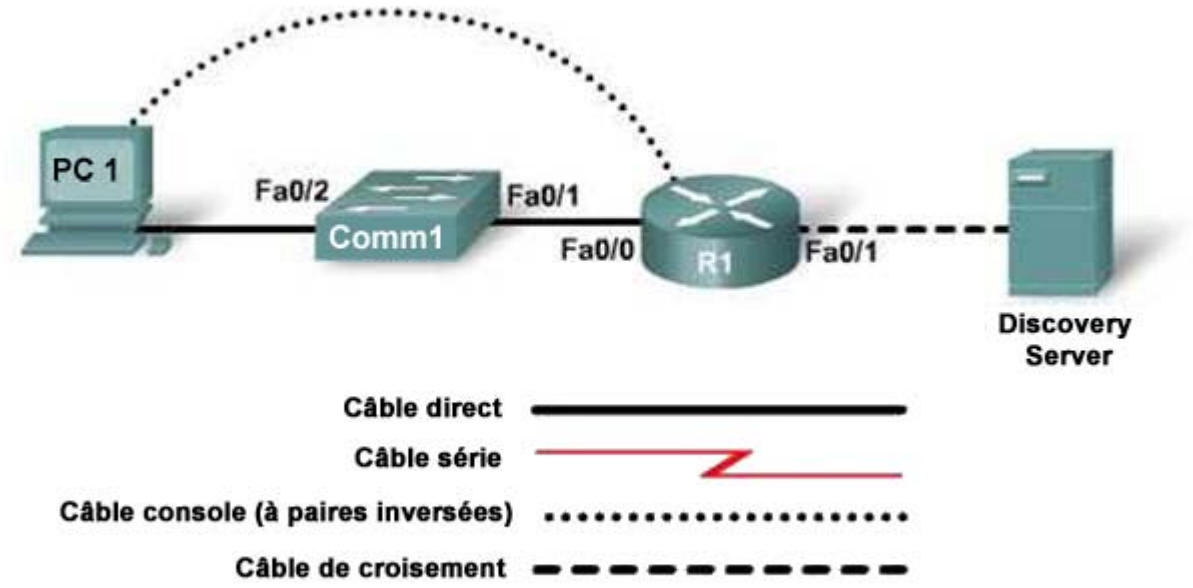
# Travaux pratiques 4.1.2 Caractéristiques des applications réseau




| Désignation du périphérique | Nom du périphérique | Adresse | Masque de sous-réseau |
|---|---|---|---|
| Serveur Discovery | Services professionnels | 172.17.1.1 | 255.255.0.0 |
| R1 | FC-CPE-1 | Fa0/1 172.17.0.1<br>Fa0/0 10.0.0.1 | 255.255.0.0<br>255.255.255.0 |
| Comm1 | FC-ASW-1 | — | — |
| PC1 | Hôte 1 | 10.0.0.200 | 255.255.255.0 |

## Objectif

- Configurer NetFlow pour observer le flux du trafic

## Résultats attendus et critères de réussite

Avant de démarrer ces travaux pratiques, prenez connaissance des tâches que vous devrez effectuer. Selon vous, quel sera le résultat de l'exécution de ces tâches ?

_____

_____

_____

Quelle est l'utilité de l'explication du flux de trafic dans une conception et une administration de réseau ?

_____

_____

_____

## Contexte / Préparation

Cisco IOS peut inclure une fonction nommée NetFlow qui fournit des informations sur les utilisateurs et les applications du réseau, les heures de pointe et le routage du trafic. NetFlow peut fournir les services suivants :

- comptabilisation du trafic réseau ;
- facturation du réseau basée sur l'utilisation ;
- planification du réseau ;
- sécurité ;
- capacités de surveillance de déni de service ;
- surveillance du réseau.

Les routeurs Cisco possédant la fonction NetFlow génèrent des enregistrements NetFlow. Vous pouvez consulter ces détails à l'aide des commandes **show**, les exporter à partir du routeur et les regrouper à l'aide du collecteur NetFlow.

Bien que mis en œuvre initialement par Cisco, NetFlow devient une norme IETF : Internet Protocol Flow Information eXport (IPFIX). Voir la RFC 3954 à l'adresse : http://www.ietf.org/rfc/rfc3954.txt.

NetFlow définit un flux de données comme une séquence unidirectionnelle de paquets qui contient les cinq valeurs suivantes :

1. adresse IP source ;
2. adresse IP de destination ;
3. port TCP source ;
4. port TCP de destination ;
5. protocole IP.

Dans ces travaux pratiques, vous allez observer les résultats de la configuration de NetFlow. Vous verrez comment l'état des flux de données du réseau actuel peut être établi afin de planifier et de mettre en œuvre une mise à niveau de réseau.

### Étape 1 : câblage et configuration du réseau actuel

a. Connectez les périphériques et configurez-les conformément à la topologie et à la configuration fournies.

   Dans ces travaux pratiques, une station de travail PC peut remplacer un serveur Discovery.

b. Exécutez une requête ping entre l'Hôte 1 et le serveur Discovery pour confirmer la connectivité du réseau.

   Dépannez la connectivité, puis établissez-la si la requête ping a échoué.

### Étape 2 : configuration de NetFlow sur les interfaces

NetFlow est configuré pour surveiller les flux de données intérieurs/extérieurs à des interfaces de routeur spécifiques. La fonction **Ingress** capture le trafic reçu par l'interface. La fonction **Egress** capture le trafic

transmis par l'interface. Dans ces travaux pratiques, le trafic sera surveillé sur les deux interfaces de routeur et dans les deux sens à partir de la session de console.

a. En mode de configuration globale, émettez les commandes suivantes :

```
FC-CPE-1(config)#interface fastethernet 0/0
FC-CPE-1(config-if)#ip flow ?
```

Notez les deux options disponibles :

_____

_____

Quelle option capture le trafic reçu par l'interface ? _____

Quelle option capture le trafic transmis par l'interface ? _____

b. Complétez la configuration de NetFlow.

```
FC-CPE-1(config-if)#ip flow egress
FC-CPE-1(config-if)#ip flow ingress
FC-CPE-1(config-if)#interface fastethernet 0/1
FC-CPE-1(config-if)#ip flow ingress
FC-CPE-1(config-if)#ip flow egress
FC-CPE-1(config-if)#exit
FC-CPE-1(config)#end
```

### Étape 3 : vérification de la configuration de NetFlow

a. À l'invite du mode d'exécution privilégié, lancez la commande **show running-config**.

Pour chaque interface FastEthernet, quelle instruction de la configuration d'exécution démontre que NetFlow est configuré ?

**interface FastEthernet0/0 :**

_____

_____

**interface FastEthernet0/1 :**

_____

_____

b. À partir du mode d'exécution privilégié, lancez la commande :

```
FC-CPE-1#show ip flow ?
```

Trois options sont disponibles :

_____

_____

_____

```
FC-CPE-1#show ip flow interface
FastEthernet0/0
  ip flow ingress
  ip flow egress
FastEthernet0/1
  ip flow ingress
  ip flow egress
```

Confirmez que le résultat ci-dessus s'affiche. Dépannez la configuration si ce résultat ne s'affiche pas.

### Étape 4 : création d'un trafic de données réseau

a. Vous pouvez examiner le flux de données capturé à l'aide de la commande **show ip cache flow** émise à partir du mode d'exécution privilégié.

```
FC-CPE-1#show ip cache flow
```

L'émission de cette commande avant tout flux de trafic de données doit générer un résultat similaire à celui présenté ici.

```
IP packet size distribution (0 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 0 bytes
  0 active, 0 inactive, 0 added
  0 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec)
Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP
Pkts
```

b. Répertoriez les sept titres de colonne mis en surbrillance et réfléchissez à l'utilisation de ces informations dans le cadre de la définition des caractéristiques du réseau.

_____

_____

_____

_____

_____

_____

_____

_____

c. Pour garantir la réinitialisation des statistiques de mémoire cache du flux, lancez la commande suivante en mode d'exécution privilégié :

```
FC-CPE-1# clear ip flow stats
```

d. Exécutez une requête ping vers le Serveur professionnel à partir de l'Hôte 1 pour générer un flux de données.

Dans la ligne de commande de l'Hôte 1, lancez la commande **ping 172.17.1.1 -n 200.**

### Étape 5 : affichage des flux de données

a. Vous pouvez consulter les détails du flux à la fin du flux de données. En mode d'exécution privilégié, lancez la commande :

```
FC-CPE-1#show ip cache flow
```

Un résultat similaire à celui présenté ci-dessous doit s'afficher. Vos travaux pratiques peuvent présenter des différences en termes de valeurs et de détails.

```
IP packet size distribution (464 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .900 .096 .000 .000 .000 .000 .002 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  5 active, 4091 inactive, 48 added
  1168 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 17416 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec)
Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow
/Flow
UDP-DNS             31      0.0         1    72      0.0       0.0
15.5
UDP-other           10      0.0         2    76      0.0       4.1
15.2
ICMP                 2      0.0       200    60      0.3     198.9
15.3
Total:              43      0.0        10    61      0.3      10.2
15.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP
Pkts
<output omitted>
```

b. Examinez le résultat et faites la liste des détails fournis dans le flux de données.

_____

_____

_____

_____

_____

_____

_____

_____

### Étape 6 : arrêt de la capture NetFlow

a. Pour désactiver une capture Netflow, lancez la commande **no ip flow** à l'invite de configuration de l'interface.

```
FC-CPE-1(config)#interface fastethernet 0/0
FC-CPE-1(config-if)#no ip flow ingress
FC-CPE-1(config-if)#no ip flow egress
FC-CPE-1(config)#interface fastethernet 0/1
FC-CPE-1(config-if)#no ip flow ingress
FC-CPE-1(config-if)#no ip flow egress
```

b. Pour s'assurer que NetFlow est désactivé, lancez la commande **ip flow interface** à partir du mode d'exécution privilégié.

```
FC-CPE-1#show ip flow interface
FC-CPE-1#
```

Aucun résultat n'est disponible si NetFlow est désactivé.

### Étape 7 : remise en état

Effacez les configurations et rechargez les routeurs et les commutateurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage souhaité et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (réseau local de l'établissement ou Internet).

### Étape 8 : remarques générales

Réfléchissez à la portée possible des types de flux de données dans un réseau et à la mise en œuvre d'un outil tel que NetFlow dans le cadre de l'analyse de ces flux.

_____

_____

_____

_____

_____

_____