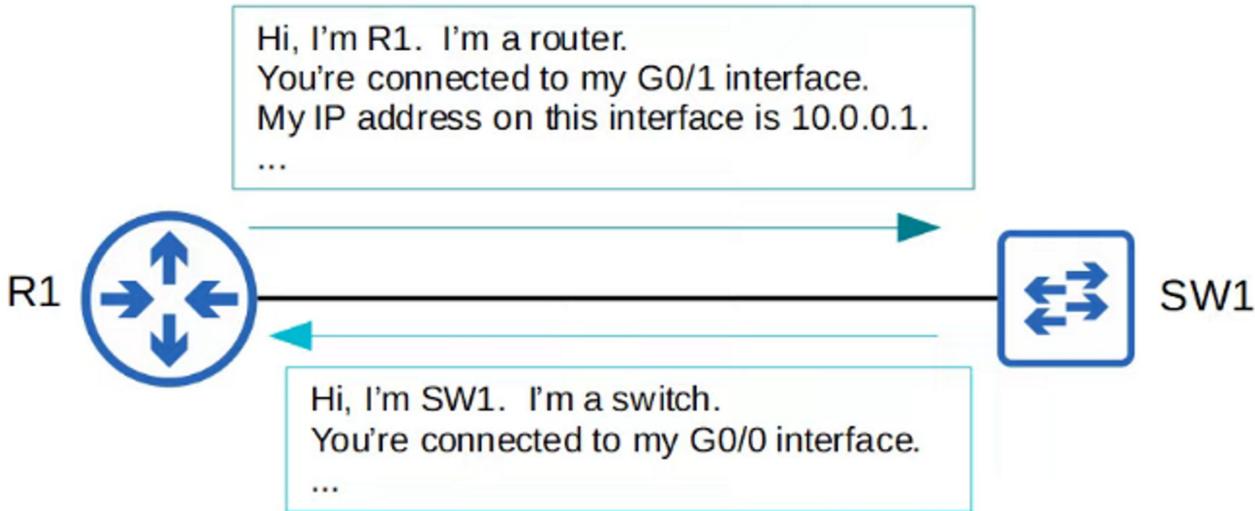


CDP (Cisco Discovery Protocol) and **LLDP (Link Layer Discovery Protocol)** are both **Layer 2 discovery protocols** used by network devices to share information about themselves with directly connected devices.

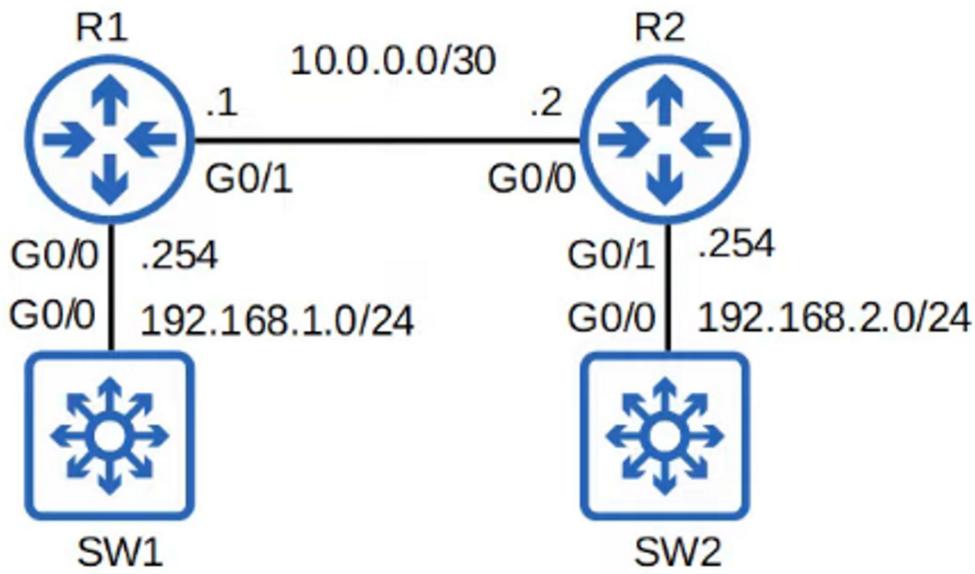


🔍 CDP (Cisco Discovery Protocol)

- **Vendor:** Proprietary to **Cisco Systems**
- **Purpose:** Allows Cisco devices (switches, routers, IP phones, etc.) to **advertise their identity and capabilities** to directly connected Cisco devices.
- **Layer:** Layer 2 (Data Link Layer)
- **Transport:** Works over Ethernet, Wi-Fi, Frame Relay, etc.
- **Information Shared:**
 - Device ID (hostname)
 - IP address
 - Platform (model)
 - Port ID (interface)
 - VLAN information
 - IOS version
 - Power requirements (for IP phones)

⚠️ Limitations:

- Only works between **Cisco devices**
- Not interoperable with other vendors



```
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
```

```
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#
```

```
R1#show cdp neighbors detail
-----
Device ID: SW1
Entry address(es):
Platform: Cisco , Capabilities: Router Switch IGMP
Interface: GigabitEthernet0/0, Port ID (outgoing port): GigabitEthernet0/0
Holdtime : 174 sec

Version :
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.
Compiled Tue 28-Jul-15 18:52 by sasyamal

advertisement version: 2
VTP Management Domain: ..
Native VLAN: 1
Duplex: full

-----
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 : 163 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

Total cdp entries displayed : 2
```

```
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 show commands summary

- R1# **show cdp**
→ shows basic information about CDP (timers, version)
- R1# **show cdp traffic**
→ displays how many CDP messages have been sent and received
- R1# **show cdp interface**
→ displays which interfaces CDP is enabled on
- R1# **show cdp neighbors**
→ lists CDP neighbors and some basic information about each neighbor
- R1# **show cdp neighbors detail**
→ lists each CDP neighbor with more detailed information
- R1# **show cdp entry name**
→ displays the same info as above, but for the specified neighbor only

5 mi

LLDP (Link Layer Discovery Protocol)

- **Vendor:** Open standard (IEEE 802.1AB)
- **Purpose:** Provides a vendor-neutral way for network devices to share information with directly connected devices.
- **Layer:** Layer 2
- **Transport:** Typically runs over Ethernet
- **Information Shared:**
 - System name and description
 - Port ID and description
 - VLAN ID
 - Management IP address
 - Capabilities (switch/router/etc.)
 - Power over Ethernet (PoE) info
- ✓ **Advantages:**
 - **Multi-vendor support**
 - Works with Cisco, HP, Juniper, Dell, etc.
 - Used in data centers, VoIP setups, and automation systems

- R1# **show lldp**
→ shows basic information about LLDP (timers, version)
- R1# **show lldp traffic**
→ displays how many LLDP messages have been sent and received
- R1# **show lldp interface**
→ displays which interfaces LLDP tx/rx is enabled on
- R1# **show lldp neighbors**
→ lists LLDP neighbors and some basic information about each neighbor
- R1# **show lldp neighbors detail**
→ lists each LLDP neighbor with more detailed information
- R1# **show lldp entry name**
→ displays the same info as above, but for the specified neighbor only

Use Cases (Both):

- Network mapping and documentation
- Troubleshooting (e.g., identifying what's on the other side of a port)
- VoIP and PoE negotiation
- Dynamic network configuration

Summary Table:

Feature	CDP	LLDP
Vendor	Cisco (Proprietary)	IEEE 802.1AB (Open Standard)
Interoperability	Cisco devices only	Multi-vendor
Information Shared	Device info, port, IP, etc.	Similar but standardized
Use Case	Cisco-centric networks	Heterogeneous networks
Enable/Disable	Interface or global config	Interface or global config

Disabling **CDP** (Cisco Discovery Protocol) and **LLDP** (Link Layer Discovery Protocol) is often **recommended in certain environments** for **security and performance reasons**. Here's a breakdown of **why** and **when** you might want to disable them:

. Security Risks

CDP/LLDP can leak sensitive information:

Both protocols send out detailed device information in plain text at Layer 2, including:

- Device hostname
- IP address
- IOS/software version
- Interface details
- VLAN configuration
- Power requirements (PoE)

Attackers on the same Layer 2 segment (e.g., in a compromised switch port or rogue device) can sniff this information and use it for:

- Network mapping
- Planning targeted attacks (e.g., version-specific exploits)
- Spoofing or man-in-the-middle (MITM) attacks

Example: A rogue device plugged into an open port in a lobby can passively collect network topology data using CDP/LLDP.