

Jose Carlos Roncero Blanco

Protocolos PPP, PAP y CHAP

PPP

Point-to-point Protocol (en español Protocolo punto a punto), también conocido por su acrónimo PPP, es un protocolo de nivel de enlace estandarizado en el documento RFC 1661. Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet.

El protocolo PPP permite establecer una comunicación a nivel de la capa de enlace TCP/IP entre dos computadoras. Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico. Ocasionalmente también es utilizado sobre conexiones de banda ancha (como PPPoE o PPPoA). Además del simple transporte de datos, PPP facilita dos funciones importantes:

- **Autenticación.** Generalmente mediante una clave de acceso.
- **Asignación dinámica de IP.** Los proveedores de acceso cuentan con un número limitado de direcciones IP y cuentan con más clientes que direcciones. Naturalmente, no todos los clientes se conectan al mismo tiempo. Así, es posible asignar una dirección IP a cada cliente en el momento en que se conectan al proveedor. La dirección IP se conserva hasta que termina la conexión por PPP. Posteriormente, puede ser asignada a otro cliente.

PPP también tiene otros usos, por ejemplo, se utiliza para establecer la comunicación entre un módem ADSL y la pasarela ATM del operador de telecomunicaciones.

También se ha venido utilizando para conectar a trabajadores desplazados (p. ej. ordenador portátil) con sus oficinas a través de un centro de acceso remoto de su empresa. Aunque esta aplicación se está abandonando en favor de las redes privadas virtuales, más seguras.

Funcionamiento

PPP consta de las siguientes fases:

- **Establecimiento de conexión.** Durante esta fase, una computadora contacta con la otra y negocian los parámetros relativos al enlace usando el protocolo LCP. Este protocolo es una parte fundamental de PPP y por ello está definido en el mismo RFC. Usando LCP se negocia el método de autenticación que se va a utilizar, el tamaño de los datagramas, números mágicos para usar durante la autenticación,...
- **Autenticación.** No es obligatorio. Existen dos protocolos de autenticación. El más básico e inseguro es PAP, aunque no se recomienda dado que manda el nombre de usuario y la contraseña en claro. Un método más avanzado y preferido por muchos ISPs es CHAP, en el cual la contraseña se manda cifrada.

- Configuración de red. En esta fase se negocian parámetros dependientes del protocolo de red que se esté usando. PPP puede llevar muchos protocolos de red al mismo tiempo y es necesario configurar individualmente cada uno de estos protocolos. Para configurar un protocolo de red se usa el protocolo NCP correspondiente. Por ejemplo, si la red es IP, se usa el protocolo IPCP para asignar la dirección IP del cliente y sus servidores DNS
- Transmisión. Durante esta fase se manda y recibe la información de red. LCP se encarga de comprobar que la línea está activa durante periodos de inactividad. Obsérvese que PPP no proporciona cifrado de datos.
- Terminación. La conexión puede ser finalizada en cualquier momento y por cualquier motivo.

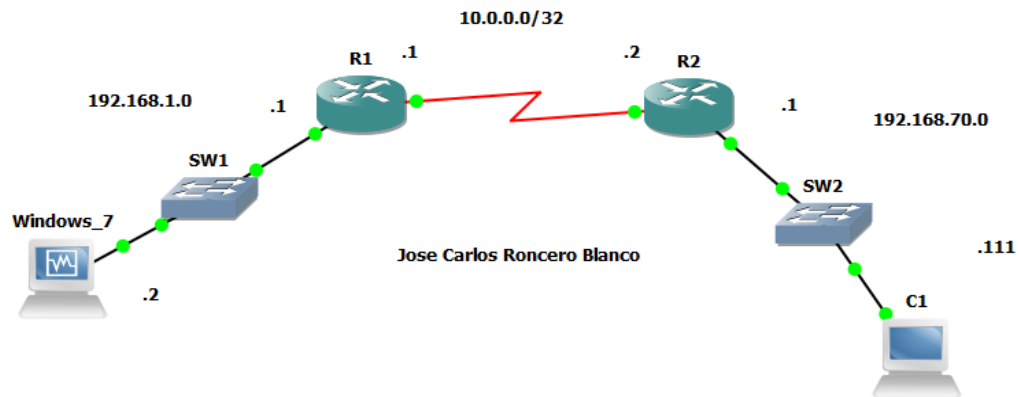
PAP

PAP son las siglas de Password Authentication Protocol un protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un proveedor de servicios de internet. PAP es un subprotocolo usado por la autenticación del protocolo PPP (Point to Point Protocol), validando a un usuario que accede a ciertos recursos. PAP transmite contraseñas o passwords en ASCII sin cifrar, por lo que se considera inseguro. PAP se usa como último recurso cuando el servidor de acceso remoto no soporta un protocolo de autenticación más fuerte.

CHAP

CHAP es un método de autenticación usado por servidores accesibles vía PPP. CHAP verifica periódicamente la identidad del cliente remoto usando un intercambio de información de tres etapas. Esto ocurre cuando se establece el enlace inicial y puede pasar de nuevo en cualquier momento de la comunicación. La verificación se basa en un secreto compartido (como una contraseña).

Vamos a pasar a realizar la interconexión entre las redes según los protocolos PPP, PAP y CHAP. Para ello nos crearemos una red como esta:



Realizaremos un enrutamiento estático en los routers y pondremos las direcciones IP para tenerlo guardado ya para los 3 tipos de conexiones

R1

```
enable
conf t
interface s1/0
ip address 10.0.0.1 255.255.255.252
no shutdown
exit
interface f2/0
ip address 192.168.1.1 255.255.255.0
no shutdown
end
enable
conf t
ip route 192.168.70.0 255.255.255.0 10.0.0.2
end
copy run sta
```

```
R1
R1#enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface s1/0
R1(config-if)#ip address 10.0.0.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface f2/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#end
R1#enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 192.168.70.0 255.255.255.0 10.0.0.2
R1(config)#end
R1#copy run sta
*Jan 31 18:43:53.547: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
*Jan 31 18:43:54.123: %SYS-5-CONFIG_I: Configured from console by console
*Jan 31 18:43:54.175: %SYS-5-CONFIG_I: Configured from console by console
R1#copy run sta
*Jan 31 18:43:55.959: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to up
R1#copy run sta
```

R2

```
enable
conf t
interface s1/0
ip address 10.0.0.2 255.255.255.252
no shutdown
exit
interface f2/0
ip address 192.168.70.1 255.255.255.0
no shutdown
end
enable
conf t
ip route 192.168.1.0 255.255.255.0 10.0.0.1
end
copy run sta
```

```
R2#enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface s1/0
R2(config-if)#ip address 10.0.0.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface f2/0
R2(config-if)#ip address 192.168.70.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#end
R2#enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 192.168.1.0 255.255.255.0 10.0.0.1
R2(config)#end
R2#copy run sta
*Jan 31 18:47:34.639: %SYS-5-CONFIG_I: Configured from console by console
*Jan 31 18:47:34.715: %SYS-5-CONFIG_I: Configured from console by console
R2#copy run sta
*Jan 31 18:47:36.191: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
*Jan 31 18:47:36.195: %ENTITY_ALARM-6-INFO: CLEAR INFO Se1/0 Physical Port Administrative State Down
*Jan 31 18:47:36.459: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to up
R2#copy run sta
```

Pasaremos a realizar la encapsulación PPP en los routers. Se quedara así:

encapsulacion ppp R1

enable

conf t

interface s1/0

encapsulacion ppp

no shutdown

end

copy run sta

```
R1
Connected to Dynamips VM "R1" (ID 0, type c7200) - Console port
Press ENTER to get the prompt.

Destination filename [startup-config]?
?Bad filename
%Error parsing filename (Bad file number)
R1#enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface s1/0
R1(config-if)#encapsulation ppp
R1(config-if)#
*Jan 31 18:53:13.039: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
R1(config-if)#no shutdown
R1(config-if)#end
R1#copy run s
*Jan 31 18:53:18.963: %SYS-5-CONFIG_I: Configured from console by console
R1#copy run sta
```

encapsulacion ppp R2

enable

conf t

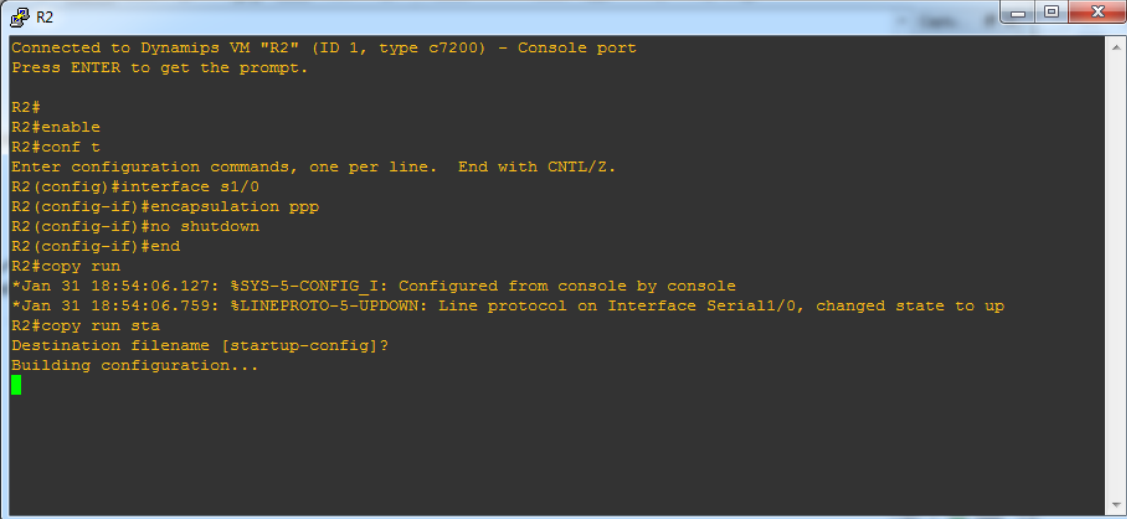
interface s1/0

encapsulacion ppp

no shutdown

end

copy run sta



```
R2
Connected to Dynamips VM "R2" (ID 1, type c7200) - Console port
Press ENTER to get the prompt.

R2#
R2#enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface s1/0
R2(config-if)#encapsulation ppp
R2(config-if)#no shutdown
R2(config-if)#end
R2#copy run
*Jan 31 18:54:06.127: %SYS-5-CONFIG_I: Configured from console by console
*Jan 31 18:54:06.759: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R2#copy run sta
Destination filename [startup-config]?
Building configuration...
█
```

ping entre equipos

Jose Carlos Windows 7 (2) [Corriendo] - Oracle VM VirtualBox

Máquina Ver Dispositivos Ayuda

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\JoseCarlos>ping 192.168.70.111

Haciendo ping a 192.168.70.111 con 32 bytes de datos:
Respuesta desde 192.168.70.111: bytes=32 tiempo=38ms TTL=126
Respuesta desde 192.168.70.111: bytes=32 tiempo=38ms TTL=126
Respuesta desde 192.168.70.111: bytes=32 tiempo=38ms TTL=126
Respuesta desde 192.168.70.111: bytes=32 tiempo=39ms TTL=126

Estadísticas de ping para 192.168.70.111:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 38ms, Máximo = 39ms, Media = 38ms

C:\Users\JoseCarlos>
```

```
C:\Windows\system32\cmd.exe - ping 192.168.1.1
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

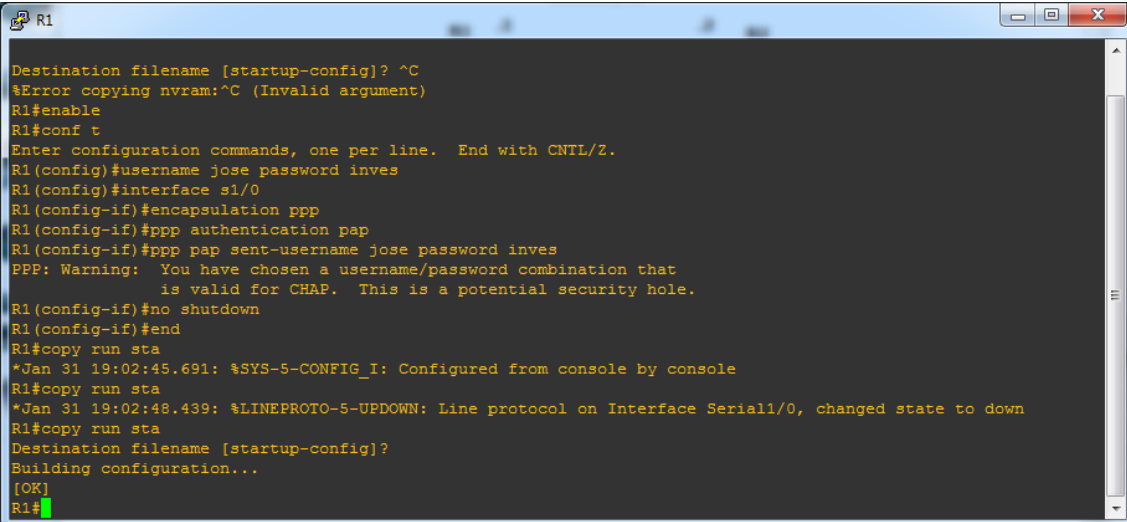
C:\Users\portatil1>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo=46ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=55ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=35ms TTL=254
```

autenticacion pap con encapsulacion ppp

R1

```
enable
conf t
username jose password inves
interface s1/0
encapsulation ppp
ppp authentication pap
ppp pap sent-username jose password inves
no shutdown
end
copy run sta
```



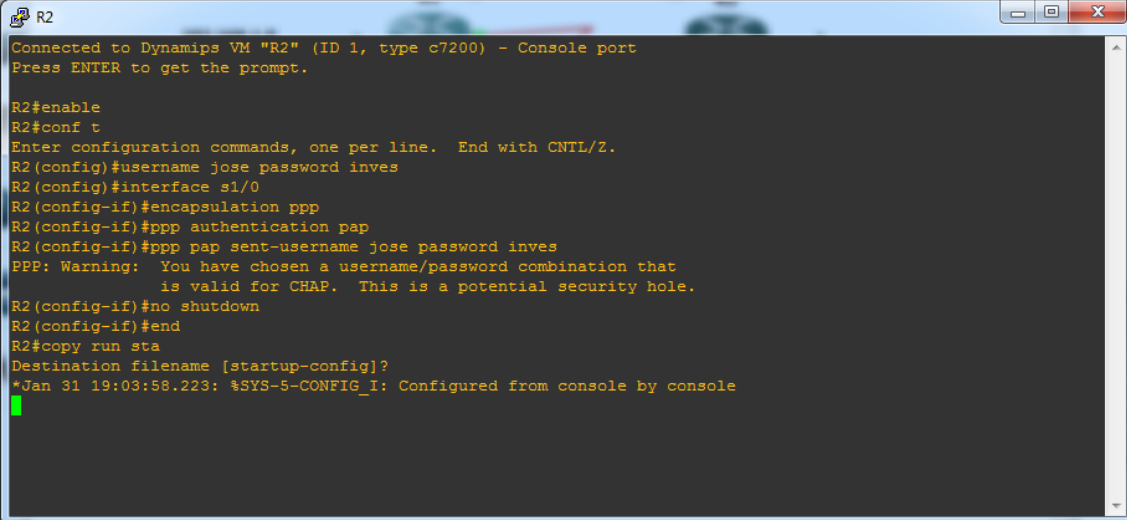
```
R1
Destination filename [startup-config]? ^C
%Error copying nvram: ^C (Invalid argument)
R1#enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#username jose password inves
R1(config)#interface s1/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username jose password inves
PPP: Warning: You have chosen a username/password combination that
               is valid for CHAP. This is a potential security hole.
R1(config-if)#no shutdown
R1(config-if)#end
R1#copy run sta
*Jan 31 19:02:45.691: %SYS-5-CONFIG_I: Configured from console by console
R1#copy run sta
*Jan 31 19:02:48.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
R1#copy run sta
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

R2

```
enable
conf t
username jose password inves
interface s1/0
encapsulation ppp
ppp authentication pap
ppp pap sent-username jose password inves
no shutdown
```


end

copy run sta



```
R2
Connected to Dynamips VM "R2" (ID 1, type c7200) - Console port
Press ENTER to get the prompt.

R2#enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username jose password inves
R2(config)#interface s1/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username jose password inves
PPP: Warning: You have chosen a username/password combination that
               is valid for CHAP. This is a potential security hole.
R2(config-if)#no shutdown
R2(config-if)#end
R2#copy run sta
Destination filename [startup-config]?
*Jan 31 19:03:58.223: %SYS-5-CONFIG_I: Configured from console by console
```

Ip entre equipos

```
Administrador: C:\Windows\system32\cmd.exe

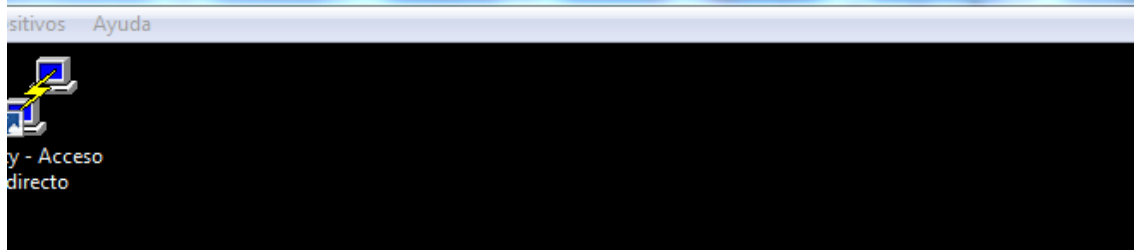
C:\Users\portatil1>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo=66ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=75ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=74ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=33ms TTL=254

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos).
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 33ms, Máximo = 75ms, Media = 62ms

C:\Users\portatil1>
```

7 (2) [Corriendo] - Oracle VM VirtualBox



```
C:\Windows\system32\cmd.exe - ping 192.168.70.111

Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\JoseCarlos>ping 192.168.70.111

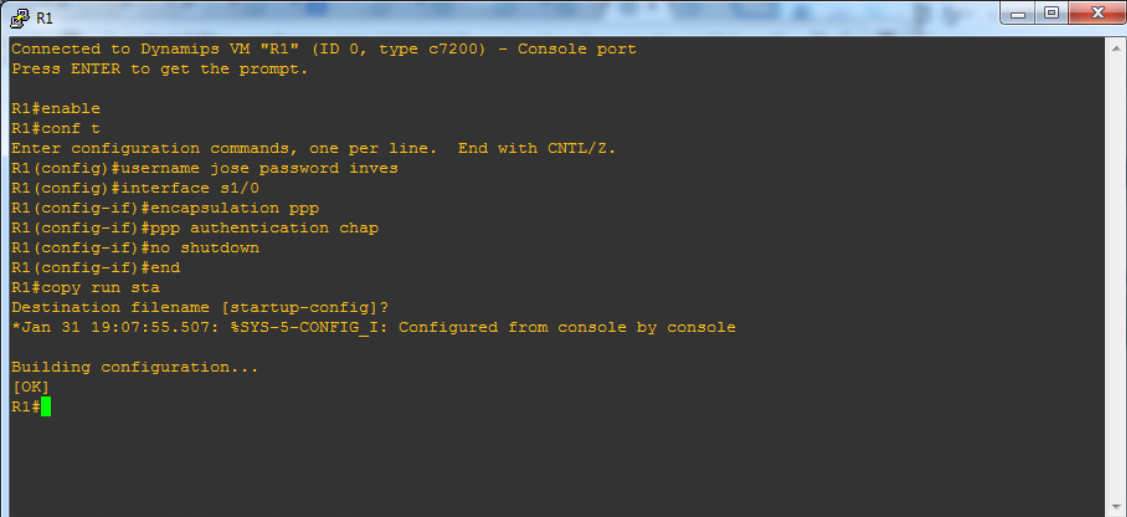
Haciendo ping a 192.168.70.111 con 32 bytes de datos:
Respuesta desde 192.168.70.111: bytes=32 tiempo=34ms TTL=126
Respuesta desde 192.168.70.111: bytes=32 tiempo=42ms TTL=126
Respuesta desde 192.168.70.111: bytes=32 tiempo=37ms TTL=126
```

Windows 7
Compilación 7601
Reproductor de Windows Media
Esta copia de Windows no es original
10:05

Chap con encapsulación ppp

R1

```
enable
conf t
username jose password inves
interface s1/0
encapsulation ppp
ppp authentication chap
no shutdown
end
copy run sta
```

A screenshot of a terminal window titled "R1". The window shows the output of a series of commands entered into a Cisco IOS configuration mode. The text is as follows:

```
R1
Connected to Dynamips VM "R1" (ID 0, type c7200) - Console port
Press ENTER to get the prompt.

R1#enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#username jose password inves
R1(config)#interface s1/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap
R1(config-if)#no shutdown
R1(config-if)#end
R1#copy run sta
Destination filename [startup-config]?
*Jan 31 19:07:55.507: %SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
R1#
```

R2

```
enable
conf t
username jose password inves
interface s1/0
encapsulation ppp
ppp authentication chap
no shutdown
end
copy run sta
```

```
R2
Connected to Dynamips VM "R2" (ID 1, type c7200) - Console port
Press ENTER to get the prompt.

R2#enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username jose password inves
R2(config)#interface s1/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
R2(config-if)#no shutdown
R2(config-if)#end
R2#copy run sta
Destination filename [startup-config]?
Building configuration...

*Jan 31 19:09:01.231: %SYS-5-CONFIG_I: Configured from console by console
*Jan 31 19:09:02.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
```

Ping entre equipos

```
C:\Users\JoseCarlos>ping 192.168.70.111

Haciendo ping a 192.168.70.111 con 32 bytes de datos:
Respuesta desde 192.168.70.111: bytes=32 tiempo=34ms TTL=126
Respuesta desde 192.168.70.111: bytes=32 tiempo=42ms TTL=126
Respuesta desde 192.168.70.111: bytes=32 tiempo=37ms TTL=126
Respuesta desde 192.168.70.111: bytes=32 tiempo=38ms TTL=126

Estadísticas de ping para 192.168.70.111:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    <0% perdidos>,
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 34ms, Máximo = 42ms, Media = 37ms

C:\Users\JoseCarlos>_
```

```
Administrador: C:\Windows\system32\cmd.exe

C:\Users\portatil1>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo=66ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=75ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=74ms TTL=254
Respuesta desde 192.168.1.1: bytes=32 tiempo=33ms TTL=254

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
            Mínimo = 33ms, Máximo = 75ms, Media = 62ms

C:\Users\portatil1>
```