• Discovering and connecting to Neighbors
• Getting information about remote devices
DISCOVERING AND CONNECTING TO NEIGHBORS
Cisco Discovery Protocol (CDP)

- Layer 2 protocol that connects lower physical media and upper network layer protocols
- Used to obtain information about neighboring devices
- Runs on all Cisco equipment over the Subnetwork Access Protocol (SNAP)
- CDP starts automatically
CDP: A layer 2 protocol
## CDP Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Mode</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cdp run</code></td>
<td>Global configuration mode</td>
<td>Enables CDP globally on the router.</td>
</tr>
<tr>
<td><code>cdp enable</code></td>
<td>Interface configuration mode</td>
<td>Enables CDP on an interface.</td>
</tr>
<tr>
<td><code>clear cdp counters</code></td>
<td>User EXEC mode</td>
<td>Resets the traffic counters to zero.</td>
</tr>
<tr>
<td><code>show cdp</code></td>
<td>Privileged EXEC mode</td>
<td>Displays the interval between transmissions of CDP advertisements, the number of seconds the CDP advertisement is valid for a given port, and the version of the advertisement.</td>
</tr>
<tr>
<td>`show cdp entry {[*</td>
<td>device-name [*] [protocol</td>
<td>version]}`</td>
</tr>
<tr>
<td><code>show cdp interface [type number]</code></td>
<td>Privileged EXEC mode</td>
<td>Displays information about interfaces on which CDP is enabled.</td>
</tr>
<tr>
<td><code>show cdp neighbors [type number] [detail]</code></td>
<td>Privileged EXEC mode</td>
<td>Displays the type of device that has been discovered, the name of the device, the number and type of the local interface (port), the number of seconds the CDP advertisement is valid for the port, the device type, the device product number, and the port ID. Issuing the detail keyword displays information on the native VLAN ID, the duplex mode, and the VTP domain name associated with neighbor devices.</td>
</tr>
</tbody>
</table>
Showing CDP neighbor entries

Device ID | Local Interface
---|---
Holdtime | Capability
Platform | Port ID

- VTP Management Domain Name (CDPv2 only)
- Native VLAN (CDPv2 only)
- Full/Half-Duplex (CDPv2 only)
## Troubleshooting CDP

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear cdp table</td>
<td>Deletes the CDP table of information about neighbors.</td>
</tr>
<tr>
<td>clear cdp counters</td>
<td>Resets the traffic counters to zero.</td>
</tr>
<tr>
<td>show cdp traffic</td>
<td>Displays CDP counters, including the number of packets sent and received and checksum errors.</td>
</tr>
<tr>
<td>show debugging</td>
<td>Displays information about the types of debugging that are enabled.</td>
</tr>
<tr>
<td>debug cdp adjacency</td>
<td>CDP neighbor information</td>
</tr>
<tr>
<td>debug cdp events</td>
<td>CDP events</td>
</tr>
<tr>
<td>debug cdp ip</td>
<td>CDP IP information</td>
</tr>
<tr>
<td>debug cdp packets</td>
<td>CDP packet-related information</td>
</tr>
<tr>
<td>cdp timer</td>
<td>Specifies how often the Cisco IOS software sends CDP updates.</td>
</tr>
<tr>
<td>cdp holdtime</td>
<td>Specifies the hold time to be sent in the CDP update packet.</td>
</tr>
<tr>
<td>show cdp</td>
<td>Displays global CDP information, including timer and hold-time information.</td>
</tr>
</tbody>
</table>
GETTING INFORMATION ABOUT REMOTE DEVICES
Troubleshooting IP addressing

- **Ping**: Uses the ICMP protocol to verify the hardware connection and the IP address of the network layer. This is a basic testing mechanism.

- **Traceroute**: Allows the location of failures in the path from the source to the destination. Trace uses Time to Live values to generate messages from each router along the path.

- **Telnet**: Verifies the application layer software between source and destination. This is the most complete test mechanism available.
Telnet

- Telnet is a virtual terminal protocol that is part of the TCP/IP protocol suite
- Used to verify the application layer software between source and destination
- Functions at the application layer of the OSI model
Establishing telnet session

- A hostname table or access to DNS for Telnet must be present for a name to work

```text
Denver>131.108.100.152
Denver>telnet 131.108.100.152
Denver>telnet paris
Denver>connect paris
Denver>paris
```
Finishing telnet sessions

Initiate a session
Denver>telnet paris

End a session
Paris>exit

Suspend a session
Paris><Ctrl><Shift><6><x>
Denver>

Resume a session
Denver><Return>

Disconnect a session
Denver>disconnect paris

Display Session
Denver#show sessions
Conn  Host          Address               Idle  Conn Name
1     Paris        131.108.100.152    0      Paris
2     Tokyo        126.102.57.63      0      Tokyo
Testing with the ping command

- The **ping** command sends a packet to the destination host and then waits for a reply packet from that host.
- The exclamation points (!) indicate each successful echo.
- A dots (.) indicate a timeout.
Testing with the trace command

• **traceroute** tests each step along the way

• If one of the routers is unreachable, three asterisks (*) will be returned instead of the name of the router

York# **traceroute** **ROME**
Type escape to abort.
Tracing the route to Rome (172.16.33.5)
  1 LONDON (172.16.12.3) 8 msec 8 msec 4 msec
  2 PARIS (172.16.16.2) 8 msec 8 msec 8 msec
  3 ROME (172.16.33.5) 8 msec 8 msec 4 msec

York#
Review

- Enable and disable CDP
- Use the `show cdp neighbors` command
- Determine which neighboring devices are connected to which local interfaces
- Gather network address information about neighboring devices using CDP
- Establish a Telnet connection
- Verify a Telnet connection
- Disconnect from a Telnet session
- Suspend a Telnet session
- Perform alternative connectivity tests
- Troubleshoot remote terminal connections