Práctica de laboratorio: Configuración de syslog y NTP

Topología

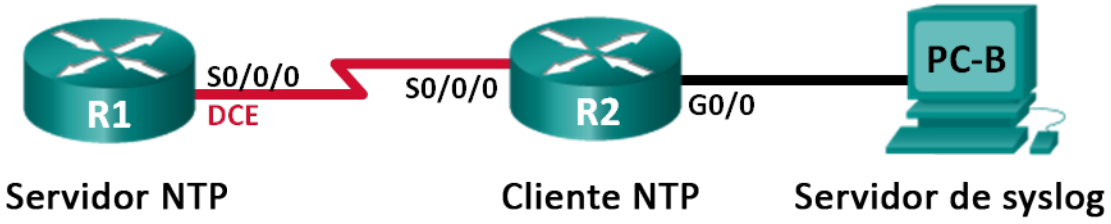


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	G0/0	172.16.2.1	255.255.255.0	N/A
PC-B	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Objetivos

Parte 1: configurar los parámetros básicos de los dispositivos

Parte 2: configurar NTP

Parte 3: Configurar syslog

Información básica/situación

Los mensajes de syslog que generan los dispositivos de red se pueden recopilar y archivar en un servidor de syslog. La información se puede utilizar para fines de control, depuración y resolución de problemas. El administrador puede controlar dónde se almacenan y se muestran los mensajes. Los mensajes de syslog se pueden marcar con la hora para analizar la secuencia de eventos de red; por lo tanto, es importante sincronizar el reloj a través de los dispositivos de red con un servidor de protocolo NTP.

En esta práctica de laboratorio, configurará el R1 como servidor NTP y el R2 como cliente syslog y NTP. La aplicación de servidor de syslog, como Tftp32d u otro programa similar, se ejecutará en la PC-B. Además, usted controlará el nivel de gravedad de los mensajes de registro que se recopilan y se archivan en el servidor de syslog.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Pueden utilizarse otros routers y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 computadora (Windows 7, Vista o XP, con un programa de emulación de terminal, como Tera Term, y software de syslog, como tftpd32)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet y seriales, como se muestra en la topología

Parte 1: Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de las interfaces, el routing, el acceso a los dispositivos y las contraseñas.

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

Paso 2: Inicializar y volver a cargar los routers según sea necesario.

Paso 3: Configurar los parámetros básicos para cada router.

a. Desactive la búsqueda del DNS.

b. Configure el nombre del dispositivo.

c. Cifre las contraseñas de texto no cifrado.

d. Cree un aviso de mensaje del día (MOTD) que advierta a los usuarios que se prohíbe el acceso no autorizado.

e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.

g. Establezca el inicio de sesión de consola en modo sincrónico.

h. Aplique las direcciones IP a las interfaces Serial y Gigabit Ethernet según la tabla de direccionamiento y active las interfaces físicas.

i. Establezca la frecuencia de reloj en **128000** para la interfaz serial DCE.

Paso 4: Configurar el routing.

Habilite OSPF de área única en los routers con la ID de proceso 1. Agregue todas las redes al proceso OSPF para el área 0.

Paso 5: Configurar la PC-B.

Configure la dirección IP y el gateway predeterminado para la PC-B según la tabla de direccionamiento.

Paso 6: Verificar la conectividad de extremo a extremo.

Verifique que cada dispositivo pueda hacer ping a todos los demás dispositivos en la red correctamente. De lo contrario, lleve a cabo la resolución de problemas hasta que haya conectividad de extremo a extremo.

Paso 7: Guardar la configuración en ejecución en la configuración de inicio.

Parte 2: Configurar NTP

En la parte 2, configurará el R1 como servidor NTP y el R2 como cliente NTP del R1. La sincronización del tiempo es importante para las funciones de syslog y de depuración. Si no se sincroniza el tiempo, es difícil determinar qué evento de red causó el mensaje.

Paso 1: Mostrar la hora actual.

Emita el comando **show clock** para mostrar la hora actual en el R1.

```
R1# show clock
*12:30:06.147 UTC Tue May 14 2013
```

En la siguiente tabla, registre la información relacionada con la hora actual que se muestra.

Fecha	
Tiempo	
Huso horario	

Paso 2: Establecer la hora.

Utilice el comando **clock set** para configurar la hora en el R1. El siguiente es un ejemplo de configuración de la fecha y la hora.

```
R1# clock set 9:39:00 05 july 2013
R1#
*Jul  5 09:39:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 12:30:54
UTC Tue May 14 2013 to 09:39:00 UTC Fri Jul 5 2013, configured from console by
console.
```

Nota: la hora también se puede configurar mediante el comando **clock timezone** del modo de configuración global. Para obtener más información sobre este comando, investigue el comando **clock timezone** en www.cisco.com a fin de determinar la zona de su región.

Paso 3: Configurar el maestro NTP.

Configure el R1 como maestro NTP mediante el comando **ntp master** *número-capa* del modo de configuración global. El número de capa indica a cuántos saltos NTP se encuentra un origen de hora autoritativo. En esta práctica de laboratorio, el nivel de capa de este servidor NTP es el número 5.

```
R1(config)# ntp master 5
```

Paso 4: Configurar el cliente NTP

a. Emita el comando **show clock** en el R2. En la siguiente tabla, registre la hora actual que se muestra en el R2.

Fecha	
Tiempo	
Huso horario	

b. Configure el R2 como cliente NTP. Utilice el comando **ntp server** para señalar a la dirección IP o al nombre de host del servidor NTP. El comando **ntp update-calendar** actualiza el calendario periódicamente con la hora de NTP.

```
R2(config)# ntp server 10.1.1.1
```

```
R2(config)# ntp update-calendar
```

Paso 5: Verificar la configuración NTP.

a. Utilice el comando **show ntp associations** para verificar que el R2 tenga una asociación NTP con el R1.

```
R2# show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~10.1.1.1        127.127.1.1      5     11     64   177 11.312  -0.018  4.298
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

b. Emita el comando **show clock** en el R1 y el R2 para comparar la marca de hora.

Nota: es posible que la sincronización de la marca de hora del R2 con la del R1 demore unos minutos.

```
R1# show clock
09:43:32.799 UTC Fri Jul 5 2013
R2# show clock
09:43:37.122 UTC Fri Jul 5 2013
```

Parte 3: Configurar syslog

Los mensajes de syslog de los dispositivos de red se pueden recopilar y archivar en un servidor de syslog. En esta práctica de laboratorio, se utilizará Tftpd32 como software de servidor de syslog. El administrador de red puede controlar los tipos de mensajes que se pueden enviar al servidor de syslog.

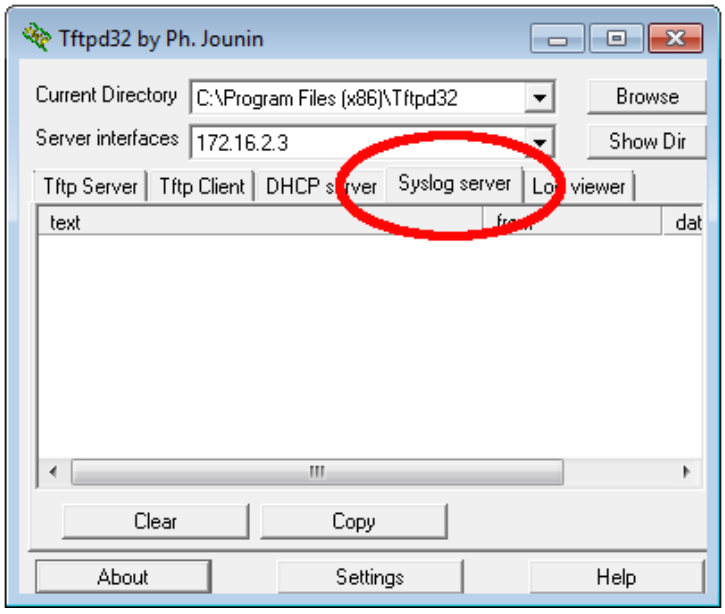
Paso 1: (Optativo) Instalar el servidor de syslog.

Si todavía no se instaló un servidor de syslog en la computadora, descargue e instale la versión más reciente de un servidor de syslog, como Tftpd32, en la computadora. La versión más reciente de Tftpd32 se puede encontrar en el siguiente enlace:

http://tftpd32.jounin.net/

Paso 2: Iniciar el servidor de syslog en la PC-B.

Después de iniciar la aplicación Tftpd32, haga clic en la ficha **Syslog server** (Servidor de syslog).



Paso 3: Verificar que el servicio de marca horaria esté habilitado en el R2.

Utilice el comando **show run** para verificar que el servicio de marca horaria esté habilitado para el registro en el R2.

```
R2# show run | include timestamp
service timestamps debug datetime msec
service timestamps log datetime msec
```

Si el servicio de marca horaria no está habilitado, utilice el siguiente comando para habilitarlo.

```
R2(config)# service timestamps log datetime msec
```

Paso 4: Configurar el R2 para registrar mensajes en el servidor de syslog.

Configure el R2 para enviar mensajes de syslog al servidor de syslog, la PC-B. La dirección IP del servidor de syslog PC-B es 172.16.2.3.

```
R2(config)# logging host 172.16.2.3
```

Paso 5: Mostrar la configuración de registro predeterminada.

Utilice el comando **show logging** para mostrar la configuración de registro predeterminada.

```
R2# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.
```

```
    Console logging: level debugging, 47 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 47 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 49 message lines logged
        Logging to 172.16.2.3  (udp port 514, audit disabled,
              link up),
              6 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging Source-Interface:       VRF Name:
```

¿Cuál es la dirección IP del servidor de syslog?

¿Qué protocolo y qué puerto usa syslog?

¿En qué nivel se encuentra habilitado el registro de traps?

Paso 6: Configurar y observar el efecto de registrar los niveles de gravedad en el R2.

a. Utilice el comando **logging trap ?** para determinar la disponibilidad de los distintos niveles de traps. Al configurar un nivel, los mensajes que se envían al servidor de syslog son del nivel de trap configurado y de cualquier nivel más bajo.

```
R2(config)# logging trap ?
  <0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
  critical       Critical conditions               (severity=2)
  debugging      Debugging messages                (severity=7)
  emergencies    System is unusable                (severity=0)
  errors         Error conditions                  (severity=3)
  informational  Informational messages            (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                (severity=4)
  <cr>
```

Si se emitió el comando **logging trap warnings**, ¿cuáles son los niveles de seguridad de mensajes que se registran?

b. Cambie el nivel de gravedad de registro a 4.

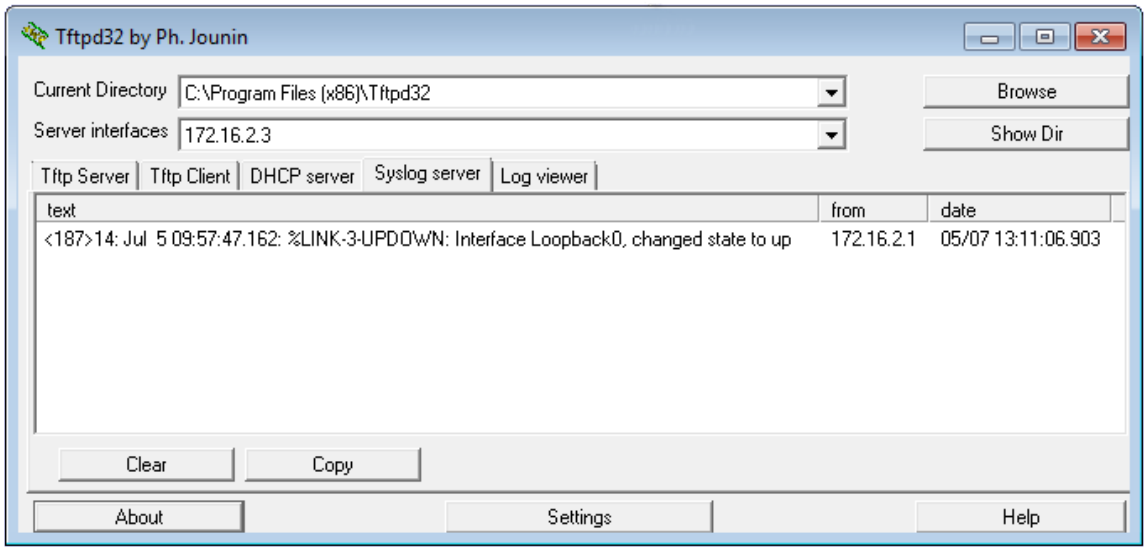
```
R2(config)# logging trap warnings
```

o

```
R2(config)# logging trap 4
```

c. Cree la interfaz Loopback0 en el R2 y observe los mensajes de registro en la ventana de la terminal y en la ventana del servidor de syslog en la PC-B.

```
R2(config)# interface lo 0
R2(config-if)#
Jul  5 09:57:47.162: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
Jul  5 09:57:48.162: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
```



d. Elimine la interfaz Loopback0 del R2 y observe los mensajes de registro.

```
R2(config-if)# no interface lo 0
R2(config)#
Jul  5 10:02:58.910: %LINK-5-CHANGED: Interface Loopback0, changed state to
administratively down
Jul  5 10:02:59.910: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to down
```

En el nivel de gravedad 4, ¿hay algún mensaje de registro en el servidor de syslog? Si apareció algún mensaje de registro, explique qué apareció y por qué.

e. Cambie el nivel de gravedad de registro a 6.

```
R2(config)# logging trap informational
```

o

```
R2(config)# logging trap 6
```

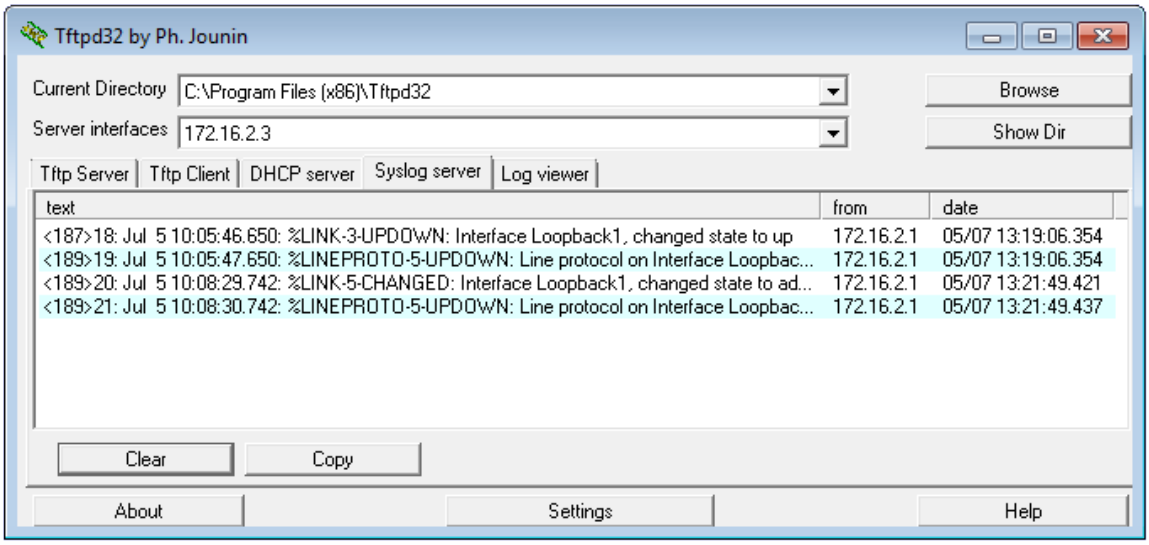
f. Borre las entradas de syslog de la PC-B. Haga clic en **Clear** (Borrar) en el cuadro de diálogo de Tftpd32.

g. Cree la interfaz Loopback 1 en el R2.

```
R2(config)# interface lo 1
Jul  5 10:05:46.650: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
Jul  5 10:05:47.650: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up
```

h. Elimine la interfaz Loopback 1 del R2.

```
R2(config-if)# no interface lo 1
R2(config-if)#
Jul  5 10:08:29.742: %LINK-5-CHANGED: Interface Loopback1, changed state to
administratively down
Jul  5 10:08:30.742: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to down
```



i. Observe el resultado del servidor de syslog. Compare este resultado con los resultados del nivel de trap 4. ¿Cuál es su observación?

Reflexión

¿Cuál es el problema de configurar un nivel de gravedad demasiado alto (el número más bajo) o demasiado bajo (el número de nivel más alto) para syslog?

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet n.º 2**	**Interfaz serial #1**	**Interfaz serial n.º 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI de ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.