Date : 13/11/23

Intervenant : Cédric Surquin.

Cisco

Lab 3-4 / Travail Pratique

Dépannage de connectivité IP à cause des ACLs

Date : 13/11/23 Intervenant : Cédric Surquin.

Objectifs

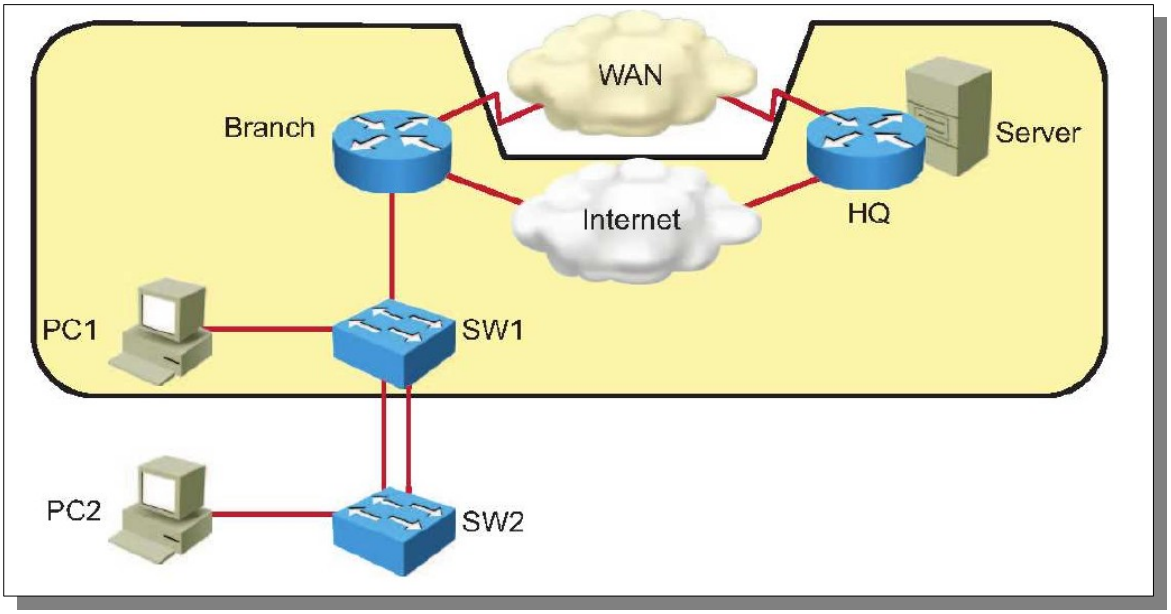
Dans ce travail pratique, vous allez identifier et traiter divers problèmes de connectivité réseau.

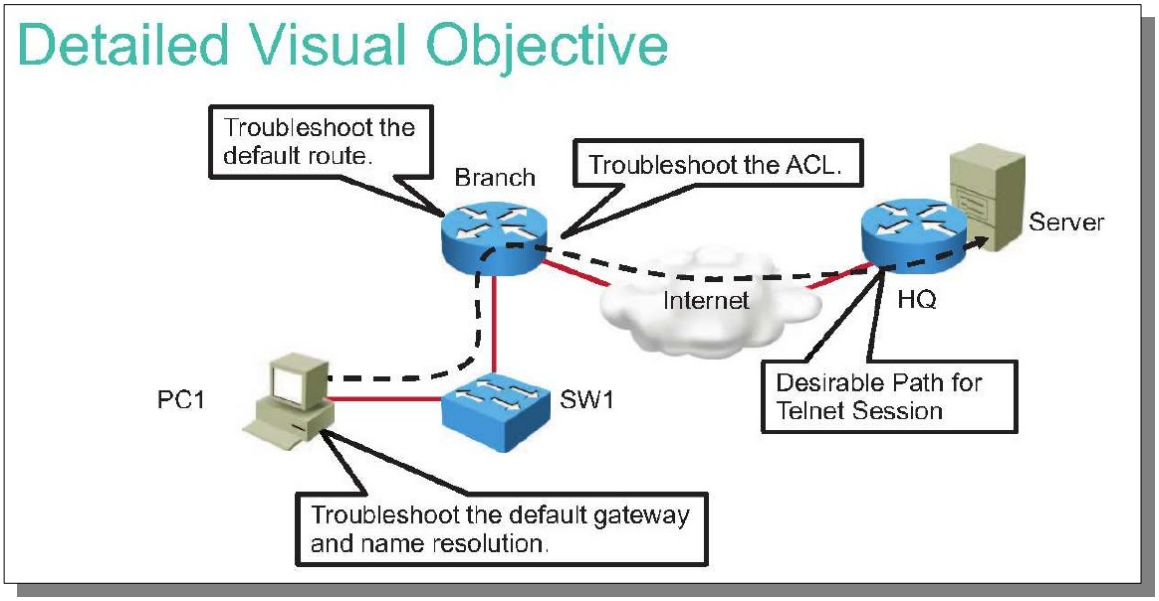
Vous aurez terminé cette activité lorsque vous aurez atteint les objectifs suivants :

1. Dépanner un problème de route par défaut
2. Dépanner un problème de configuration ACL
3. Dépanner un problème de passerelle par défaut
4. Dépanner un problème de résolution de nom

Date : 13/11/23 Intervenant : Cédric Surquin.

Visualisation des objectifs :





Date : 13/11/23 Intervenant : Cédric Surquin.

Ressources Requises :

Ci-joint les ressources requises pour ce TP

Liste de commandes :

Le tableau décrit les commandes utilisées dans cette activité et sont classées alphabétiquement afin que vous puissiez facilement localiser les informations dont vous avez besoin. Reportez-vous à cette liste si vous avez besoin d'aide lors de la configuration et la poursuite de cette activité.

Commandes	Descriptions
configure terminal	Entre dans le mode de configuration
ip access-list extended *ACL_name*	Définis une ACL et entre en mode de configuration de celle-ci.
ip route *network mask next-hop*	Configure une route statique
permit protocol source destination **eq** port	Ajoute une déclaration d'autorisation dans l'ACL, via un port
ping *ip_address*	Vérifie la connectivité IP.
show interfaces *interface*	Affiche le status et les statistiques d'une interface précise.
show ip access-lists	Affiche toutes les ACLs crée sur l'appareil
show ip interface	Affiche les détails de la configuration IP d'une interface
show ip route	Affiche la table de routage de l'appareil
telnet *ip_address [tcp_port]*	Initie une connexion distante via le protocole Telnet, en précisant potentiellement un port spécifique
traceroute *ip_address*	Trace les adresses IP

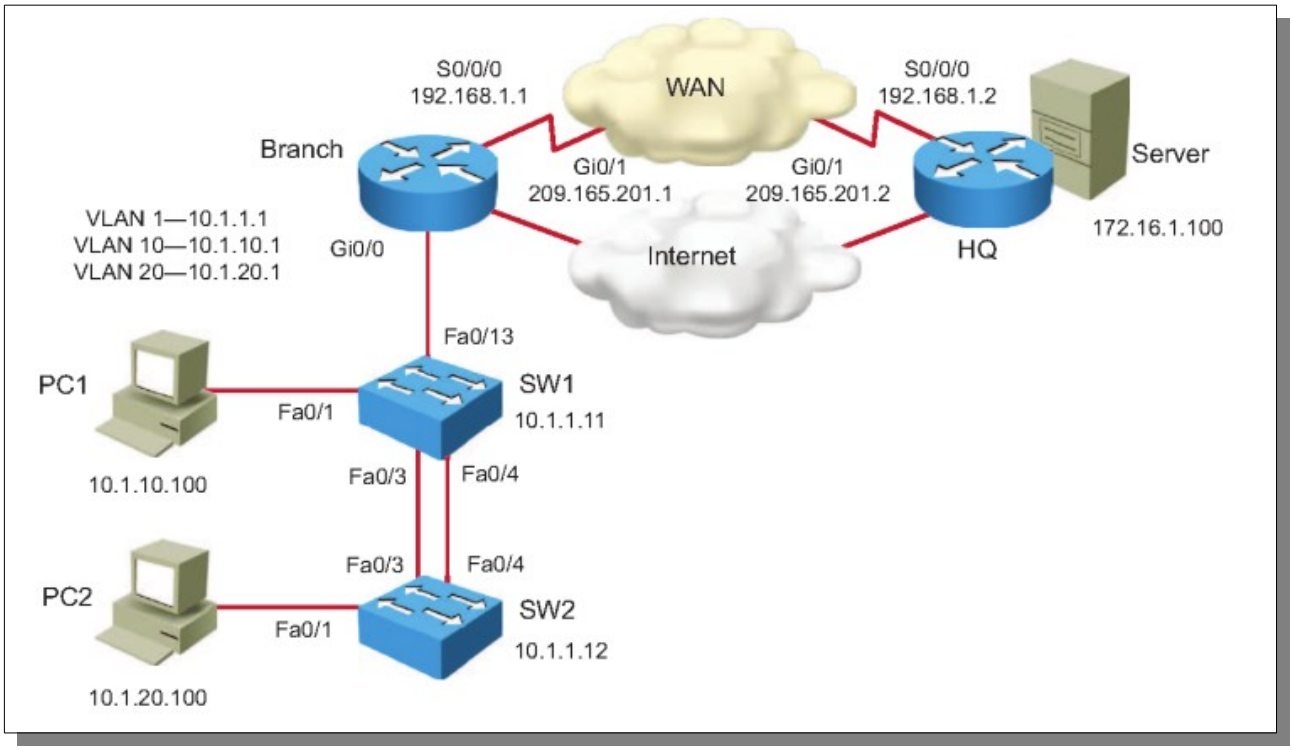
Date : 13/11/23 Intervenant : Cédric Surquin.

Aide à la mise en place :

Appareil	Périphériques
Branch	Cisco 2901 ISR
Headquarters	Cisco 2901 ISR
SW1	Catalyst 2960 Series Switch
SW2	Catalyst 2960 Series Switch
PC1	N’importe quel PC
PC2	N’importe quel PC

Topologie et Adressage IP

Les appareils sont connectés par le biais de leurs interfaces Ethernet. La capture ci-dessous illustre la topologie, les noms et les types d’interfaces, ainsi que les adresses IP qui sont utilisées dans ce lab.

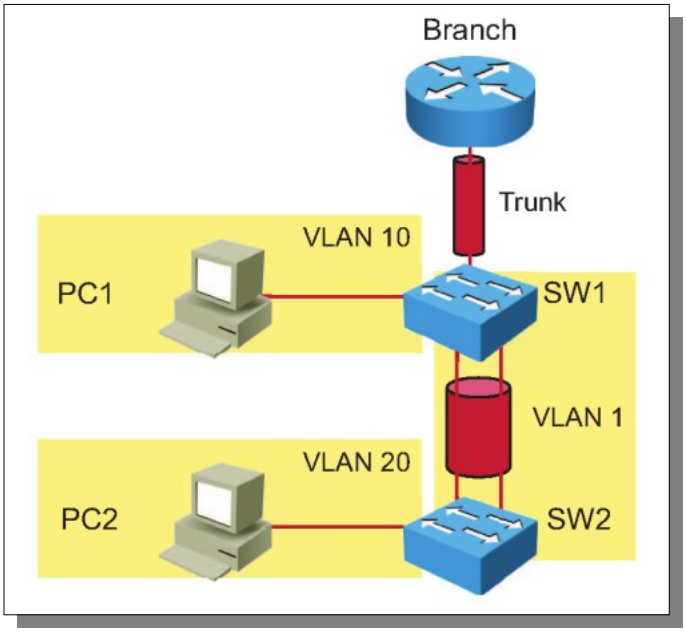


Appareils	Interfaces	Adresses IP
Branch	Gi0/0.1 (VLAN 1)	10.1.1.1/24
Branch	Gi0/0.10 (VLAN 10)	10.1.10.1/24
Branch	Gi0/0.20 (VLAN 20)	10.1.20.1/24

Branch	Gi0/1	209.165.201.1/27
Branch	Serial0/0/0	192.168.1.1/24
Branch	Loopback10	10.100.100.100/32
HQ	GigabitEthenet0/1	209.165.201.2/27
HQ	Serial0/0/0	192.168.1.2/24
HQ	Loopback0	172.16.1.100/24
SW1	VLAN 1	10.1.1.11/24
SW2	VLAN 1	10.1.1.12/24
PC1	Connection réseau local par interface Ethernet	10.1.1.100/24
PC2	Connection réseau local par interface Ethernet	10.1.1.101/24

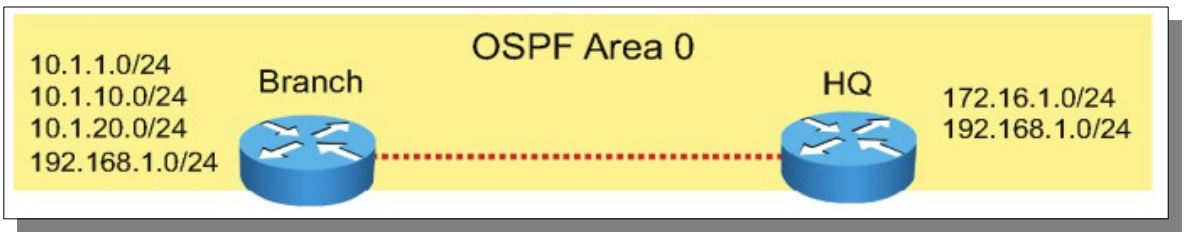
Configuration Trunk et VLAN

3 VLANs sont configurés sur les switchs. VLAN1 est utilisé à des fins de gestion, VLAN10 est utilisé pour la connexion de PC1, et VLAN20 est utilisé pour la connexion de PC2. Les liens entre SW1 et SW2 sont agrégés en un LAG utilisant la technologie Etherchannel, qui sert de port Trunk. SW1 et le routeur Branch communiquent eux aussi via un port Trunk. La figure ci-dessous vous expose cette topologie logique.



Routage IP

Comme le montre la capture ci-dessous, le protocole de routage OSPF est activé et configuré sur chaque routeur.



Date : 13/11/23 Intervenant : Cédric Surquin.

Tâche 1 : Dépanner une route par défaut

Vous avez été informé que l'utilisateur se trouvant dans le VLAN10 ne peut établir une connexion Telnet ou HTTP vers le serveur. En tant qu'ingénieur réseau, vous devez diagnostiquer et corriger le problème. Vous allez tout d'abord effectuer des tests sur le switch auquel l'utilisateur est censé pouvoir se connecter. L'ingénieur réseau senior vous confirme que le problème ne se trouve pas entre le switch SW1 et le routeur Branch. Vous avez également obtenu comme information que le nom du serveur doit pointer vers l'adresse IP 172.16.1.100

L'interface Serial 0/0/0 sur le routeur Branch est éteinte, et le restera durant la durée de ce travail pratique. Le routeur Branch ne doit avoir une connectivité qu'avec le routeur HQ à travers l'interface GigabitEthernet0/1.

Étape 1 :

Sur SW1, vérifiez que vous puissiez joindre le serveur à 172.16.1.100

```
SW1#ping 172.16.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

Le ping ne fonctionne pas. Le retour à l'écran nous indique un échec, que la destination n'est pas atteignable et qu'un PDU d'erreur est reçu.

Caractère	Description
!	Chacun de ces points indique la réception d'une réponse
.	Chacun de ces points indique que le serveur ne nous a pas retourné de réponse pour chaque sollicitation.
U	Un message PDU signalant une destination inatteignable a été reçu
Q	Indique que la destination est trop occupée pour répondre.
M	Ne peut pas fragmenter le paquet
?	Type de paquet inconnu
&	L'espérance de vie du paquet a été dépassé

Étape 2 :

Sur SW1, tracez le trafic jusqu'au serveur 172.16.1.100

```
SW1#traceroute 172.16.1.100
Type escape sequence to abort.
Tracing the route to Server (172.16.1.100)
  1 10.1.1.1 0 msec 8 msec 0 msec
  2 10.1.1.1 !H  *  !H
```

D'après la commande traceroute et son retour à l'écran, on peut voir que l'hôte est inatteignable et que le dernier saut/routeur à pouvoir nous répondre à pour IP 10.1.1.1

Cela nous indique qu'il y a un problème potentiel sur ce routeur avec IP 10.1.1.1
D'après le diagramme réseau, vous vous apercevez que l'adresse 10.1.1.1 se trouve sur le routeur Branch. Vous allez concentrer toute votre attention sur ce routeur Branch.

Caractère	Description
*	La sonde ne répond pas
A	Refusé par règle administrative (ex : une ACL)
Q	Destination trop occupée
I	Interrompu par l'utilisateur
U	Port inatteignable
H	Hôte inatteignable
N	Réseau inatteignable
P	Protocol inatteignable
T	Absence de réponse dans le délai imparti
?	Paquet de type inconnu

Étape 3 :

Sur le routeur Branch, vérifiez que l'interface GigabitEthenet0/1, qui se connecte à Internet, soit opérationnelle.

```
Branch#show interfaces GigabitEthernet 0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 5475.d08e.9ad9 (bia 5475.d08e.9ad9)
  Description: Link to HQ
  Internet address is 209.165.201.1/27
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
```

L'interface est pleinement opérationnelle.

Étape 4 :

Sur le routeur Branch, vérifiez qu'il y a une route vers le serveur 172.16.1.100
Il devrait y avoir une route statique configurée sur le routeur Branch

```
Branch#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is not set
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.1.1.0/24 is directly connected, GigabitEthernet0/0.1
L        10.1.1.1/32 is directly connected, GigabitEthernet0/0.1
C        10.1.10.0/24 is directly connected, GigabitEthernet0/0.10
L        10.1.10.1/32 is directly connected, GigabitEthernet0/0.10
C        10.1.20.0/24 is directly connected, GigabitEthernet0/0.20
L        10.1.20.1/32 is directly connected, GigabitEthernet0/0.20
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.201.0/27 is directly connected, GigabitEthernet0/1
L        209.165.201.1/32 is directly connected, GigabitEthernet0/1
```

Le routeur Branch ne dispose d'aucune route spécifique vers le serveur. De plus, il ne semble pas y avoir de route par défaut !

Étape 5 :

Sur le routeur Branch, configurez une route statique par défaut vers le prochain saut se trouvant l'adresse 209.165.201.2, puis vérifiez à nouveau la table de routage de l'appareil

```
Branch#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is 209.165.201.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 209.165.201.2
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.1.1.0/24 is directly connected, GigabitEthernet0/0.1
L        10.1.1.1/32 is directly connected, GigabitEthernet0/0.1
C        10.1.10.0/24 is directly connected, GigabitEthernet0/0.10
L        10.1.10.1/32 is directly connected, GigabitEthernet0/0.10
C        10.1.20.0/24 is directly connected, GigabitEthernet0/0.20
L        10.1.20.1/32 is directly connected, GigabitEthernet0/0.20
     209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.201.0/27 is directly connected, GigabitEthernet0/1
L        209.165.201.1/32 is directly connected, GigabitEthernet0/1
```

La route par défaut devrait apparaître en tant que route statique, et la passerelle de dernier recours devrait se trouver dans la table de routage du routeur Branch.

A ce stade, vous pouvez ping le serveur à 172.16.1.100 depuis le switch 1. Il devrait être réussi.

Tâche 2 : Dépannez une ACL

Dans cette tâche, vous allez continuer à diagnostiquer et dépanner en vérifiant si l'utilisateur du VLAN 10 peut atteindre le serveur via Telnet et ou HTTP. L'utilisateur de PC1 ne devrait être autorisé qu'à utiliser HTTP, Telnet, traceroute, et le ping vers et depuis le serveur à 172.16.1.100

Étape 1 :

Sur le switch SW1, utilisez Telnet pour vous connecter à 172.16.1.100 sur le port 23 et le port 80

```
SW1#telnet 172.16.1.100 23
Trying 172.16.1.100, 80 ...
% Destination unreachable; gateway or host down
SW1#telnet 172.16.1.100 80
Trying 172.16.1.100, 80 ...
% Destination unreachable; gateway or host down
```

Étape 2 :

Sur le switch1, tracez la connexion jusqu'à 172.16.1.100

```
SW1#traceroute 172.16.1.100
Type escape sequence to abort.
Tracing the route to Server (172.16.1.100)
  1 10.1.1.1 0 msec 8 msec 0 msec
  2 10.1.1.1 !A  *  !A
```

D'après la sortie de la commande, on peut voir que les paquets ayant l'adresse 10.1.1.1 sont refusés administrativement par le routeur. Il doit y avoir une ACL qui interdit le Telnet ainsi que le HTTP.

Étape 3 :

Sur le routeur Branch, examinez les interfaces pour voir si des ACLs leur sont assignées.

Notez qu'il existe une ACL, appelée « Outbound-ACL », dans le sens de sortie de l'interface GigabitEthernet0/1

```
Branch#show ip interface | include GigabitEthernet|access list
GigabitEthernet0/0 is up, line protocol is up
GigabitEthernet0/0.1 is up, line protocol is up
  Outgoing access list is not set
  Inbound  access list is not set
GigabitEthernet0/0.10 is up, line protocol is up
  Outgoing access list is not set
  Inbound  access list is not set
GigabitEthernet0/0.20 is up, line protocol is up
  Outgoing access list is not set
  Inbound  access list is not set
GigabitEthernet0/1 is up, line protocol is up
  Outgoing access list is Outbound-ACL
  Inbound  access list is not set
```

Étape 4 :

Sur le routeur Branch, examinez l'ACL appelée 'Outbound-ACL'.

```
Branch#show ip access-lists Outbound-ACL
Extended IP access list Outbound-ACL
    10 permit icmp any any
    20 permit tcp any any eq ftp
    30 permit tcp any any eq ftp-data
```

L'ACL autorise ici le trafic ICMP (le ping) d'où qu'il vienne et ou qu'il aille, puis permet le trafic utilisant le protocole de couche 4 TCP, mais uniquement pour les protocoles applicatifs de type FTP. Tous les autres protocoles sont implicitement refusés, ce qui explique que ni le Telnet ni le HTTP ne soient fonctionnels. Il faut rectifier cela.

Étape 5 :

Sur le routeur Branch, ajustez l'ACL Outbound-ACL pour autoriser le trafic Telnet (23), et HTTP (80), en TCP

Étape 6 :

Sur SW1, vérifiez que la connexion soit fonctionnelle en telnet via son port standard, puis via le port 80.

```
SW1#telnet 172.16.1.100
Trying 172.16.1.100 ... Open
HQ>exit
[Connection to 172.16.1.100 closed by foreign host]
SW1#


SW1#telnet 172.16.1.100 80
Trying 172.16.1.100, 80 ... Open
exit
```

Les 2 connexions sont fonctionnelles. À ce stade, il est plus que probable que l'utilisateur du VLAN 10 puisse atteindre le serveur via ces 2 protocoles.

Tâche 3 : Dépannez la passerelle par défaut et les paramètres de résolution de nom

Dans cette tâche, vous allez diagnostiquer la passerelle par défaut et le paramètre de résolution de nom de PC1, qui est connecté au VLAN10.

Sur le schéma réseau, vous voyez que la passerelle par défaut pour le VLAN 10 se trouve à 10.1.10.1. De plus, l'ingénieur réseau expérimenté a confirmé qu'aucun serveur DNS n'était paramétré sur le domaine. L'utilisateur va devoir faire une association manuelle entre le nom du serveur et son IP sur son post (fichier host)

Étape 1 :

Sur PC1, ouvrez l'invité de commande et vérifiez que le ping vers le serveur ne fonctionne pas.

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

PC1 ne peut pas joindre 172.16.1.100 via son nom

Sur un véritable ordinateur, il faudrait aller dans le fichier texte « host » de votre système d'exploitation et écrire une ligne mentionnant le nom du serveur, suivi d'une tabulation, et de l'adresse IP du serveur. Si vous travaillez sur Packet Tracer, nous allons ignorer ce problème de résolution de noms.

Étape 2 :

Sur PC1, traçons une tentative de connexion au serveur se trouvant à 172.16.1.100 nous devrions obtenir le résultat suivant :

```
C:\Windows\System32\drivers\etc>tracert Server
Tracing route to Server [172.16.1.100]
over a maximum of 30 hops:
  1  Windows7 [10.1.10.100]  reports: Destination host unreachable.
Trace complete.
C:\Windows\System32\drivers\etc>
```

Cela ne fonctionne pas. Enquêtons sur la configuration de PC1

Étape 3 :

Utilisons la commande ipconfig sur l'invité de commande de PC1 et vérifions la configuration de la passerelle par défaut.

```
C:\Windows\System32\drivers\etc>ipconfig
Windows IP Configuration
Ethernet adapter LAB:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::dc6d:98e9:82b7:d637%13
   IPv4 Address. . . . . . . . . . . : 10.1.10.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.10.10
<output omitted>
```

La passerelle par défaut n'est pas correctement configurée, il faut la redéfinir sur 10.1.10.1 plutôt que 10.1.10.10

Étape 4 :

Faites une nouvelle tentative de ping depuis l'invité de commande PC1, celui-ci doit désormais fonctionner.

```
C:\Windows\System32\drivers\etc>ping Server
Pinging Server [172.16.1.100] with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time=2ms TTL=254
Reply from 172.16.1.100: bytes=32 time=1ms TTL=254
Reply from 172.16.1.100: bytes=32 time=1ms TTL=254
Reply from 172.16.1.100: bytes=32 time=1ms TTL=254
Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Windows\System32\drivers\etc>
```

FIN DE CE TRAVAIL PRATIQUE