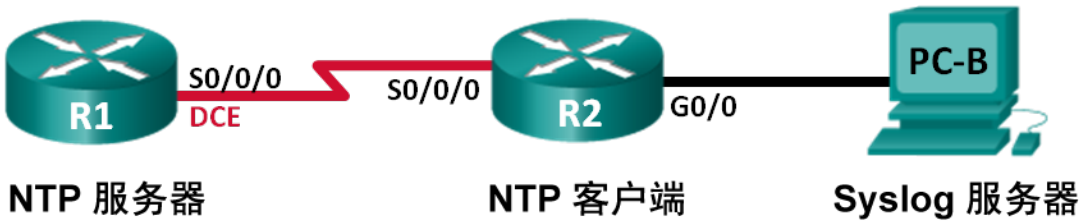
实验 – 配置系统日志和 NTP

拓扑



地址分配表

设备	接口	IP 地址	子网掩码	默认网关
R1	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	不适用
R2	S0/0/0	10.1.1.2	255.255.255.252	不适用
	G0/0	172.16.2.1	255.255.255.0	不适用
PC-B	NIC	172.16.2.3	255.255.255.0	172.16.2.1

目标

第 1 部分：配置基本设备设置

第 2 部分：配置 NTP

第 3 部分：配置系统日志

背景/场景

可收集网络设备生成的系统日志消息并将其存档在系统日志服务器上。该信息可用于监控、调试和故障排除用途。管理员可控制消息存储和显示的位置。系统日志消息可带时间戳，以分析网络事件的顺序；因此，在采用网络时间协议 (NTP) 服务器的网络设备之间保持时钟同步非常重要。

在该实验中，您将把 R1 配置为 NTP 服务器，并且把 R2 配置为系统日志和 NTP 客户端。系统日志服务器应用（如 Tftp32d 或其他类似程序）将在 PC-B 上运行。此外，您将控制系统日志服务器上收集并存档的日志消息的严重性级别。

注：CCNA 动手实验所用的路由器是采用思科 IOS 15.2(4)M3 版（universalk9 映像）的思科 1941 集成多业务路由器 (ISR)。也可使用其他路由器以及思科 IOS 版本。根据型号以及思科 IOS 版本的不同，可用命令和产生的输出可能与实验显示的不一样。请参考本实验末尾的“路由器接口汇总表”以了解正确的接口标识符。

注：确保路由器的启动配置已经清除。如果不确定，请联系教师。

所需资源

- 2 台路由器（采用思科 IOS 15.2(4)M3 版通用映像的思科 1941 或同类路由器）
- 1 台 PC（具有 Tera Term 等终端仿真程序以及 Tftpd32 等系统日志软件的 Windows 7、Vista 或 XP）
- 用于通过控制台端口配置思科 IOS 设备的控制台电缆
- 拓扑所示的以太网和串行电缆

第 1 部分：配置基本设备设置

在第 1 部分中，您将设置网络拓扑并配置基本设置，例如接口 IP 地址、路由、设备接入和密码。

步骤 1： 建立如拓扑图所示的网络。

步骤 2： 如有必要，请初始化并重新加载路由器。

步骤 3： 为每台路由器配置基本设置。

a. 通过控制台连接到路由器，然后进入全局配置模式。

b. 复制以下基本配置并将其粘贴到路由器上的运行配置中。

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited.#
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

c. 根据拓扑指示配置主机名。

d. 根据地址分配表将 IP 地址应用到串行和千兆以太网接口，并激活物理接口。

e. 对于 DCE 串行接口，将时钟速率设置为 **128000**。

步骤 4： 配置路由。

启用路由器中的 RIPv2。将所有网络添加到 RIPv2 进程。

步骤 5： 配置 PC-B。

根据地址分配表为 PC-B 配置 IP 地址和默认网关。

步骤 6： 检验端到端连通性

验证每台设备是否都能够成功 ping 网络中的其他设备。如果不能，请排除故障直至端到端连接正常。

步骤 7： 将运行配置保存到启动配置。

第 2 部分：配置 NTP

在第 2 部分中，您将把 R1 配置为 NTP 服务器，并且将 R2 配置为 R1 的 NTP 客户端。同步时间对于系统日志和调试功能非常重要。如果时间未同步，将很难确定导致生成消息的网络事件。

步骤 1： 显示当前时间。

发出 **show clock** 命令以显示 R1 上的当前时间。

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

在下表中记录与所显示的当前时间有关的信息。

日期	
时间	
时区	

步骤 2： 设置时间。

使用 **clock set** 命令设置 R1 上的时间。以下为设置日期和时间的示例。

```
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.
```

注：还可在全局配置模式下使用 **clock timezone** 命令设置时间。有关该命令的更多信息，请研究 www.cisco.com 上的 **clock timezone** 命令以确定您所在地区的时区。

步骤 3： 配置 NTP 主设备。

在全局配置模式下，使用 **ntp master** *stratum-number* 命令将 R1 配置为 NTP 主设备。层级数 (stratum number) 表示 NTP 距离权威时间源的跳数。在本实验中，数字 5 是该 NTP 服务器的层级。

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

步骤 4： 配置 NTP 客户端。

a 在 R2 中发出 **show clock** 命令。在下表中记录 R2 显示的当前时间。

日期	
时间	
时区	

b 将 R2 配置为 NTP 客户端。使用 **ntp server** 命令指向 NTP 服务器的 IP 地址或主机名。**ntp update-calendar** 命令会根据 NTP 时间定期更新日历。

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

步骤 5： 验证 NTP 配置。

a 使用 **show ntp associations** 命令验证 R2 已与 R1 建立 NTP 关联。

```
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 在 R1 和 R2 中发出 **show clock** 以比较时间戳。

注：可能需要几分钟才能使 R2 中的时间戳与 R1 同步。

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

第 3 部分：配置系统日志

可收集网络设备的系统日志消息并将其存档在系统日志服务器上。在本实验中，Tftpd32 将用作系统日志服务器软件。网络管理员可控制可发送到系统日志服务器的消息类型。

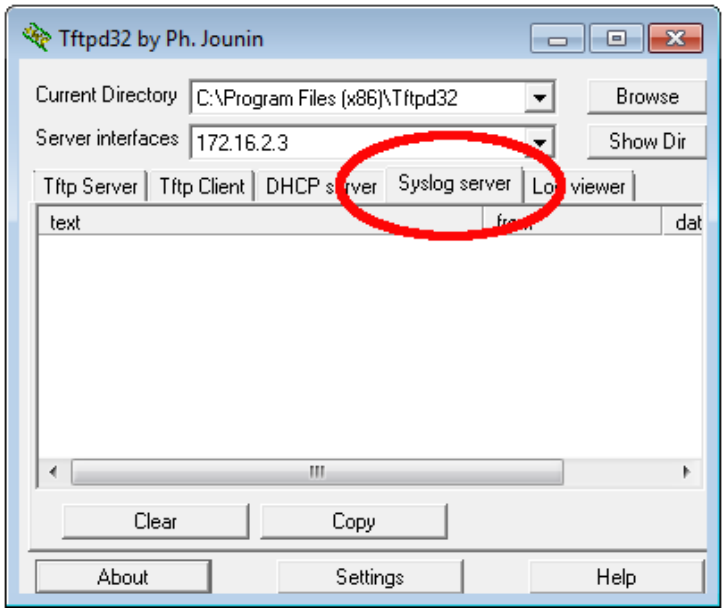
步骤 1： （可选）安装系统日志服务器。

如果 PC 中尚未安装系统日志服务器，请在 PC 中下载并安装最新版本的系统日志服务器（例如 Tftpd32）。最新版本的 Tftpd32 可在以下链接位置上找到：

http://tftpd32.jounin.net/

步骤 2： 在 PC-B 中启动系统日志服务器。

启动 Tftpd32 应用后，点击**系统日志服务器**选项卡。



步骤 3： 验证 R2 中是否已启用时间戳服务。

使用 **show run** 命令验证在 R2 中是否已为日志记录启用时间戳服务。

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

如果未启用时间戳服务，请使用以下命令进行启用。

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

步骤 4： 配置 R2 以将消息记录到系统日志服务器。

配置 R2 以将系统日志消息发送到系统日志服务器 PC-B。PC-B 系统日志服务器的 IP 地址是 172.16.2.3。

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

步骤 5： 显示默认的日志记录设置。

使用 **show logging** 命令显示默认日志记录设置。

```
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:
```

系统日志服务器的 IP 地址是什么？_____

系统日志使用的协议和端口分别是什么？_____

陷阱日志记录启用的级别是什么？_____

步骤 6： 在 R2 中，配置日志记录严重性级别并观察其影响。

a 使用 **logging trap ?** 命令确定各种陷阱级别的可用性。当配置一个级别时，消息会以配置的陷阱级别以及任何较低的级别发送到系统日志服务器。

```
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>
```

如果发出 **logging trap warnings** 命令，所记录的消息严重性级别是什么？

_____

b 将日志记录的严重性级别更改为 4。

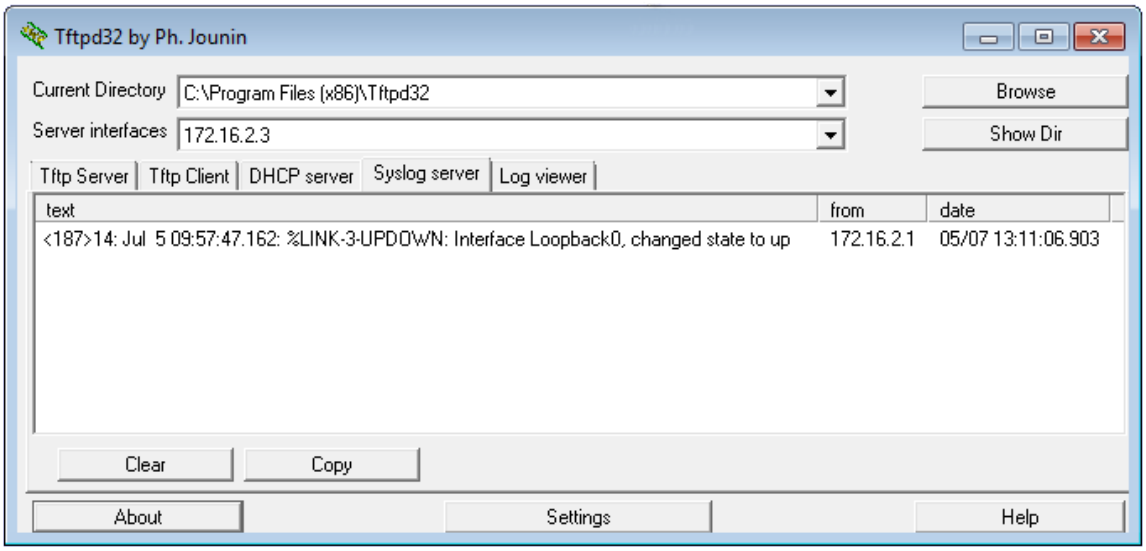
```
R2(config)# logging trap warnings
```

或

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

c 在 R2 中创建接口 Loopback0 并观察 PC-B 中终端窗口和系统日志服务器窗口的日志消息。

```
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 删除 R2 中的 Loopback 0 接口并观察日志消息。

```
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
```

在严重性级别 4，系统日志服务器中是否存在任何日志消息？如果出现任何日志消息，请解释出现的内容和原因。

_____

_____

_____

_____

e 将日志记录的严重性级别更改为 6。

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

或

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

f 清除 PC-B 中的系统日志条目。在 Tftpd32 对话框中点击**清除**。

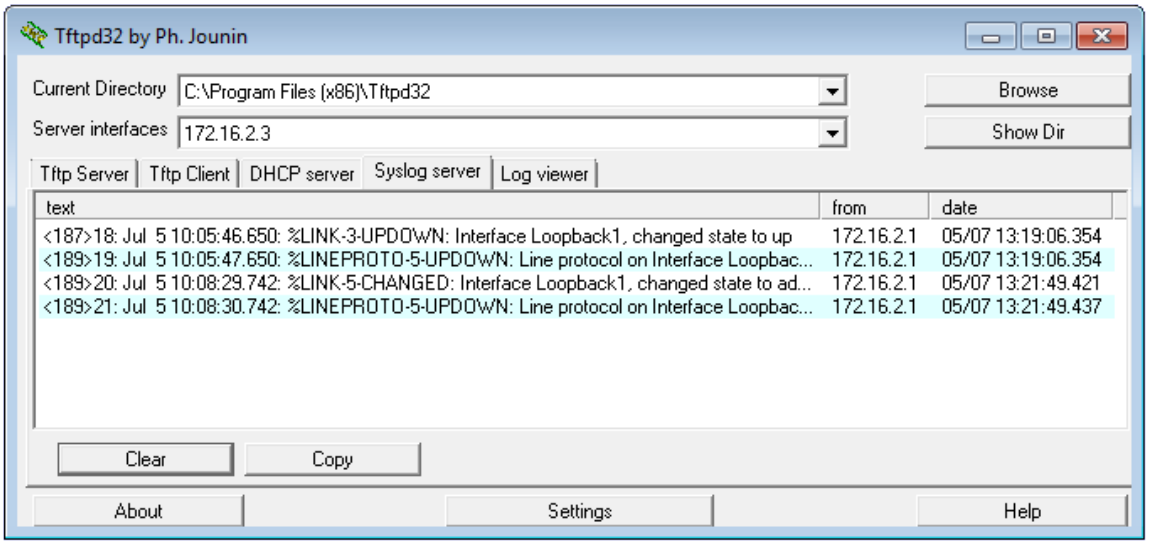
g 在 R2 中创建 Loopback 1 接口。

```
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 从 R2 中删除 Loopback 1 接口。

```
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 观察系统日志服务器输出。将此结果与陷阱级别 4 中的结果进行比较。您观察出了什么？

_____

_____

_____

思考

将系统日志的严重性级别设置得过高（级别数字最小）或过低（级别数字最大）会有什么问题？

_____

_____

_____

路由器接口汇总表

路由器接口汇总				
路由器型号	**以太网接口 1**	**以太网接口 2**	**串行接口 1**	**串行接口 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)

注：若要了解如何配置路由器，请查看接口来确定路由器类型以及路由器拥有的接口数量。我们无法为每类路由器列出所有的配置组合。下表列出了设备中以太网和串行接口组合的标识符。此表中未包含任何其他类型的接口，但实际的路由器可能会含有其他接口。例如 ISDN BRI 接口。括号中的字符串是约定缩写，可在思科 IOS 命令中用来代表接口。