desempaquetando ssh (de .../ssh_1%3a5.5p1-4ubuntu6_all.deb) ...
Procesando disparadores para man-db ...
Procesando disparadores para ureadahead ...
ureadahead will be reprofiled on next reboot
Procesando disparadores para ufw ...
Configurando openssh-client (1:5.5p1-4ubuntu6) ...
Configurando openssh-server (1:5.5p1-4ubuntu6) ...
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
ssh start/running, process 3683
Configurando ssh (1:5.5p1-4ubuntu6) ...
root@vican-virtual-machine: # cd /etc/ssh
root@vican-virtual-machine: /etc/ssh# ls
moduli      sshd_config  ssh_host_dsa_key.pub  ssh_host_rsa_key.pub
ssh_config  ssh_host_dsa_key  ssh_host_rsa_key
root@vican-virtual-machine: /etc/ssh#
  
```

Editamos el archivo de configuración sshd_config
Vemos que el puerto es el 22, el servicio ssh se queda
escuchando en el puerto 22

Protocol es 2, se usa el protocolo 2 que es más seguro que el 1

```

root@vican-virtual-machine: /etc/ssh
GNU nano 2.2.4 Archivo: sshd_config
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768
  
```

PermitRootLogin =yes es para permitir que se conecte root, por
seguridad no se debería permitir

```

root@vicen-virtual-machine: /etc/ssh
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.4 Archivo: sshd config

HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
#PermitRootLogin yes
StrictModes yes

RSAAuthentication yes

```

PermitEmptyPasswords= no, para no permitir sin contraseña

```

root@vicen-virtual-machine: /etc/ssh
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.4 Archivo: sshd config

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunneled clear text passwords
#PasswordAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

# GSSAPI options
#GSSAPIAuthentication no

```

X11Forwarding = yes , permite ejecutar aplicaciones en el servidor

```

root@vicen-virtual-machine: /etc/ssh
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.4 Archivo: sshd config

# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes

X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no

#MaxStartups 10:30:60

```

Para conectarnos usamos ssh nombre_usuario@host si queremos ejecutar aplicaciones le ponemos delante del usuario el parámetro -X

En mi caso pongo ssh [vicen@127.0.0.1](#)

```

vicen@vicen-virtual-machine: /etc/ssh
vicen@vicen-virtual-machine: /etc/ssh$ ssh vicen@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
RSA key fingerprint is 4e:fe:a7:1b:02:d7:25:66:a7:2c:ed:07:78:2f:22:f0.
Are you sure you want to continue connecting (yes/no)?

```

Decimos que yes y nos pide la contraseña

```

vicen@vicen-virtual-machine: /etc/ssh
vicen@vicen-virtual-machine: /etc/ssh$ ssh vicen@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
RSA key fingerprint is 4e:fe:a7:1b:02:d7:25:66:a7:2c:ed:07:78:2f:22:f0.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '127.0.0.1' (RSA) to the list of known hosts.
vicen@127.0.0.1's password:

```

Vemos como se establece la conexión

```

vicen@vicen-virtual-machine: ~
vicen@127.0.0.1's password:
Linux vicen-virtual-machine 2.6.35-22-generic #33-Ubuntu SMP Sun Sep 19 20:34:50
UTC 2010 i686 GNU/Linux
Ubuntu 10.10

Welcome to Ubuntu!
 * Documentation: https://help.ubuntu.com/

New release 'natty' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

vicen@vicen-virtual-machine:~$

```

b) Conexión al servidor SSH mediante cliente GNU/Linux y cliente Windows.

Cliente Ubuntu Instalamos ssh

```

root@vicen-virtual-machine: /home/vicen
Ubuntu Archivo Editar Ver Buscar Terminal Ayuda
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
E: No se ha podido localizar el paquete openssh
root@vicen-virtual-machine:/home/vicen# apt-get install ssh
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  openssh-client openssh-server
se:Paquetes sugeridos:
  libpam-ssh keychain openssh-blacklist openssh-blacklist-extra rssh
  molly-guard
Se instalarán los siguientes paquetes NUEVOS:
  openssh-server ssh
Se actualizarán los siguientes paquetes:
  openssh-client
1 actualizados, 2 se instalarán, 0 para eliminar y 364 no actualizados.
Necesito descargar 1144kB de archivos.
Se utilizarán 864kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? s
AVISO: ¡No se han podido autenticar los siguientes paquetes!
  openssh-client openssh-server ssh
¿Instalar estos paquetes sin verificación [s/N]?

```

Ahora nos vamos a conectar desde el cliente con dirección ip
10.33.13.41 al servidor que tiene ip 10.33.13.40
Para ello ponemos ssh vicen@10.33.13.40

```

vicen@vicen-virtual-machine: ~
Ubuntu Archivo Editar Ver Buscar Terminal Ayuda
From 10.33.13.41 icmp_seq=2 Destination Host Unreachable
From 10.33.13.41 icmp_seq=3 Destination Host Unreachable
From 10.33.13.41 icmp_seq=6 Destination Host Unreachable
From 10.33.13.41 icmp_seq=7 Destination Host Unreachable
^Z
[2]+  Detenido      ping 10.33.13.1
vicen@vicen-virtual-machine:/etc/ssh$ ssh vicen@10.33.13.40
The authenticity of host '10.33.13.40 (10.33.13.40)' can't be established.
RSA key fingerprint is 4e:fe:a7:1b:02:d7:25:66:a7:2c:ed:07:78:2f:22:f0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.33.13.40' (RSA) to the list of known hosts.
vicen@10.33.13.40's password:
Linux vicen-virtual-machine 2.6.35-22-generic #33-Ubuntu SMP Sun Sep 19 20:34:50
  UTC 2010 i686 GNU/Linux
Ubuntu 10.10

Welcome to Ubuntu!
 * Documentation: https://help.ubuntu.com/

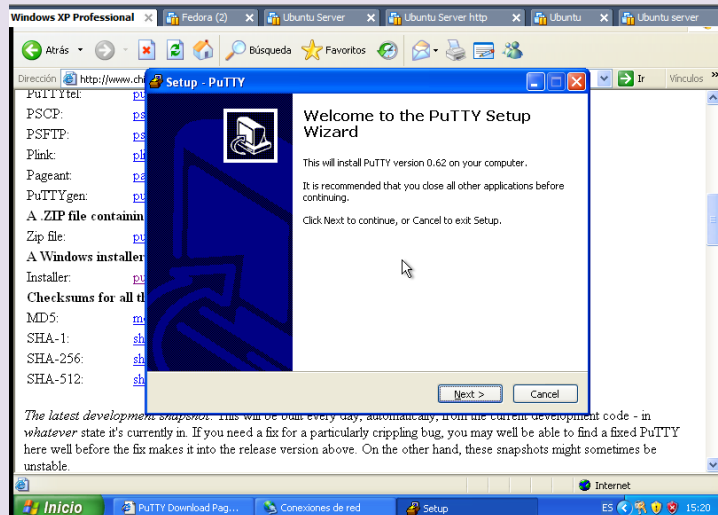
New release 'natty' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Jan 28 19:39:16 2012 from localhost.localdomain
vicen@vicen-virtual-machine:~$

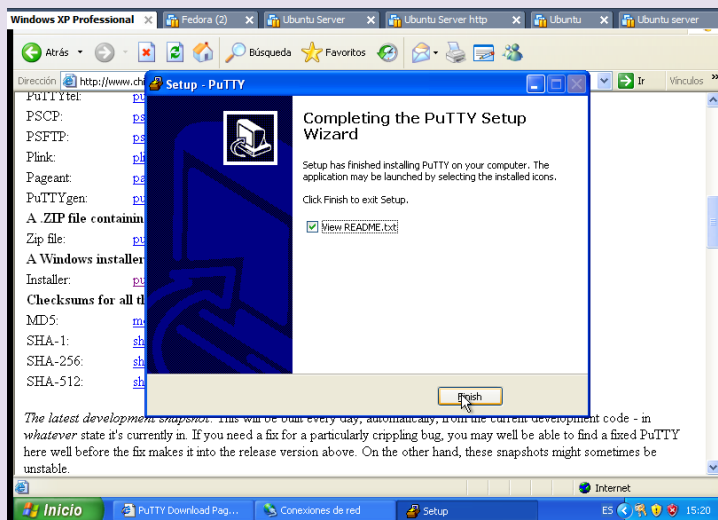
```

CLIENTE WINDOWS

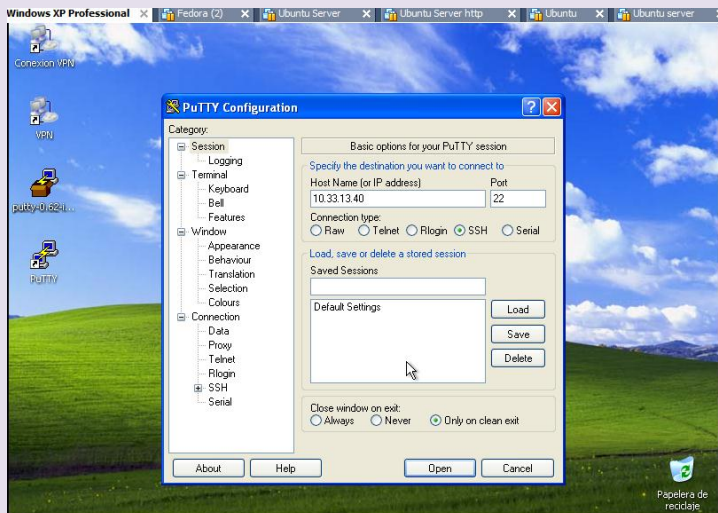
Instalamos putty



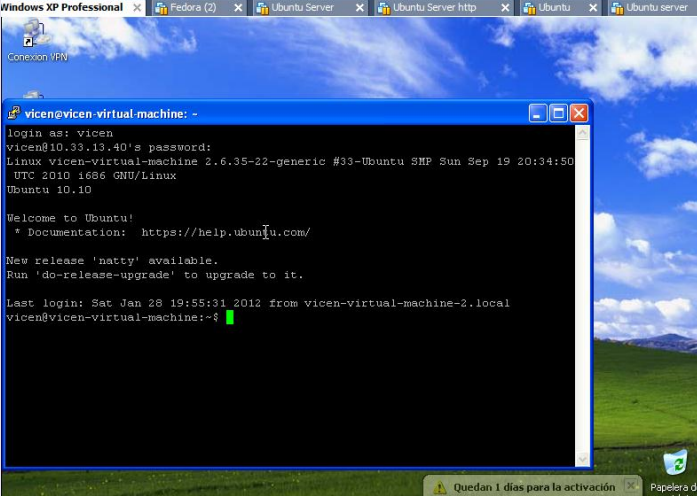
Instalación terminada



Configuramos putty poniendo la dirección del servidor
10.33.13.40



Una vez que le damos a open nos pide login: vicen y contraseña:
inves y accedemos



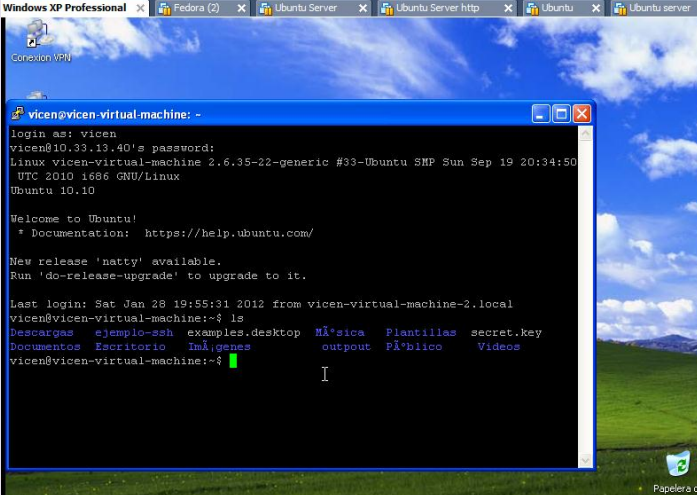
```
vicen@vicen-virtual-machine: -
login as: vicen
vicen@10.33.13.40's password:
Linux vicen-virtual-machine 2.6.35-22-generic #33-Ubuntu SMP Sun Sep 19 20:34:50
UTC 2010 1686 GNU/Linux
Ubuntu 10.10

Welcome to Ubuntu!
 * Documentation: https://help.ubuntu.com/

New release 'natty' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Jan 28 19:55:31 2012 from vicen-virtual-machine-2.local
vicen@vicen-virtual-machine:~$
```

Hacemos un ls y comprobamos que tenemos acceso al Ubuntu
que he configurado anteriormente como servidor ssh



```
vicen@vicen-virtual-machine: -
login as: vicen
vicen@10.33.13.40's password:
Linux vicen-virtual-machine 2.6.35-22-generic #33-Ubuntu SMP Sun Sep 19 20:34:50
UTC 2010 1686 GNU/Linux
Ubuntu 10.10

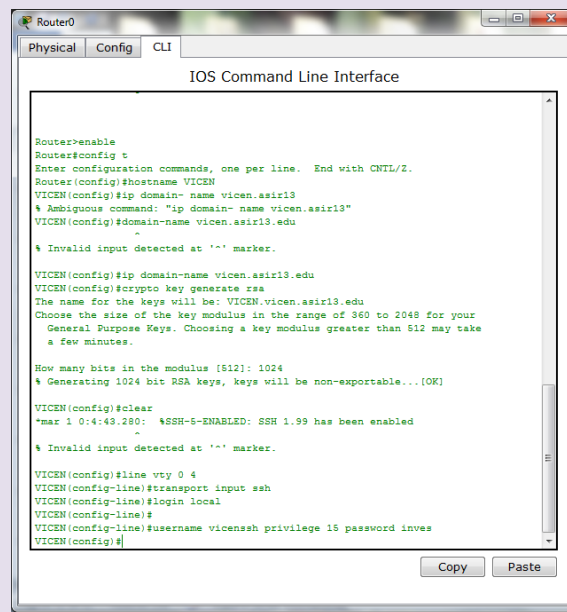
Welcome to Ubuntu!
 * Documentation: https://help.ubuntu.com/

New release 'natty' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Jan 28 19:55:31 2012 from vicen-virtual-machine-2.local
vicen@vicen-virtual-machine:~$ ls
Descargas  ejemplo-ssh  examples.desktop  Música  Plantillas  secret.key
Documentos Escritorio  Imágenes        output  Pí'blico  Videos
vicen@vicen-virtual-machine:~$
```

Escritorio de Ubuntu

Activamos la conexión telnet



```
Router0
Physical Config CLI
IOS Command Line Interface

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname VICEN
VICEN(config)#ip domain-name vicen.asir13
% Ambiguous command: "ip domain-name vicen.asir13"
VICEN(config)#domain-name vicen.asir13.edu
VICEN(config)#
% Invalid input detected at '^' marker.

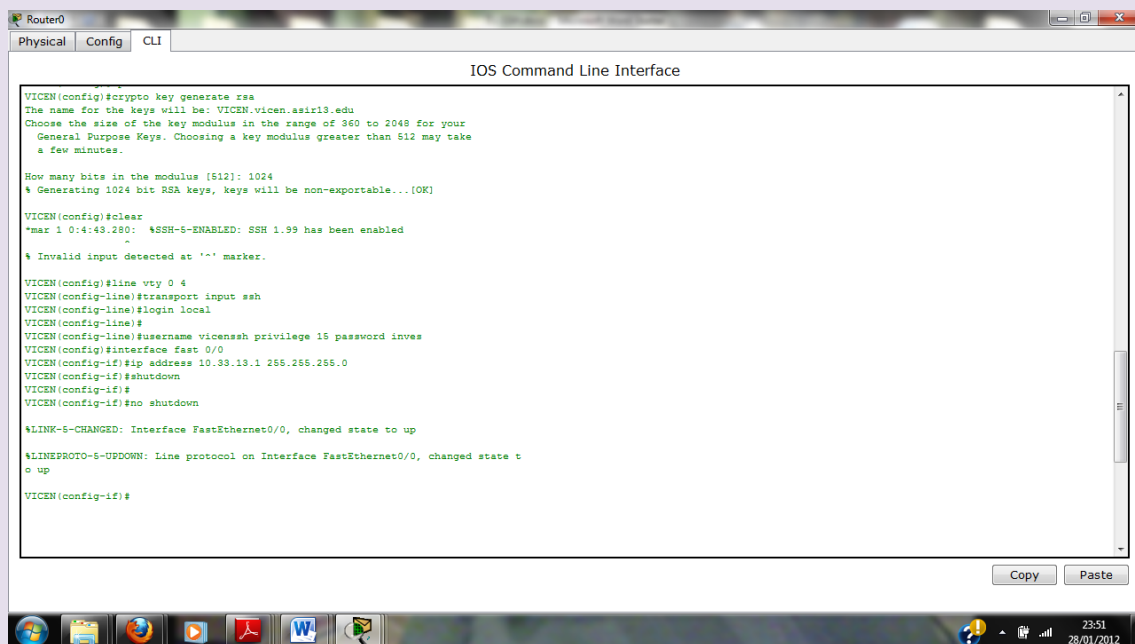
VICEN(config)#ip domain-name vicen.asir13.edu
VICEN(config)#crypto key generate rsa
The name for the keys will be: VICEN.vicen.asir13.edu
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

VICEN(config)#clear
*Mar 1 0:4:43.280: %SSH-5-ENABLED: SSH 1.99 has been enabled
VICEN(config)#
% Invalid input detected at '^' marker.

VICEN(config)#line vty 0 4
VICEN(config-line)#transport input ssh
VICEN(config-line)#login local
VICEN(config-line)#
VICEN(config-line)#username vicenssh privilege 15 password inves
VICEN(config-line)#
VICEN(config)#
```

configuramos interfaz del router



```
Router0
Physical Config CLI
IOS Command Line Interface

VICEN(config)#crypto key generate rsa
The name for the keys will be: VICEN.vicen.asir13.edu
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

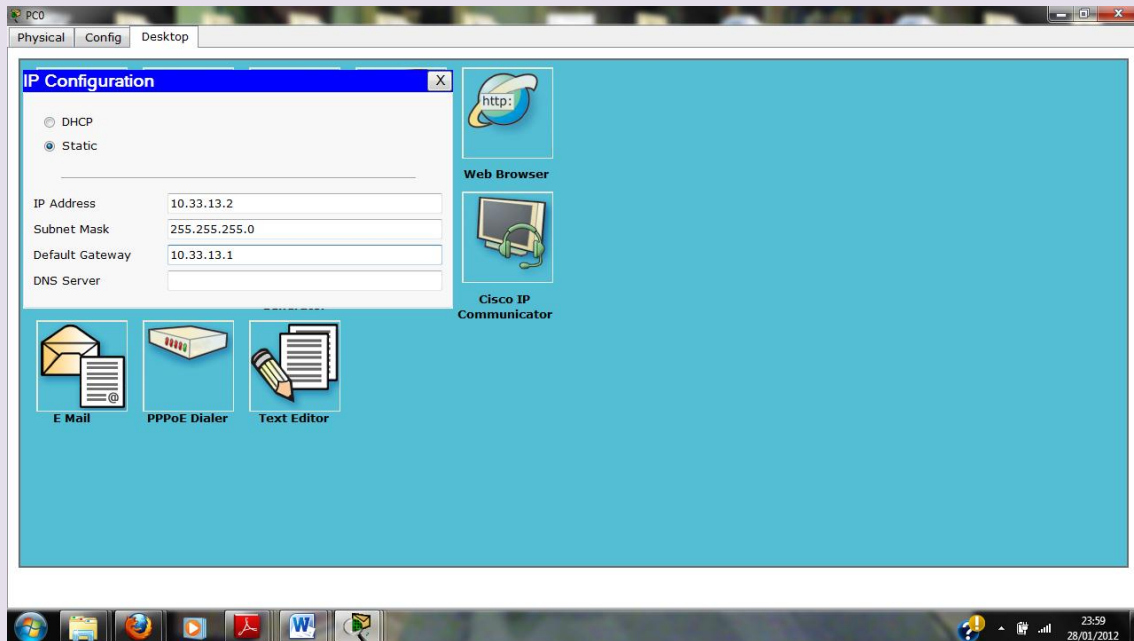
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

VICEN(config)#clear
*Mar 1 0:4:43.280: %SSH-5-ENABLED: SSH 1.99 has been enabled
VICEN(config)#
% Invalid input detected at '^' marker.

VICEN(config)#line vty 0 4
VICEN(config-line)#transport input ssh
VICEN(config-line)#login local
VICEN(config-line)#
VICEN(config-line)#username vicenssh privilege 15 password inves
VICEN(config)#interface fast 0/0
VICEN(config-if)#ip address 10.33.13.1 255.255.255.0
VICEN(config-if)#shutdown
VICEN(config-if)#
VICEN(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
VICEN(config-if)#
```

Configuramos el cliente



Vamos a la terminal del cliente y ponemos ssh -l vicen 10.33.13.1 (dirección ip del router) y vemos que conectamos

INVALID COMMAND = Ponía un 1 en lugar de una l

