Travaux pratiques 4.5.1 : Étude des protocoles TCP et UDP à l'aide de Netstat

Schéma de topologie

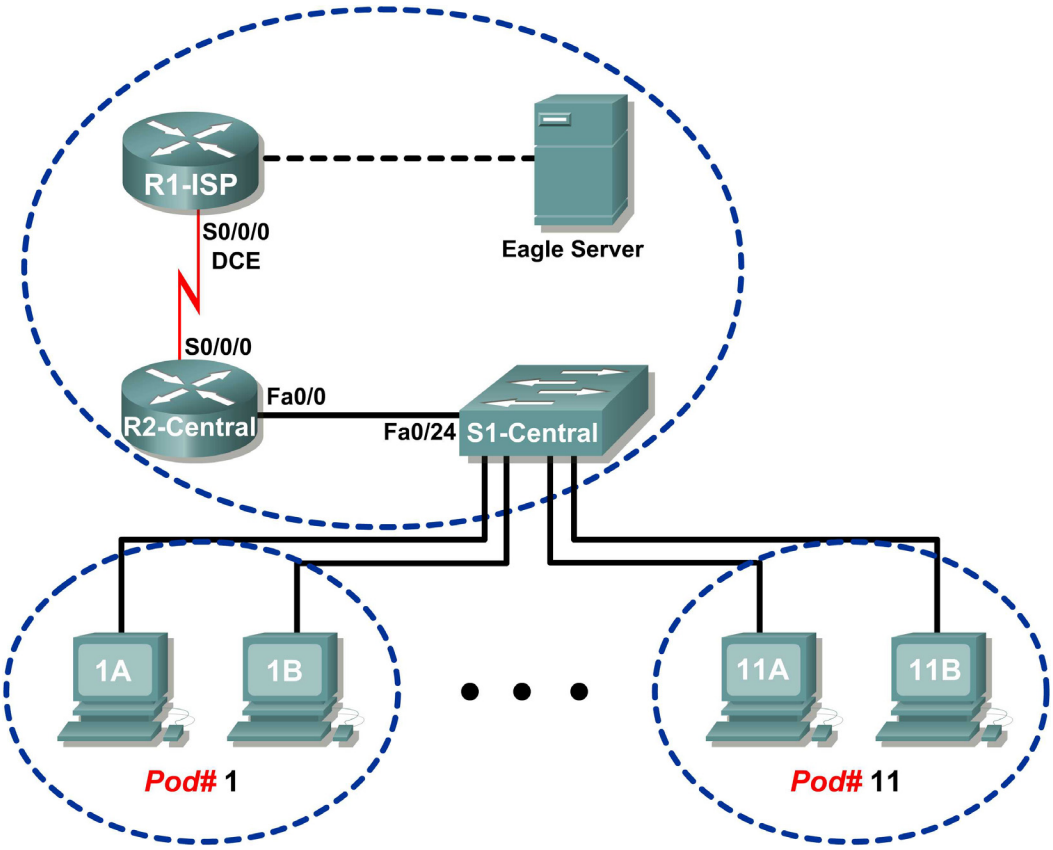

Tableau d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	S/O
	Fa0/0	192.168.254.253	255.255.255.0	S/O
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	S/O
	Fa0/0	172.16.255.254	255.255.0.0	S/O
Eagle Server	S/O	192.168.254.254	255.255.255.0	192.168.254.253
	S/O	172.31.24.254	255.255.255.0	S/O
host*Pod#*A	S/O	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#*B	S/O	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	S/O	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

- Décrire les paramètres et les résultats courants de la commande **netstat**
- Observer les informations de protocole sur un ordinateur hôte pod à l'aide de la commande **netstat**

Contexte

netstat est l'abréviation d'un utilitaire de statistiques réseau disponible à la fois sur les ordinateurs fonctionnant sous Windows et Unix / Linux. L'attribution de paramètres optionnels à cette commande génère des résultats différents. La commande **netstat** permet d'afficher les connexions réseau entrantes et sortantes (TCP et UDP), les informations de table de routage d'ordinateur hôte et les statistiques d'interface.

Scénario

Au cours de ces travaux pratiques, le participant examine la commande **netstat** sur un ordinateur hôte pod et règle les options de sortie de **netstat** afin d'analyser et de comprendre l'état du protocole TCP/IP de la couche transport.

Tâche 1 : description des paramètres et des résultats courants de la commande netstat

Ouvrez une fenêtre de ligne de commande en cliquant sur Démarrer | Exécuter. Tapez **cmd** et appuyez sur **OK**.

Pour afficher l'aide sur la commande **netstat**, utilisez les options **/?** comme affiché ci-dessous :

```
C:\> netstat /? <Entrée>
```

Reportez-vous au résultat obtenu avec la commande **netstat** /? pour indiquer les options qui correspondent le mieux aux descriptions dans le tableau suivant :

Option	Description
	Affiche toutes les connexions et tous les ports d'écoute.
	Affiche les adresses et les numéros de port sous forme numérique.
	Affiche de nouvelles statistiques toutes les cinq secondes. Appuyez sur Ctrl+C pour mettre fin à ce nouvel affichage.
	Affiche les connexions relatives au protocole défini pour proto : TCP, UDP, TCPv6 ou UDPv6. Si vous utilisez l'option -s pour afficher les statistiques par protocole, n'importe laquelle de ces valeurs peut être associée à proto : IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP ou UDPv6.
	Affiche à nouveau toutes les connexions et tous les ports d'écoute toutes les 30 secondes.
	Affiche uniquement les connexions ouvertes. Il s'agit d'un problème délicat.

Lorsque les statistiques **netstat** relatives aux connexions TCP s'affichent, l'état du protocole TCP s'affiche également. Au cours de sa durée de vie, une connexion TCP passe par toute une série d'états. Le tableau suivant comprend la liste des états TCP rapportés par **netstat** tels que définis dans le document RFC 793, Transmission Control Protocol, de septembre 1981 :

État	Description de la connexion
LISTEN	La connexion locale attend une requête de connexion de la part d'un périphérique distant.
ESTABLISHED	La connexion est établie et des données peuvent être échangées via cette connexion. Il s'agit de l'état normal correspondant à la phase de transfert de données.
TIME-WAIT	La connexion locale attend qu'un délai par défaut soit écoulé avant d'envoyer une requête de fin de connexion et de fermer la connexion. Il s'agit d'une situation normale. Ce délai est généralement compris entre 30 et 120 secondes.
CLOSE-WAIT	La connexion est fermée, mais attend une requête de fin de la part de l'utilisateur local.
SYN-SENT	La connexion locale attend une réponse à la requête de connexion envoyée. La connexion passe rapidement par cet état.
SYN_RECEIVED	La connexion locale attend une validation de la requête de connexion. La connexion passe rapidement par cet état. Si vous remarquez que de multiples connexions sont en état SYN_RECEIVED, une attaque TCP SYN est peut-être en cours d'exécution.

Les adresses IP qui s'affichent avec la commande **netstat** se répartissent en plusieurs catégories :

Adresse IP	Description
127.0.0.1	Cette adresse fait référence à l'hôte local ou à cet ordinateur.
0.0.0.0	Adresse globale signifiant « N'importe lequel ».
Adresse distante	Adresse du périphérique distant connecté à l'ordinateur.

Tâche 2 : observation des informations de protocole sur un ordinateur hôte pod à l'aide de la commande netstat

Étape 1 : utilisation de netstat pour afficher les connexions existantes

Dans la fenêtre de ligne de commande utilisée au cours de la tâche 1 ci-dessus, tapez la commande **netstat –a** :

```
C:\> netstat –a <Entrée>
```

Un tableau récapitulant les informations de protocoles (TCP et UDP), d'adresse locale, d'adresse distante et d'état s'affiche. Les adresses et protocoles pouvant être convertis en noms s'affichent.

L'option –n force netstat à afficher le résultat au format brut. Dans la fenêtre de ligne de commande, tapez la commande **netstat –an** :

```
C:\> netstat –an <Entrée>
```

Naviguez entre les résultats des deux commandes à l'aide de la barre de défilement vertical. Comparez les résultats, en notant les numéros de port connus convertis en noms.

Indiquez trois connexions TCP et trois connexions UDP provenant du résultat de la commande **netstat –a**, ainsi que les numéros de port convertis correspondants du résultat de la commande **netstat –an**. Si une conversion est possible pour moins de trois connexions, notez-le dans le tableau.

Connexion	Proto Adresse locale	Adresse distante	État

Reportez-vous au résultat suivant de **netstat**. Un nouvel ingénieur réseau soupçonne une attaque externe sur les ports 1070 et 1071 de son ordinateur hôte. Que pourriez-vous lui répondre ?

```
C:\> netstat –n
Connexions actives
Proto  Adresse locale         Adresse distante       État
TCP    127.0.0.1:1070         127.0.0.1:1071         ESTABLISHED
TCP    127.0.0.1:1071         127.0.0.1:1070         ESTABLISHED
C:\>
```

_____

_____

Étape 2 : établissement de plusieurs connexions TCP simultanées et enregistrement du résultat de la commande netstat

Au cours de cette tâche, vous allez établir plusieurs connexions simultanées avec Eagle Server. Vous utiliserez la commande **telnet** pour accéder aux services réseau d'Eagle Server et disposerez ainsi de plusieurs protocoles à examiner à l'aide de `netstat`.

Ouvrez quatre fenêtres de ligne de commande supplémentaires. Organisez-les de façon à ce qu'elles soient toutes visibles. Ces quatre fenêtres utilisées pour les connexions telnet à Eagle Server peuvent être relativement petites et occuper environ la moitié de la largeur de l'écran et le quart de la hauteur de l'écran. Les fenêtres de collecte des informations de connexion doivent, quant à elles, occuper environ la moitié de la largeur de l'écran et la totalité de sa hauteur.

Plusieurs services réseau d'Eagle Server répondront à une connexion telnet. Les informations suivantes seront utilisées :

- DNS : serveur de noms de domaine, port 53
- FTP : serveur FTP, port 21
- SMTP : serveur de messagerie SMTP, port 25
- TELNET : serveur Telnet, port 23

Comment expliquer l'échec d'une commande telnet envoyée aux ports UDP ?

_____

_____

Pour fermer une connexion telnet, appuyez simultanément sur les touches <CTRL>]. L'invite telnet s'affiche (Microsoft Telnet>). Tapez **quit <Entrée>** pour fermer la session.

Dans la première fenêtre de ligne de commande telnet, envoyez une commande telnet à Eagle Server sur le port 53. Dans la deuxième fenêtre de ligne de commande telnet, envoyez une commande telnet sur le port 21. Dans la troisième fenêtre de ligne de commande telnet, envoyez une commande telnet sur le port 25. Enfin, dans la quatrième fenêtre de ligne de commande telnet, envoyez une commande telnet sur le port 23. Voici la commande à utiliser pour une connexion telnet sur le port 21 :

```
C:\> telnet eagle-server.example.com 53
```

Dans la grande fenêtre de ligne de commande, enregistrez les connexions établies avec Eagle Server. Le résultat qui s'affiche est semblable à celui présenté ci-dessous. Si votre vitesse de frappe est lente, il est possible qu'une connexion soit fermée avant que toutes les connexions soient effectuées. Les connexions prennent fin au bout d'un certain délai d'inactivité.

```
Proto  Adresse locale         Adresse distante       État
TCP    192.168.254.1:1688     192.168.254.254:21     ESTABLISHED
TCP    192.168.254.1:1691     192.168.254.254:25     ESTABLISHED
TCP    192.168.254.1:1693     192.168.254.254:53     ESTABLISHED
TCP    192.168.254.1:1694     192.168.254.254:23     ESTABLISHED
```

Tâche 3 : remarques générales

L'utilitaire **netstat** permet d'afficher les connexions réseau (TCP et UDP) entrantes et sortantes, les informations de table de routage d'ordinateur hôte et les statistiques d'interface.

Tâche 4 : confirmation

Fermez les connexions établies de façon abrupte (en fermant la fenêtre de ligne de commande), puis exécutez la commande **netstat –an**. Essayez de déterminer les connexions qui se trouvent dans un état différent de ESTABLISHED.

Tâche 5 : nettoyage

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

