



# **Configuración de Interfaces y Aprovisionamiento Básico.**




## 1. Configuración de la Interfaz de Usuario

Tanto la interfaz de usuario como los modos de configuración de usuario permiten al administrador del sistema configurar las distintas características en los equipos HUAWEI. Actualmente existe una serie de interfaces empleadas con esta finalidad:

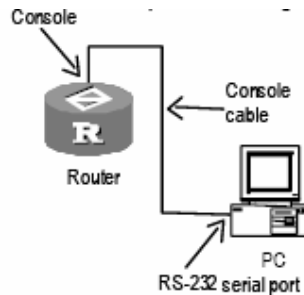
Los equipos HUAWEI definen 4 tipos de interfaces de usuarios asociados con los modos de configuración antes mencionados:

- **Puerta de Consola (CON):** El puerto de consola es un puerto del tipo dispositivo de línea. En un router, el puerto de consola EIA/TIA-232 se utiliza para permitirle a los usuarios realizar configuraciones.
- **Puerto Auxiliar (AUX):** El puerto auxiliar es un puerto del tipo dispositivo de línea. En un router, el puerto auxiliar EIA/TIA-232 DTE entrega la capacidad de conexiones de discado vía MODEM. (NO APLICABLE PARA ESTE MODELO)
- **Puerto Asincrónico (TTY):** La interfaz de usuario TTY es empleado cuando un usuario desea conectarse al router a través de un puerto serial asincrónico o a través de un puerto sincrónico/asincrónico (trabajando en modo asincrónico).
- **Línea Virtual (VTY):** Un puerto virtual es una línea Terminal lógica empleada para el acceso mediante telnet al router y es generalmente conocido como VTY (Virtual Type Line).

### 1.1 Configuración a través de Consola

 **Nota:** Las siguientes configuraciones de interfaces se aplican tanto para Switches como Routers Huawei. Las imágenes explicativas aparecen Routers, pero para el caso de Switches la idea es la misma.

**Paso 1:** Para ingresar al ambiente de configuración local, conecte el puerto serial de su PC (o terminal) a el puerto de consola del Switch usando el cable estándar RS-232 como se muestra en la figura siguiente.



**Paso 2:** Corra el programa de emulación de terminal (Win9x o Hyper Terminal por ejemplo) en el PC, y configure los parámetros de comunicación como sigue:

Bits per Second: 9600

Data bits: 8

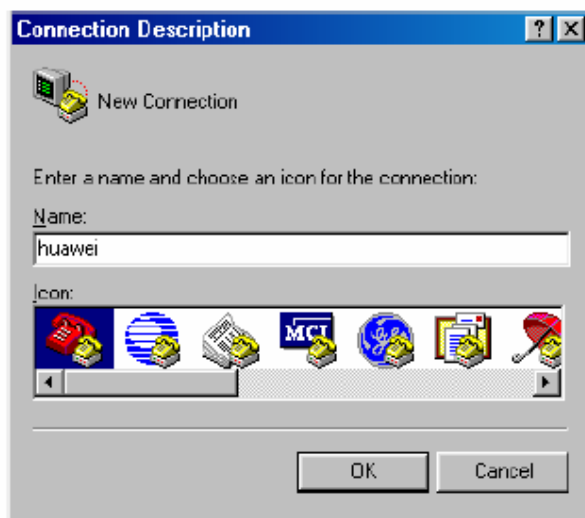
Stop bits: 1

Parity: None

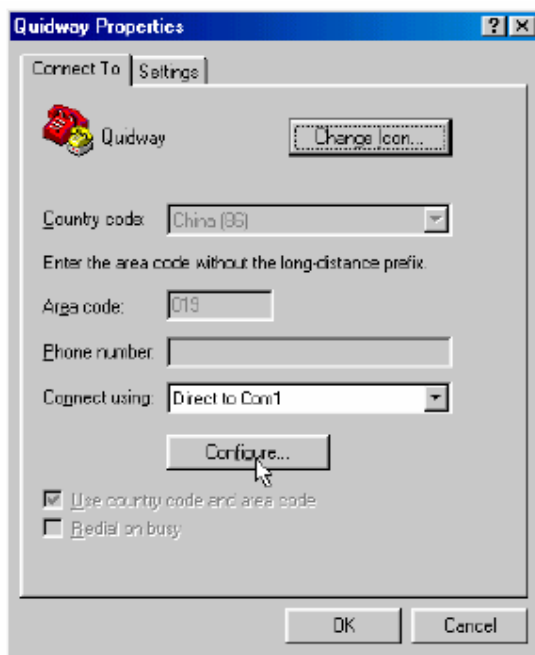
Flow Control: None

TermType: VT100

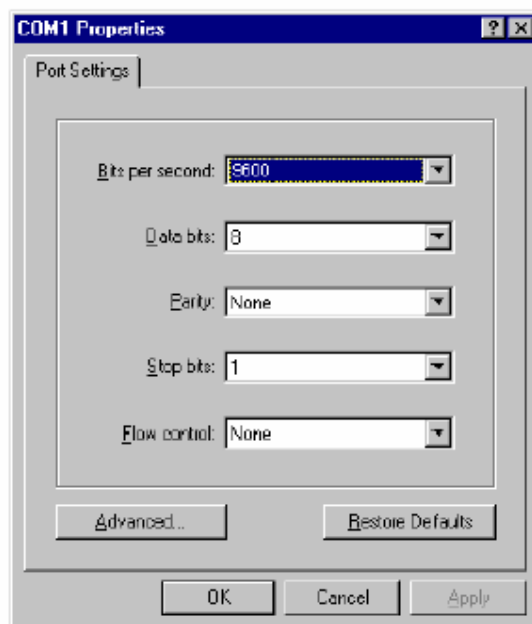
En las siguientes imágenes se explica con mas detalle:



***Nueva Conexión***



***Configurar el puerto de conexión***



**Configurar los parámetros de comunicación**

**Paso 3:** El Switch corre el Power-On-Self-Test (POST), una vez completada esta etapa presiona <Enter> hasta que el símbolo de la línea de comando, como <Quidway> aparezca.

**Paso 4:** Ingrese los comandos para configurar el Switch o ver su estado. Cuando necesite ayuda ingrese “?” para ver mas información acerca de los comandos.

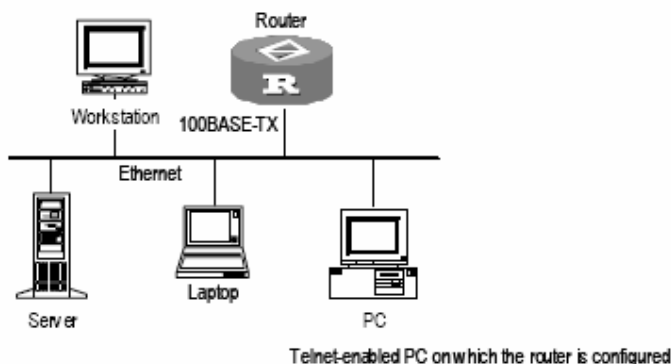
## 1.2 Configuración a través de Telnet

Puedes ingresar al Switch a través de Telnet vía LAN o WAN siempre y cuando:

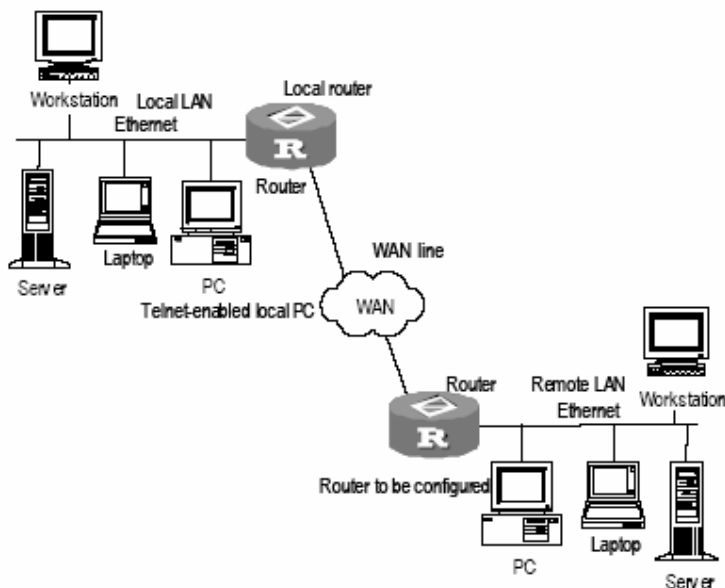
1. Esta no es la primera vez que se prende el equipo
2. Se han configurado correctamente las direcciones IP en las interfaces del Switch.
3. Se han configurado correctamente la autenticación de ingreso y reglas de control de acceso (se explica mas adelante en este manual).
4. Existe al menos una ruta alcanzable entre la consola terminal y el Switch.

Siga los siguientes pasos para ingresar al ambiente de configuración

**Paso 1:** Conecte el puerto Ethernet del Pc al un puerto Ethernet del Switch a través de la LAN si es en un ambiente local o a través de la WAN si es en un ambiente remoto, como se muestra en las siguientes figuras.

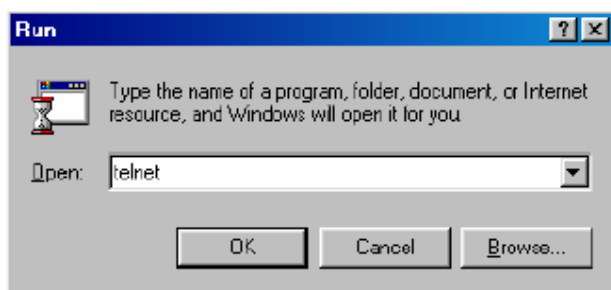


#### *Ambiente LAN*

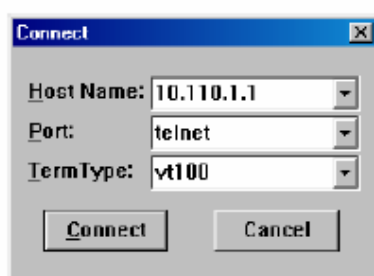


#### *Ambiente WAN*

**Paso 2:** Corra el programa Telnet en el PC y configure el terminal type a VT100 como se muestra a continuación.



**Corra el Telnet**



**Configure la conexión**

**Nota:** EL Host Name que muestra la figura es el host name o dirección IP del Switch remoto.

**Paso 3:** Ingrese la dirección IP del Switch en el PC local para establecer conexión. Si la autenticación es exitosa, el sistema desplegará el símbolo de la línea de comando <Quidway>.

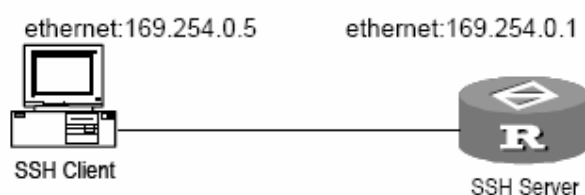
**Paso 4:** Ingrese los comandos para configurar el Switch o ver su estado. Cuando necesite ayuda ingrese “?” para ver mas información acerca de los comandos.

**Nota:** Cuando ingrese al Switch para configurarlo, sea cuidados con modificar la dirección IP, ya que provocará la desconexión del enlace. Si sucede esto, reingrese con la nueva dirección IP.

### 1.3 Configuración a través de SSH.

Secure Shell (SSH) provee alto nivel de seguridad de información y autenticación para proteger su equipo de ataques tales como spoofing de direcciones IP o interceptación de password en texto plano. Estos ataques suceden usualmente cuando los usuarios ingresan al equipo desde una red remota que es insegura. El Switch puede conectarse a múltiples clientes SSH para establecer conexiones con Switch o hosts Unix que corren servidores SSH. Los procedimientos de configuración son similares a los del Telnet.

Paso 1: Conecte el puerto Ethernet del PC a un puerto Ethernet que este en la LAN, para una configuración remota hagalo a través de la WAN.



Paso 2: Configure los parámetros SSH en el Switch. (Se verá en detalles mas adelante en el manual).

Paso 3: Corra el cliente SSH en el PC, y configure los parámetros, incluyendo la dirección IP del el Switch remoto, versión del SSH y el RSA. Luego de esto se establecerá la conexión con el equipo.

### 1.4 Configuración a través de Web-based Network Management.

Puedes ingresar al Switch a través de Web-based Network Management vía LAN o WAN siempre y cuando:

1. Esta no es la primera vez que se prende el equipo
2. Se han configurado correctamente las direcciones IP en las interfaces del Switch.





3. Se han configurado correctamente la autenticación de ingreso y reglas de control de acceso (se explica mas adelante en este manual).
4. Existe al menos una ruta alcanzable entre la consola terminal y el Switch.

Paso 1: Conectar el puerto Ethernet del PC a una puerta Ethernet del Switch si se esta en un ambiente LAN o a través de la WAN si es un ambiente remoto.

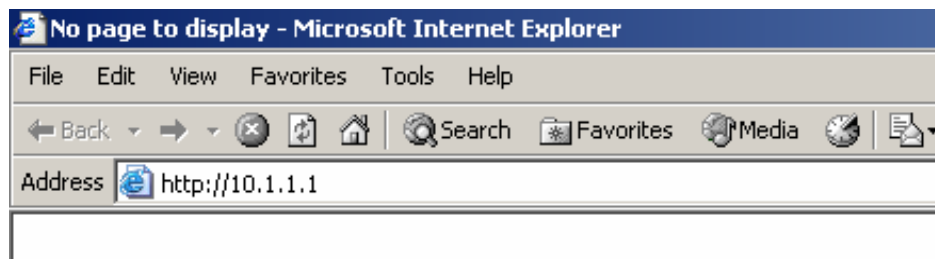
Paso 2: Si no ha sido configurado en un principio el servicio Web, se debe hacer de esta forma:

```
[Quidway]web set-package [nombre_del_archivo] . Ej: http3.1.3-0060.web
```

En las nuevas versiones del VRP se hacen de la siguiente forma:

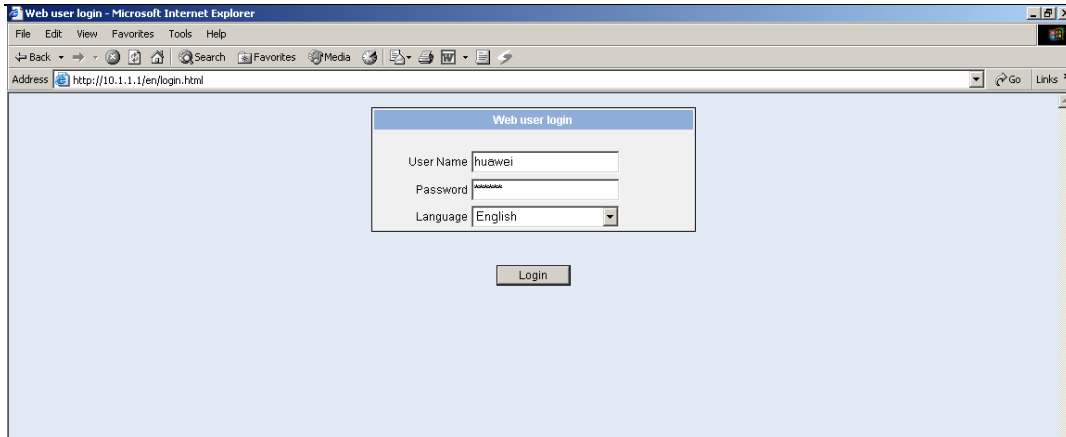
```
<Quidway>boot web-package [nombre_del_archivo]
```

Paso 3: Abrir el Navegador Web (Web-based Network Management es soportado por IE 5.5, IE6.0, Netscape 7.1 y Mozilla 1.4 como mínimo) e ingresar la dirección IP del Switch.

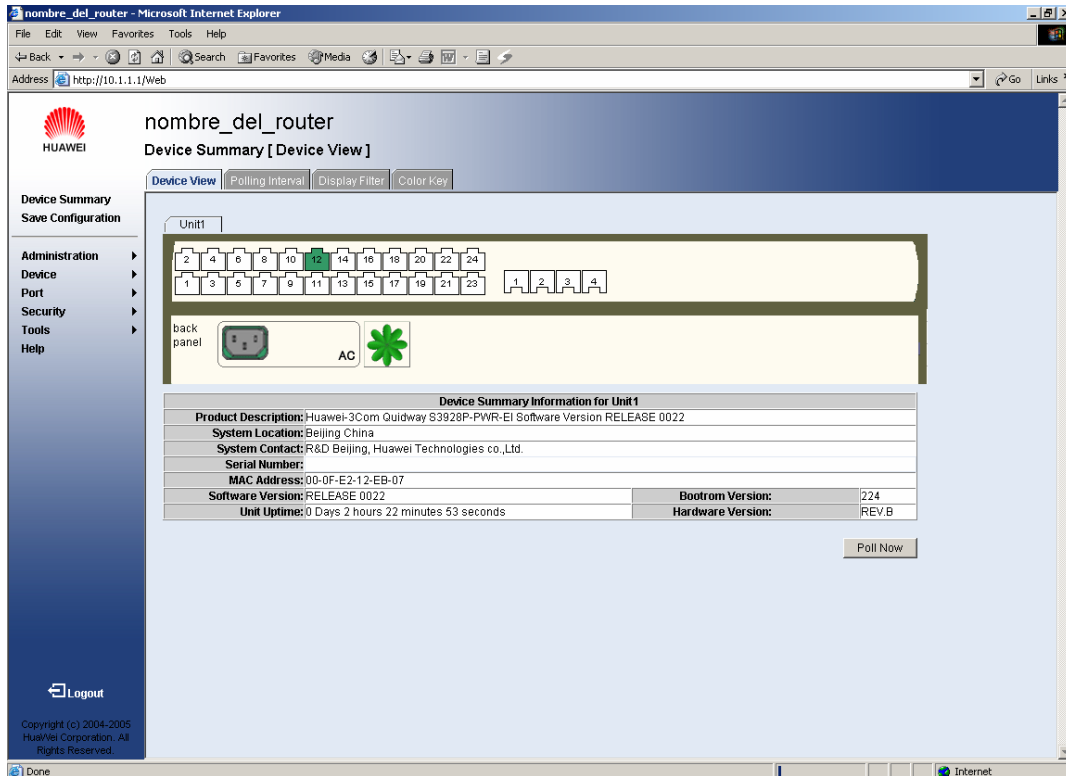


**Nota:** La dirección ingresada corresponde a la dirección IP de alguna VLAN configurada en el Switch. Asegúrese que el PC esté conectado a la puerta Ethernet de la VLAN correspondiente. De otra forma no se podrá establecer comunicación.

Paso 4: Ingrese el nombre de usuario y password configurados previamente en el Switch (los detalles de esto se verá mas adelante) y elija idioma.



Paso 5: Si los pasos anteriores han sido configurados correctamente se ingresará a la siguiente interface de configuración.



**Nota:** Las opciones y herramientas de configuración variarán dependiendo del nivel de privilegios establecidos para el usuario.



---

## 2. Administración de Usuarios

Un router no posee un password de usuario cuando se enciende por primera vez. Bajo esas condiciones, cualquier usuario puede realizar configuraciones en el equipo mientras se conecte a través de consola. Un usuario remoto puede acceder vía telnet si el router ha sido configurado con dirección IP. Para asegurar seguridad en la red, es necesario configurar un usuario y password para el router con el fin de permitir la administración de estos.

### **2.1 Clasificación de Usuarios**

De acuerdo con los servicios disponibles para los usuarios, estos pueden ser clasificados en las siguientes categorías:

1. **Usuario de Hyperterminal:** Que accede al router vía Consola o puerto AUX.
2. **Usuario de Telnet:** Que accede al router a través de comandos Telnet;
3. **Usuario FTP:** Establece conexiones FTP con el router para transmitir paquetes;
4. **Usuarios PPP:** Establece conexiones PPP (tales como discado y PPPoA) con el router para acceder a la red;
5. **Usuario SSH:** Establece conexiones SSH para ingresar al router;
6. **Usuario PAD:** Establece conexiones PAD con el router para acceder a la red.
7. **Usuario Web:** establece conexiones a través de HTTP usando las mismas configuraciones de ingreso que para un usuario Telnet.

Un usuario puede tener múltiples servicios al mismo tiempo. De esta forma, un mismo usuario puede ejecutar múltiples funciones.



---

## 2.2 Prioridad de Usuarios

El sistema maneja jerarquías para los usuarios Telnet e HyperTerminal. De acuerdo con esta jerarquía, los usuarios se clasifican en 4 niveles: visitante, monitor, sistema y administración, todos estos identificados con números del 0 al 3. Después de que los usuarios de los distintos niveles logean, sólo pueden emplear comandos de su mismo nivel o inferiores. Si el tipo de autenticación que se está utilizando es mediante **password** o si simplemente no se utiliza autenticación, el nivel de comandos al que el usuario puede acceder depende del nivel configurado en la interfaz de usuario.

Por ejemplo, si el nivel de prioridad de un usuario es 2, él solo puede acceder a comandos de nivel 0 hasta 2. El usuario con nivel de prioridad 3 puede acceder a todos los comandos. Los comandos que los usuarios de cada nivel pueden acceder se muestran en la siguiente tabla:

Prioridad de Usuario	Nombre	Comando
0	Visit	Ping, tracert, telnet
1	Monitor	Ping, tracert, telnet, display, debugging
2	System	Todos los comandos de configuración (excepto los de administración) y los comandos con nivel de prioridad 0 y 1
3	Manage	Todos los comandos

## 2.1 Autenticación de Usuario

El sistema autentifica a los usuarios cuando estos se conectan. Existen 4 tipos de métodos de autenticación:

- Autenticación local;
- Autenticación en servidor AAA;
- Autenticación mediante password;
- Sin autenticación.

No se recomienda no utilizar autenticación, debido a que usuarios pueden acceder al router sin nombre de usuario ni password. La autenticación mediante password es levemente segura, debido a que requiere a cada usuario



que se conecte que el ingreso del password asociado. Cuando se emplea autenticación local o mediante un servidor AAA, se debe ingresar un nombre de usuario y password que correspondan a los configurados en el router o en el servidor AAA. Los usuarios de discado se autentifican usualmente a través de servidores AAA mientras que los usuarios telnet y de terminal lo realizar de forma local.

## **2.3 Configuración de la administración de usuario**

La administración de los usuarios incluye:

- Configurar el modo de autenticación;
- Configurar el nombre de usuario y password
- Configurar la prioridad del usuario
- Configurar los servicios para el usuario

El propósito de la autenticación de usuario es permitir al usuario legal conectarse y emplear el router y prevenir que los usuarios ilegales lo hagan.

### **2.3.1 Configuración del modo de autenticación de usuario**

Al configurar el modo de autenticación de usuario, se puede configurar el método de autenticación que se empleará cuando un usuario acceda el router a través de la interfaz de usuario especificada.

<code>authentication-mode { password   scheme [ command-authorization ] }</code>
--

**None:** Indica que no se emplea autenticación.

**Password:** Indica autenticación empleando password pero no usuario.

**Scheme:** Indica autenticación empleando el esquema AAA (autenticación local, RADIUS/HWTACACS)



## 2.3.2 Configuración de usuario y password

### Autenticación mediante password

Esta configuración se realiza en el modo de visualización de la interfaz.

```
set authentication password { cipher | simple } clave
```

**Simple:** Indica que se configure el password en texto plano.

**Cipher:** Indica que se configura el password con texto encriptado.

### 2.3.3 Autenticación local con nombre de usuario y password

Si se elige autenticación local, será necesario emplear nombre de usuario y password.

Operación	Comando
Configurar nombre de usuario (en system view).	<b>local-user</b> <i>nombre-usuario</i>
Eliminar usuario (en system view).	<b>undo local-user</b> { <i>nombre-usuario</i>   <b>all</b> }
Configurar un password para el usuario local (en local user view).	<b>password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>
Cancelar el password del usuario local (en local user view).	<b>undo password</b>

**Simple:** Indica que se configura el password en texto plano

**Cipher:** Indica que se configura el password en texto cifrado.



## 2.3.4 Configuración de Servicios de Usuario

El comando **service-type** permite configurar el nivel de comandos que un usuario puede utilizar en un determinado servicio. Esto se clasifica en 4 niveles: **visita, monitoreo, configuración y administración.**

- **Nivel de Visita (Level 0):** Los comandos de este nivel permiten realizar diagnóstico (tales como **ping** y **tracert**), comandos **telnet**, etc. La operación de grabar la configuración no está permitida en este nivel.
- **Nivel de Monitoreo (Level 1):** Los comandos de este nivel, incluyen (además de los anteriores), los comandos **display** y **debugging**, son empleados para mantención del sistema, servicio de diagnóstico de fallas, etc. La operación de grabar la configuración no está permitida en este nivel
- **Nivel de Configuración (Level2):** Permite la ejecución de comandos de configuración, tales como comandos de ruteo y otros comandos en las distintas capas de red, son empleados para entregar servicios directos de red al usuario.
- **Nivel de Administración (Level 3):** Permite la ejecución de todo tipo de comandos

Los servicios a los cuales pueden acceder los usuarios son los siguientes:

ftp	Servicio FTP
lan-access	Servicio LAN-ACCESS
ssh	Servicio Secure Shell
telnet	Servicio TELNET
terminal	Servicio TERMINAL

*Estos servicios dependen del modelo y tipo de equipo.*



## Ejemplo de Configuración:

```
[Quidway] local-user prueba
[Quidway-luser-prueba] password cipher huawei123
[Quidway-luser-prueba] service-type telnet level 0
```

En el ejemplo de configuración que se muestra, se configura el usuario local **prueba**, con clave encriptada **huawei123**, que tendrá acceso al servicio **telnet** con un nivel de prioridad **0**.

### 2.3.5 Configuración de servicios SSH.

Paso 1: Los procedimientos de configuración varían dependiendo del modo de autenticación. Sin embargo, todos los procedimientos deben comenzar creando la key local del RSA usando los siguientes comandos

```
[Quidway]user-interface vty 0 4
[Quidway-ui-vty0-4]authentication-mode scheme
[Quidway-ui-vty0-4]protocol inbound ssh
[Quidway-ui-vty0-4]quit
[Quidway]local-user huawei
[Quidway-luser-huawei]password cipher huawei
[Quidway-luser-huawei]service-type ssh
[Quidway-luser-huawei]quit
[Quidway]ssh user huawei authentication-type password
[Quidway]domain huawei
[Quidway-isp-huawei]scheme local
[Quidway-isp-huawei]quit
```

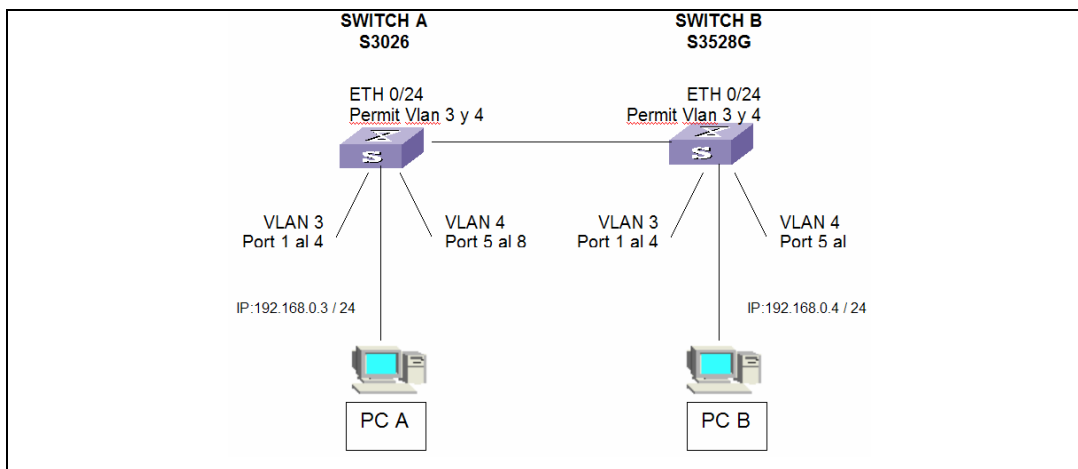
Los valores por defecto para el time-out de autenticación, tiempo de reintento y de actualización de la key de SSH puede ser adaptada. Después de estas configuraciones, puedes correr el software cliente SSH que soporte SSH 2.0 en otros terminales conectados al Switch. Ahora puedes acceder al Switch con el username huawei y el password huawei.



## Configuraciones Básicas de Protocolos.

### Configuración VLAN

#### Escenario:



#### Pasos: (Se aplica la misma configuración para ambos Switches)

1. Creación de VLAN y asignación de puertos físicos del Switch a las VLANs. Cabe señalar que por defecto, todos los puertos pertenecen a la VLAN de administración que es la 1. En el siguiente ejemplo se están agregando puertos por rango, igualmente se pueden agregar en forma individual.

```
[SwitchA]vlan 3
[SwitchA-vlan3]port eth 0/1 to eth 0/4
[SwitchA-vlan3]vlan 4
[SwitchA-vlan4]port eth 0/5 to eth 0/8
[SwitchA-vlan4]quit
[SwitchA]
```

2. Creación de puerto Trunk. Los puertos trunk son aquellos que permiten la transmisión de los datos originados en distintas VLANs, empleando la encapsulación definida por el estándar IEEE 802.1q.  
En el ejemplo se configura el puerto Ethernet 0/24 como trunk, permitiendo el paso de las VLANs 3 y 4.



```
[SwitchA]int eth 0/24
[SwitchA -Ethernet0/24]port link-type trunk
[SwitchA y-Ethernet0/24]port trunk permit vlan 3 to 4
[SwitchA y-Ethernet0/24]quit
[SwitchA]
```

### 3. Configuración de Puerto Híbrido.

Los puertos híbridos son aquellos que permiten la transmisión de datos pertenecientes a ciertas VLANs con y sin tag de acuerdo a como se configure.

En el siguiente ejemplo se muestra la configuración de un puerto híbrido que permitirá la transmisión de la VLAN 2 con tag y la 3 sin tag

```
[Quidway-Ethernet1/0/22]port link-type hybrid
[Quidway-Ethernet1/0/22]port hybrid vlan 2 tagged
[Quidway-Ethernet1/0/22]port hybrid vlan 3 untagged
```

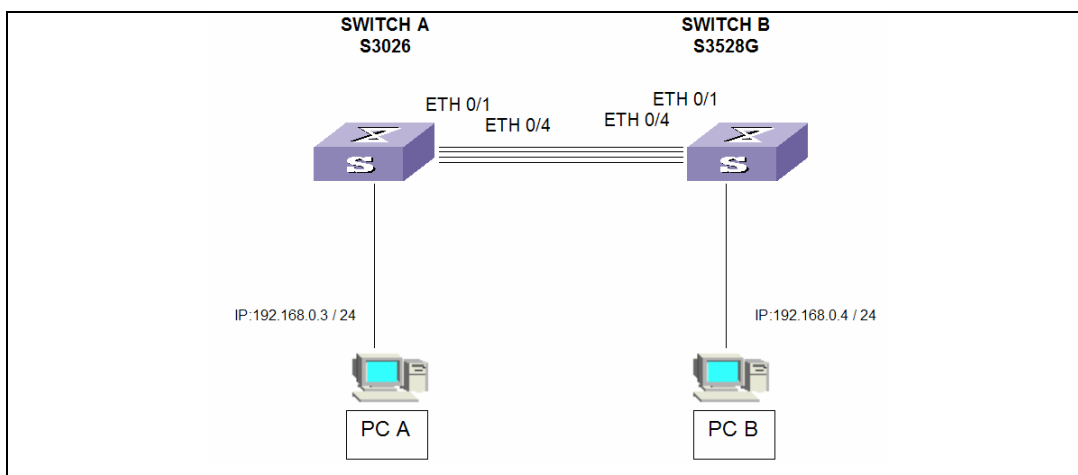
## Configuración Link-Aggregation

Link aggregation consiste en la agregación de varios puertos juntos para implementar el balance de carga de entrada y salida sobre los puertos miembros del grupo, y aumentar la estabilidad de la conexión.

Para los puertos miembros en un grupo, sus configuraciones básicas deben ser las mismas. Esto significa que si un puerto es Trunk, los otros puertos también deben serlo, si un puerto cambia a Access, los otros también.

Los Switches Ethernet Serie 3900 pueden soportar hasta 8 grupos de agregación. Cada grupo puede tener hasta 8 puertos Ethernet de 100 Mbps o cuatro puertos Gigabit SPF como máximo. Para la serie S3900-SI series, los puertos en el grupo de agregación deben pertenecer físicamente a la misma unidad.

### Escenario:



**Pasos:** (Se aplica la misma configuración para ambos Switches).

Habilitar LACP (Link Aggregation Control Protocol) en cada uno de los puertos.

Por defecto viene desactivado.

```
[Quidway-Ethernet1/0/1]lACP enable
```



1. Crear el grupo de agregación.

```
[Quidway]link-aggregation group 1 mode manual
```

2. Agregar cada interface al grupo anteriormente definido.

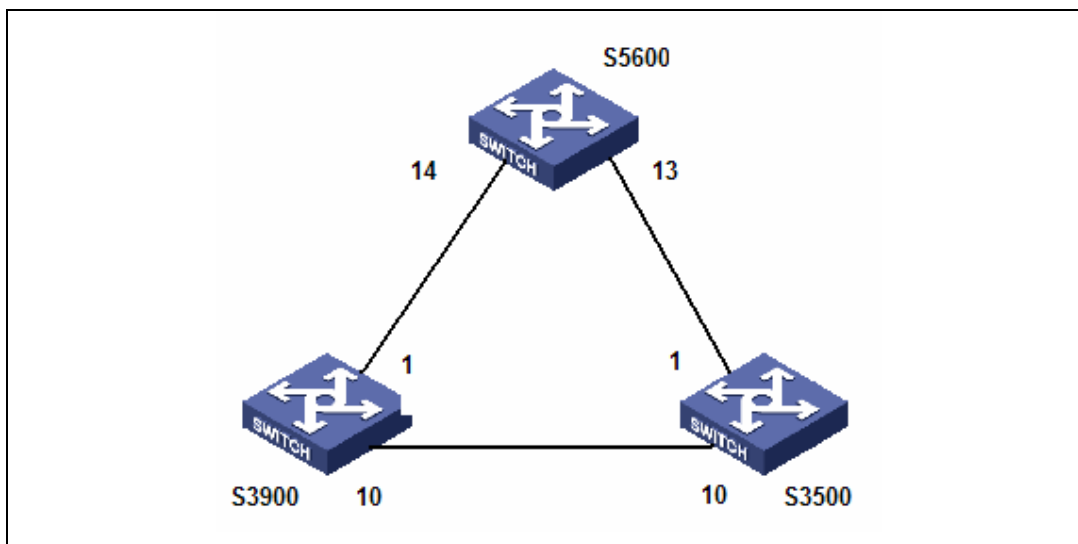
```
[Quidway-Ethernet1/0/1]port link-aggregation group 1  
[Quidway-Ethernet1/0/2]port link-aggregation group 1  
[Quidway-Ethernet1/0/3]port link-aggregation group 1  
[Quidway-Ethernet1/0/4]port link-aggregation group 1
```

**Nota:** Todos los puertos debes estar configurado con la misma velocidad (10, 100 o auto) y el mismo modo duplex (full, half o auto)

## Spanning Tree Protocol

Spanning Tree es un protocolo diseñado para evitar el loops en Switchs con rutas redundantes. Lo que hace es desactivar un enlace para evitar los loops, y solo activarse en el momento en que alguno de los otros enlaces falle. Para esto elige un Switch como "root", que es el que tiene mas bajo "Bridge ID", y el enlace con el costo mas alto hacia el root bridge desde cualquiera de los otros Switches (que no son root) es desactivado. Un administrador puede manipular la elección del root alterando la prioridad por defecto del Switch.

Supongamos la siguiente configuración:



Se presentan 3 switch, S5600(2) ROOT , S3900 y S3500.

1. Habilitación del protocolo Spanning Tree en forma global. El comando se muestra de la siguiente forma (por defecto viene desactivado):

```
[Quidway]stp enable
```



2. Para asignar el switch como ROOT debemos cambiar el valor de su prioridad por uno menor. Los switch traen por defecto la prioridad 32768. El comando empleado para configurar la prioridad se muestra a continuación:

```
[Quidway]stp priority 28672
```

***Nota: El valor de la prioridad debe ser modificado en saltos de 4096.***

3. Para la activación de RSTP (Rapid Spanning Tree) o de MSTP (Multiple Spanning Tree) se hace de la forma siguiente.

```
[Quidway]stp mode rstp
```

```
[Quidway]stp mode mstp
```



## Recuperación de Contraseñas.

En el caso de que olvide la(s) contraseña(s) de acceso al equipo, existe un procedimiento que nos permite eliminar el archivo de configuración inicial, que es donde se alejan dichos passwords.

1. Apague y Encienda el equipo.
2. Cuando le de la opción, ingrese al menú del Bootrom del equipo (ctrl + b) y elija la opción 4 para eliminar archivos de la flash:

```
Press Ctrl-B to enter Boot Menu... 1

password:

      BOOT MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Enter your choice(0-9): 4
```

3. Se desplegará un nuevo menú que muestra todos los archivos disponibles en la memoria flash del equipo, elija la opción que corresponda para borrar el archivo de configuración (en este caso sería vrpcfg.cfg)



```
Enter your choice(0-9): 4
File Number  File Size(bytes)  File Name
=====1
      5009062   s3900ei-vrp310-r0022-224.bin
2      4         snmpboots
3     151        private-data.txt
4     1967       vrpcfg.cfg
Free Space: 4575232 bytes
The current application file is s3900ei-vrp310-r0022-224.bin
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute
Please input the file number to delete: 4
The file you selected is vrpcfg.cfg. Delete it? Yes or No(Y/N) Y
Deleting file.....done!
```

4. Luego reinicie el equipo.

```
BOOT MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Enter your choice(0-9): 0
```

5. El equipo se reiniciará con la configuración de fábrica.





En algunas versiones es posible recuperar el archivo de configuración original. Esto debido a que al borrar un archivo este realmente no se elimina, si no que es llevado a un equivalente a la papelera de reciclaje. Por lo tanto, para verificar si la versión de software que estamos utilizando tiene la característica de que los archivos eliminados desde el menú de BootRoom no son eliminados permanentemente si no que son marcados, debemos realizar la siguiente prueba:

Ejecute el siguiente comando:

```
<Quidway>dir /all
Directory of unit1>flash:/

-rw-  2290      Jan 01 1970 00:00:31  [vrpcfg.cfg]
-rw-  673984    Apr 02 2000 00:33:34  http3.1.3-0043.web
-rw-  5009062   Jan 01 1970 00:01:06  s3900-vrp310-r0013-223-64-ei.bin
-rwh   4        Apr 01 2000 23:55:15  snmpboots
-rw-  5028602   Apr 02 2000 00:14:35  s3900ei-vrp310-r0022-224.bin

15367 KB total (4470 KB free)
```

En este caso en particular, aparece el archivo entre corchetes cuadrados, lo que quiere decir que se encuentra eliminado, pero que puede ser recuperado.

6. Para recuperar el archivo ejecute el siguiente comando:

```
<Quidway>undelete vrpcfg.cfg
Undelete flash:/vrpcfg.cfg? (y/n)
% undelete file flash:/vrpcfg.cfg
```

7. Para revisar el contenido del dicho archivo, ejecute el siguiente comando:

```
<Quidway>more vrpcfg-cfg
```

Si la contraseña esta en modo cifrado, no podrá ser recuperada, se deberá crear una nueva. De ser el caso, tenga precaución de no reiniciar el equipo sin haber cambiado la contraseña y grabado la nueva configuración.