Évaluation de la sécurité : Utilisation des commandes de diagnostic

Objectifs

Partie 1: Collecter les paramètres des périphériques de l'utilisateur final

Partie 2: Collecter des informations sur les périphériques réseau

Partie 3: Diagnostiquer les problèmes de connectivité

Contexte/scénario

Dans cette activité Packet Tracer (PT), vous utiliserez diverses commandes pour collecter des informations sur les périphériques et résoudre les problèmes de configuration et de connectivité des périphériques. Les informations sur le périphérique incluent l'adresse IP, la passerelle par défaut et les paramètres du serveur DNS. Ces paramètres sont essentiels pour permettre à un périphérique de communiquer sur les réseaux et de se connecter à Internet.

Instructions

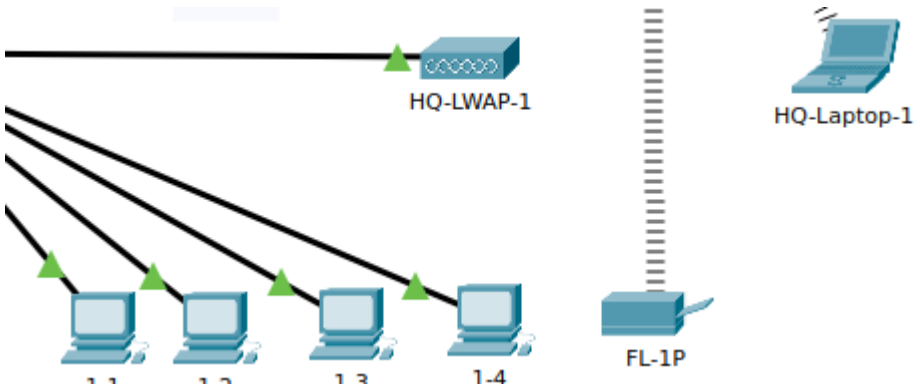
Partie 1: collecte des paramètres des périphériques de l'utilisateur final

Dans cette partie, vous documenterez les paramètres d'adresse IP des terminaux.

Étape 1: Documentez les paramètres de l'adresse IP pour HQ-Laptop-1.

a. L'activité s'ouvre dans le cluster **HQ**. L'**armoire de brassage** est le grand châssis noir situé dans le coin inférieur gauche du premier étage. Localisez tous les périphériques au premier étage: PC **1-1**, **1-2**, **1-3** et **1-4**. imprimante **FL-1P** ; et **HQ-Laptop-1**.

Capture d'écran des périphériques localisés :



b. Cliquez **HQ-Laptop-1** > **Desktop** tab > **Command Prompt**.

c. Entrez la commande **ipconfig**.

Quelle adresse IPv4 est affichée pour la **connexion sans fil0**?

```
Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::20A:F3FF:FEE4:EEAA
   IPv6 Address....................: ::
   Autoconfiguration IPv4 Address..: 169.254.238.170
   Subnet Mask.....................: 255.255.0.0
   Default Gateway.................: ::
                                     0.0.0.0
```

l'ip sans file du pc HQ-Laptop-1

Si l'adresse IPv4 est dans la plage 169.254.0.0/16, quelle méthode est utilisée pour attribuer des adresses IPv4? Pourquoi l'ordinateur portable reçoit-il une adresse IPv4 dans la plage 169.254.0.0/16?

1. La méthode utilisée c'est **APIPA** (Automatic Private IP Addressing).
2. L'ordi chope cette adresse parce qu'il a **pas réussi à contacter le serveur DHCP**.

En effet, au démarrage il a demandé une IP sur le réseau, mais personne lui a répondu (serveur DHCP HS ou cable débranché). Du coup, Windows s'est auto-attribué une adresse en 169.254... pour pas rester sans rien, c'est une adresse de secours mais t'aura pas internet avec ca.

Si l'adresse IPv4 est 169.254.0.0/16, attendez quelques secondes et répétez la commande **ipconfig**.

Lorsque l'adresse IPv4 ne fait plus partie de la plage 169.254.0.0/16, quelles sont les informations d'adressage IP qui s'affichent? Notez vos réponses dans le tableau ci-dessous.

```
Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::20A:F3FF:FEE4:EEAA
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.50.4
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.50.1
```

l'ip sans file du pc HQ-Laptop-1 est maintenant 192.168.50.4

Complétez le tableau ci-dessous :

FastEthernet0	Information sur l'adressage IP
Adresse physique	000A.F3E4.EEAA
Adresse IPv6 locale	FE80::20A:F3FF:FEE4:EEAA
Adresse IPv6	
Adresse IPv4	169.254.238.170
Masque de sous-réseau	255.255.0.0
Passerelle par défaut	
Serveur DNS	92.168.50.1

Partie 2: Analyser un incident dans une entreprise de vente au détail

Dans cette partie, vous documenterez les informations sur le lien vers le FAI. Vous documenterez ensuite les informations d'adressage IP pour tous les terminaux du siège social et découvrirez que les périphériques appartiennent à différents réseaux locaux virtuels (VLAN).

Étape 1: Collectez les informations de connexion réseau sur la liaison entre le siège et le FAI.

Le routeur HQ-Edge est le routeur entre le réseau du siège et le FAI. Nous devons identifier les informations sur le périphérique en amont situé dans le FAI.

a. Dans le rack de gauche de l'armoire de brassage, cliquez sur HQ -Edge > onglet CLI.

b. Appuyez sur Entrée pour obtenir l'invite HQ-Edge>, puis saisissez la commande enable.

c. Entrez la commande show ip route | begin Gateway.

Quelle est l'adresse de la passerelle de dernier recours (ou passerelle par défaut)?

L'adresse de la passerelle de dernier recours est : 0.0.0.0

```
HQ-Edge#show ip route | begin Gateway
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
```

Pourquoi l'adresse du saut suivant ne s'affiche-t-elle pas?

C'est l'adresse standard utilisée pour diriger tout le trafic qui ne correspond à aucune autre route spécifique vers Internet

d. Entrer la commande **show running-config | begin ip route**.

Comment la route par défaut est-elle configurée? Utilise-t-il l'adresse du saut suivant?

Parce que la route par défaut a été configurée en utilisant une interface de sortie (ex: `Serial0/0/0`) au lieu d'une adresse IP de saut suivant.

```
HQ-Edge#show running-config | begin ip route
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0
!
ip flow-export version 9
!
!
ip access-list standard NAT-PERMIT
 permit 192.168.10.0 0.0.0.255
 permit 192.168.20.0 0.0.0.255
 permit 192.168.99.0 0.0.0.15
 permit 192.168.75.0 0.0.0.7
ip access-list standard ADMIN-ONLY
 permit 192.168.99.0 0.0.0.255
 deny any
access-list 101 permit ip 192.168.10.0 0.0.0.255 10.0.3.0 0.0.0.255
access-list 101 permit ip 192.168.20.0 0.0.0.255 10.0.3.0 0.0.0.255
access-list 101 permit ip 192.168.75.0 0.0.0.255 10.0.3.0 0.0.0.255
access-list 101 permit ip 192.168.99.0 0.0.0.255 10.0.3.0 0.0.0.255
access-list 101 permit icmp any 10.0.3.0 0.0.0.255
ip access-list extended NAT-NOVPN
 permit ip 192.168.0.0 0.0.255.255 10.2.0.0 0.0.255.255
 permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.255.255
 permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.0.255
 permit ip 192.168.0.0 0.0.255.255 172.0.0.0 0.0.255.255
```

e. Entrer la commande **show cdp neighbors detail**.

Quelle est l'adresse IPv4 de l'adresse du saut suivant (FAI)?

l'adresse IPv4 de l'adresse du FAI est : 10.0.0.49

```
HQ-Edge#show cdp neighbors detail

Device ID: ISP
Entry address(es):
  IP address : 10.0.0.49
Platform: cisco PT1000, Capabilities: Router
Interface: GigabitEthernet0/0/0, Port ID (outgoing port): GigabitEthernet1/0
Holdtime: 147

Version :
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

advertisement version: 2
Duplex: full
```

Quel port du routeur du FAI est connecté à HQ-Edge?

FAI est connecté à HQ-Edge sur le port de sortie : GigabitEthernet1/0

```
Port ID (outgoing port): GigabitEthernet1/0
```

Quelle version d'IOS est utilisée sur le routeur du FAI?

Version 12.2(28)

```
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
```

f. Exécutez la commande **ping 10.0.0.49** .

```
HQ-Edge#ping 10.0.0.49

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.49, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

g. Exécutez la commande **show arp**.

Quelle est l'adresse MAC de l'interface du routeur du **FAI** qui est connecté à **HQ-Edge**?

l'adresse MAC de l'interface du routeur du FAI qui est connecté à HQ-Edge est : 0060.2FE1.903B

```
HQ-Edge#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.49               0   0060.2FE1.903B  ARPA   GigabitEthernet0/0/0
Internet  10.0.0.50               -   0000.0C99.CB04  ARPA   GigabitEthernet0/0/0
HQ-Edge#
```

h. Fermez HQ-Edge et quittez l'armoire de brassage.

Étape 2: Collectez les informations de connexion réseau sur les périphériques au siège.

a. À partir de 1-1, 1-2, 1-3, 1-4, FL-1P et HQ-Laptop-1, utilisez la commande ipconfig pour trouver leurs adresses IPv4 et leurs passerelles par défaut.

Appareil	Adresse IPv4	Passerelle par défaut
1-1	192.168.10.2	192.168.10.1
1-2	192.168.10.3	192.168.10.1
1-3	192.168.20.2	192.168.20.1
1-4	192.168.20.3	192.168.20.1
FL-1P	(Via DHCP sur réseau .50)	192.168.50.1
HQ-Laptop-1	192.168.50.3	192.168.50.1

b. Sur PC **1-1**, ouvrez l'**invite de commande**, puis saisissez la commande **arp -a**.

Quelle information s'affiche?

```
C:\>arp -a
No ARP Entries Found
```

c. Utilisez la commande **ping** pour envoyer une commande ping à **1-2**, **1-3**, **1-4**, **FL-1P** et **HQ-Laptop-1**.

d. Exécutez la commande **arp -a**.

Quelle information s'affiche?

```
Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```
PC1-1 à PC1-2

```
Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```
PC1-1 à PC1-3

```
Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```
PC1-1 à PC1-4

```
Ping statistics for 192.168.50.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```
PC1-1 à HQ-Laptop-1

Pourquoi les entrées de la table ARP ne contiennent-elles pas d'informations sur les périphériques des réseaux 192.168.20.0 et 192.168.50.0 alors que la commande ping a abouti?

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.10.1          000a.41ea.6b47        dynamic
  192.168.10.3          0002.4a8a.d20e        dynamic
```

Le protocole ARP fonctionne uniquement sur le réseau local (diffusion). Pour communiquer avec des appareils situés sur d'autres réseaux (comme le 20.0 ou 50.0), le PC envoie les données à l'adresse MAC de sa passerelle par défaut (le routeur). C'est donc l'adresse MAC de la passerelle qui apparaît, pas celle du destinataire final.

e. Pour trouver la route empruntée par un paquet pour atteindre le serveur DNS, saisissez la commande tracert 10.2.0.125.

Quelle information s'affiche?

```
C:\>tracert 10.2.0.125

Tracing route to 10.2.0.125 over a maximum of 30 hops:

  1    2 ms      0 ms      0 ms      192.168.10.1
  2    0 ms      0 ms      0 ms      10.0.0.49
  3    *         0 ms      0 ms      10.2.0.125

Trace complete.
```

Combien de routeurs, ou sauts, y a-t-il entre PC 1-1 et le serveur DNS?

Il y a 2 routeurs (sauts) entre le PC et le serveur.

Partie 3: Diagnostiquer les problèmes de connectivité

Dans cette section, vous allez utiliser diverses commandes et techniques de diagnostic. Vous utiliserez la commande nslookup pour interroger un serveur DNS et dépanner une base de données DNS. Vous diagnostiquerez ensuite l'échec d'un ping, mais l'accès web. Enfin, vous utiliserez la commande netstat pour détecter les ports à l'écoute sur le périphérique cible.

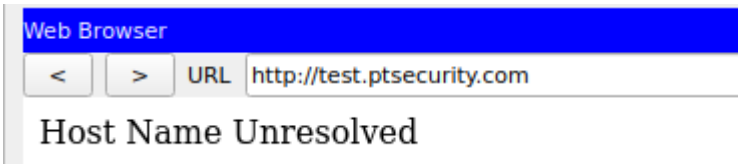
Étape 1: test d'une URL pour analyser un problème de connectivité.

a. Sur le PC 1-1, Fermez la fenêtre de Command Prompt et cliquez sur Web Browser.

b. Saisissez l'URL test.ptsecurity.com.

La page web s'affiche-t-elle? Si non, quel est le message?

Non. Message "Host Name Unresolved"



c. Entrez l'adresse IP**192.168.75.2**.

La page web s'affiche-t-elle?

OUi la page web s'affiche.

Pourquoi la page web s'affiche-t-elle en utilisant l'adresse IP, mais pas le nom de domaine?

Il s'agit d'un problème de DNS. Le serveur web fonctionne et est accessible via le réseau (IP), mais l'ordinateur n'arrive pas à traduire le nom "test.ptsecurity.com" en adresse IP.

Étape 2: utilisez la commande nslookup pour vérifier le service DNS.

a. Fermez **le navigateur internet**, et cliquez **Command Prompt**.

b. Saisissez la commande **ping test.ptsecurity.com**.

Quel est le message affiché?

Qu'indique le message?

```
C:\>ping test.ptsecurity.com
Ping request could not find host test.ptsecurity.com. Please check the name and try again.
C:\>
```

La requête Ping n'a pas pu trouver l'hôte.

Le PC ne peut pas résoudre le nom de domaine en adresse IP car le serveur DNS est injoignable ou ne connaît pas ce nom.

c. Saisissez la commande **nslookup test.ptsecurity.com**.

Quel est le message affiché?

```
Server: [10.2.0.125]
Address:  10.2.0.125
*** UnKnown can't find test.ptsecurity.com: Non-existent domain.
```

Quel serveur est le serveur DNS par défaut?

Le serveur DNS par défaut est : 10.2.0.125

```
Address:  10.2.0.125
```

e. Saisissez la commande **nslookup test.ptsecurity.com 192.168.99.3** et appuyez sur **Entrée**.

Remarque: la convergence de Packet Tracer peut prendre plusieurs secondes.

Quel est le message affiché?

```
C:\>nslookup test.ptsecurity.com 192.168.99.3

Server: [192.168.99.3]
Address:  192.168.99.3
DNS request timed out.
            timeout was 15000 milli seconds.

Server: [192.168.99.3]
Address:  192.168.99.3

Non-authoritative answer:
Name:   test.ptsecurity.com
Address:   192.168.75.2
```

À l'étape 2c, pourquoi le nom de domaine ne peut-il pas être résolu?

Le nom de domaine n'a pas pu être résolu à l'étape 2c parce que le serveur DNS par défaut (configuré automatiquement sur le PC, probablement 10.2.0.125) est en panne, mal configuré ou injoignable.

En spécifiant manuellement un autre serveur (le 192.168.99.3) à l'étape 2e, la résolution a fonctionné, ce qui prouve que le problème venait bien du premier serveur DNS interrogé et non du PC lui-même.

Étape 3: utilisez le résultat de la commande ping pour diagnostiquer les problèmes de connectivité.

a. Saisissez la commande **ping mail.cybercloud.com**.

Quel est le message affiché?

```
C:\>ping mail.cybercloud.com.
Ping request could not find host mail.cybercloud.com.. Please check the name and try again.
```

Quelles sont les informations indiquées par le message?

Ce message indique que le serveur DNS n'a pas réussi à trouver (résoudre) le nom de domaine demandé. Contrairement à un problème de connexion réseau (où l'on verrait une IP), ici l'ordinateur ne sait même pas quelle est l'adresse IP de destination.

b. Saisissez la commande **ping www.ptsecurity.com**.

Quel est le message affiché?

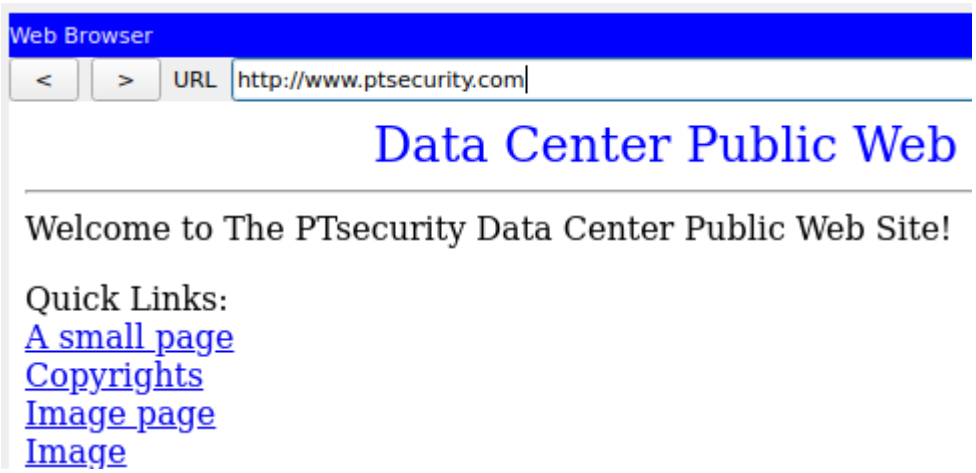
```
C:\>ping www.ptsecurity.com

Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: Destination host unreachable.
Reply from 10.0.0.3: Destination host unreachable.
Reply from 10.0.0.3: Destination host unreachable.
Reply from 10.0.0.3: Destination host unreachable.

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

Quelles sont les informations indiquées par le message?

Le DNS fonctionne pour ce site spécifique et le serveur web est accessible.

c. Fermez **l'invite de commande**, ouvrez le **navigateur web**, puis accédez à **www.ptsecurity.com**.

La page web s'affiche-t-elle?



Quelle conclusion pouvez-vous tirer?

L'accès Web (HTTP) fonctionne parfaitement pour le site `ptsecurity.com`

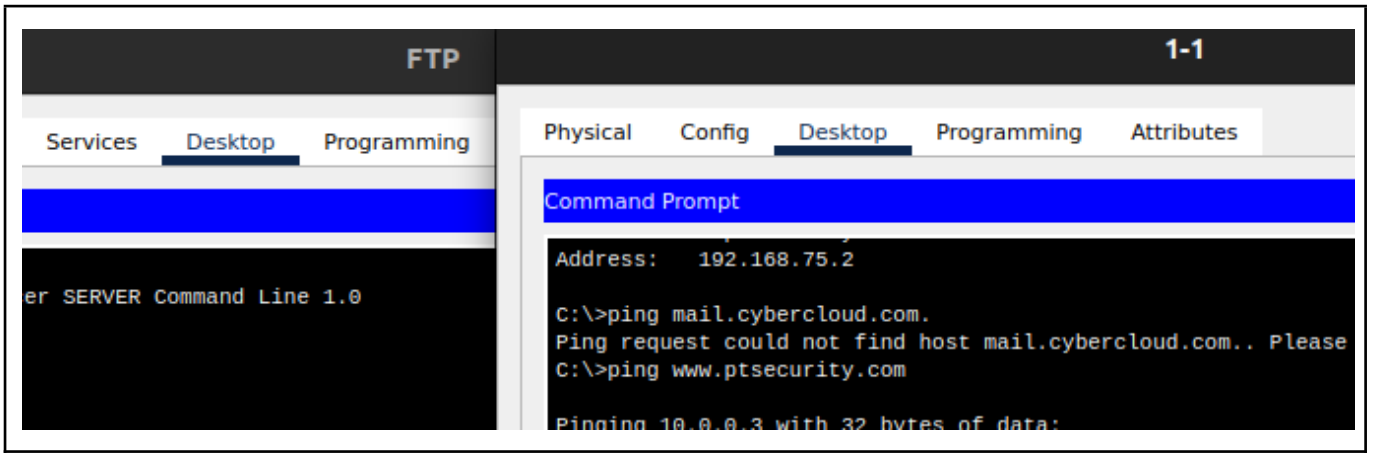
Étape 4: utilisez la commande netstat pour rechercher les ports actifs et en écoute.

a. Fermez le navigateur web et rouvrez l'invite de commande.

b. Au siège, cliquez sur l'armoire de brassage.

c. Dans le rack de droite, cliquez sur l'onglet Serveur FTP > Bureau > Invite de commandes.

d. Disposez les fenêtres d'invite de commande de PC 1-1 et du serveur FTP côte à côte.



e. Dans la fenêtre PC 1-1, saisissez la commande netstat.

Quel est le message affiché? Affiche-t-il des données?

Le message est `Active Connections`. Non, il n'affiche pas de données (la liste est vide) car il n'y a aucune connexion active pour le moment.

```
Active Connections

  Proto  Local Address          Foreign Address        State
```

g. Sur le serveur **FTP**, saisissez la commande **ipconfig** pour déterminer son adresse IP.

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::290:21FF:FE64:E9B9
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.75.2
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.75.1
```

h. À partir du **PC 1-1**, démarrez une session FTP avec le serveur FTP.

```
C:\>ftp 192.168.75.2
Trying to connect...192.168.75.2
Connected to 192.168.75.2
220- Welcome to PT Ftp server
Username:
```

i. Sur le serveur **FTP**, saisissez la commande **netstat**.

Quel est le message affiché? Y a-t-il de nouvelles informations?

"Invalid or non supported command"

Quel est le port d'écoute et quel est l'état de la connexion?

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.10.3:1028      192.168.75.2:21        CLOSING
```

Port d'écoute : 21,

État de la connexion : ESTABLISHED

j. Sur PC **1-1**, saisissez **bob** comme nom d'utilisateur.

k. Depuis le serveur **FTP**, saisissez la commande **netstat**.

Les informations affichées changent-elles?

Non rien n'a changer.

l. Sur **PC 1-1**, saisissez **cisco123** comme mot de passe.

m. À partir de **PC 1-1**, saisissez la commande **dir**.

```
ftp>dir

Listing /ftp directory from 192.168.75.2:
```

n. Depuis le serveur **FTP**, saisissez la commande **netstat**.

Qu'indique cette nouvelle entrée?

```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              CLOSED
  TCP    0.0.0.0:110            0.0.0.0:0              CLOSED
  TCP    0.0.0.0:8443           0.0.0.0:0              CLOSED
  TCP    192.168.75.2:21        192.168.10.3:1029      ESTABLISHED
```

o. À partir de **PC 1-1**, saisissez la commande **put Sample2.txt** et appuyez sur **Entrée**. Cela va charger le fichier Sample2.txt sur le serveur **FTP**.

```
Listing /ftp directory from 192.168.75.2:
ftp>put Sample2.txt

Writing file Sample2.txt to 192.168.75.2:
File transfer in progress...

[Transfer complete - 43 bytes]

43 bytes copied in 0.079 secs (544 bytes/sec)
```

p. Depuis le serveur **FTP**, entrer la commande **netstat**.

Les informations affichées changent-elles?

```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              CLOSED
  TCP    0.0.0.0:110            0.0.0.0:0              CLOSED
  TCP    0.0.0.0:8443           0.0.0.0:0              CLOSED
  TCP    192.168.75.2:21        192.168.10.2:1035      ESTABLISHED
C:\>
```

q. Attendez quelques secondes, puis saisissez à nouveau la commande **netstat**.

Les informations affichées changent-elles?

Oui, les informations changent de nouveau. La connexion de données se coupe car le fichier a fini d'être chargé sur le serveur.

r. Sur **PC 1-1**, saisissez la commande **quit**.

s. Depuis le serveur **FTP**, saisissez la commande **netstat**.

Les informations affichées changent-elles?

```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.10.2:1038      192.168.75.2:21        CLOSING
C:\>
```

t. Sur le PC **1-1,Fermez la fenêtre de**Command Prompt **et cliquez surWeb Browser**.

u. Accédez à **192.168.75.2**.

v. Depuis le serveur **FTP**, saisissez la commande **netstat**.

Les informations affichées changent-elles?

Oui, une nouvelle ligne s'ajoute. Elle correspond au trafic Web sur le port 80. On y voit l'adresse du serveur connectée à celle du PC 1-1 avec l'état ESTABLISHED, ce qui prouve que la page "Data Center Public Web" est en cours de chargement ou vient d'être chargée

Qu'est-ce que cette nouvelle entrée indique?

Cette ligne matérialise le lien réseau entre les deux machines. Elle prouve qu'un canal de communication est ouvert et que le PC et le serveur dialoguent activement.

VALIDATION :