23/08/2024

Atelier 00 – activité 4 - Configuration des protocoles CDP et LLDP

**Document de l’atelier :**

[Bloc2\_sem3-4\_Atelier-00-activite-1\_Inter-VLAN\_Routing Challenge.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-1_Inter-VLAN_Routing%20Challenge.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-2\_Découverte-NAT-RIP-01.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-2_Découverte-NAT-RIP-01.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-3-Map-a-Network-Using-CDP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-3-Map-a-Network-Using-CDP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-4-Configure-CDP-and-LLDP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-4-Configure-CDP-and-LLDP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-5-Configure-and-Verify-NTP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-5-Configure-and-Verify-NTP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-6-reconstruction-reseau.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-6-reconstruction-reseau.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-7-Syslog-NTP-and-SSH-debut .pka](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-7-Syslog-NTP-and-SSH-debut%20.pka)

[Bloc2\_sem3-4\_Atelier-00-activite-8-Troubleshoot-VTP-and-DTP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-8-Troubleshoot-VTP-and-DTP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-9-SSH-sur-routeur-et-switch.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-9-SSH-sur-routeur-et-switch.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-10-authentification.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-10-authentification.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-11-authentification.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-11-authentification.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-12-Data-Center-Exploration-Physical-Mode.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-12-Data-Center-Exploration-Physical-Mode.docx)

Table des matières

[1. Topologie 2](#_Toc176817681)

[2. Table d’adressage 2](#_Toc176817682)

[3. Objectifs 2](#_Toc176817683)

[4. Contexte/Scénario 3](#_Toc176817684)

[5. Ressources requises 3](#_Toc176817685)

[6. Câblez le réseau conformément à la topologie. 4](#_Toc176817686)

[7. Configurez les paramètres de base des périphériques pour les commutateurs. 4](#_Toc176817687)

[8. Configurez les paramètres de base des périphériques pour les routeurs. 6](#_Toc176817688)

[9. Détection réseau à l’aide du protocole LLDP 14](#_Toc176817689)

# Topologie

Une image contenant texte, diagramme, ligne, capture d’écran

Description générée automatiquement

# Table d’adressage

|  |  |  |  |
| --- | --- | --- | --- |
| **Appareil** | **Interface** | **Adresse IP** | **Masque de sous-réseau** |
| Passerelle | FA0/0 | 192.168.NumUTI.254 | 255.255.255.0 |
| SE2/0 | 209.165.200.226 | 255.255.255.252 |
| ISP | Se0/1/0 (ETCD) | 209.165.200.225 | 255.255.255.252 |

# Objectifs

Partie 1 : Créer le réseau et configurer les paramètres de base des périphériques

Partie 2 : Détection réseau à l’aide du protocole CDP

Partie 3 : Détection réseau à l’aide du protocole LLDP

# Contexte/Scénario

CDP (Cisco Discovery Protocol) est un protocole propriétaire de Cisco conçu pour la détection réseau. Il s’exécute au niveau de la couche liaison de données. Il peut partager des informations, telles que les noms des périphériques et les versions IOS, avec d’autres périphériques Cisco connectés physiquement.

LLDP (Link Layer Discovery Protocol) est un protocole ouvert utilisé sur la couche liaison de données à des fins de détection réseau. Il est principalement utilisé avec les périphériques du réseau local. Les périphériques réseau annoncent des informations, telles que leurs identités et fonctionnalités, à leurs voisins.

Dans le cadre de ce TP, vous devrez documenter les ports connectés à d’autres commutateurs en utilisant les protocoles CDP et LLDP. Vous devrez également activer ou désactiver ces protocoles de détection suivant les besoins et analyser les résultats obtenus.

**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). Les commutateurs utilisés sont des modèles Cisco Catalyst 2960 équipés de Cisco IOS version 15.0(2) (image lanbasek9). D’autres routeurs, commutateurs 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**: vérifiez que la mémoire des routeurs et des commutateurs a été effacée et qu’aucune configuration de démarrage n’est présente.

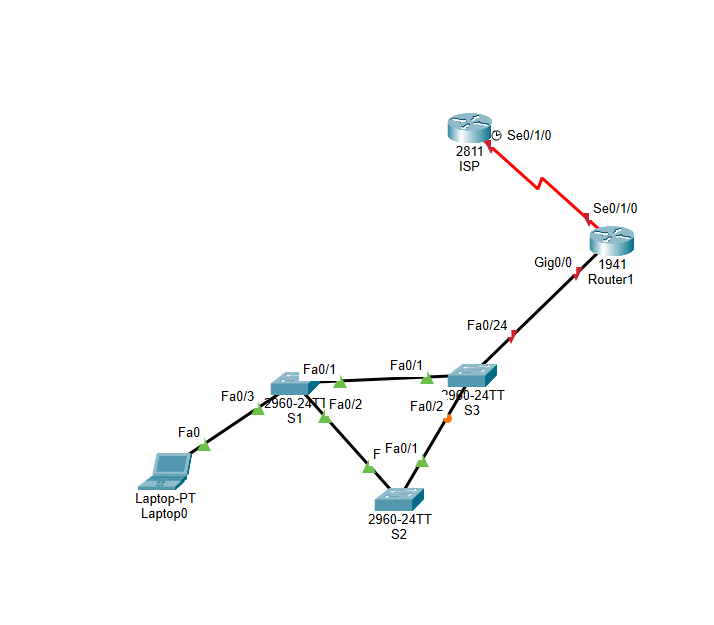
# Ressources requises

* 1 routeur Cisco 2811 servant à l’ISP, dans un nuage distant.
* 1 routeur (Cisco 1941 équipé de Cisco IOS version 15.2(4)M3 image universelle ou similaire)
* 3 commutateurs (Cisco 2960 équipés de Cisco IOS version 15.0(2) image lanbasek9 ou similaire)
* Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
* Câbles Ethernet conformément à la topologie

**Créer le réseau et configurer les paramètres de base des périphériques**

Dans la première partie, vous allez mettre en place la topologie du réseau, et configurer les paramètres de base sur le routeur et les commutateurs.

# Câblez le réseau conformément à la topologie.



# Configurez les paramètres de base des périphériques pour les commutateurs.

Accédez au périphérique par la console et activez le mode d’exécution privilégié.

Passez en mode de configuration.

Désactivez la recherche DNS pour empêcher le commutateur d’essayer de traduire les commandes saisies comme s’il s’agissait de noms d’hôtes.

Configurez le nom d’hôte conformément à la topologie.

Vérifiez que les ports de commutateur auxquels sont connectés des câbles Ethernet sont activés.

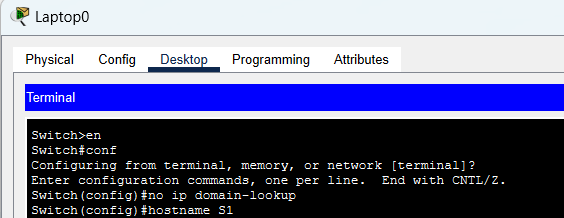
Enregistrez la configuration en cours dans le fichier de configuration initiale.

Switch>en

Switch#conf

Switch(config)#no ip domain-lookup

Switch(config)#hostname S1

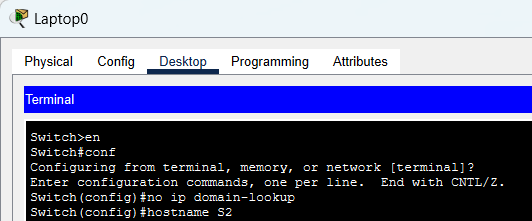


Switch>en

Switch#conf

Switch(config)#no ip domain-lookup

Switch(config)#hostname S2

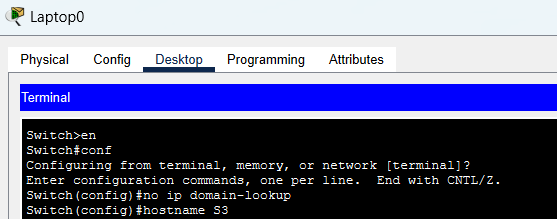


Switch>en

Switch#conf

Switch(config)#no ip domain-lookup

Switch(config)#hostname S3

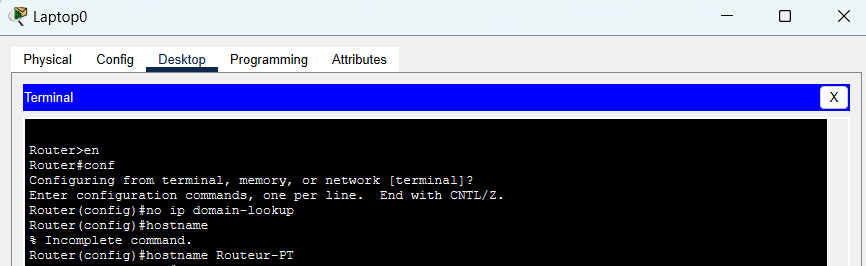


Router>en

Router#conf

Router(config)#no ip domain-lookup

Router(config)#hostname Routeur-PT



Routeur-PT(config)#interface g0/0

Routeur-PT(config-if)#no shutdown

Routeur-PT(config-if)#exit

Routeur-PT(config)#interface S0/1/0

Routeur-PT(config-if)#no shutdown

Router>en

Router#conf

Router(config)#no ip domain-lookup

Router(config)#hostname ISP

ISP(config)#interface s0/1/0

ISP(config-if)#no shutdown

# Configurez les paramètres de base des périphériques pour les routeurs.

Accédez au périphérique par la console et activez le mode d’exécution privilégié, puis passer en mode de configuration.

Copiez et collez les configurations suivantes dans les routeurs, en les adaptant à votre cas personnel.

**FAI :**

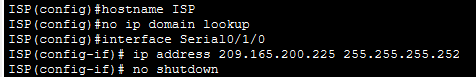
hostname ISP

no ip domain lookup

interface Serial0/1/0

ip address 209.165.200.225 255.255.255.252

no shutdown



**Gateway :**

hostname Gateway

no ip domain lookup

interface g0/0

ip address 192.168.33.254 255.255.255.0

ip nat inside

no shutdown

interface Serial0/1/0

ip address 209.165.200.226 255.255.255.252

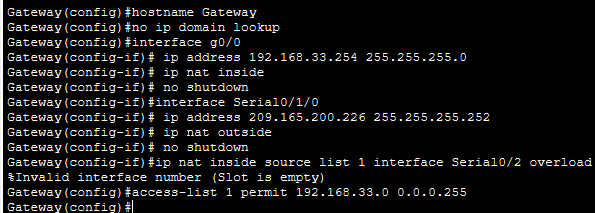
ip nat outside

no shutdown

ip nat inside source list 1 interface Serial0/2 overload

access-list 1 permit 192.168.33.0 0.0.0.255

Enregistrez la configuration en cours dans le fichier de configuration initiale.



* 1. **Détection réseau à l’aide du protocole CDP**

Sur les périphériques Cisco, le protocole CDP est activé par défaut. Vous l’utiliserez pour détecter les ports qui sont actuellement connectés.

Sur le routeur Gateway, entrez la commande **show cdp** en mode d’exécution privilégié afin de vérifier. Faire ressortir les éléments probants.

Les éléments probants de la commande show cdp sur le routeur Gateway :

Envoi de paquets CDP, Le routeur envoie des paquets CDP toutes les 60 secondes pour découvrir les appareils voisins.

Valeur de holdtime, Les informations sur le routeur sont conservées par les appareils voisins pendant 180 secondes avant d'être considérées comme obsolètes.

CDPv2 activé, La version 2 de CDP est activée, offrant des fonctionnalités supplémentaires pour la découverte des appareils.

À quelle fréquence les paquets CDP sont-ils envoyés ? Prouvez-le.

Les paquets CDP sont envoyés toutes les 60 secondes. On peut le voir grâce a la commande show cdp .



\_\_\_\_\_\_\_\_\_\_\_

Si le protocole CDP est désactivé sur le routeur Gateway, activez-le en exécutant la commande **cdp run** en mode de configuration globale.

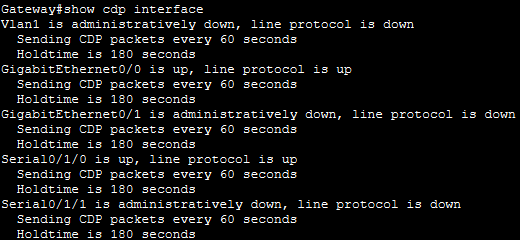
Gateway(config)# **cdp run**

Gateway(config)# **end**



Exécutez la commande **show cdp interface** pour répertorier les interfaces qui participent aux annonces CDP.

Gateway# **show cdp interface**



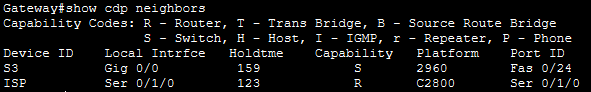
Montrer combien d’interfaces participe à l’annonce CDP ? Quelles sont les interfaces actives ?

On peut voir sur la capture d’écran qu’il y a 4 interfaces qui participent à l’annonce CDP qui sont g0/0, g0/1, s0/1/0 et s0/1/1.

Les deux interfaces qui sont active sont s0/1/0 et g0/0 car il sont en "line protocol is up" en français est "le protocole de ligne est actif".

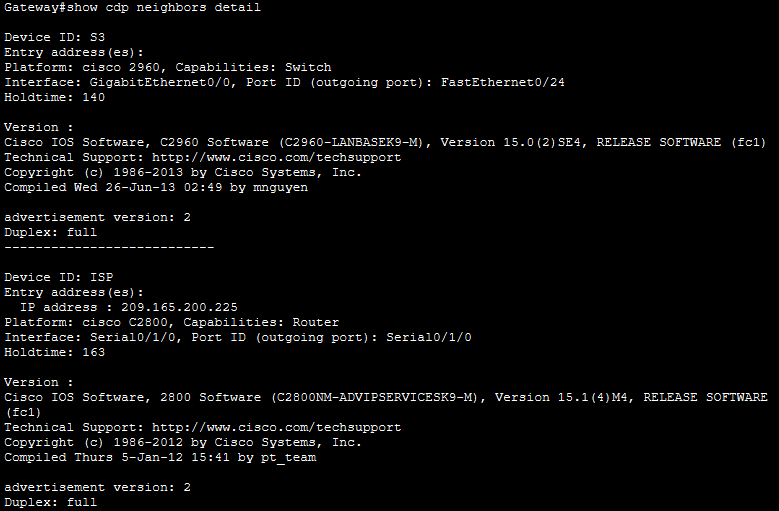
Exécutez la commande **show cdp neighbors** pour déterminer les voisins CDP.

Gateway# **show cdp neighbors**



Pour plus d’informations sur les voisins CDP, exécutez la commande **show cdp neighbors detail.**

Gateway# **show cdp neighbors detail**



Que pouvez-vous apprendre du périphérique ISP et du commutateur S3 à partir de la sortie de la commande **show cdp neighbors detail** ? Qui peut en avoir besoin ?Y-a-t-il des risques associés à cette connaissance, analyser chacun des éléments découverts ?

À partir de la sortie de la commande `show cdp neighbors detail`, on apprend que le périphérique ISP est un routeur Cisco C2800 avec l'adresse IP 209.165.200.225 et la version logicielle 15.1(4)M4, tandis que le commutateur S3 est un Cisco 2960 connecté en GigabitEthernet, sans adresse IP indiquée, et utilisant la version logicielle 15.0(2)SE4.

Ces informations peuvent être utiles aux administrateurs réseau pour la gestion et la configuration, a sécurité pour évaluer les risques, et aux hackers malveillants pour planifier des attaques. Les risques incluent l'exposition d'adresses IP pour des attaques DDoS, l'exploitation de vulnérabilités sur les versions IOS connues, la cartographie du réseau via les interfaces et ports, et l'utilisation de détails de configuration pour perturber le réseau.

Le protocole CDP doit donc être activé uniquement en cas de réel besoin pour l'administration du réseau.

À partir de la sortie de la commande show cdp neighbors detail, nous pouvons apprendre plusieurs choses sur les périphériques voisins, notamment l'ISP et le commutateur S3. Voici une analyse détaillée :

Configurez l’interface SVI sur S3. Utilisez une adresse IP disponible sur le réseau 192.168.NumUTI.0/24. Configurez 192.168.NumUTI.254 comme passerelle par défaut.

S3(config)# **interface vlan 1**

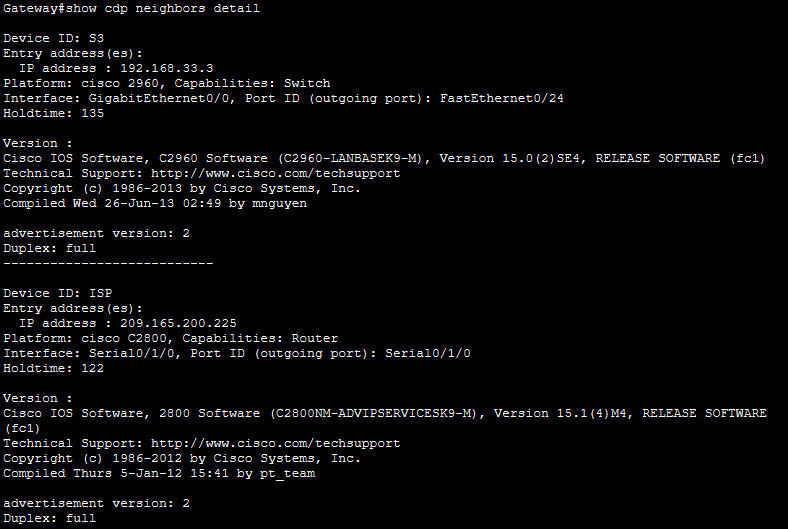
S3(config-if)# **ip address 192.168.33.3 255.255.255.0**

S3(config-if)# **no shutdown**

S3(config-if)# **exit**

S3(config)# **ip default-gateway 192.168.33.254**

Exécutez la commande **show cdp neighbors detail** sur le routeur Gateway. Quelles sont les autres informations disponibles ?



Les autres informations disponibles sont pour S3 l’adresse IP spécifiée 192.168.33.3 et pour ISP l’adresse IP spécifiée 209.165.200.225.

Également pour le holdtime c’est pour S3 135 secondes (dans la première sortie, c'était 140 secondes). Et pour ISP 122 secondes (dans la première sortie, c'était 163 secondes).

Pour des raisons de sécurité, il est conseillé de désactiver le protocole CDP sur une interface en contact avec un réseau externe. Exécutez la commande **no cdp enable** en mode de configuration d’interface sur l’interface s0/1/0 du routeur Gateway.

Gateway(config)# **interface s0/1/0**

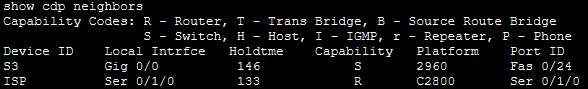
Gateway(config-if)# **no cdp enable**

Gateway(config-if)# **end**

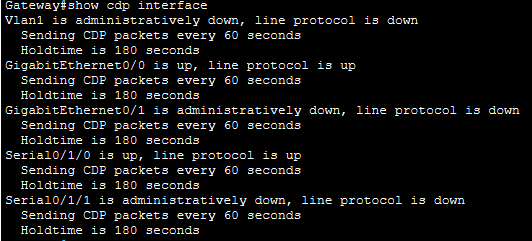
****

Pour vérifier que le protocole CDP a bien été désactivé sur l’interface s0/1/0, exécutez la commande **show cdp neighbors** ou **show cdp interface**. Il se peut que vous deviez attendre l’expiration du délai de rétention. Le délai de rétention équivaut à la période pendant laquelle les périphériques réseau conservent les paquets CDP avant de les supprimer. Montrer que vous obtenez bien ce que vous souhaitiez obtenir.

Gateway# **show cdp neighbors**



Est-ce que l’interface s0/1/0 du routeur Gateway possède toujours des contiguïtés avec les autres interfaces ? On pourra avantageusement utiliser la commande « **show cdp interface »,** pour répondre à la question. Montrer le résultat obtenu en y apposant votre analyse.



L'interface sl0/1/0 du routeur Gateway est active, comme l'indique la sortie de la commande show cdp interface, où il est précisé que l'interface est "up" et que le protocole de ligne est également "up" donc oui l’interface s0/1/0 possède toujours des contiguïtés. Cela signifie qu'elle peut envoyer et recevoir des paquets CDP, confirmant ainsi sa connectivité avec d'autres appareils. En revanche, d'autres interfaces, comme Vlan1, G0/1 et s0/1/1, sont désactivées, ce qui les empêche de communiquer. Par conséquent, l'interface s0/1/0 maintient une contiguïté avec l'interface correspondante de l'appareil ISP, permettant une communication fonctionnelle.

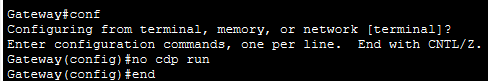
Haut du formulaire

Pour désactiver le protocole CDP globalement, exécutez la commande **no cdp run** en mode de configuration globale.

Gateway# **conf t**

Gateway(config)# **no cdp run**

Gateway(config)# **end**



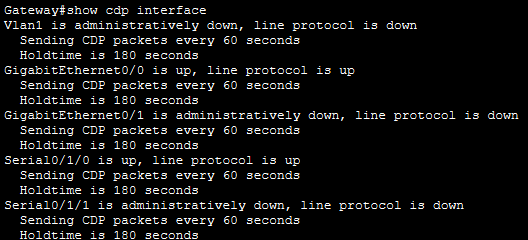
Quelle(s) commande(s) allez-vous utiliser pour vérifier que le protocole CDP a bien été désactivé ?

La commande que j'ai utilisée pour vérifier que CDP était désactivé est `show cdp`. On peut également utiliser `show cdp interface`.

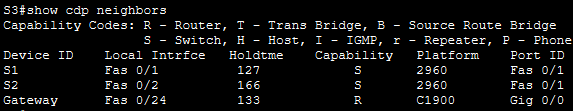
Activez le protocole CDP à l’échelle du routeur Gateway. Sur combien d’interfaces le protocole CDP est-il activé ? Quelles sont les interfaces où le protocole CDP est désactivé ?

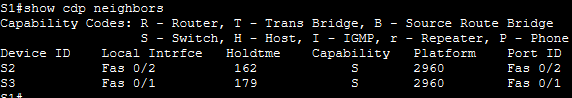


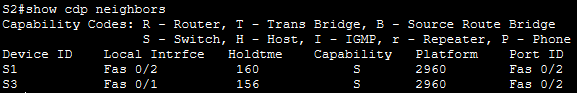


On peut voir qu'il y a 2 interfaces sur lesquelles CDP est activé et 3 sur lesquelles il est désactivé. Les interfaces activées sont G0/0 et s0/1/0, et celles désactivées sont Vlan1 (administratively down, line protocol is down), G0/1 (administratively down, line protocol is down) et s0/1/1 (administratively down, line protocol is down).

Accédez à tous les commutateurs par la console et utilisez les commandes CDP pour déterminer les ports Ethernet connectés à d’autres périphériques. Vous trouverez, ci-dessous, un exemple des commandes CDP pour le commutateur S3.







S3# **show cdp neighbors**

Capability Codes : R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,

D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID Local Intrfce Holdtme Capability Platform Port ID

Gateway Fas 0/5 143 R B S I CISCO1941 Gig 0/1

S2 Fas 0/2 173 S I WS-C2960- Fas 0/4

S1 Fas 0/4 171 S I WS-C2960- Fas 0/4

# Détection réseau à l’aide du protocole LLDP

Il se peut que le protocole LLDP soit activé par défaut sur les périphériques Cisco. Vous l’utiliserez pour détecter les ports qui sont actuellement connectés.

Sur le routeur Gateway, entrez la commande **show lldp** en mode d’exécution privilégié.

Gateway# **show lldp**

% LLDP is not enabled



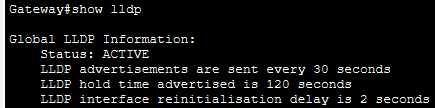
Si le protocole LLDP est désactivé, entrez la commande **lldp run** en mode de configuration globale.

Gateway(config)# **lldp run**

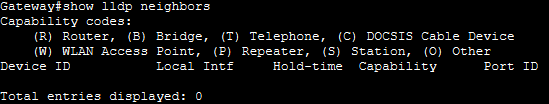
****

Utilisez la commande **show lldp** pour vérifier que le protocole LLDP est bien activé sur le routeur Gateway. Montrer que c’est bien le cas.

Gateway# **show lldp**

****

Exécutez la commande **show lldp neighbors**. Quels sont les périphériques voisins du routeur Gateway ?



La commande show lldp neighbors indique qu'il n'y a actuellement aucun périphérique voisin détecté sur le routeur Gateway, comme le montre la ligne "Total entries displayed: 0". Cela peut signifier qu'aucun appareil compatible LLDP n'est connecté ou que LLDP n'est pas activé. Pour vérifier les périphériques voisins, il est recommandé d'utiliser la commande show cdp neighbors.

S’il n’y a aucun voisin LLDP pour le routeur Gateway, activez le protocole LLDP sur les commutateurs et sur ISP. Exécutez la commande **lldp run** en mode de configuration globale sur les périphériques.

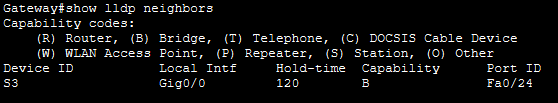
S1(config)# **lldp run**

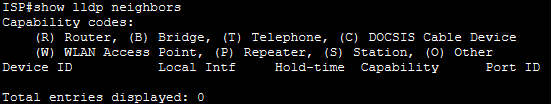
S2(config)# **lldp run**

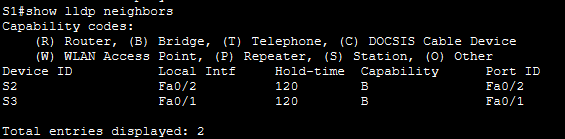
S3(config)# **lldp run**

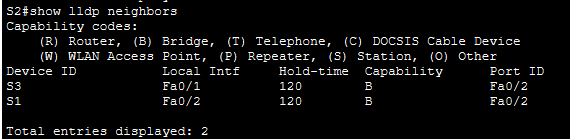
ISP(config)# **lldp run**

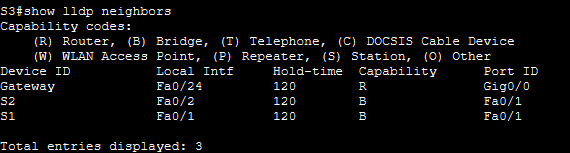
Exécutez la commande **show lldp neighbors** sur les commutateurs et sur le routeur afin de répertorier les ports compatibles avec LLDP. Le résultat pour le routeur Gateway est affiché ci-dessous. Quel est-il pour les autres actifs du réseau ?











Gateway# **show lldp neighbors**

Capability codes:

(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device

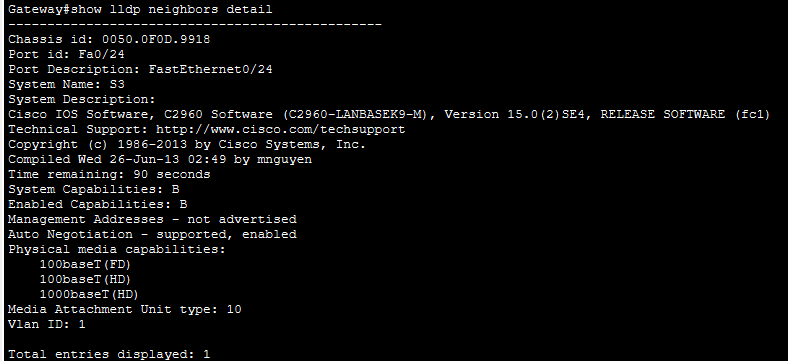
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID Local Intf Hold-time Capability Port ID

S3 Gi0/1 120 B Fa0/5

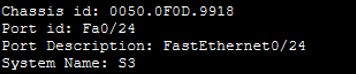
Total entries displayed: 1

Exécutez la commande **show lldp neighbors detail** sur le routeur Gateway.



Quel est le port utilisé sur le commutateur S3 pour établir la connexion au routeur Gateway ?

Le port utilisé sur le commutateur S3 pour établir la connexion au routeur Gateway est FastEthernet0/24.



Quel est selon vous le protocole le plus intéressant à utiliser pour les administrateurs réseau ? Quel est selon vous celui qui est le plus facile à gérer en termes de sécurité du réseau ?

Protocole le plus intéressant : Le protocole CDP est le plus intéressant car il fournit des informations détaillées sur les périphériques voisins, facilitant ainsi la gestion et le dépannage des réseaux Cisco.

Protocole le plus facile à gérer en termes de sécurité : LLDP est considéré comme plus facile à gérer en matière de sécurité, car il est un standard ouvert, compatible avec divers équipements, et permet de configurer des paramètres de sécurité pour réduire les risques.