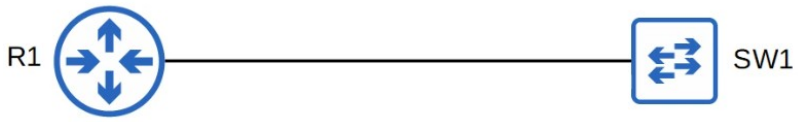
Cours 36 : CDP & LLDP

Dans ce cours nous verrons ce que sont les deux couches 2 de découvertes de protocoles qui sont CDP et LLDP.
Nous ferons une introduction à la couche 2 de découverte de protocole, puis nous verrons en détail comment fonctionne les protocole Cisco Discovery Protocol (CDP) et Link Layer Discovery Protocol (LLDP)

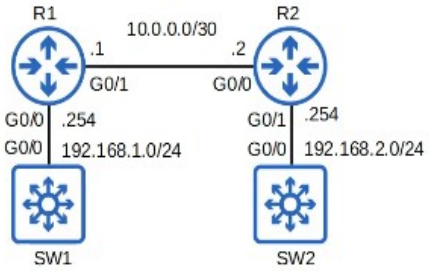
La couche 2 de découverte des protocoles comme CDP et LLDP servent à partager et découvrir des informations à propos des appareils voisins (connectés).
Il sont appelés couche 2 de découverte de protocole puisque les protocoles eux mêmes fonctionnent avec la couche couche 2 et n'utilisent pas d'adresse IP.
En voyant des captures Wireshark on pourra observer qu'il n'est pas présent de paquets IP à l'intérieur de la trame envoyés par CDP et LLDP.
Bien qu'ils se soit des protocoles de couche 2 de découverte de protocoles, ils peuvent être utilisés pour partager des informations de couche 3 comme les adresses IP. Les informations partagés incluent les nom d'hôtes, les adresses IP, les types d'appareils, etc..
CDP est un protocole propriétaire Cisco développé par Cisco pour les appareils Cisco. donc si le réseau utilisé seulement des appareils Cisco CDP est adapté, par contre si le réseau est composé de plusieurs vendeurs comme Cisco, Juniper, Palo Alto, il faudra utiliser le protocole : LLDP.
LLDP est un protocole de l'industrie standard, IEEE 802.1AB.
Puisque ces protocoles partagent des informations à propos des appareils du réseau, ils peuvent être considérés comme risqués en sécurité et ne sont pas souvent utilisés, les administrateurs ou ingénieurs réseau peuvent décider s'ils veulent les utiliser ou non dans le réseau.
Pour comprendre comment ces protocoles fonctionnent voici deux appareils R1 et SW1 :



R1 envoie de manière périodique des trames à SW1 en lui donnant des informations comme le nom du routeur R1, le type d'appareils, l'ID d'interface, l'adresse IP, etc...
SW1 de même et envoie aussi périodiquement des trames à R1. A noter que SW1 n'envoie pas d'informations comme l'adresse IP à R1 puisqu'il s'agit d'un Switch son interface n'a pas d'adresse IP.

Voyons plus en détail le fonctionnement de CDP.
CDP est donc un protocole Cisco propriétaire, il est activé par défaut sur les appareils Cisco (Routeurs, Switchs, les pare feu, les téléphones IP, etc..).
Les messages CDP sont envoyés périodiquement en multicast à l'adresse MAC 0100 0CCC CCCC
Puisque les messages utilisent une adresse MAC il faudra penser au message redirigés à plusieurs appareils mais en vérité ça n'est pas le cas. Lorsqu'un appareil reçoit un message CDP il procède donc le message mais ne le repartage pas aux autres appareils. Donc ça n'est que les appareils connectés directement qui sont des voisins CDP.
Par défaut les messages CDP sont envoyés toutes les 60 secondes à toutes les interfaces actives.
Ce sont des messages qui contiennent des informations comme le hostname, l'adresse IP, etc...
Lorsque l'appareil reçoit ces messages CDP depuis l'appareil voisin il ajoute une entrée de l'appareil dans sa table de voisin.
Si un voisin est déconnecté il y a un temps d'attente de 180 secondes, puis si le voisin n'est plus détecté il est supprimé de la table de voisins CDP.

Cela fait que les tables de voisins CDP n'ont pas d'entrées d'anciens voisins qui ne sont plus existants.
Il y a deux versions de CDP, Version 1 et Version 2, la version 2 est utilisé par défaut.
La version CDP Version 1 est ancienne donc il n'y a probablement pas besoin de l'utiliser.
Les principales différences entre les V1 et V2 est qu'il y a quelques fonctionnalités avancés comme l'habilité d'identifier un VLAN natif.
Pour démontrer l'utilisation de CDP nous utiliserons le réseau suivant :



Deux routeurs et deux commutateurs multicouches sont utilisés nous n'utilisons pas les fonctions de couches 3 sur les commutateurs.
Voici les commandes basiques à utiliser pour vérifier la configuration CDP :

```
R1#show cdp
R1#show cdp trafic
R1 show cdp interfaces
```

```
R1#show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is  enabled
R1#
R1#show cdp traffic
CDP counters :
        Total packets output: 105, Input: 112
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0,
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 105, Input: 112
R1#
```

```
R1#show cdp interface
GigabitEthernet0/0 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/2 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/3 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

 cdp enabled interfaces : 4
 interfaces up          : 2
 interfaces down        : 2
```

la commande `show cdp` permet d'afficher la fréquence de temps d'envois de messages CDP, il est de 60 secondes par défaut, et de 180 secondes de temps d'attente de réponse (holdtime)
Par défaut cette commande affiche aussi quelle version de CDP est utilisé, la version 2 est celle utilisé par défaut.
Il est à noter que si CDP n'est pas activé sur un appareil on recevra le message suivant :

```
R1#show cdp
% CDP is not enabled
R1#
```

La commande `show cdp traffic` permet d'afficher combien de paquets et d'avertissements CDP l'appareil a envoyé et reçu.
La commande `show cdp interface` permet d'afficher des informations basiques à propos de chacune des interfaces. Il est aussi possible de spécifier certaines interface en entrant la commande mais lorsque l'on entre la commande sans préciser l'interface, on reçoit des informations sur toutes les interfaces.
Sur le résultat de la commande de la capture d'écran on peut voir l'information « encapsulation ARPA », il s'agit d'un type d'encapsulation Ethernet connu comme Ethernet 2.

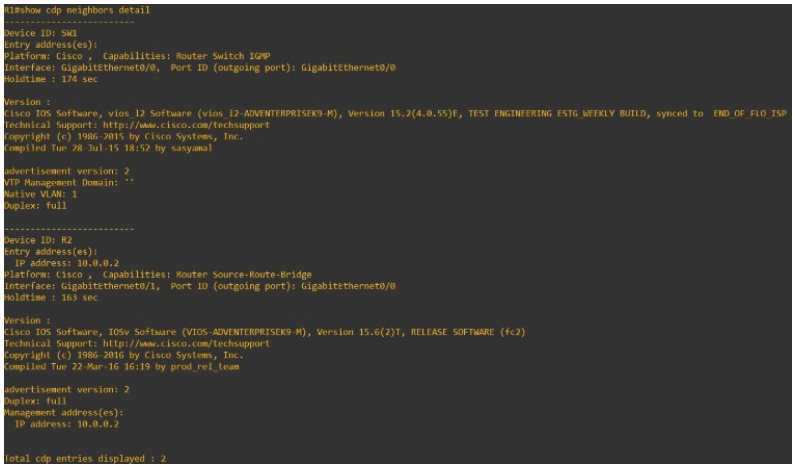
Pour afficher la table des voisins CDP on lance la commande :
`R1#show cdp neighbors`

```
R1#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
SW1              Gig 0/0           153           R S I           Gig 0/0
R2               Gig 0/1           146            R B            Gig 0/0

Total cdp entries displayed : 2
R1#
```

Ces commandes permettent d'afficher des informations essentiels à propos de CDP, pour afficher des informations additionnels on peut utiliser la commande :
`R1#show cdp neighbors detail`



Comme on peut le voir plus d'informations apparaît pour chaque appareils voisins.
Par exemple le nom de l'OS, le type de VLAN (lorsqu'un commutateur) etc...

Si l'on veut afficher des informations détaillés à propos d'un seul appareil, il est possible de lancer la commande :
`R1#show cdp entry R2`

```
R1#show cdp entry R2
-------------------------
Device ID: R2
Entry address(es):
  IP address: 10.0.0.2
Platform: Cisco ,  Capabilities: Router Source-Route-Bridge
Interface: GigabitEthernet0/1,  Port ID (outgoing port): GigabitEthernet0/0
Holdtime : 178 sec

Version :
Cisco IOS Software, IOSv Software (VIOS-ADVENTERPRISEK9-M), Version 15.6(2)T, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Tue 22-Mar-16 16:19 by prod_rel_team

advertisement version: 2
Duplex: full
Management address(es):
  IP address: 10.0.0.2
```

CDP est activé par défaut sur l'appareil mais aussi sur chacunes des interfaces par défaut.
Pour activer/désactiver CDP on peut lancer la commande :

```
R1(config)#[no] cdp run
```

Pour activer/désactiver une interface spécifique on peut lancer la commande :

```
R1(config-if)#[no] cdp enable
```

Il est possible de configurer le temps de CDP en lançant la commande :

```
R1(config)#cdp timer seconds
```

Pour configurer le temps d'attente CDP on lance la commande :

```
R1(config)#cdp holdtime seconds
```

Pour activer/désactiver CDPv2 on lance la commande :

```
R1(config)#[no] cdp advertise-v2
```

Voyons à présent plus en détail le fonctionnement pour la configuration du protocole
LLDP (Link Layer Discovery Protocol)
LLDP est un protocole de l'industrie standard (IEEE 802.1AB)
CDP était le protocole originel et LLDP a été inventé plus tard pour qu'il y ait une version standard au niveau industriel.
Ce protocole est désactivé par défaut sur les appareils Cisco, donc il faut l'activer manuellement pour l'utiliser.
Un appareil peut lancer CDP et LLDP en même temps donc il n'y pas nécessité à en désactiver un.
Les messages LLDP sont périodiquement envoyés à l'adresse MAC multicast : 0180.C200.000E
Lorsqu'un appareil reçoit des messages LLDP, il procède le message mais ne le partage pas aux autres appareils voisins.
Donc seulement les appareils directement connectés peuvent devenir des voisins LLDP.
Par défaut les messages LLDP sont envoyés toutes les 30 secondes, et toutes les 120 secondes pour les messages d'attente de réponses.
LLDP a également un temps additionnel appelé le « délai de réinitialisation ».
Si LLDP est activé de manière global ou bien sur une interface spécifique le temps aura un délai de l'initialisation actuelle de LLDP et le temps sera de 2 secondes par défaut.
Voici les commandes nécessaires dans la configuration de LLDP.
Puisque LLDP est désactivé par défaut, il faut l'activer sur toutes les interfaces. La configuration est légèrement différente de CDP.
Pour activer LLDP on lance la commande :

```
R1(config)#lldp run
```

C'est la même commande que pour CDP sauf que l'on remplace cdp par lldp. Si l'on veut le désactiver on lance la commande :

```
R1(config)#no lldp run
```

Pour activer LLDP sur une interface spécifique (tx) on utilise la commande suivante :

```
R1(config-if)#lldp transmit
```

Cette commande lancé fera que l'interface commencera à lancer des messages LLDP.
Par contre lorsqu'il recevra un message LLDP, il le rejettera.
Pour activer LLDP en réception il faut lancer une autre commande qui est :

```
R1(config-if)#lldp receive
```

Pour configurer le temps d'envois des messages de LLDP on lance la commande suivante :

```
R1(config)#lldp timer secondes
```

Pour configurer le temps d'attente de réponse entre les messages on lance la commande :

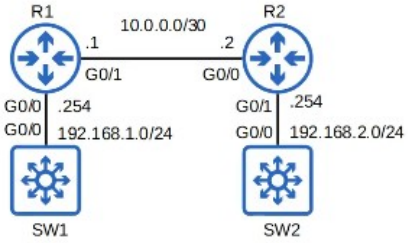
```
R1(config)#lldp holdtime secondes
```

Pour réinitialiser le temps LLDP on lance la commande :

```
R1(config)#lldp reinit secondes
```

Ces commandes sont similaires à la configuration CDP la différence se situe dans la configuration des interfaces ou il faut activer la transmission et la réception dans LLDP.

Sur le réseau suivant LLDP a été activé sur les interfaces.



Voici le résultat des commandes pour afficher la configuration des interfaces :

```
R1#show lldp
R1#show lldp trafic
R1#show lldp interface
```

```
R1#show lldp traffic

LLDP traffic statistics:
    Total frames out: 4
    Total entries aged: 0
    Total frames in: 3
    Total frames received in error: 0
    Total frames discarded: 0
    Total TLVs discarded: 0
    Total TLVs unrecognized: 0
R1#
R1#show lldp interface

GigabitEthernet0/0:
    Tx: enabled
    Rx: enabled
    Tx state: IDLE
    Rx state: WAIT FOR FRAME

GigabitEthernet0/1:
    Tx: enabled
    Rx: enabled
    Tx state: IDLE
    Rx state: WAIT FOR FRAME

GigabitEthernet0/2:
    Tx: enabled
    Rx: enabled
    Tx state: INIT
    Rx state: WAIT PORT OPER

GigabitEthernet0/3:
    Tx: enabled
    Rx: enabled
    Tx state: INIT
    Rx state: WAIT PORT OPER
```

```
R1#show lldp

Global LLDP Information:
    Status: ACTIVE
    LLDP advertisements are sent every 30 seconds
    LLDP hold time advertised is 120 seconds
    LLDP interface reinitialisation delay is 2 seconds
```

Voici la commande pour afficher la table de voisins sur LLDP :

```
R1#show lldp neighbors
```

```
R1#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
SW1                 Gi0/0          120                        Gi0/0
R2                  Gi0/1          120        R               Gi0/0

Total entries displayed: 2
```

Le résultat de la commande affiche des informations similaires à la commande pour afficher la table de voisins CDP

Pour afficher en détail la configuration de la table de voisin on lance la commande suivante :

```
R1#show lldp neighbors detail
```

```
R1#show lldp neighbors detail
------------------------------------------------
Local Intf: Gi0/0
Chassis id: 0c04.41d2.1a00
Port id: Gi0/0
Port Description: GigabitEthernet0/0
System Name: SW1

System Description:
Cisco IOS Software, vios_l2 Software (vios_l2-ADVENTERPRISEK9-M), Version 15.2(4.0.55)E, TEST ENGINEERING ESTG_WEEKLY BUILD, synced to  END_OF_FLO_ISP
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compi

Time remaining: 99 seconds
System Capabilities: B,R
Enabled Capabilities - not advertised
Management Addresses - not advertised
Auto Negotiation - not supported
Physical media capabilities - not advertised
Media Attachment Unit type - not advertised
Vlan ID: - not advertised

------------------------------------------------
Local Intf: Gi0/1
Chassis id: 0c04.418d.a400
Port id: Gi0/0
Port Description: GigabitEthernet0/0
System Name: R2

System Description:
Cisco IOS Software, IOSv Software (VIOS-ADVENTERPRISEK9-M), Version 15.6(2)T, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Tue 22-Mar-16 16:19 by prod_rel_team

Time remaining: 92 seconds
System Capabilities: B,R
Enabled Capabilities: R
Management Addresses:
    IP: 10.0.0.2
```

Cette commande permet d'afficher quelques informations de plus par rapport à CDP, comme par exemple : la section « System Capabilities : B,R » permet de dire que le système voisin peut faire office de pont mais aussi de routeur. (C'est un commutateur niveau 3)
La section « Enabled capabilities » indique quelle mode de fonctionnement est activé sur le système voisin.
Il est possible de n'afficher les détail de l'interface de seulement un appareil spécifié la commande est la suivante :
R1#lldp entry SW1

Dans ce cas les informations du SW1 sont affichés :

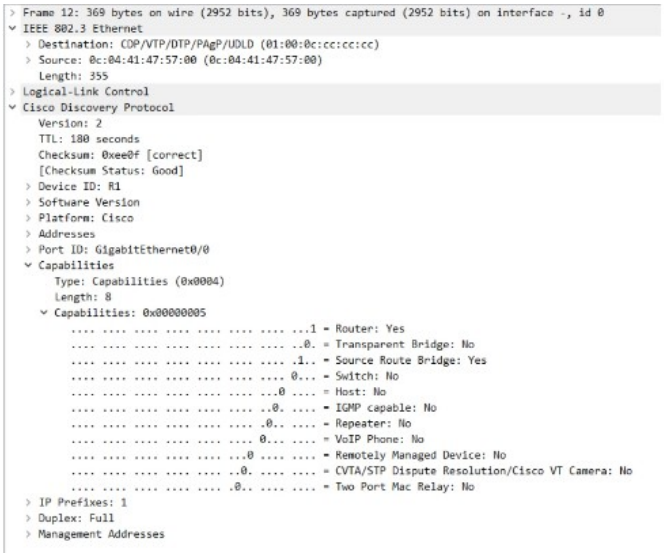
```
R1#show lldp entry SW1

Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
------------------------------------------------
Local Intf: Gi0/0
Chassis id: 0c04.41d2.1a00
Port id: Gi0/0
Port Description: GigabitEthernet0/0
System Name: SW1

System Description:
Cisco IOS Software, vios_l2 Software (vios_l2-ADVENTERPRISEK9-M), Version 15.2(4.0.55)E, TEST ENGINEERING ESTG_WEEKLY BUILD, synced to  END_OF_FLO_ISP
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compi

Time remaining: 119 seconds
System Capabilities: B,R
Enabled Capabilities: R
Management Addresses - not advertised
Auto Negotiation - not supported
Physical media capabilities - not advertised
Media Attachment Unit type - not advertised
Vlan ID: - not advertised
```

Voici une capture Wireshark de CDP :



On peut voir le TTL qui est de 180 seconde, c’est le même que celui configuré avec la commande `lldp holdtime`

Voici une capture Wireshark de LLDP :

On peut voir affiché ici les fonctions possibles sur SW1 qui sont le routage et le pont (ou Bridge)