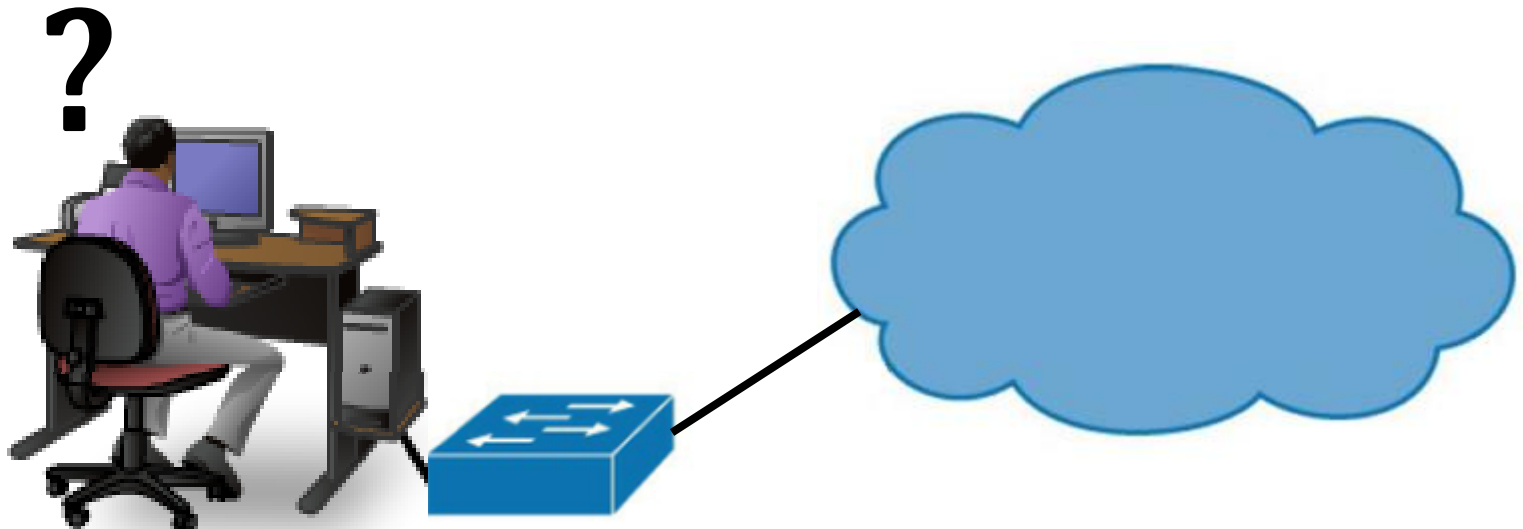


Discovery Protocols

Réseaux d'entreprise

Quelle topologie ?

- Un Administrateur a besoin dans quelques situations de RE-découvrir la topologie du réseau
 - CDP : Cisco Discovery Protocol
 - LLDP : Link Layer Discovery Protocol (IEEE 802.1ab)



CDP

- Protocole de couche 2 propriétaire de Cisco
- Mises à jour par défaut toutes les 60 secondes.
- Information retenue (holdtime) 3×60 secondes = 180s.

```
R1#show cdp
```

```
Global CDP information:
```

```
  Sending CDP packets every 60 seconds
```

```
  Sending a holdtime value of 180 seconds
```

```
  Sending CDPv2 advertisements is enabled
```

- Activé par défaut sur toutes les interfaces
 - Désactiver CDP globalement

```
R1(config)#no cdp run
```
 - Désactiver CDP par interface

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

Utilisation de CDP

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

Device ID	Loc	Intrf	Holdtme	Cap	Platform	Port ID
ASW1		Eth0/1	133	S	2960	Eth0/2
R3		S0/0	140	R	ISR4300	S0/1

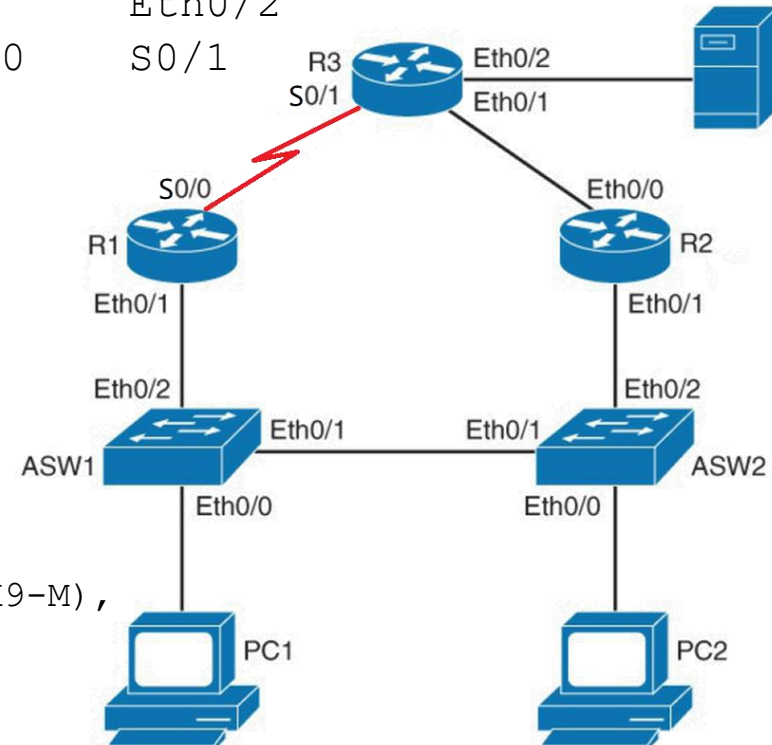
R1#show cdp neighbors detail

Device ID: ASW1
Entry address(es):
IP address : 10.10.1.101
Platform: cisco 2960, Capabilities: Switch
Interface: Ethernet0/2, Port ID (outgoing port): Ethernet0/1
Holdtime: 141

Version :

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M),
Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)

...[omited]...



LLDP

- Protocole de couche 2 standardisé par IEEE : 802.1ab
- Ne fonctionne que sur les interfaces **Ethernet**
- Mises à jour par défaut toutes les **30** secondes.
- Information retenue (holdtime) 4×30 secondes = **120s**.

```
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
```

- Désactiver pour les équipements cisco
 - **Activer CDP globalement**

```
R1(config)#lldp run
```
 - **Désactiver CDP par interface**

```
R1(config-if)#no lldp receive  
R1(config-if)#no lldp transmit
```

Utilisation de LLDP

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
ASW1	Eth 0/1	120	B	Eth0/2

R1#show lldp neighbors detail

Chassis id: 0007.EC07.0919

Port id: Eth0/1 Port Description: Ethernet0/1

System Name: ASW1

System Description: Cisco IOS Software, C2960Software
C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE(fc1)

...[omited]...

System Capabilities: B - Enabled Capabilities: B

Management Addresses - not advertised

Auto Negotiation - supported, enabled

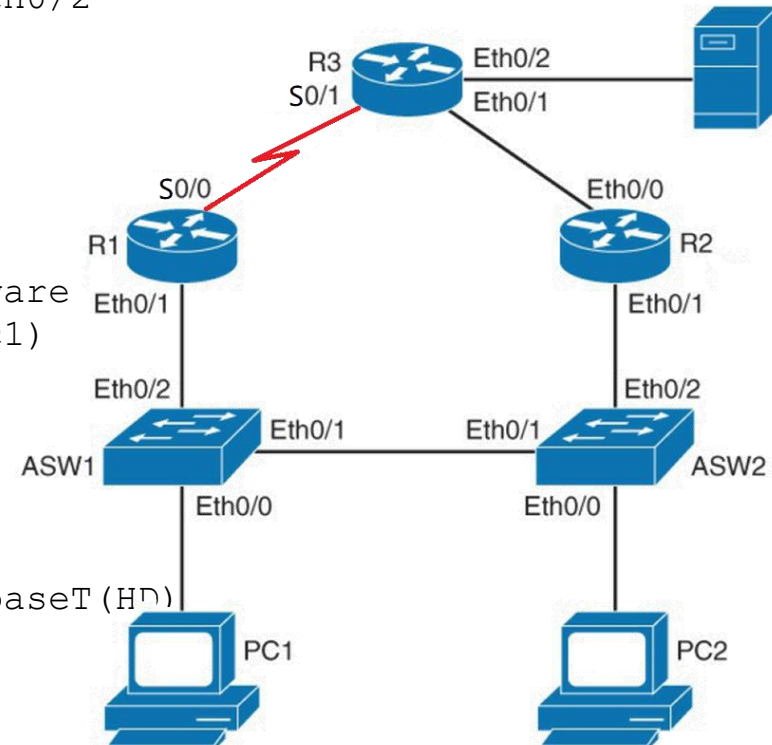
Physical media capabilities:

100baseT(FD), 100baseT(HD), 1000baseT(FD), 1000baseT(HD)

Media Attachment Unit type: 10

Vlan ID: 1

...[omited]...



Autres

- Media Endpoint Discovery (LLDP-MED) est une amélioration de LLDP qui offre les fonctionnalités suivantes :
 - Découverte automatique des LAN policies (VLAN, priorités L2, Diffserver) activant le réseau plug-and-play
 - Localisation de périphériques par découverte permettant la création des bases de données (avec la VoIP, permettant un service d'urgence)
 - Gestion de l'alimentation PoE étendue et automatisée pour les périphériques terminaux
 - Gestion d'inventaire : suivre les périphériques et collecter leurs caractéristiques.
- Pour la couche 3 le Network discovery est assuré par ICMPv6
- Les protocoles Network discovery facilitent l'analyse et la gestion d'un réseau. Mais en même temps, en terme de sécurité, ils constituent une vulnérabilité majeure. Puisque l'utilisateur malveillant profitera de la même facilité. Attention à décider de les désactiver; certains services (PoE, Voice VLAN, ...) dépendent de CDP/LLDP