Travaux pratiques : configuration de Syslog et de NTP

Topologie

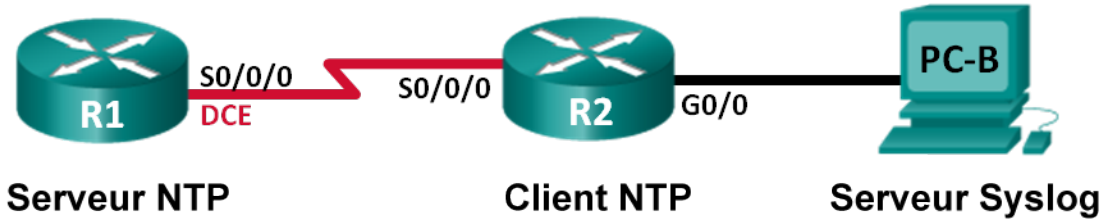


Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	S0/0/0 (ETCD)	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	Carte réseau	172.16.2.3	255.255.255.0	172.16.2.1

Objectifs

Partie 1 : Configuration des paramètres de base des périphériques

Partie 2 : Configuration de NTP

Partie 3 : Configuration de Syslog

Contexte/scénario

Les messages Syslog qui sont générés par les périphériques réseau peuvent être collectés et archivés sur un serveur Syslog. Ces informations peuvent être utilisées à des fins de surveillance, de débogage et de dépannage. L'administrateur peut contrôler où les messages sont stockés et affichés. Les messages Syslog peuvent être horodatés de manière à permettre l'analyse de la séquence des événements réseau ; par conséquent, il est important de synchroniser l'horloge des périphériques réseau avec un serveur NTP (Network Time Protocol).

Au cours de ces travaux pratiques, vous allez configurer R1 en tant que serveur NTP et R2 en tant que client Syslog et NTP. L'application du serveur Syslog, telle que Tftp32d ou d'autres programmes similaires, sera exécutée sur le PC-B. Par ailleurs, vous contrôlerez le niveau de gravité des messages de journaux qui sont rassemblés et archivés dans le serveur Syslog.

Remarque : Les routeurs utilisés lors des travaux pratiques CCNA sont des routeurs à services intégrés (ISR) Cisco 1941 équipés de Cisco IOS version 15.2(4)M3 (image universalk9). D'autres routeurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ceux indiqués dans les travaux pratiques. Reportez-vous au tableau récapitulatif des interfaces du routeur à la fin de ce TP pour obtenir les identifiants d'interface corrects.

Remarque : Vérifiez que la mémoire des routeurs a été effacée et qu'aucune configuration initiale n'est présente. En cas de doute, contactez votre formateur.

Ressources requises

- 2 routeurs (Cisco 1941 équipés de Cisco IOS version 15.2(4)M3 image universelle ou similaire)
- 1 PC (Windows 7, Vista ou XP doté d'un programme d'émulation du terminal, tel que Tera Term, et d'un logiciel Syslog, tel que Tftpd32)
- Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
- Câbles Ethernet et série conformément à la topologie

Partie 1 : Configuration des paramètres de base des périphériques

Dans la Partie 1, vous allez configurer la topologie du réseau ainsi que les paramètres de base, comme les adresses IP d'interface, le routage, l'accès aux périphériques et les mots de passe.

Étape 1 : Câblez le réseau conformément à la topologie indiquée.

Étape 2 : Initialisez et redémarrez les routeurs, le cas échéant.

Étape 3 : Configurez les paramètres de base pour chaque routeur.

a. Accédez au routeur par la console et passez en mode de configuration globale.

b. Copiez la configuration de base suivante et collez-la dans la configuration en cours sur le routeur.

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

c. Configurez le nom d'hôte comme illustré dans la topologie.

d. Appliquez les adresses IP aux interfaces série et Gigabit Ethernet, conformément à la table d'adressage, et activez les interfaces physiques.

e. Réglez la fréquence d'horloge sur **128000** pour l'interface série DCE.

Étape 4 : Configurez le routage.

Activez le protocole RIPv2 sur les routeurs. Ajoutez tous les réseaux au processus RIPv2.

Étape 5 : Configurez PC-B.

Configurez l'adresse IP et la passerelle par défaut de PC-B, conformément à la table d'adressage.

Étape 6 : Vérifiez la connectivité de bout en bout.

Vérifiez que chaque périphérique peut envoyer avec succès une requête ping à n'importe quel autre périphérique du réseau. Si la réponse est non, effectuez un dépannage jusqu'à ce que la connectivité de bout en bout soit assurée.

Étape 7 : Enregistrez la configuration en cours en tant que configuration initiale.

Partie 2 : Configuration de NTP

Dans la Partie 2, vous allez configurer R1 en tant que serveur NTP et R2 en tant que client NTP de R1. La synchronisation de l'heure est importante pour les fonctions de Syslog et de débogage. Si l'heure n'est pas synchronisée, il est difficile de déterminer quel événement réseau est à l'origine du message.

Étape 1 : Affichez l'heure actuelle.

Exécutez la commande **show clock** pour afficher l'heure actuelle sur R1.

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

Enregistrez dans le tableau ci-dessous les informations relatives à l'heure actuelle affichée.

Date	
Heure	
Time Zone	

Étape 2 : Réglez l'heure.

Utilisez la commande **clock set** pour régler l'heure sur R1. Vous trouverez ci-dessous un exemple de réglage de la date et de l'heure.

```
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.
```

Remarque : Il est également possible de régler l'heure à l'aide de la commande **clock timezone** en mode de configuration globale. Pour plus d'informations sur cette commande, recherchez la commande **clock timezone** à l'adresse www.cisco.com afin de déterminer votre fuseau horaire.

Étape 3 : Configurez le NTP maître.

Configurez R1 en tant que NTP maître à l'aide de la commande **ntp master** *numéro-strate* en mode de configuration globale. Le numéro de strate indique le nombre de sauts NTP par rapport à une source temporelle faisant autorité. Dans ces travaux pratiques, le niveau de strate de ce serveur NTP est égal à 5.

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

Étape 4 : Configurez le client NTP.

a. Exécutez la commande **show clock** sur R2. Enregistrez dans le tableau ci-dessous l'heure actuelle affichée sur R2.

Date	
Heure	
Time Zone	

b. Configurez R2 en tant que client NTP. Utilisez la commande **ntp server** pour pointer vers l'adresse IP ou le nom d'hôte du serveur NTP. La commande **ntp update-calendar** met périodiquement à jour le calendrier avec l'heure NTP.

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

Étape 5 : Vérifiez la configuration de NTP.

a. Utilisez la commande **show ntp associations** pour vérifier que R2 possède une association NTP avec 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. Exécutez la commande **show clock** sur R1 et R2 pour comparer l'horodatage.

Remarque : La synchronisation de l'horodatage sur R2 avec R1 peut prendre quelques minutes.

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

Partie 3 : Configuration de Syslog

Les messages Syslog en provenance des périphériques réseau peuvent être collectés et archivés sur un serveur Syslog. Dans ces travaux pratiques, le programme Tftpd32 sera utilisé en tant que logiciel serveur Syslog. L'administrateur réseau peut contrôler les types de messages pouvant être envoyés au serveur Syslog.

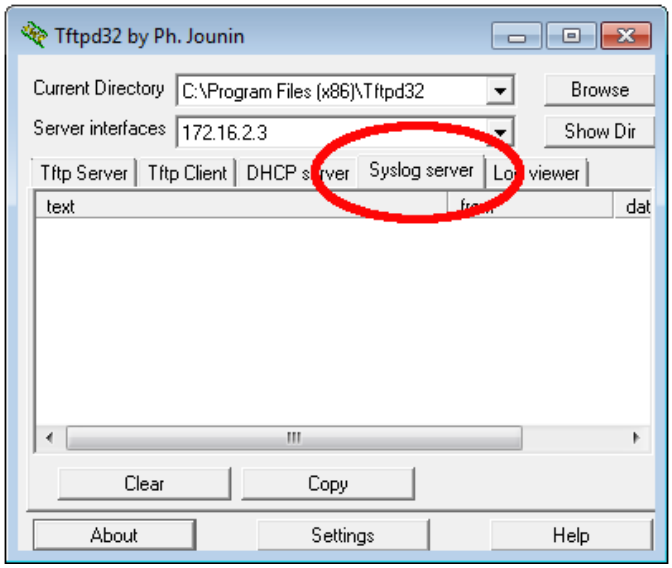
Étape 1 : (Facultatif) Installez le serveur Syslog.

Si un serveur Syslog n'a pas encore été installé sur le PC, téléchargez et installez la dernière version d'un logiciel serveur Syslog, tel que Tftpd32, sur le PC. La dernière version de Tftpd32 est disponible à l'adresse suivante :

http://tftpd32.jounin.net/

Étape 2 : Démarrez le serveur Syslog sur PC-B.

Après le démarrage de l'application Tftpd32, cliquez sur l'onglet **syslog server**.



Étape 3 : Vérifiez que le service d'horodatage est activé sur R2.

Utilisez la commande **show run** pour vérifier que le service d'horodatage est activé pour la journalisation sur R2.

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

Si le service d'horodatage n'est pas activé, exécutez la commande suivante pour l'activer.

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

Étape 4 : Configurez le routeur R2 pour consigner les messages vers le serveur Syslog.

Configurez le routeur R2 pour envoyer des messages Syslog vers le serveur Syslog et vers le PC-B. L'adresse IP du serveur Syslog du PC-B est 172.16.2.3.

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

Étape 5 : Affichez les paramètres de journalisation par défaut.

Utilisez la commande **show logging** pour afficher les paramètres de journalisation par défaut.

```
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:
```

Quelle est l'adresse IP du serveur Syslog ? _____

Quel protocole et quel port le serveur Syslog utilise-t-il ? _____

À quel niveau le déroutement de journalisation est-il activé ? _____

Étape 6 : Configurez et observez l'effet des niveaux de gravité de la journalisation sur R2.

a. Utilisez la commande **logging trap ?** pour déterminer les différentes disponibilités des niveaux de TRAP. Lors de la configuration d'un niveau, les messages envoyés au serveur Syslog correspondent au niveau de déroutement configuré ainsi qu'à tous les niveaux inférieurs.

```
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)
  urgences    Système inutilisable                (gravité = 0)
  erreurs         Conditions d'erreur                 (gravité = 3)
  informatif  Messages informatifs            (gravité = 6)
  notifications  Conditions normales mais significatives (gravité = 5)
  avertissements       Conditions d'avertissement                (gravité = 4)
  <cr>
```

Si la commande **logging trap warnings** a été exécutée, quels niveaux de gravité des messages sont consignés ?

_____

b. Modifiez le niveau de gravité de la journalisation à 4.

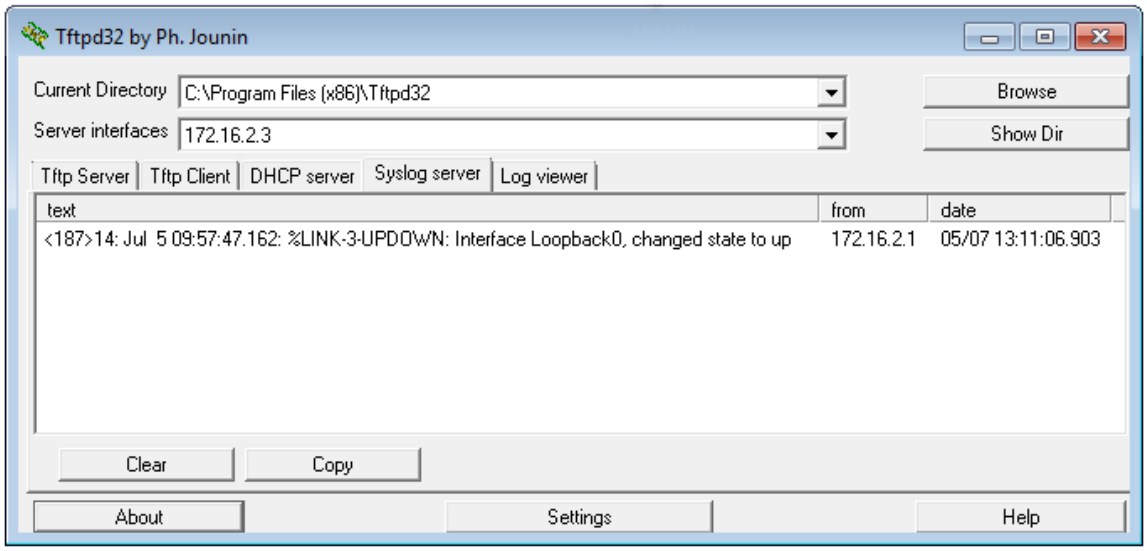
```
R2(config)# logging trap warnings
```

ou

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

c. Créez l'interface Loopback0 sur R2 et observez les messages de journalisation à la fois sur la fenêtre du terminal et sur la fenêtre du serveur Syslog sur 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. Supprimez l'interface Loopback0 sur R2 et observez les messages de journalisation.

```
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
```

Y a-t-il des messages de journalisation sur le serveur Syslog de niveau de gravité 4 ? Si des messages de journalisation apparaissent, expliquez ce qui est affiché et pourquoi cela est affiché.

_____

_____

_____

_____

e. Modifiez le niveau de gravité de la journalisation à 6.

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

ou

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

f. Effacez les entrées syslog sur le PC-B. Cliquez sur **Clear** dans la boîte de dialogue de Tftpd32.

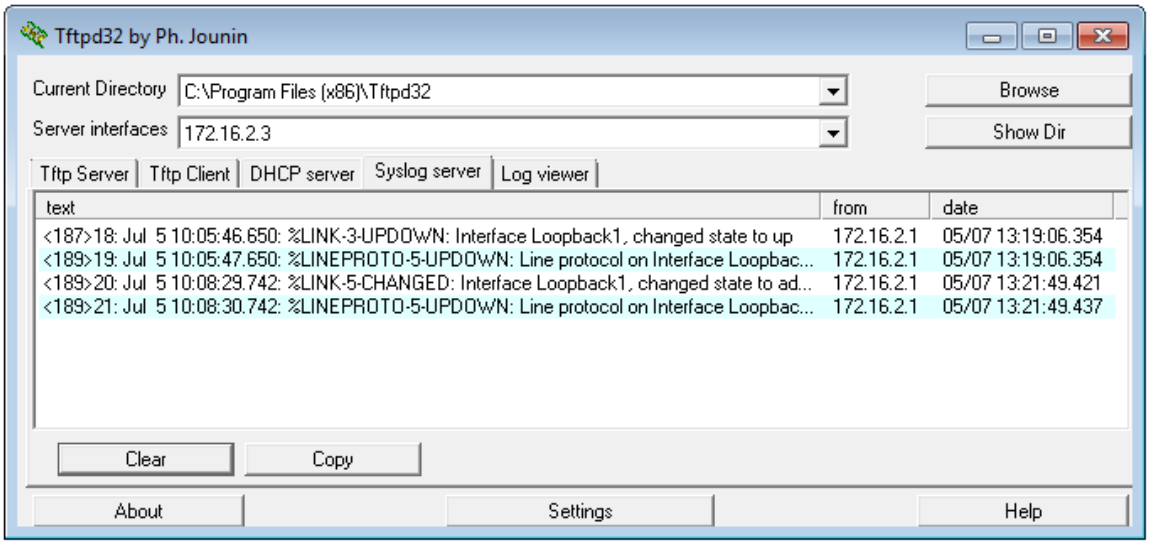
g. Créez l'interface Loopback1 sur R2.

```
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. Supprimez l'interface Loopback1 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. Observez le résultat du serveur Syslog. Comparez ce résultat avec celui correspondant au niveau de déroutement 4. Que remarquez-vous ?

_____

_____

_____

Remarques générales

Quel est le problème occasionné par la définition d'un niveau de gravité trop élevé (numéro de niveau minimum) ou trop faible (numéro de niveau maximum) pour le serveur Syslog ?

_____

_____

_____

Tableau récapitulatif des interfaces des routeurs

Résumé des interfaces des routeurs				
Modèle du routeur	**Interface Ethernet 1**	**Interface Ethernet 2**	**Interface série 1**	**Interface série 2**
1 800	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)
1 900	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)
2 801	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)
2 811	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)
2 900	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)

Remarque : Pour savoir comment le routeur est configuré, observez les interfaces afin d'identifier le type de routeur ainsi que le nombre d'interfaces qu'il comporte. Il n'est pas possible de répertorier de façon exhaustive toutes les combinaisons de configurations pour chaque type de routeur. Ce tableau inclut les identifiants des différentes combinaisons d'interfaces Ethernet et série possibles dans le périphérique. Ce tableau ne comporte aucun autre type d'interface, même si un routeur particulier peut en contenir un. L'exemple de l'interface RNIS BRI peut illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans les commandes Cisco IOS.