APIC Enterprise Module - Zero Touch Deployment
FCS – Release 1.0

Zero touch deployment aims to provide enhanced, secure and integrated solution for enterprise network customers to ease new network device rollout process or provisioning updates to an existing network. When the newly installed network device is able to discover the Controller (PnP server), the controller creates a database entry for this device that allows the network admin to provision the device with appropriate image and configuration. This capability eliminates manual intervention, saving time and potential errors.

The APIC EM Zero Touch Deployment service will work for network devices running Cisco IOS software that supports the PnP agent functionality.

Deployment Use Cases

1. New device provisioning (Ad-hoc OR Un-Claimed device provisioning)

- This use case is for the scenario where the new device is not part of a site roll out process or the admin has not pre-provisioned it in the Controller.
- The assumption is that the network admin has created a list of all valid network devices in the Controller. The Controller will ignore any device that is not part of this list. This list contains the Serial number and UDI information for every network.
- New device boots up and is able to discover the Controller.
- The Controller will then match this new device against the list of all valid network devices (match based on Serial number and UDI information). Once this check is done, the new device will show up automatically in the Inventory database. Any device that is not part of the valid network devices list in the Controller will be ignored and not shown in the Inventory database.
- Network admin can then provision this device by specifying the configuration file and image information.

2. RMA

- Network admin prepares the Controller for upcoming RMA by identifying device from Controller inventory as RMA candidate. The Serial number and the UDI

information of the replacement (new) network device are also pre-provisioned in the Controller as part of this step.

- At remote site, installer plugs-in new device replacing existing mal-functioning device (like to like: same device type and model).
- New device boots up and is able to discover the Controller. This new device will then show up in the Inventory database.
- The Controller does a match of this new device against the pre-provisioned RMA replacement device list to find out exact device match (match based on Serial number and UDI information already entered in the Controller). This is an automated process where the admin does not need to do anything after the old device has been identified as RMA candidate.
- Newly plugged-in device get the same configuration and image as the old device.

3. New Site Provisioning

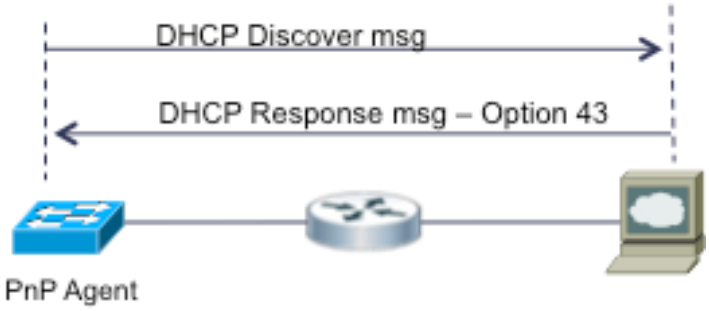
- Network admin pre-provisions the entire site / branch via this use case (new site or clone an existing site).
- All Cisco devices for this new site are pre-provisioned in the Controller inventory (Serial number, model info etc.) with image and configuration file information.
- As and when the new devices are powered up, the new devices reach out to the controller. The Controller matches the new devices against pre-provisioned devices, pushes the configured image and configuration file to this new device.

Controller (PnP Server) Discovery

Plug and Play Solution can work with or without DHCP and/or DNS Servers in a typical enterprise branch network. DHCP/DNS Server can provide PnP Server's (APIC-EM) IP address and/or DNS name to the Cisco device running PnP Agent. DHCP based method is preferred as this the best way to achieve zero touch deployment with scale.

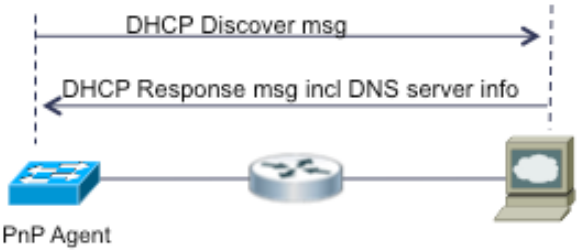
1. DHCP based lookup

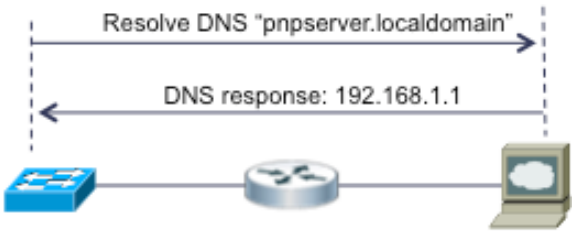
The PnP agent on the network device starts with no configuration and will send out a DHCP discovery message after device bootup. The DHCP server will respond to this request with the Controller (PnP server) IP address using DHCP option 43.



2. DNS based lookup

The PnP agent on the network device starts with no configuration and will send out a DHCP discovery message after device bootup. The DHCP server responds with the client IP address, default router and DNS server information. The DNS server is configured to resolve pnpserver.localdomain, which allows the PnP agent on the network device to talk to the Controller (PnP server). The "localdomain" is the customer's domain.





3. Cloud based lookup

Cloud based aspect of the solution comes into play only after the DHCP option 43, and the DNS lookup for "pnpserver.localdomain" have failed. A cloud-based solution is option 3 for the PnP agent running on the device.
The cloud-based solution still requires DNS. The PnP agent on the device will attempt to reach a server on a cisco hosted website with url "devicehelper.cisco.com/device-helper". If successful, the PnP agent contacts this server, and waits. The owner of the network device must login into the site "devicehelper.cisco.com/device-helper" and 'claim' the device with the PID and the serial number. After successfully claiming the device, the owner will redirect the PnP agent to the Controller by providing the IP Address of the controller.

Platform support

Routers Platforms (IOS-XE 3.12S / 15.4(2)T) -

- Cisco ISR G2 (800, 1900, 2900, 3900)

- Cisco ISR G3
- Cisco ASR 1K (IOS-XE 3.12)

Switch Platforms (IOS-XE 3.6.0E / 15.2(2)E)

- Cisco Catalyst 4500
- Cisco Catalyst 4900
- Cisco Catalyst 3K (3560-C, 3560-X, 3750-X, 3650, 3850)
- Cisco Catalyst 2K (2960-C, 2960-XR, 2960-X, 2960-SF, 2960-S)