FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA

Informe
Trabajo Dirigido
EL682

Alumno : Daniel A. Díaz P.
Profesor : Victor Grimblatt H.
Fecha : 26/11/2009

Índice General

1. Introducción

El presente documento corresponde al informe del ramo "Trabajo Dirigido" (EL682) del Departamento de Ingeniería Eléctrica de la Universidad de Chile. Éste es básicamente una guía para dar conocimiento del procedimiento para acceder al software instalado por Synopsys® en el departamento.

Synopsys® es una empresa de alta tecnología dedicada al desarrollo e investigación de la automatización del diseño electrónico (EDA por sus siglas en inglés). Ésto se traduce en creación de herramientas de software, propiedad intelectual (IP) y servicios utilizados en el diseño y manufactura de circuitos integrados [1].

Synopsys® proporcionó al Departamento de Ingeniería Eléctrica una serie de herramientas instaladas en el servidor *tiuque*, además de habilitar la sala E015 con computadores para el uso de estas herramientas. En este informe se dará una breve descripción del laboratorio y software instalado, y se mostrará como acceder a ellas desde un equipo dentro o fuera de la red de la Universidad de Chile.

2. Descripción del Laboratorio

El laboratorio se encuentra ubicado en la sala E015 del Departamento de Ingeniería Eléctrica de la Universidad de Chile. El espacio está compartido entre computadores aportados por Synopsys® para el uso de las herramientas de software, y por un espacio dedicado al trabajo de investigación sobre una "Nariz Electrónica" (con el Profesor Nicolás Beltrán a cargo).

2.1. Equipamiento

El laboratorio, en lo referente a lo proporcionado por Synopsys, posee 5 computadores denominados ic01, ic02, ic03, ic04 y ic05. Éstos se ubican como se muestra en la figura 1:

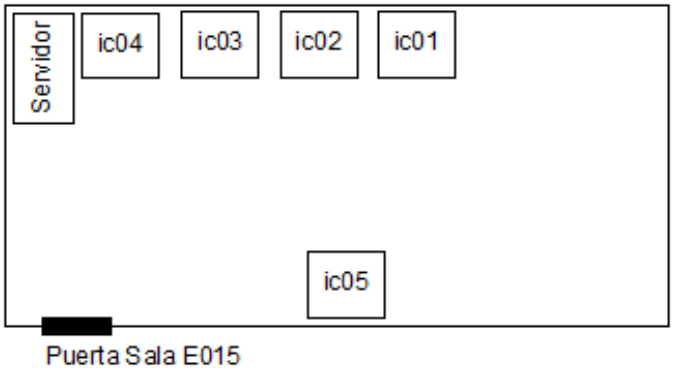

Figura 1: Ubicación Equipos

Cada equipo tiene asignada una dirección IP estática, a continuación se detalla la identificación de la red:

- Dirección IP: 192.168.75.10N (Donde N va de 1 a 5 de acuerdo a la identificación del equipo).
- Puerta de enlace predeterminada: 192.168.75.0
- DNS primaria: 200.9.97.3
- DNS secundaria: 200.9.100.1

Cada equipo tiene instalado 2 sistemas operativos: CentOS y Windows XP. Las cuentas para acceso general se muestran a continuación:

- **CentOS**
  Username: icguest
  Password: guestic

- **Windows XP**
  Username: IC-Lab
  Password: snpsc101

2.2. Herramientas Instaladas

A continuación se listan las herramientas instaladas en el servidor **privado** *tiuque* y una breve descripción de ellas:

- **Verilog Coded Simulator (VCS):** Esta herramienta permite compilar un diseño a nivel comportamental o RTL para verificar errores de sintaxis y generar archivos de simulación.
- **Design Compiler (DC):** Se utiliza principalmente para la síntesis lógica, dando lugar a la elección de librería de tecnología y restricciones del diseño.
- **IC Compiler (IC):** Permite realizar síntesis de netlist-a-GDSII o netlist-a-clock tree (síntesis física).
- **Cosmos:** Editor Esquemático/*Layout*.
- **Sentaurus:** Es un conjunto de herramientas TCAD (Technology Computer Aided Design).
- **Paramos:** Es una herramienta de extracción de parámetros SPICE (Simulation Program with Integrated Circuits Emphasis).
- **HSPICE:** Es un simulador optimizante de circuitos análogos. Se puede utilizar para simular circuitos eléctricos en régimen permanente, transiente y en el dominio de las frecuencias.
- **STAR-RCXT:** Se utiliza para extraer parásitos de base de datos conectadas que representan los *layouts* de diseños de circuitos integrados.
- **HERCULES:** Es una herramienta jerárquica de verificación física que permite realizar chequeos de reglas de diseño (DRC), chequeos de reglas eléctricas (ERC) y verificación de *Layout*-versus-Esquemático (LVS) en un diseño de circuito integrado.

2.3. Manejo de Cuentas y Herramientas en el Servidor

El encargado del laboratorio en el departamento de Ingeniería Eléctrica es el Profesor Nicolás Beltrán. Entonces:

- Para la creación de cuentas (en el servidor *tiuque*) para alumnos de algún ramo, éstas se deben pedir con el profesor del ramo, quién a su vez se comunicaría con el profesor a cargo del laboratorio.
- El profesor Nicolás Beltrán posee una lista con las herramientas que pueden ser instaladas. En caso de que algún alumno/profesor tenga un interés particular en alguna herramienta que no esté instalada, éste puede contactarse con el Profesor Beltrán para la instalación de la herramienta. Es posible que se requiera soporte de Synopsys para la instalación de alguna herramienta, lo cual también se debe realizar a través del Profesor Beltrán.

3. Acceso a Herramientas de Synopsys®

Las herramientas están diseñadas para ser corridas en una plataforma Linux, por lo cual, si se requiere utilizar la interfaz gráfica (como por ejemplo para un simulador gráfico), se necesita de un servidor X para poder usarla. La mayor parte del proceso de diseño se puede realizar a través de línea de comando y *Tcl*, por lo cual el uso de interfaz gráfica tiene su mayor importancia en la simulación gráfica.

3.1. Acceso desde FCFM

3.1.1. Linux

Para conectarse al servidor *tiuque* basta con escribir la siguiente línea de comando en un terminal y luego ingresar la clave (*password*) corresponidente:

```
ssh -X username@tiuque.die.uchile.cl
```

Donde *username* es el nombre de usuario asignado por el encargado de las herramientas de Synopsys® en el departamento. La opción *-X* habilitado el servidor X de manera de poder utilizar la interfaz gráfica al correr alguna herramienta que posea una, por ejemplo, DVE.

3.1.2. Microsoft Windows

En caso de conectarse sin la necesidad de interfaz gráfica, basta hacerlo a través de la versión de SSH de Microsoft Windows, como se muestra en la siguiente figura:

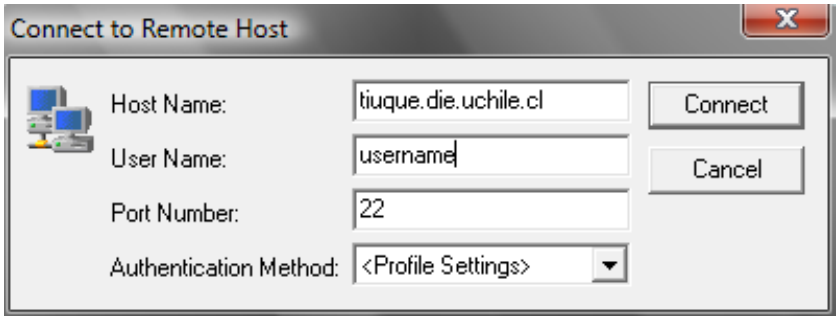

Figura 2: Ventana de Conexión en Windows

Luego solo es necesario ingresar el *password*.

En caso de querer interfaz gráfica, es necesario instalar algún emulador de servidor X como **Cygwin/X**, el cual no es cubierto en este documento. Una vez instalado y configurado se debe realizar lo descrito en la sección anterior.

3.2. Acceso Remoto

Para conectarse desde cualquier lugar con acceso a internet, es necesario conectarse de alguna manera a la red de la Universidad. La forma tradicional es conectarse a la VPN (Virtual Private Network) de la Facultad utilizando el cliente VPN de Cisco en el caso de Microsoft Windows, o bien, el cliente VPN integrado de Linux (el cual puede que no esté por defecto). Otra manera desde Linux es hacer un túnel SSH a través de alguno de los servidores públicos de la facultad, como *gorrion*.

Una vez establecida la conexión con la VPN de la facultad, se debe conectar al servidor *tiuque* de la misma manera como se describe en la sección 3.1.

3.2.1. Linux

VPN

Antes de crear la conexión VPN a la facultad, se debe cerciorar de que los siguientes paquetes esten instalados: vpnc, NetworkManager-vpnc y vpnc-consoleuser. También debe estar el NetworkManager Applet que generalmente viene por defecto en varias distribuciones Linux.

Luego se debe hacer click izquierdo en el ícono del NetworkManager del *system tray* que se muestra en la figura (en el caso mostrado el ícono corresponde a una conexión inalámbrica):

Figura 3: NetworkManager en el System Tray

Luego se debe ir a Conexiones VPN ->Configurar VPN ->Añadir. Aparece una ventana para editar la información de la conexión VPN, se deben ingresar los datos como se muestran en la figura 4, donde *username* corresponde al nombre de usuario proporcionado por la facultad para ingresar a sus servicios. Se finaliza guardando la conexión al presionar en “Aplicar”.

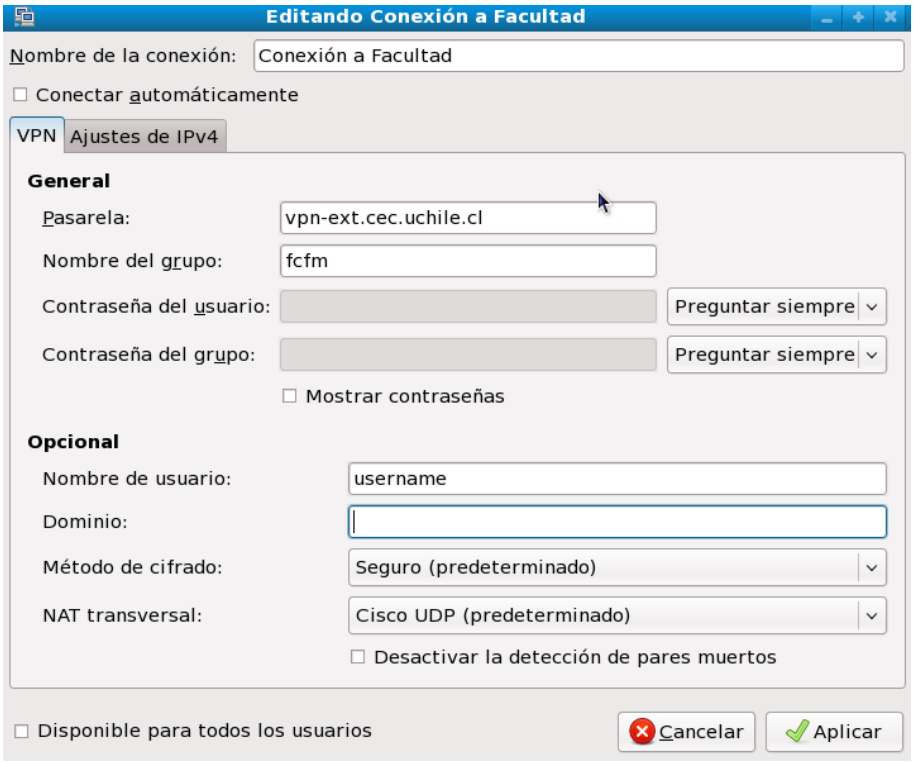

Figura 4: Nueva Conexión VPN

Para utilizar la conexión recién creada se debe hacer nuevamente en el ícono de Network-Manager e ir a Conexiones VPN ->Conexión a Facultad. Aparacerá una ventana preguntando dos claves secretas. *Contraseña* corresponde a la relativa al *username* anterior, mientras que para *Contraseña del grupo* se debe ingresar **facultad**.

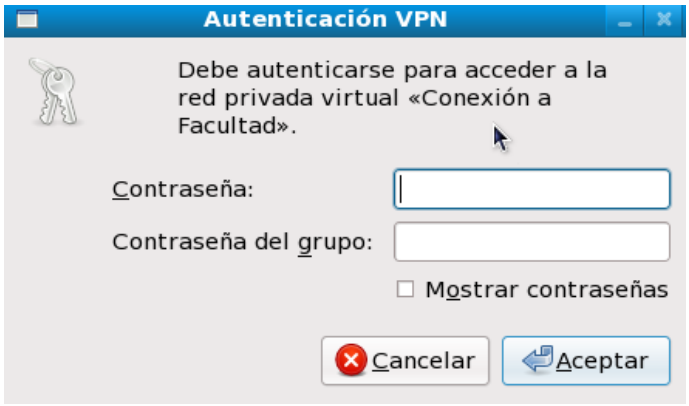

Figura 5: Ventana de Contraseñas

Túnel

Esta manera de conectarse al servidor de las herramientas de Synopsys® requiere de que SSH esté instalado en el sistema (aunque generalmente viene por defecto). Luego se deben seguir los siguientes pasos [3]:

1. Editar o crear en caso de que no exista el archivo llamado `.ssh/config` en la carpeta personal (home), y se debe agregar lo siguiente:

   ```
   Host tiuque.die.uchile.cl
   port [PUERTO LOCAL]
   ```

   Donde [PUERTO LOCAL] va a ser el puerto a través del cual se conecte el computador con el servidor, y es deseable que sea un número superior a 1000, ya que mcuho de los puertos entre 0 y 1000 están reservados para otras aplicaciones.

2. Editar el archivo `/etc/hosts` el cual debería contener por defecto lo siguiente:

   ```
   127.0.0.1 localhost
   ```

   Se debe modificar para que quede como sigue:

   ```
   127.0.0.1 localhost tiuque.die.uchile.cl
   ```

3. Luego se debe correr el siguiente comando:

   ```
   ssh -X -f username@gorrion.die.uchile.cl -N -L [PUERTO LOCAL]:tiuque.die.uchile.cl:22
   ```

   Donde *username* es el nombre de usuario en el servidor que se va a usar como intermediario, en este ejemplo *gorrion*.

4. Después se debe ingresar el *password* correspondiente al *username* del servidor intermediario y colocar *yes* en caso de que SSH de una advertencia.

Con esto ya se encuentra en condiciones para conectarse a *tiuque* como se menciona en la sección 3.1.

3.2.2. Microsoft Windows

La manera de conectarse a la VPN de la FCFM a través de Microsoft Windows se explica en [2]. A continuación solo se repite dicha información para tener todo compactado en un solo documento.

El cliente se puede descargar desde:

```
http://www.cec.uchile.cl/vpn/download/Windows/vpnclient-win.exe
```

Luego de instalado, se debe correr el cliente VPN, y hacer *click* en "New" para crear una nueva conexión (solo necesario la primera vez en que se va a conectar). Con esto debería aparecer una ventana y se debe llenar como muestra la siguiente figura:

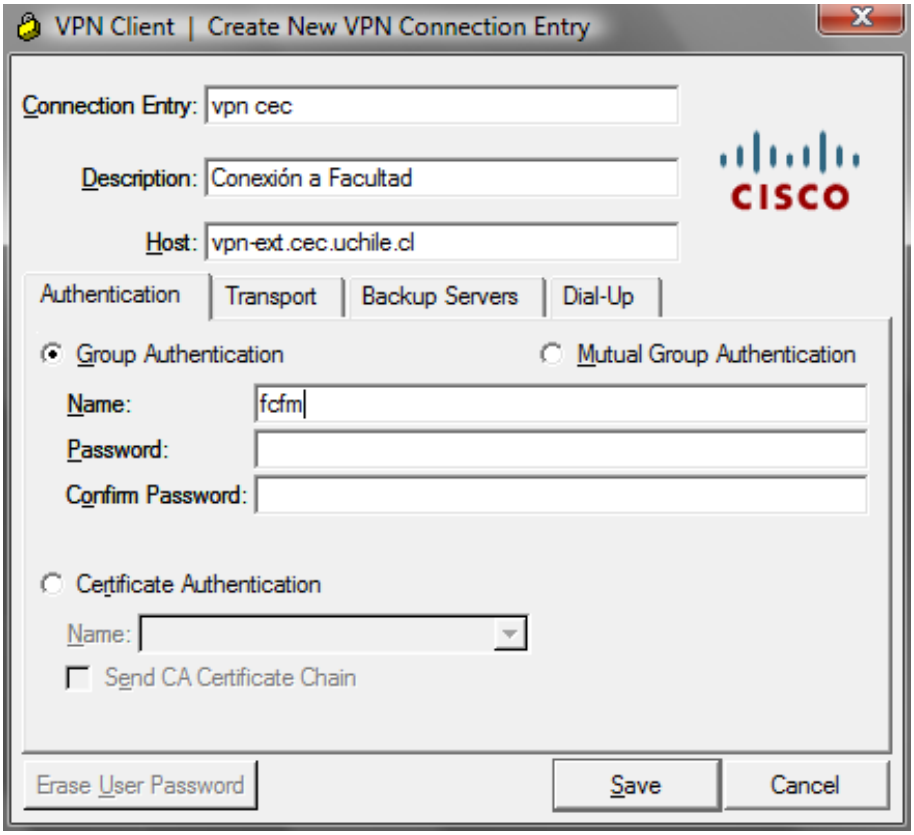

Figura 6: Nueva Conexión VPN

En las celdas de *Password* y *Confirm Password* se debe colocar **facultad**. Con esto se tiene lista la conexión y basta guardar, luego hacer doble-click en la conexión creada (en la ventana principal del cliente) y luego ingresar el *Username* y *Password* correspondientes a los proporcionados por la Facultad para ingreso en cuentas CEC, U-Cursos, etc.

Referencias

[1] Synopsys.com. [En línea] <http://www.synopsys.com>.

[2] Centro de Computación. *"Servicio VPN"* <http://www.cec.uchile.cl/vpn/>.

[3] BYU Computer Science Department . *"SSH Tunnels"* <http://docs.cs.byu.edu/general/ssh_tunnels.html>.