Travaux pratiques : collecte et analyse de données NetFlow (version de l'instructeur)

Remarque à l'intention de l'instructeur : le texte en rouge ou surligné en gris apparaît uniquement dans la version de l'instructeur.

Topologie

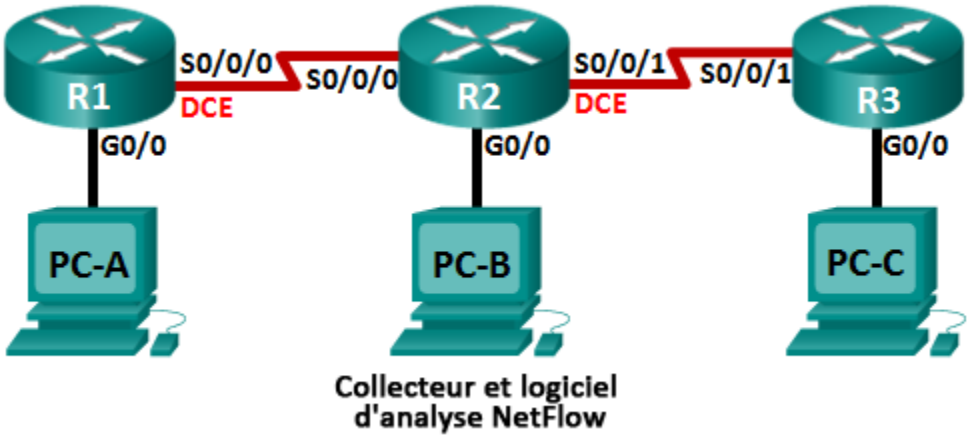

Table d'adressage

Périphérique	Interface	Adresse IP	Passerelle par défaut
R1	G0/0	192.168.1.1/24	N/A
	S0/0/0 (DCE)	192.168.12.1/30	N/A
R2	G0/0	192.168.2.1/24	N/A
	S0/0/0	192.168.12.2/30	N/A
	S0/0/1 (DCE)	192.168.23.1/30	N/A
R3	G0/0	192.168.3.1/24	N/A
	S0/0/1	192.168.23.2/30	N/A
PC-A	NIC	192.168.1.3	192.168.1.1
PC-B	NIC	192.168.2.3	192.168.2.1
PC-C	NIC	192.168.3.3	192.168.3.1

Objectifs

Partie 1 : création du réseau et configuration des paramètres de base du périphérique

Partie 2 : configuration de NetFlow sur un routeur

Partie 3 : analyse de NetFlow à l'aide de l'interface en ligne de commande

Partie 4 : découverte du collecteur et du logiciel d'analyse NetFlow

Contexte/scénario

NetFlow est une technologie Cisco IOS qui fournit des statistiques sur les paquets traversant un routeur ou un commutateur multicouche Cisco. NetFlow permet la surveillance du réseau et de la sécurité, la planification réseau, l'analyse du trafic et la comptabilité IP. Il est important de ne pas confondre l'objectif et les résultats de NetFlow avec ceux du matériel et du logiciel de capture de paquets. La capture de paquets enregistre toutes les informations possibles à la sortie ou à l'entrée d'un périphérique réseau en vue d'une analyse ultérieure, tandis que NetFlow cible des données statistiques spécifiques.

Flexible NetFlow est la technologie NetFlow la plus récente, améliorant la version d'origine de NetFlow en y ajoutant la possibilité de personnaliser les paramètres d'analyse du trafic. Flexible NetFlow utilise le format d'exportation de la version 9. De nombreuses commandes de Flexible NetFlow sont prises en charge à partir de la version 15.1 de Cisco IOS.

Au cours de ces travaux pratiques, vous allez configurer NetFlow de manière à capturer à la fois des paquets d'entrée et de sortie. Vous utiliserez des commandes **show** afin de vérifier que NetFlow est opérationnel et qu'il collecte des informations statistiques. Vous explorerez également les options disponibles du collecteur et du logiciel d'analyse NetFlow.

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 de routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque : assurez-vous que les routeurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre instructeur.

Remarque à l'intention de l'instructeur : reportez-vous au Manuel de travaux pratiques pour l'instructeur, pour connaître les procédures d'initialisation et de redémarrage des périphériques.

Ressources requises

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

Partie 1 : Création du réseau et configuration des paramètres de base du périphérique

Dans cette 1re partie, vous allez configurer la topologie du réseau et les paramètres de base sur les PC hôte et les routeurs.

Étape 1 : Câblez le réseau conformément à la topologie.

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

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

a. Désactivez la recherche DNS.

b. Configurez les noms des périphériques conformément à la topologie.

c. Attribuez **class** comme mot de passe chiffré du mode d'exécution privilégié.

d. Attribuez **cisco** en tant que mots de passe de console et vty, puis activez la connexion.

e. Chiffrez tous les mots de passe en clair.

f. Configurez une bannière MOTD pour avertir les utilisateurs que tout accès non autorisé est interdit.

g. Configurez **logging synchronous** pour la ligne de console.

h. Définissez la fréquence d'horloge pour toutes les interfaces série DCE sur **128000**.

i. Configurez les adresses IP telles qu'indiquées dans la table d'adressage.

j. Configurez le protocole OSPF en utilisant l'ID de processus 1 et annoncez l'ensemble des réseaux. Les interfaces Ethernet doivent être passives.

k. Créez une base de données locale sur R3 avec le nom d'utilisateur **admin**, le mot de passe **cisco** et le niveau de privilège défini à **15**.

l. Sur R3, activez le service HTTP et authentifiez les utilisateurs HTTP en utilisant la base de données locale.

m. Copiez la configuration en cours en tant que configuration de démarrage.

Étape 4 : Configurez les hôtes PC.

Étape 5 : Vérifiez la connectivité de bout en bout.

Tous les périphériques doivent pouvoir s'envoyer mutuellement des requêtes ping au sein de la topologie. Le cas échéant, procédez à un dépannage jusqu'à ce que la connectivité de bout en bout soit établie.

Remarque : il peut être nécessaire de désactiver le pare-feu du PC pour que les requêtes ping puissent aboutir.

Partie 2 : Configuration de NetFlow sur un routeur

Dans la Partie 2, vous allez configurer NetFlow sur le routeur R2. NetFlow capturera la totalité du trafic d'entrée et de sortie au niveau des interfaces série de R2 et exportera les données vers le collecteur NetFlow, à savoir PC-B. La version 9 de Flexible NetFlow sera utilisée pour l'exportation des données vers le collecteur NetFlow.

Étape 1 : Configurez la capture NetFlow.

Configurez la capture des données NetFlow sur les deux interfaces série. Capturez des données à partir des paquets d'entrée et de sortie.

```
R2(config)# interface s0/0/0
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
R2(config-if)# interface s0/0/1
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
```

Étape 2 : Configurez l'exportation des données NetFlow.

Utilisez la commande **ip flow-export destination** pour identifier l'adresse IP et le port UDP du collecteur NetFlow vers lequel le routeur doit exporter les données NetFlow. Le numéro de port UDP 9996 sera utilisé pour cette configuration.

```
R2(config)# ip flow-export destination 192.168.2.3 9996
```

Étape 3 : Configurez la version d'exportation de NetFlow.

Les routeurs Cisco qui exécutent Cisco IOS 15.1 prennent en charge les versions 1, 5 et 9 de NetFlow. Le format de données d'exportation de la version 9 est le plus polyvalent, mais il n'est pas compatible avec les versions précédentes. Exécutez la commande **ip flow-export version** pour définir la version de NetFlow.

```
R2(config)# ip flow-export version 9
```

Étape 4 : Vérifiez la configuration de NetFlow.

a. Exécutez la commande **show ip flow interface** pour passer en revue les informations d'interface de capture NetFlow.

```
R2# show ip flow interface
Serial0/0/0
  ip flow ingress
  ip flow egress
Serial0/0/1
  ip flow ingress
  ip flow egress
```

b. Exécutez la commande **show ip flow export** pour passer en revue les informations d'exportation de données NetFlow.

```
R2# show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  192.168.2.3 (9996)
  Version 9 flow records
  388 flows exported in 63 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

Partie 3 : Analyse de NetFlow à l'aide de l'interface en ligne de commande

Dans la Partie 3, vous allez générer du trafic de données entre R1 et R3 afin d'observer la technologie NetFlow.

Étape 1 : Générez du trafic de données entre R1 et R3.

a. Établissez une connexion Telnet entre R1 et R3 en utilisant l'adresse IP 192.168.3.1. Entrez le mot de passe **cisco** pour passer en mode d'exécution utilisateur. Entrez le mot de passe **class** pour activer le mode d'exécution global. Exécutez la commande **show run** pour générer du trafic Telnet. Maintenez votre session Telnet active pour le moment.

b. À partir de R3, exécutez la commande **ping 192.168.1.1 repeat 1000** afin d'envoyer une requête ping à l'interface G0/0 de R1. Cette commande a pour effet de générer du trafic ICMP via R2.

c. À partir de PC-A, accédez à R3 en utilisant l'adresse IP 192.168.3.1. Connectez-vous avec le nom d'utilisateur **admin** et le mot de passe **cisco**. Gardez le navigateur ouvert une fois la connexion à R3 établie.

Remarque : assurez-vous que le bloqueur de fenêtres intempestives est désactivé sur votre navigateur.

Étape 2 : Affichez un résumé des statistiques de gestion des comptes NetFlow.

Sur R2, exécutez la commande **show ip cache flow** afin d'afficher les modifications apportées au résumé des données NetFlow, notamment la distribution de la taille des paquets, les informations relatives aux flux IP, les protocoles capturés et l'activité d'interface. Notez que les protocoles s'affichent dorénavant dans les données récapitulatives.

```
R2# show ip cache flow
IP packet size distribution (5727 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .147 .018 .700 .000 .001 .001 .001 .001 .011 .009 .001 .002 .000 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .001 .097 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 114 added
  1546 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 112 added, 112 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics 00:07:35
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           4      0.0        27    43      0.2       5.0      15.7
TCP-WWW            104      0.2        14   275      3.4       2.1       1.5
ICMP                 4      0.0      1000   100      8.8      27.9      15.4

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Total:             112      0.2        50   146     12.5       3.1       2.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/0       192.168.12.1    Null          224.0.0.5       59 0000 0000    43
Se0/0/1       192.168.23.2    Null          224.0.0.5       59 0000 0000    40
```

Étape 3 : Clôturez la session Telnet ainsi que celle du navigateur.

a. Exécutez la commande **exit** sur R1 afin de vous déconnecter de la session Telnet avec R3.

b. Fermez la session du navigateur sur PC-A.

Étape 4 : Effacez les statistiques de gestion des comptes NetFlow.

a. Sur R2, exécutez la commande **clear ip flow stats** pour effacer les statistiques de gestion des comptes NetFlow.

```
R2# clear ip flow stats
```

b. Exécutez à nouveau la commande **show ip cache flow** afin de vérifier que les statistiques de gestion des comptes NetFlow ont été réinitialisées. Notez que, même si vous ne générez plus de données via R2, des données sont recueillies par NetFlow. Dans l'exemple ci-dessous, l'adresse de destination de ce trafic est l'adresse de multidiffusion 224.0.0.5, ou les données LSA OSPF.

```
R2# show ip cache flow
IP packet size distribution (124 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 1.00 .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, 278544 bytes
  2 active, 4094 inactive, 2 added
  1172 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  2 active, 1022 inactive, 2 added, 2 added to flow
  0 alloc failures, 0 force free
  1 chunk, 0 chunks added
  last clearing of statistics 00:09:48
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
IP-other             2      0.0       193    79      0.6    1794.8       5.7
Total:               2      0.0       193    79      0.6    1794.8       5.7


SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/0       192.168.12.1    Null          224.0.0.5       59 0000 0000    35

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/1       192.168.23.2    Null          224.0.0.5       59 0000 0000    33
```

Partie 4 : Découverte du collecteur et du logiciel d'analyse NetFlow

Le collecteur et le logiciel d'analyse NetFlow sont disponibles auprès de nombreux fournisseurs. Certains logiciels sont fournis gratuitement, d'autres pas. L'URL suivante pointe vers une page Web récapitulative de quelques-uns des logiciels NetFlow disponibles gratuitement : http://www.cisco.com/en/US/prod/iosswrel/ps6537/ps6555/ps6601/networking_solutions_products_genericcontent0900aecd805ff72b.html

Examinez cette page Web afin de vous familiariser avec quelques-uns des collecteurs et logiciels d'analyse NetFlow disponibles.

Remarques générales

1. Quel est l'objectif du collecteur NetFlow ?

   _____

   _____

   _____

   Le collecteur NetFlow reçoit les données NetFlow exportées à partir des routeurs et des commutateurs sur le réseau. Il filtre et regroupe ces données conformément aux stratégies définies par l'administrateur réseau, et stocke ces données récapitulatives ou agrégées, au lieu des données de flux brutes, afin de minimiser l'espace disque nécessaire.

2. Quel est l'objectif du logiciel d'analyse NetFlow ?

   _____

   _____

   _____

   Le logiciel d'analyse NetFlow permet de visualiser et d'analyser quasiment en temps réel les données de flux enregistrées et agrégées. Il permet de spécifier le routeur, le schéma d'agrégation et l'intervalle de temps que vous voulez utiliser pour la visualisation. Il permet ensuite de trier et de présenter ces données sous une forme utile pour les utilisateurs (graphiques à barres, graphiques en secteurs ou histogrammes des rapports triés).

3. Quels sont les sept champs critiques utilisés par la version d'origine de NetFlow pour distinguer les flux ?

   _____

   _____

   Adresse IP source, adresse IP de destination, numéro de port source, numéro de port de destination, type de protocole de couche 3, marquage TOS (type de service), interface logique d'entrée.

Tableau récapitulatif des interfaces de routeur

Résumé des interfaces de routeur				
Modèle du routeur	**Interface Ethernet 1**	**Interface Ethernet 2**	**Interface série 1**	**Interface série 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)

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 combinaisons possibles des interfaces Ethernet et série 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 de Cisco IOS.

Configurations des périphériques (étape finale)

Routeur R1

```
R1# show run
Building configuration...

Current configuration : 1592 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
```

```
!
ip cef
!
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.12.1 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 shutdown
!
router ospf 1
 passive-interface GigabitEthernet0/0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
password 7 030752180500
 logging synchronous
 login
line aux 0
```

```
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 02050D480809
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Routeur R2

```
R2# show run
Building configuration...

Current configuration : 1808 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
```

```
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 192.168.12.2 255.255.255.252
 ip flow ingress
 ip flow egress
!
interface Serial0/0/1
 ip address 192.168.23.1 255.255.255.252
 ip flow ingress
 ip flow egress
 clock rate 128000
!
router ospf 1
 passive-interface GigabitEthernet0/0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip flow-export version 9
ip flow-export destination 192.168.2.3 9996
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
 password 7 14141B180F0B
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
```

```
 stopbits 1
line vty 0 4
 password 7 060506324F41
 login
 transport input all
!
scheduler allocate 20000 1000
!
End
```

Routeur R3

```
R3# show run
Building configuration...

Current configuration : 1769 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
username admin privilege 15 secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
```

```
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 192.168.23.2 255.255.255.252
!
router ospf 1
 passive-interface GigabitEthernet0/0
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.23.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
ip http server
ip http authentication local
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
 exec-timeout 0 0
 password 7 01100F175804
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 0822455D0A16
 login
 transport input all
!
scheduler allocate 20000 1000
!
```

```
end
```