Laboratório - Configuração de Syslog e NTP

Topologia

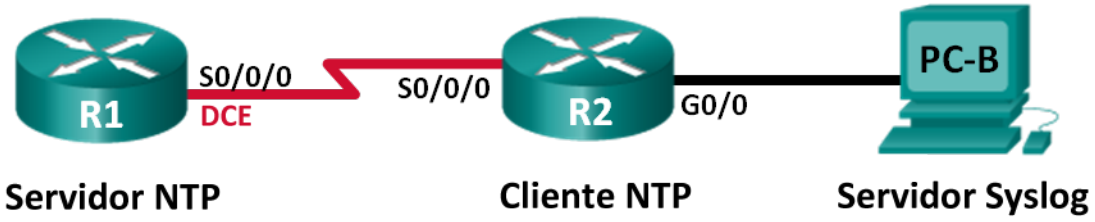


Tabela de Endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway Padrão
R1	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/D
R2	S0/0/0	10.1.1.2	255.255.255.252	N/D
	G0/0	172.16.2.1	255.255.255.0	N/D
PC-B	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Objetivos

Parte 1: Implementar as Configurações Básicas do Dispositivo

Parte 2: Configurar o NTP

Parte 3: Configurar o Syslog

Histórico/Cenário

As mensagens de syslog geradas pelos dispositivos de rede podem ser coletadas e arquivadas em um Servidor syslog. As informações podem ser usadas para fins de monitoramento, depuração, identificação e solução de problemas. O administrador pode controlar onde as mensagens são armazenadas e exibidas. As mensagens de Syslog podem receber um carimbo de data/hora para análise da sequência dos eventos de rede; portanto, é importante sincronizar o relógio nos dispositivos de rede com um Servidor NTP (Network Time Protocol).

Neste laboratório, você configurará R1 como o Servidor NTP e R2 como um syslog e cliente NTP. O aplicativo do servidor syslog, como Tftp32d ou outro programa similar, executará em PC-B. Além disso, você controlará o nível de gravidade das mensagens de log coletadas e arquivadas no servidor syslog.

Observação: os roteadores usados nos laboratórios práticos CCNA são Roteadores de Serviços Integrados (ISRs) Cisco 1941 com software IOS Cisco versão 15.2(4) M3 (imagem universalk9). Podem ser usados outros roteadores e outras versões do Cisco IOS. Dependendo do modelo e da versão do Cisco IOS, os comandos disponíveis e a saída produzida podem ser diferentes dos mostrados nos laboratórios. Consulte a tabela Resumo das Interfaces dos Roteadores no final deste laboratório para obter os identificadores de interface corretos.

Observação: confira se os roteadores foram apagados e se não há configuração inicial. Se estiver em dúvida, entre em contato com o instrutor.

Recursos necessários

- 2 roteadores (Cisco 1941 com a versão 15.2(4)M3 do Cisco IOS, imagem universal ou semelhante)
- 1 PC (Windows 7, Vista ou XP com programa de emulação de terminal, por exemplo, Tera Term, e software Syslog, como tftpd32)
- Cabos de console para configurar os dispositivos Cisco IOS por meio das portas de console
- Cabos Ethernet e seriais, conforme mostrado na topologia

Parte 1: Implementar as Configurações Básicas do Dispositivo

Na parte 1, você configurará a topologia da rede e definirá as configurações básicas, como os endereços IP da interface, o roteamento, o acesso aos dispositivos e as senhas.

Etapa 1: Cabeie a rede conforme mostrado na topologia.

Etapa 2: Inicialize e recarregue os roteadores conforme o necessário.

Etapa 3: Defina as configurações básicas de cada Roteador.

a. Use o console para se conectar ao roteador e entre no modo de configuração global.

b. Copie a configuração básica a seguir e cole-a na configuração atual no roteador.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. (O acesso não autorizado é
estritamente proibido.) #
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

c. Configure o nome do host conforme mostrado na topologia.

d. Aplique os endereços IP às interfaces serial e Gigabit Ethernet, de acordo com a tabela de endereçamento e ative as interfaces físicas.

e. Defina a velocidade do clock como **128000** para as interfaces seriais DCE.

Etapa 4: Configure o roteamento.

Habilite o RIPv2 nos roteadores. Adicione todas as redes ao processo RIPv2.

Etapa 5: Configure o PC-B.

Configure o endereço IP e o gateway padrão de PC-B de acordo com a tabela de endereçamento.

Etapa 6: Verifique a conectividade fim a fim.

Verifique se todos os dispositivos podem executar ping em todos os outros dispositivos na rede com êxito. Caso contrário, faça a identificação e solução de problemas até que haja conectividade fim a fim.

Etapa 7: Salve a configuração em execução na configuração de inicialização.

Parte 2: Configurar NTP

Na parte 2, você configurará R1 como o Servidor NTP e R2 como o cliente NTP de R1. O horário sincronizado é importante para as funções syslog e debug. Se a hora não estiver sincronizada, será difícil determinar qual evento de rede causou a mensagem.

Etapa 1: Exiba a hora atual.

Emita o comando **show clock** para exibir a hora atual em R1.

```
R1# show clock
*12:30:06,147 UTC Tue May 14 2013
```

Anote as informações referentes à hora atual exibida na tabela a seguir.

Data	
Tempo	
Fuso horário	

Etapa 2: Ajuste a hora.

Use o comando **clock set** para definir a hora em R1. Um exemplo de como definir a data e a hora é mostrado a seguir.

```
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.
```

Observação: também é possível definir a hora com o comando **clock timezone** no modo de configuração global. Para obter mais informações sobre esse comando, pesquise o comando **clock timezone** em www.cisco.com para determinar a zona correspondente à sua região.

Etapa 3: Configure o mestre do NTP.

Configure R1 como o mestre de NTP com o comando **ntp master** *stratum-number* no modo de configuração global. Stratum number indica o número de saltos de NTP com relação a uma fonte de tempo autoritativa. Neste laboratório, o número 5 é o nível de stratum desse Servidor NTP.

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

Etapa 4: Configure o cliente NTP.

a. Emita o comando **show clock** em R2. Registre a hora atual exibida em R2 na tabela a seguir.

Data	
Tempo	
Fuso horário	

b. Configure R2 como cliente NTP. Use o comando **ntp server** para apontar para o endereço IP ou nome do host do Servidor NTP. O comando **ntp update-calendar** atualiza o calendário periodicamente com a hora do NTP.

```
R2(config)# ntp server 10.1.1.1
R2(config)# ntp update-calendar
```


Etapa 5: Verifique a configuração do NTP.

a. Use o comando **show ntp associations** para verificar se R2 tem uma associação de NTP com 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 **show clock** em R1 e R2 para comparar o carimbo de data e hora.

Observação: uma demora de alguns minutos poderá ocorrer antes que o carimbo de data e hora em R2 sincronize com R1.

```
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 o syslog

As mensagens de syslog dos dispositivos de rede podem ser coletadas e arquivadas em um Servidor syslog. Neste laboratório, Tftpd32 será usado como o software do Servidor syslog. O administrador de rede pode controlar os tipos de mensagens enviadas ao Servidor syslog.

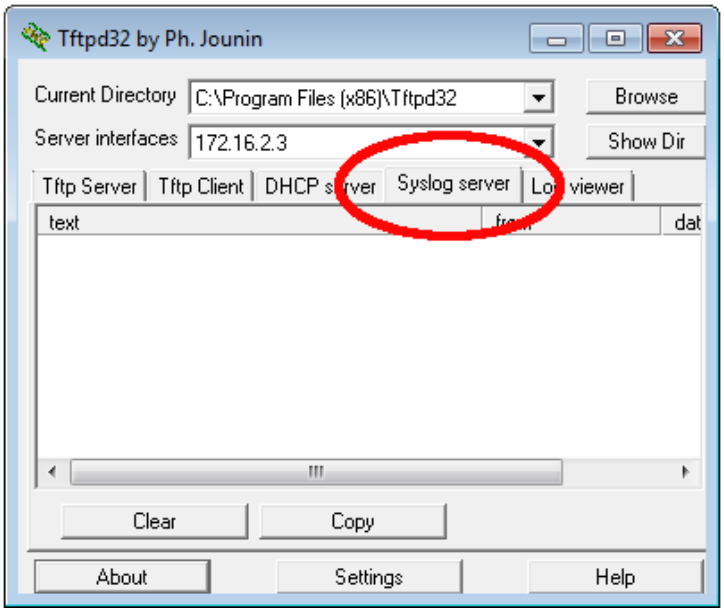
Etapa 1: (Opcional) Instale o Servidor syslog.

Se ainda não houver um Servidor syslog instalado no PC, baixe e instale a versão mais recente de um Servidor syslog, como Tftpd32, no PC. A versão mais recente de Tftpd32 pode ser encontrada no seguinte link:

http://tftpd32.jounin.net/

Etapa 2: Inicie o Servidor syslog em PC-B.

Após a inicialização do aplicativo Tftpd32, clique na guia **Servidor Syslog**.



Etapa 3: Verifique se o serviço de carimbo de data e hora está habilitado em R2.

Use o comando **show run** para verificar se o serviço de carimbo de data e hora está habilitado para registro em R2.

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

Caso contrário, use o comando a seguir para ativá-lo.

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

Etapa 4: Configure R2 para registrar mensagens no Servidor syslog.

Configure R2 para enviar as mensagens do Syslog ao servidor syslog, PC-B. O endereço IP do servidor syslog PC-B é 172.16.2.3.

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

Etapa 5: Exiba as configurações de registro padrão.

Use o comando **show logging** para exibir as configurações de registro padrão.

```
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:
```


Qual é o endereço IP do Servidor syslog? _____

Syslog utiliza qual protocolo e qual porta? _____

O trap logging está ativado em qual nível? _____

Etapa 6: Configure e observe o efeito do registro de níveis de gravidade em R2.

a. Use o comando **logging trap ?** para determinar a disponibilidade dos vários níveis de armadilha. Durante a configuração de um nível, as mensagens enviadas para o Servidor syslog correspondem ao nível de interceptação (trapping) configurado e a todos os níveis inferiores.

```
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>
```

Se o comando **logging trap warnings** tiver sido emitido, quais níveis de gravidade de mensagens serão registrados?

_____

b. Altere o nível de gravidade do registro para 4.

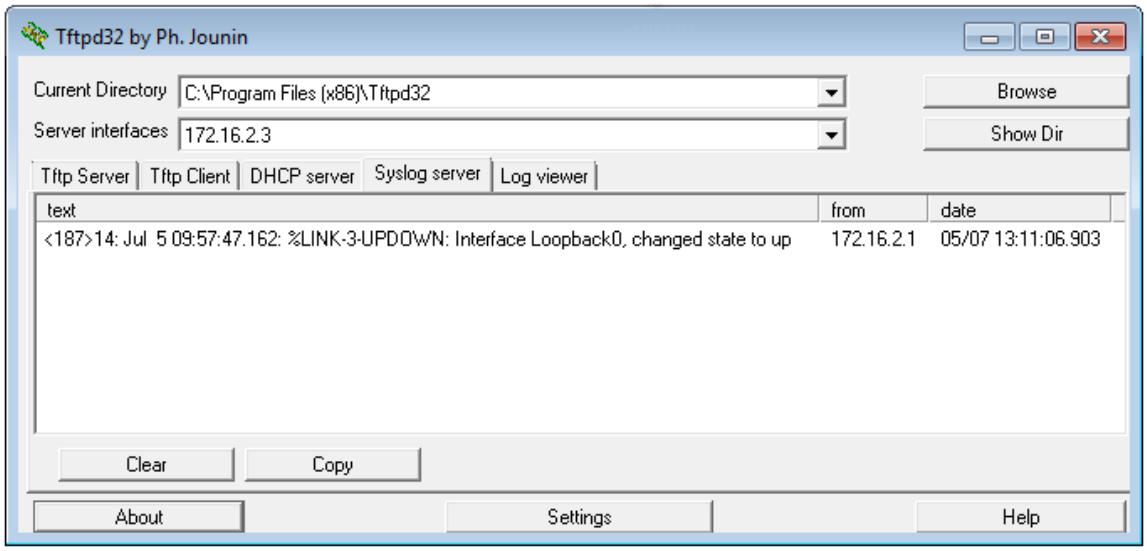
```
R2(config)# logging trap warnings
```

ou

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

c. Crie a interface Loopback0 em R2 e observe as mensagens de log na janela do terminal e na janela do Servidor syslog em 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. Remova a interface Loopback 0 em R2 e observe as mensagens de log.

```
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
```

No nível de gravidade 4,há alguma mensagem de log no Servidor syslog? Se houver alguma mensagem de log, explique o que ela diz e por quê.

_____

_____

_____

_____

e. Altere o nível de gravidade do registro para 6.

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

ou

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

f. Apague as entradas de syslog no PC-B. Clique em **Clear** na caixa de diálogo Tftpd32.

g. Crie a interface Loopback 1 em R2.

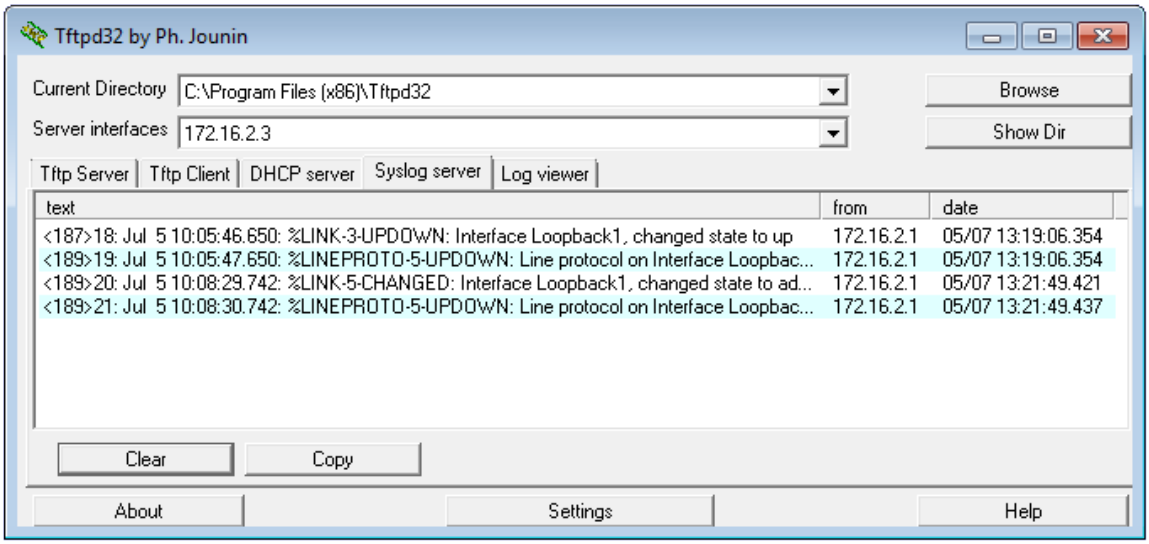
```
R2(config)# interface lo 1
Jul  5 10:05:46.650: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
Jul  5 10:05:47.650: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up
```

h. Remova a interface Loopback 1 de 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 a saída do Servidor syslog. Compare esse resultado com os resultados do nível de interceptação (trapping) 4. O que você observa?

_____

_____

_____

Reflexão

Qual é o problema de se definir um nível de gravidade muito alto (número de nível mais baixo) ou muito baixo (número de nível mais alto) para syslog?

_____

_____

_____

Tabela de Resumo das Interfaces dos Roteadores

Resumo das Interfaces dos Roteadores				
Modelo do Roteador	**Interface Ethernet 1**	**Interface Ethernet 2**	**Interface Serial 1**	**Interface Serial 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)

Observação: para descobrir como o roteador está configurado, examine as interfaces para identificar o tipo de roteador e quantas interfaces ele tem. Não há como listar efetivamente todas as combinações de configurações para cada classe de roteador. Esta tabela inclui identificadores para as combinações possíveis de Ethernet e Interfaces seriais no dispositivo. Esse tabela não inclui nenhum outro tipo de interface, embora um roteador específico possa conter algum. Um exemplo disso poderia ser uma interface ISDN BRI. A string entre parênteses é a abreviatura legal que pode ser usada no comando do Cisco IOS para representar a interface.

