

Surveillance du réseau

- La surveillance du fonctionnement du réseau
- fournit à un administrateur réseau les informations nécessaires à la gestion proactive du réseau et à l'établissement de rapports relatifs aux statistiques d'utilisation du réseau.
- **L'activité des liaisons, les taux d'erreur et l'état des liaisons** sont quelques-uns des facteurs qui permettent à un administrateur réseau de déterminer l'état et l'utilisation d'un réseau.

debug ip packet

```
*Feb 4 20:07:09.283: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-Null0, changed state to up
*Feb 4 20:07:09.291: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Feb 4 20:07:09.299: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Feb 4 20:07:09.307: %LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
*Feb 4 20:07:09.943: %SYS-5-CONFIG_I: Configured from memory by console
*Feb 4 20:07:10.263: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 15.3(3)XB12, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Tue 19-Nov-13 04:39 by prod_rel_team
*Feb 4 20:07:10.291: %SNMP-5-COLDSTART: SNMP agent on host R1 is undergoing a cold start
*Feb 4 20:07:10.343: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
*Feb 4 2
R1#
R1#
R1#
R1#0:07:10.343: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to down
*Feb 4 20:07:10.347: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to down
*Feb 4 20:07:10.403: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Feb 4 20:07:10.407: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*Feb 4 20:07:11.947: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
```

```
R1(config)#int loop 0
R1(config-if)#
R1(config-if)#
*Feb 4 20:07:35.119; %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R1(config-if)#
```

- trois protocoles qu'un administrateur réseau peut utiliser pour surveiller le réseau.
- Les protocoles **Syslog**, **SNMP** et **NetFlow** sont des protocoles populaires.
- Le protocole NTP (Network Time Protocol) est utilisé pour synchroniser les paramètres de temps de plusieurs périphériques, ce qui est particulièrement important lors de la comparaison des fichiers journaux de différents périphériques.

Le protocole syslog

- Le protocole Syslog est un protocole simple utilisé par un périphérique IP faisant office de client Syslog, afin d'envoyer des messages textuels de journal vers un autre périphérique IP, à savoir le serveur Syslog. Le protocole Syslog est actuellement défini dans la RFC 5424.
- L'implémentation d'une méthode de journalisation est une partie importante de la **sécurité du réseau et du dépannage réseau**.
- informations relatives aux modifications de configuration
- aux violations des listes de contrôle d'accès
- à l'état des interfaces,,,,

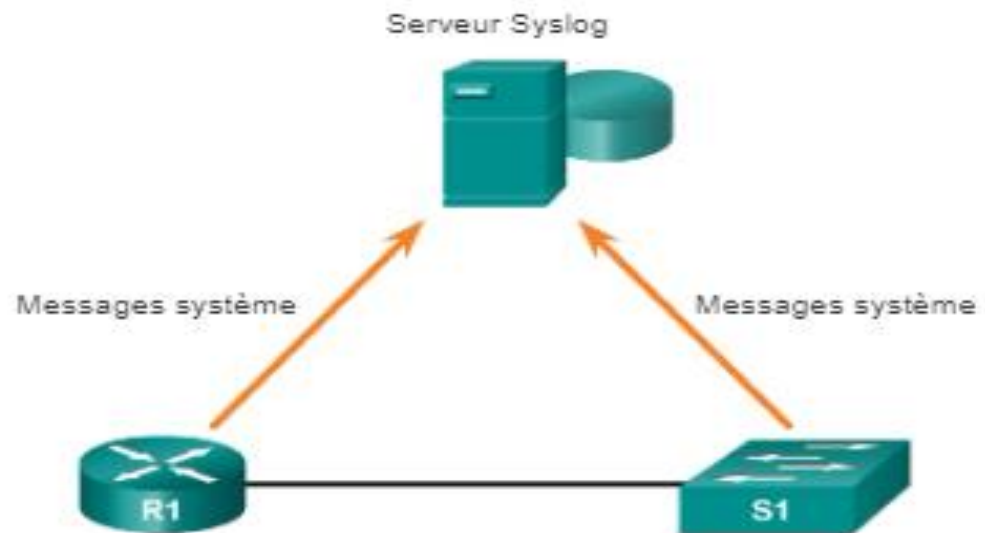
Présentation de Syslog

- Le protocole Syslog permet aux périphériques réseau d'envoyer leurs messages système sur le réseau aux serveurs Syslog.
- Ces messages peuvent être non critiques ou significatifs.
- Les administrateurs réseau peut :
- Stocker
- interpréter et d'afficher ces messages
- être alertés des messages susceptibles d'avoir le plus d'impact sur l'infrastructure réseau

Présentation de Syslog

- Syslog est un terme utilisé pour décrire une norme.
- Il sert également à décrire le protocole développé pour cette norme.
- Le protocole Syslog a été développé pour les systèmes UNIX dans les années 1980

Le protocole Syslog utilise le port UDP 514 pour envoyer des messages de notification d'événement sur des réseaux IP à des collecteurs de messages d'événement,



- De nombreux périphériques réseau prennent en charge le protocole Syslog, comme les routeurs, les commutateurs, les serveurs d'applications, les pare-feu...
- Syslog assume trois fonctions principales :
 1. La capacité à collecter les informations de journalisation pour la surveillance et le dépannage
 2. La capacité à sélectionner le type d'information de journalisation capturée
 3. La capacité à spécifier les destinations des messages Syslog capturés

- Les messages d'événement peuvent être envoyés à un ou plusieurs des éléments suivants :

1) Console : la journalisation de la console est activée par défaut. Les messages sont consignés sur la console et peuvent être affichés lors de la modification ou du test du routeur ou du commutateur à l'aide d'un logiciel d'émulation de terminal, après l'établissement d'une connexion avec le port de console du routeur.

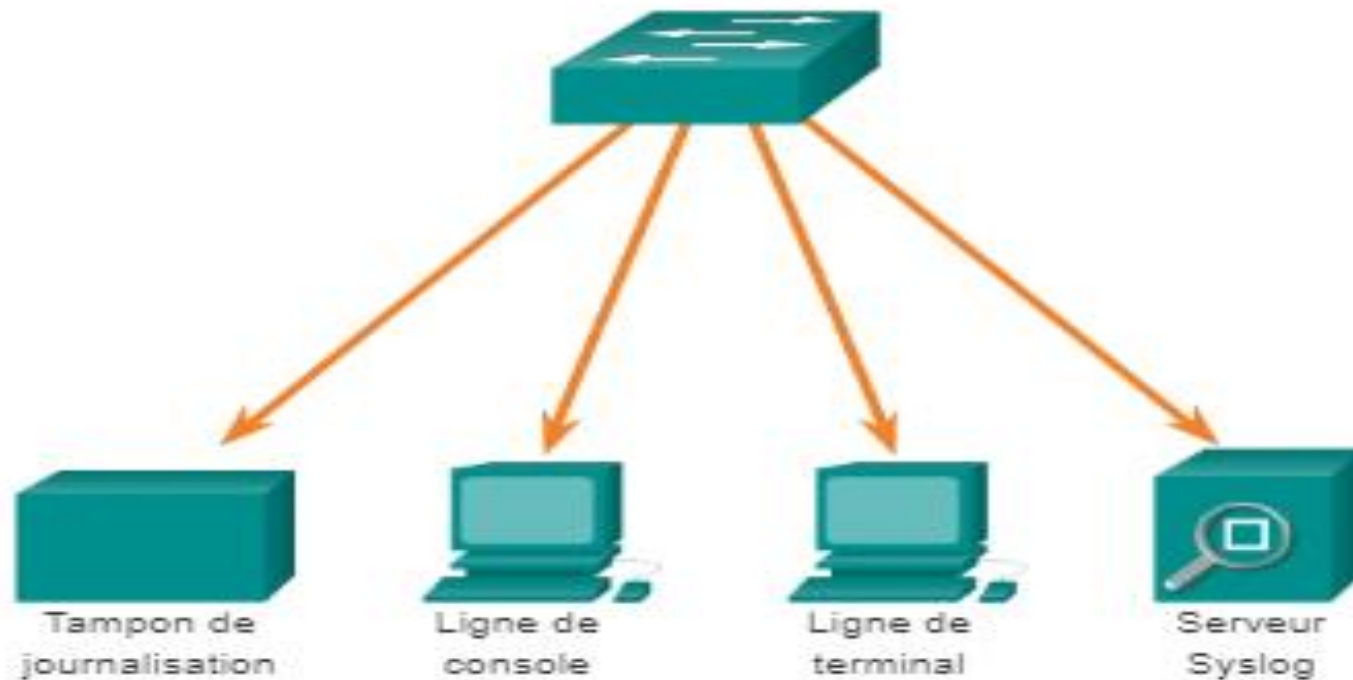
```
R1#terminal monitor
% Console already monitors
R1#
```

2) Lignes de terminal : les sessions d'exécution activées peuvent être configurées de manière à recevoir les messages de journal sur n'importe quelle ligne de terminal. Comme pour la journalisation de la console, ce type de journalisation n'est pas stocké par le routeur et n'est par conséquent utile que pour l'utilisateur de cette ligne.

3) Tampon de journalisation - Le tampon de journalisation est un outil de dépannage un peu plus utile, car les messages de journal sont stockés en mémoire pendant un certain temps. Toutefois, les messages de journal sont effacés lors du redémarrage du périphérique.

4) Syslog : les routeurs et commutateurs Cisco peuvent être configurés de manière à transférer les messages de journal vers un service Syslog externe. Ce service peut résider sur un nombre quelconque de serveurs ou de stations de travail, notamment des systèmes exécutant Microsoft Windows ou Linux. Syslog est l'outil de journalisation des messages le plus populaire, car il permet le stockage des messages de routeur sur une longue période, et ce, dans un emplacement centralisé.

Options de destination des messages Syslog



- Il est possible de surveiller à distance les messages système en affichant les journaux sur un serveur Syslog ou en accédant au périphérique par le biais de Telnet, de SSH ou du port de console.

Format de message Syslog

dysfonctionnements logiciels
ou matériels

Les transitions d'interface
à l'état « up » ou « down »
ainsi que les messages
de redémarrage du
système s'affichent au
niveau de notification.

exécution de diverses
commandes **debug**

Gravité	Niveau de gravité	Explication
Urgence	Niveau 0	Système inutilisable
Alerte	Niveau 1	Action immédiate requise
Critique	Niveau 2	Condition critique
Erreur	Niveau 3	Condition d'erreur
Avertissement	Niveau 4	Condition d'avertissement
Notification	Niveau 5	Événement normal mais important
Informatif	Niveau 6	Message informatif
Débogage	Niveau 7	Message de débogage

- Chaque message Syslog contient un niveau de gravité et une capacité. Plus les numéros des niveaux sont petits, plus les alarmes Syslog sont critiques

le niveau de gravité

	Niveau	Mot-clé	Description	Définition
Niveau le plus élevé	0	urgences	Système inutilisable	LOG_EMERG
	1	alertes	Action immédiate requise	LOG_ALERT
	2	critique	Existence de conditions critiques	LOG_CRIT
	3	erreurs	Existence de conditions d'erreur	LOG_ERR
	4	avertissements	Existence de conditions d'avertissement	LOG_WARNING
	5	notifications	Événement normal mais important	LOG_NOTICE
	6	informatif	Message d'information uniquement	LOG_INFO
Niveau le plus bas	7	débogage	Messages de débogage	LOG_DEBUG

Les champs contenus dans le message Syslog du logiciel Cisco IOS

Champ	Explication
numéro d'ordre	Horodatage des messages de journal avec un numéro d'ordre uniquement si la commande de configuration globale <code>service sequence-numbers</code> est configurée.
horodatage	Date et heure du message ou de l'événement, visibles uniquement si la commande de configuration globale <code>service timestamps</code> est configurée.
établissement	Établissement auquel le message se réfère
gravité	Code à un seul chiffre de 0 à 7, représentant la gravité du message.
MOYEN MNÉMOTECHNIQUE	Chaîne de texte décrivant le message de façon unique.
description	Chaîne de texte contenant des informations détaillées sur l'événement signalé.

capacité

- seq no: timestamp: %facility-severity-MNEMONIC: description
- Exemple de résultat sur un commutateur Cisco en ce qui concerne la modification d'état à la valeur « up » d'une liaison EtherChannel :
- 00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
- Dans ce cas, la capacité est LINK et le niveau de gravité est égal à 3, avec une valeur mnémonique UPDOWN.
- Si la journalisation des listes de contrôle d'accès est configurée, le périphérique génère des messages Syslog lorsque des paquets satisfont à la condition d'un paramètre.

- configurer l'horloge du périphérique réseau.
- manuellement, à l'aide de la commande **clock set**
- automatiquement, à l'aide du protocole NTP.

- NTP (Network Time Protocol) est un protocole réseau qui permet à une machine de mettre à jour son horloge en se synchronisant sur des serveurs de temps présents sur Internet. Le principe de NTP est de mettre la machine à l'heure en étudiant les temps de propagation sur le réseau, de façon précise.



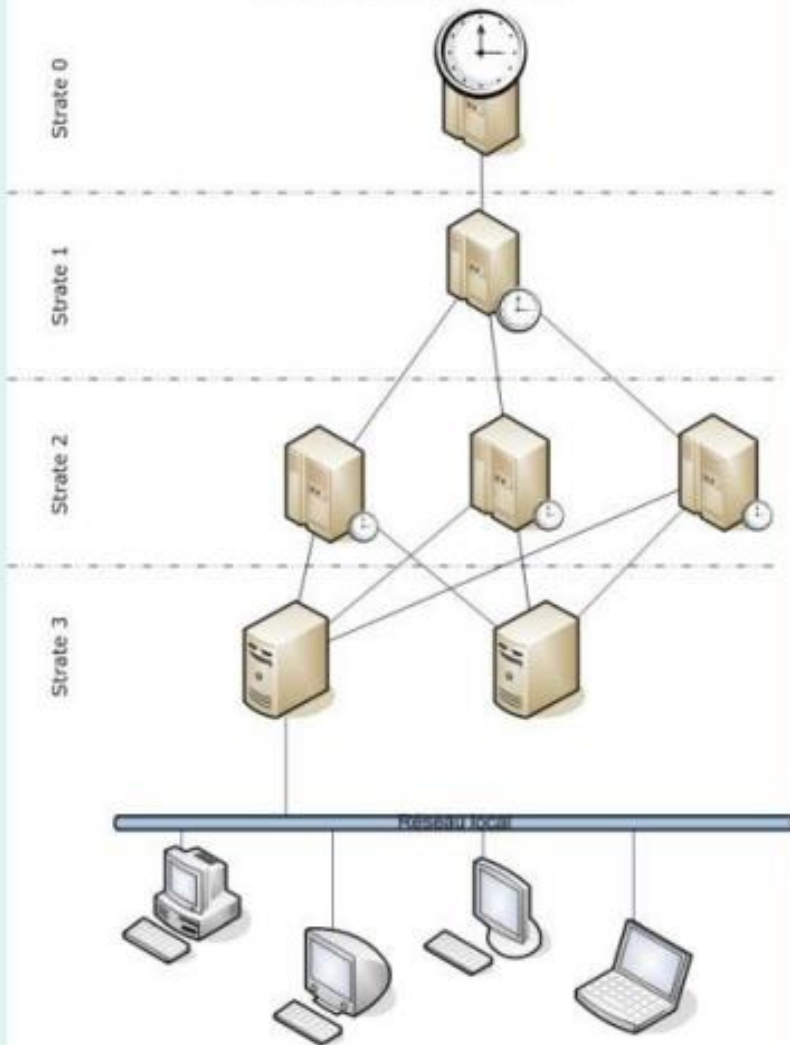
- Utilisé pour synchroniser le temps entre les ordinateurs de l'Internet, le protocole de synchronisation du réseau garantit à un client ou serveur une précision d'un millième de seconde pour les réseaux locaux (LAN), et jusqu'à quelques dizaines de millièmes de secondes pour les réseaux étendus (WAN) par rapport à un serveur primaire.
- Le NTP est un protocole client-serveur appartenant à couche d'application et il est à l'écoute sur le port UDP 123.

horloges atomiques.

- pour qu'une horloge dérive d'une seconde complète, une seconde en 160 millions d'années.



Hiérarchie des serveurs NTP



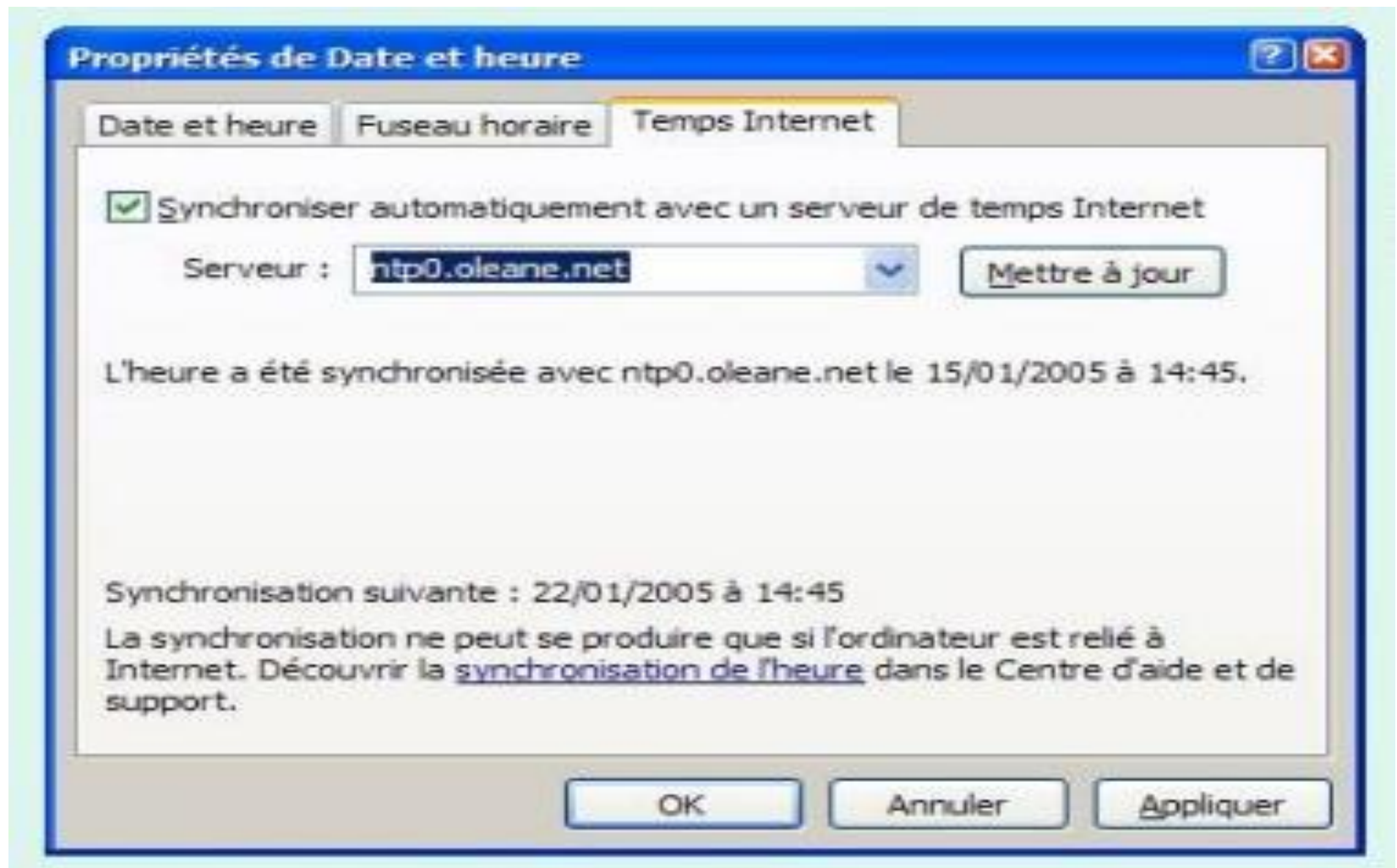
- Les serveurs de strate 0, qui sont des horloges atomiques. Ce sont les serveurs de référence.

- Les serveurs de strate 1. Ils se synchronisent sur les serveurs de strate 0. Leur dérive est de 1 seconde pour 10 000 ans...

- Les serveurs de strate 2. Ils se synchronisent sur les serveurs de strate 1. Ce sont généralement des serveurs publics.








- Les serveurs de strate 3. Ils se synchronisent sur les serveurs de strate 2. Ce sont généralement les serveurs que l'on installe dans une entreprise pour synchroniser tous les ordinateurs du réseau

- **Nombre de serveurs NTP** • Strate 1 : Il en existe environ 230 dans le monde. • Strate 2 : Les serveurs secondaires (environ 4500)(ex: serveurs de campus universitaires) se synchronisent sur plusieurs serveurs primaires en mode client/serveur, et avec d'autres serveurs secondaires en mode symétrique.



Liste des serveur NTP

Active Servers

	Afrique	81
	Asie	330
	Europe	3016
	Amérique du Nord	1032
	Oceania	158
	Amérique du Sud	67
	Mondial	4411
	Tous les Réserveurs de Serveurs	4655



**NTP Pool
Project**

Djibouti — dj.pool.ntp.org (4)

Algeria — dz.pool.ntp.org (0)

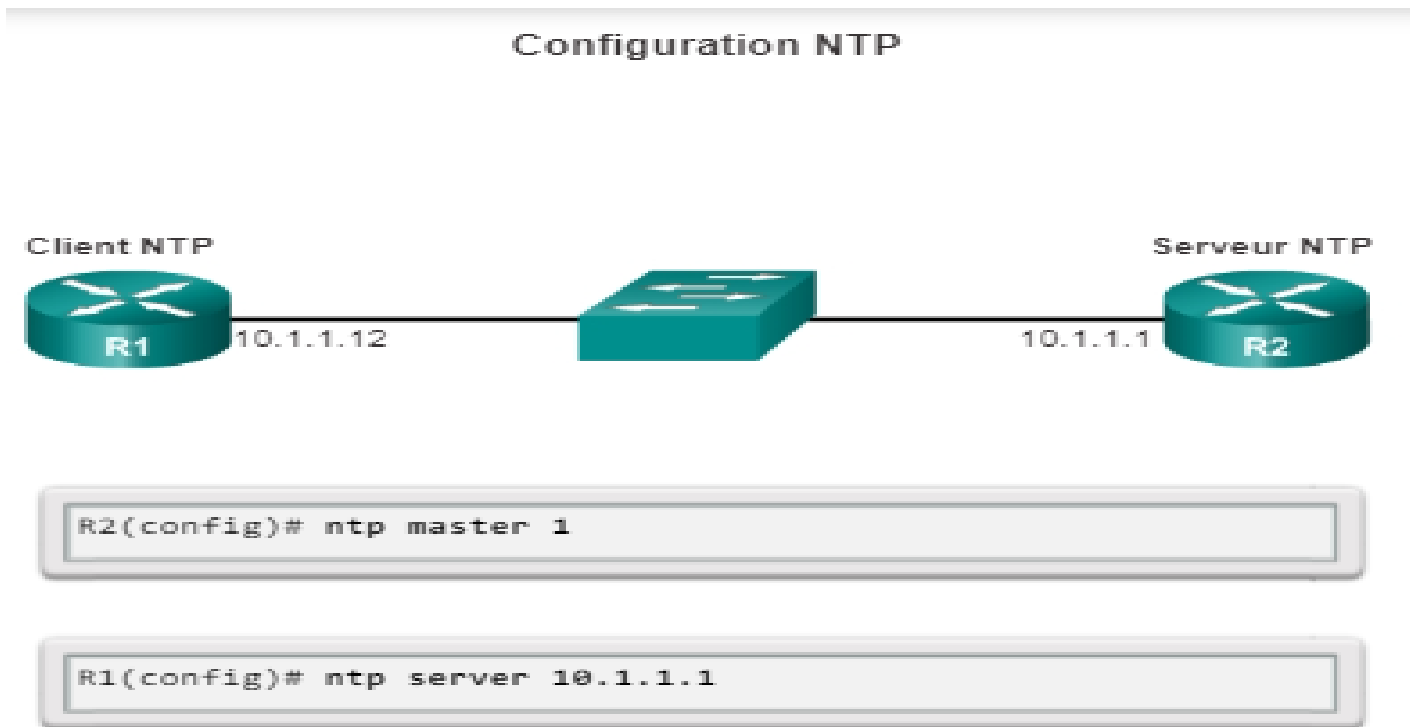
Egypt — eg.pool.ntp.org (4)

Western Sahara — eh.pool.ntp.org (0)

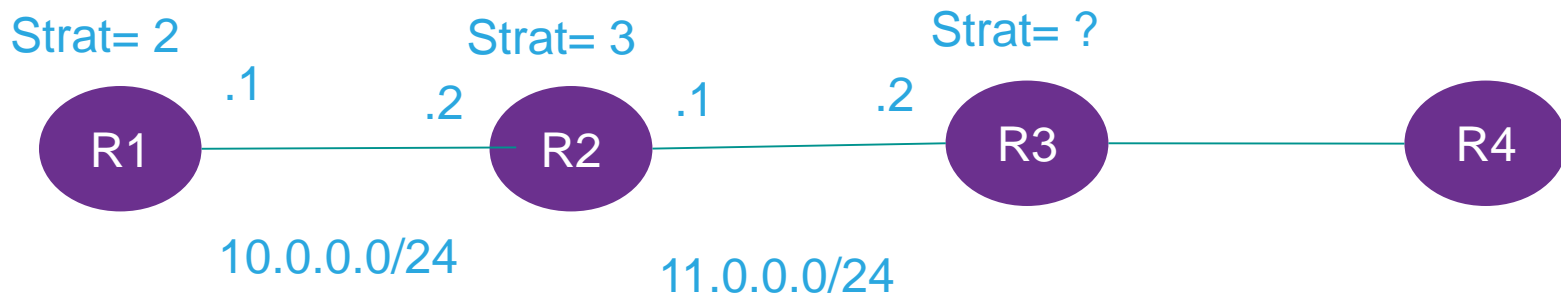
Eritrea — er.pool.ntp.org (0)

Horodatage de service

- Il est possible d'horodater les messages de journal et de définir l'adresse source des messages Syslog. Cela permet d'améliorer le débogage et la gestion en temps réel.
- Le routeur R1 est configuré en tant que client NTP, tandis que le routeur R2 fait office de serveur NTP



1. NTP Serveur
2. NTP client
3. NTP peer (exemple entre R2 et R3)



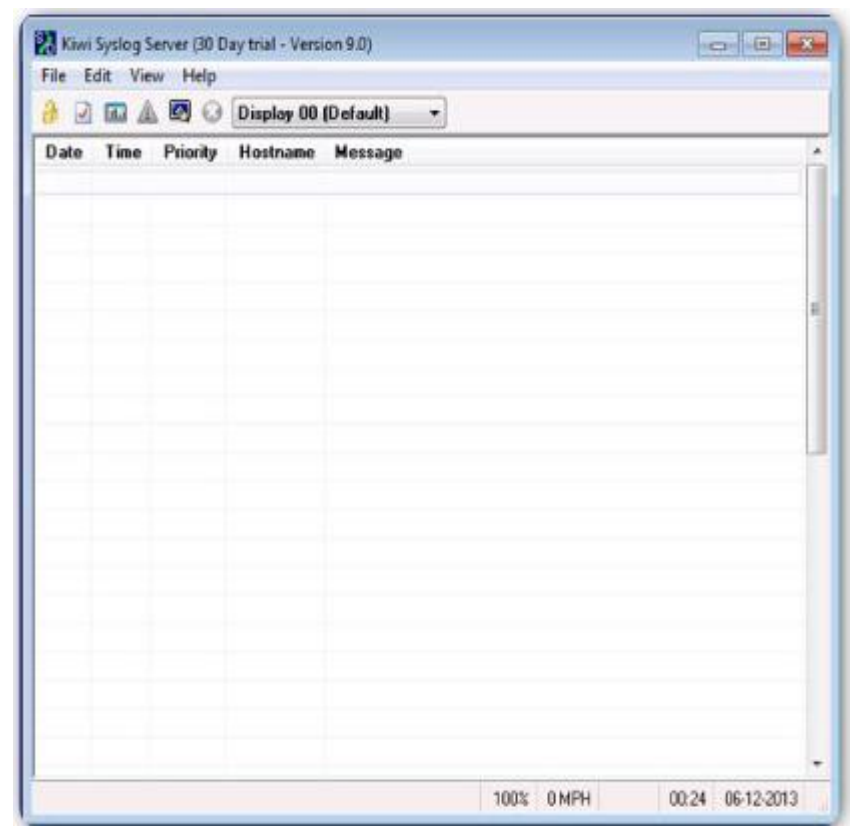
4. R2 # ntp peer 11.0.0.2
5. R3 # ntp peer 11.0.0.1

- Afin d'éviter que quiconque sur les périphériques, il sera utile de limiter l'accès au service NTP
- ip access-list standard LAN_R1
- permit 192.168.1.0 0.0.0.255
- ntp access-group serve-only LAN_R1

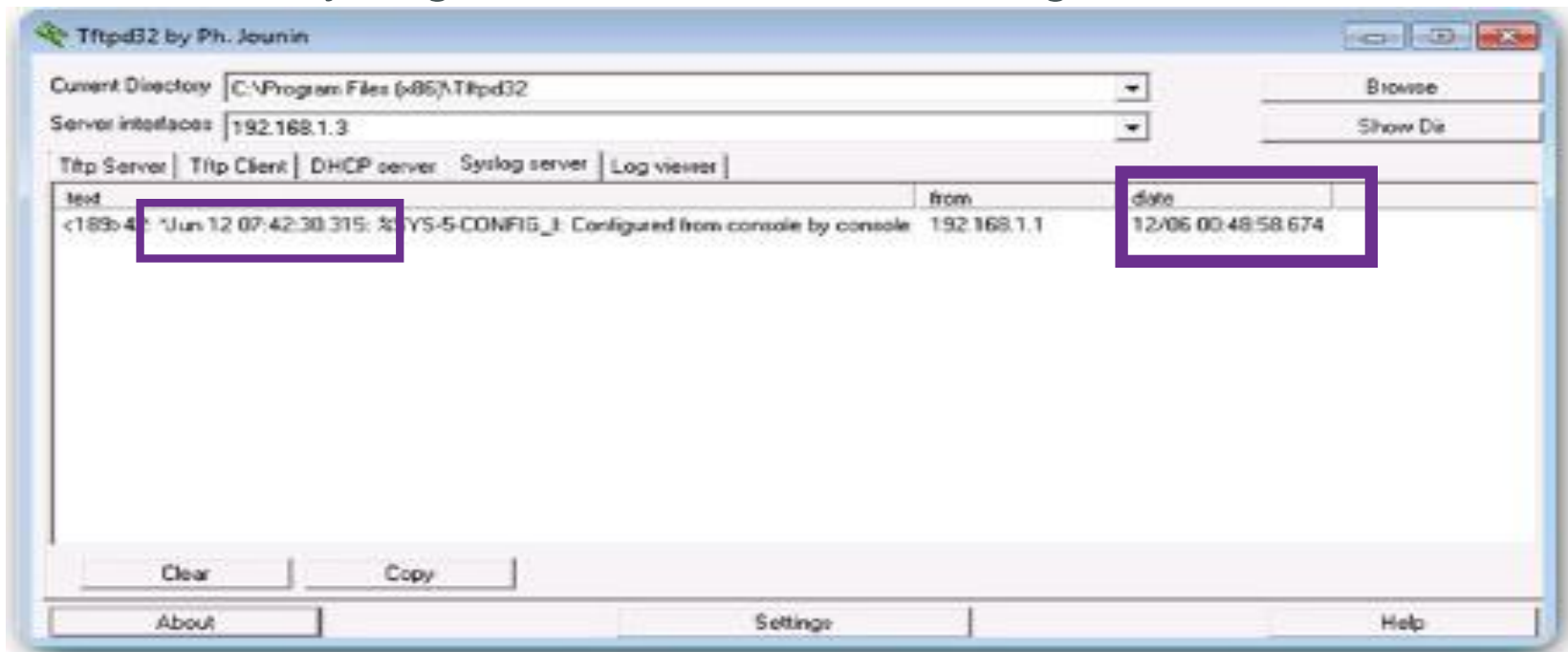
Configuration de Syslog

- Il existe plusieurs versions freeware et shareware de Syslog, ainsi que des versions commerciales destinées aux entreprises.

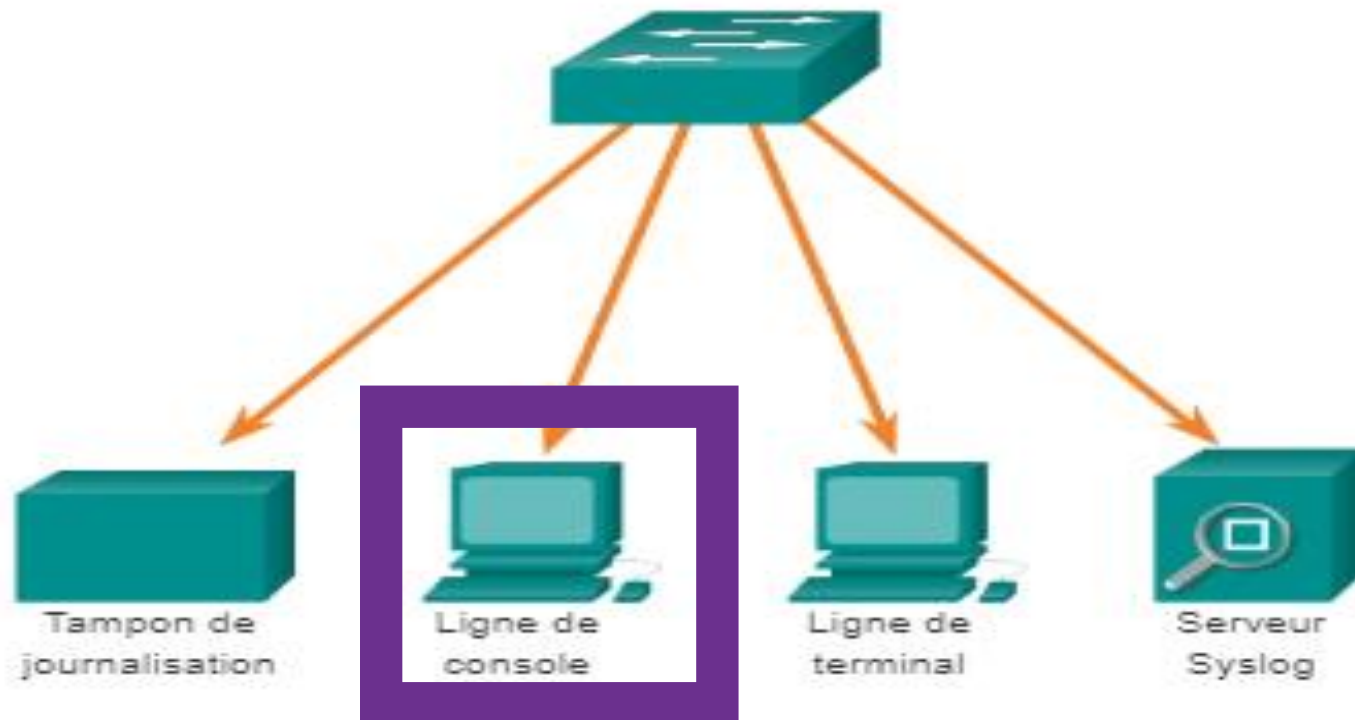
Syslog Kiwi



- Le serveur Syslog fournit une interface pour l'affichage des résultats Syslog. Si des horodatages sont configurés sur le périphérique réseau qui est à la source des messages Syslog, la date et l'heure de chaque message s'affichent dans les résultats du serveur Syslog, comme le montre la Figure 2.

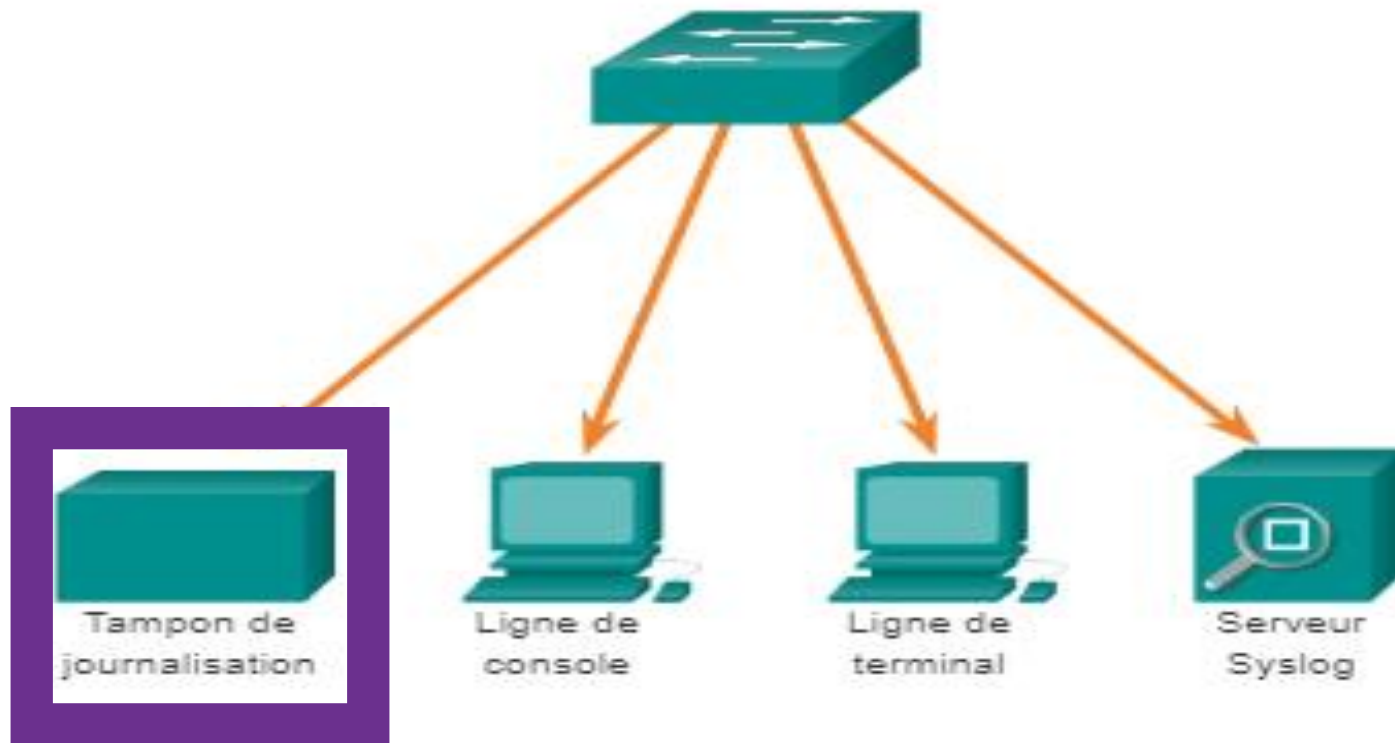


Options de destination des messages Syslog



- Par défaut, les routeurs et commutateurs Cisco envoient des messages journaux à la console pour tous les niveaux de gravité.
- **Commande : logging console**

Options de destination des messages Syslog



- **Commande : logging buffered**
- **Visualisation des logs en tampon : Show logging**

```
R1(config)#logging buffered ?
<0-7>          Logging severity level
<4096-2147483647> Logging buffer size
alerts         Immediate action needed          (severity=1)
critical       Critical conditions              (severity=2)
debugging      Debugging messages              (severity=7)
discriminator  Establish MD-Buffer association
emergencies    System is unusable               (severity=0)
errors         Error conditions                 (severity=3)
filtered       Enable filtered logging
informational  Informational messages            (severity=6)
notifications  Normal but significant conditions (severity=5)
warnings       Warning conditions              (severity=4)
xml            Enable logging in XML to XML logging buffer
<cr>
```

```
R1(config)#logging buffered 5
```

- Router(config)#logging buffer 20000000 debugging

```

R1(config)#logging buffered ?
<0-7>          Logging severity level
<4096-2147483647> Logging buffer size
alerts         Immediate action needed          (severity=1)
critical       Critical conditions              (severity=2)
debugging      Debugging messages              (severity=7)
discriminator  Establish MD-Buffer association
emergencies    System is unusable              (severity=0)
errors         Error conditions                (severity=3)
filtered       Enable filtered logging
informational   Informational messages          (severity=6)
notifications  Normal but significant conditions (severity=5)
warnings       Warning conditions              (severity=4)
xml            Enable logging in XML to XML logging buffer
<cr>

R1(config)#logging buffered 5

```

```
R1(config)#int loop 0
R1(config-if)#shut
R1(config-if)#
*Feb  4 20:14:26.347: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down
*Feb  4 20:14:27.347: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down
R1(config-if)#no shut
R1(config-if)#
*Feb  4 20:14:35.163: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
*Feb  4 20:14:36.163: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
```



```
R1#show logging
syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushed)
filtering disabled)
```

```
No Active Message Discriminator.
```

```
No Inactive Message Discriminator.
```

```
Console logging: level debugging, 18 messages logged, xml disabled,
                  filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
                  filtering disabled
Buffer logging: level notifications, 18 messages logged, xml disabled,
                 filtering disabled
Exception Logging: size (8192 bytes)
```

```
Count and timestamp logging messages: disabled
Persistent logging: disabled
```

```
No active filter modules.
```

```
Trap logging: level informational, 27 message lines logged
Logging Source-Interface:          VRF Name:
```

```
Log Buffer (8192 bytes):
```

```
*Feb  4 20:13:35.023: %SYS-5-CONFIG_I: Configured from console by console
*Feb  4 20:14:26.347: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down
*Feb  4 20:14:27.347: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down
*Feb  4 20:14:35.163: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
*Feb  4 20:14:36.163: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
*Feb  4 20:14:39.655: %SYS-5-CONFIG_I: Configured from console by console
```

```
R1#
```

```
R1#
```

```
R1#
```

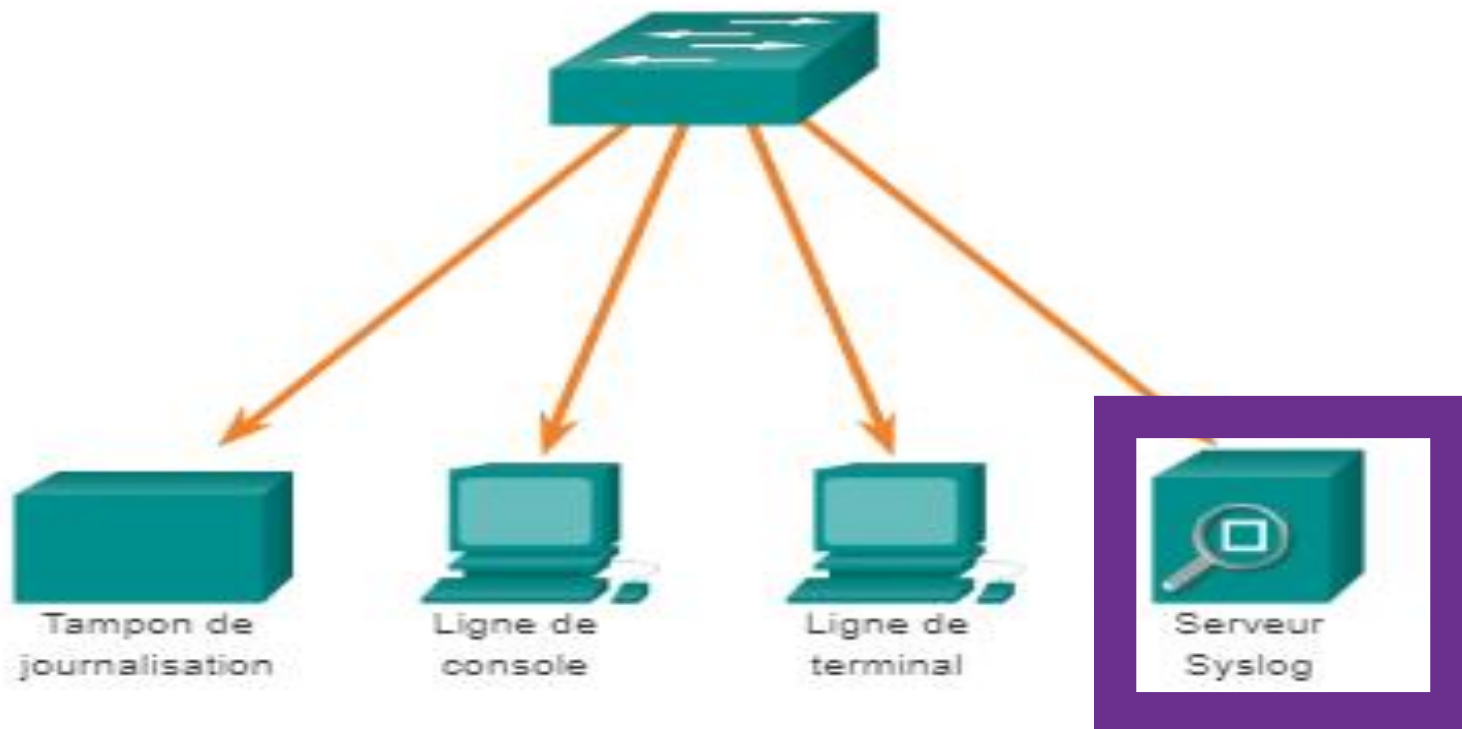
```
R1#clear logging
```

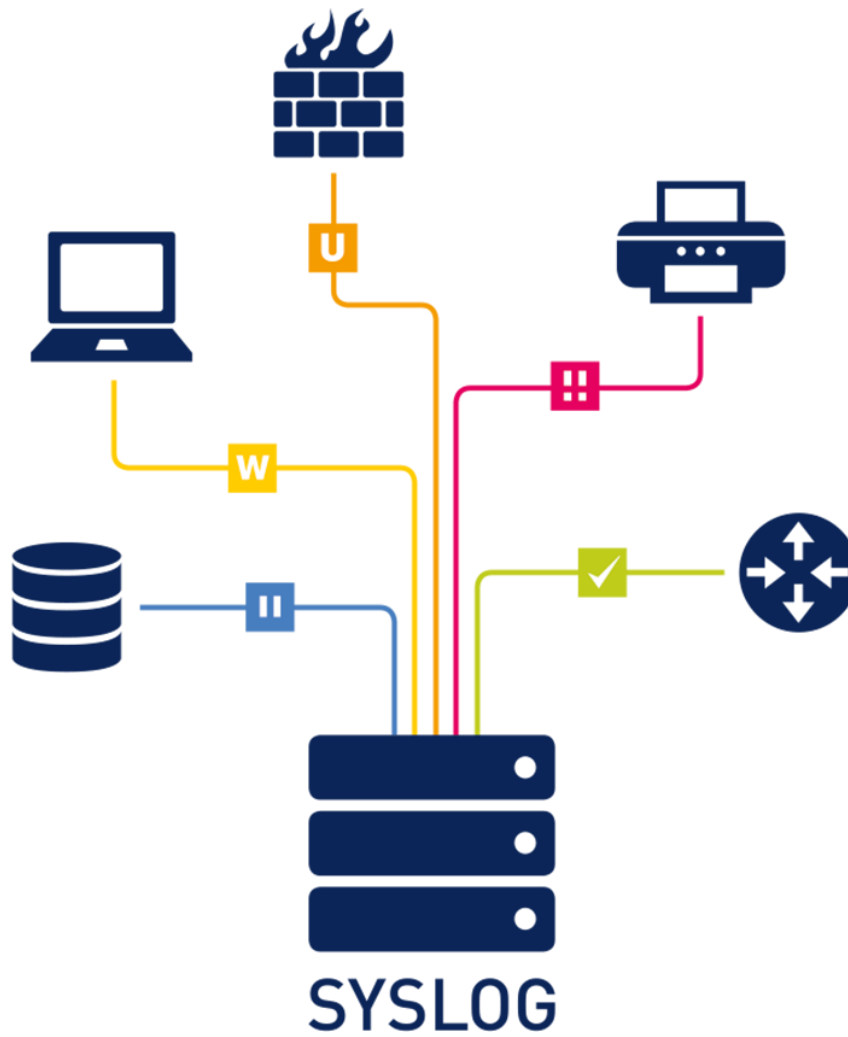
```
R1#debug ip packet detail
IP packet debugging is on (detailed)
R1#
R1#
R1#
R1#
R1#ping 192.168.1.13
```

```
R1#ping 192.168.1.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.13, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/20/36 ms
R1#
*Feb  4 20:17:00.923: FIBipv4-packet-proc: route packet from (local) src 192.168.1.20 dst 192.168.1.13
*Feb  4 20:17:00.923: FIBfwd-proc: packet routed by adj to FastEthernet0/0 192.168.1.13
*Feb  4 20:17:00.923: FIBipv4-packet-proc: packet routing succeeded
*Feb  4 20:17:00.927: IP: s=192.168.1.20 (local), d=192.168.1.13 (FastEthernet0/0), len 100, sending
*Feb  4 20:17:00.927:      ICMP type=8, code=0
*Feb  4 20:17:00.931: IP: s=192.168.1.20 (local), d=192.168.1.13 (FastEthernet0/0), len 100, sending full p
acket
*Feb  4 20:17:00.931:      ICMP type=8, code=0
*Feb  4 20:17:00.935: IP: s=192.168.1.13 (FastEthernet0/0), d=192.168.1.20, len 100, input feature
*Feb  4 20:17:00.939:      ICMP type=0, code=0, MCI Check(94), rtype 0, forus FALSE, sendself FALSE, mtu 0,
fwdchk FALSE
*Feb  4 20:17:00.939: FIBipv4-packet-proc: route packet from FastEthernet0/0 src 192.168.1.13 dst 192.168.1
```

```
R1(config)#logging buffered 7  
R1(config)#logging console 6  
R1(config)#
```

Options de destination des messages Syslog





```
R1(config)#logging host ?
  Hostname or A.B.C.D  IP address of the syslog server
  ipv6                 Configure IPv6 syslog server

R1(config)#logging host 192.168.1.13
R1(config)#
*Feb  4 20:23:12.367: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.13 port 514 started - CLI ini
```

Display 00 (Default)				
Date	Time	Priority	Hostname	Message
02-04-2019	20:23:14	Local7.Info	192.168.1.20	34: *Feb 4 20:23:12.367: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.13 port 514 started - CLI initiated

```

R1(config)#logging origin-id ?
  hostname    Use origin hostname as ID
  ip          Use origin IP address as ID
  ipv6        Use origin IPv6 address as ID
  string      Define a unique text string as ID
  <cr>

R1(config)#logging origin-id hostname

```

Date	Time	Priority	Hostname	Message
02-04-2019	20:24:52	Local7.Notic	192.168.1.20	35: R1: *Feb 4 20:24:51.059: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed
02-04-2019	20:23:14	Local7.Info	192.168.1.20	34: *Feb 4 20:23:12.367: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.13 port 514 s

```

R1(config)#logging origin-id string "cisco device"
R1(config)#

```

file edit view manage help

Date	Time	Priority	Hostname	Message
02-04-2019	20:25:42	Local7.Notic	192.168.1.20	36: cisco device: *Feb 4 20:25:40.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback3, changed state to up
02-04-2019	20:24:52	Local7.Notic	192.168.1.20	35: R1: *Feb 4 20:24:51.059: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
02-04-2019	20:23:14	Local7.Info	192.168.1.20	34: *Feb 4 20:23:12.367: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.13 port 514 started - CLI initiated

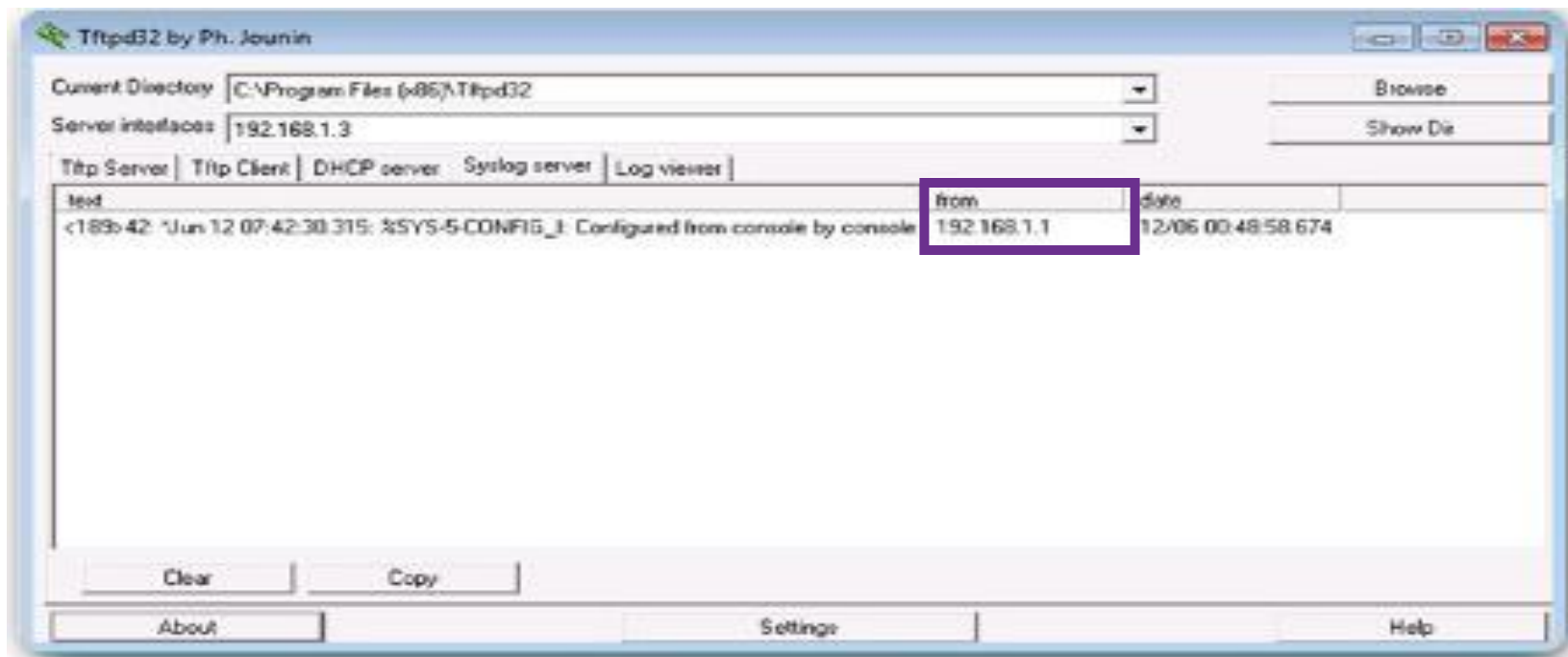
- Dans l'exemple de la Figure 2, les messages système du niveau 0 (urgences) à 5 (notifications) sont envoyés au serveur Syslog à l'adresse 209.165.200.225.

```
R1(config)# logging host 209.165.200.225  
R1(config)# logging trap notifications  
R1(config)# logging on
```

Configuration de Syslog

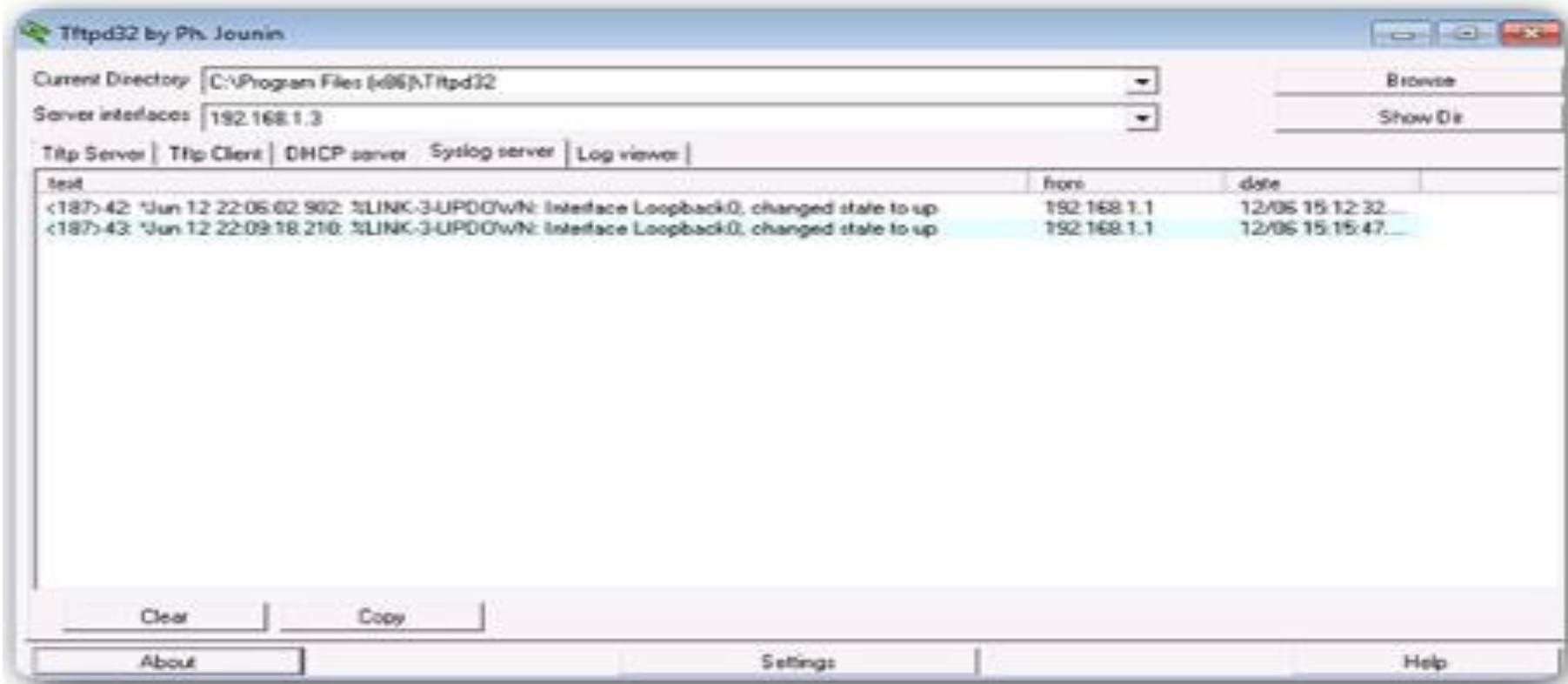
- **Étape 1.** Configurez le nom d'hôte ou l'adresse IP de destination du serveur Syslog en mode de configuration globale :
- R1(config)# **logging 192.168.1.3**
- **Étape 2.** Contrôlez les messages qui seront envoyés au serveur Syslog à l'aide de la commande de mode de configuration globale **logging trap level**. Par exemple, afin de limiter les messages à ceux des niveaux 4 et inférieurs (0 à 4), exécutez l'une des deux commandes équivalentes suivantes :
- R1(config)# **logging trap 4**
- R1(config)# **logging trap warning**

Severity Level	Level Name	Description
0	Emergencies	System unusable
1	Alerts	Immediate action needed
2	Critical	Critical conditions
3	Errors	Error conditions
4	Warnings	Warning conditions
5	Notifications	Normal but significant conditions
6	Informational	Informational messages only
7	Debugging	Debugging messages



- le routeur R1 est configuré pour envoyer les messages de journal des niveaux 4 et inférieurs au serveur Syslog à l'adresse 192.168.1.3. L'interface source est définie à G0/0. Une interface de bouclage est créée, puis arrêtée, puis réactivée. Le résultat de la console reflète ces actions.

```
R1(config)# logging 192.168.1.3
R1(config)# logging trap 4
R1(config)# logging source-interface gigabitEthernet 0/0
R1(config)# interface loopback 0
R1(config-if)#
*Jun 12 22:06:02.902: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:06:03.902: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:06:03.902: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to
host 192.168.1.3 port 514 started - CLI initiated
R1(config-if)# shutdown
R1(config-if)#
*Jun 12 22:06:49.642: %LINK-5-CHANGED: Interface Loopback0,
changed state to administratively down
*Jun 12 22:06:50.642: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to down
R1(config-if)# no shutdown
R1(config-if)#
*Jun 12 22:09:18.210: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:09:19.210: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
R1(config-if)#
```

- le serveur Syslog Tftpd32 a été configuré sur un ordinateur avec l'adresse IP 192.168.1.3. les seuls messages qui apparaissent sur le serveur Syslog sont ceux dont le niveau de gravité est égal à 4 ou moins (plus sévère). Les messages de niveau de gravité égal à 5 ou plus (moins grave) s'affichent dans les résultats de la console du routeur, mais n'apparaissent pas dans les résultats du serveur Syslog,

- Vous pouvez utiliser la commande **show logging** pour afficher tous les messages qui ont été consignés.
- l'exécution de la commande **show logging | begin June 12 22:35** affiche le contenu du tampon de journalisation à partir du 12 juin.

```
R1# show logging | begin Jun 12 22:35
*Jun 12 22:35:46.206: %LINK-5-CHANGED: Interface Loopback0,
changed state to administratively down
*Jun 12 22:35:47.206: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to down
*Jun 12 22:35:55.926: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:35:56.926: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:49:52.122: %SYS-5-CONFIG_I: Configured from console by
console
*Jun 12 23:15:48.418: %SYS-5-CONFIG_I: Configured from console by
console
R1#
```