Deploy Router Using Bootz

With the Bootz protocol, you can securely and seamlessly provision network devices accurately within minutes and without any manual intervention.

Table 1: Feature History Table

Feature	Release Information	Feature Description
Bootz Protocol Provisioning	Release 7.11.1	This feature allows devices in the network to establish a secure connection with the remote Bootz server and authenticate information using a three-step validation process involving validation of the network device, the Bootz server, and onboarding information. This eliminates security risks or malicious actions during remote provisioning.

- In a secured network such as datacenter, the zero-touch provisioning mechanism helps you provision hundreds of remote devices without your intervention. But, the access devices are typically in an insecure network. There is a high risk of malicious actions on the device, such as adding an unauthorized or infected device. Security is a critical aspect while remotely provisioning the network devices.

  Bootz combines seamless automation with security. Network devices can securely establish a connection with the Bootz server and authenticate the onboarding information that it receives. The process eliminates any security risks or malicious actions during the provisioning of remote devices.

Onboard Devices Using Bootz Workflow

The Cisco IOS XR software supports Bootz provisioning capabilities. Bootz, which is an alternative to the secure ZTP workflow, uses the Google Remote Procedure Call (gRPC) protocol for fetching information from a remote server. The Bootz workflow uses the following processes to onboard the remote devices securely:

1. **Router Validation**: The Bootz server authenticates the router before providing bootstrapping data.
2. **Server Validation**: The router device in turn validates the Bootz server to make sure that the onboarding is performed for the correct network. Upon completion, the Bootz server sends the bootstrapping data (for example, a YANG data model) or artifact to the router.
3. **Artifact Validation**: The configuration validates the bootstrapping data or artifact received from the Bootz server.

Obtain Ownership Voucher

Ownership Voucher is used to identify the owner of the device by verifying the owner certificate that is stored in the device. Cisco supplies Ownership Voucher in response to your request. You must submit the Pinned Domain Certificate and device serial numbers with the request. Cisco generates and provides the Ownership Voucher to you.

Contact Cisco Support to obtain a voucher. Provide the following details to request for ownership voucher certificate:

- Pinned Domain certificate (PDC): PDC is an X.509 v3 certificate structure that uses Distinguished Encoding Rules (DER). This certificate is used by the router to trust a public key infrastructure in order to verify a domain certificate supplied to the router separately in the bootstrapping data. This certificate could be an end-entity certificate, including a self signed entity.
- Order details with the Serial numbers of the routers

For example,

```
{
       "expires-on": "2016-10-21T19:31:42Z",
       "assertion": "verified",
       "serial-number": "JADA123456789",
       "idevid-issuer": "base64encodedvalue==",
       "pinned-domain-cert": "base64endvalue==",
       "last-renewal-date": "2017-10-07T19:31:42Z"
    }
```

Based on the details that you provide, Cisco generates the ownership voucher in .vcj format. For example, DCA213140YX.vcj.

Build Bootstrapping Data

The following describe the components of Bootz:

- **Onboarding Device (Router):** The router is a Cisco device that you want to provision and connect to your network. Bootz is supported only on platforms that have Hardware TAM support.

- **DHCP Server:** The Bootz process relies on the DHCP server to provide the URL to access the bootstrapping information.
- **Bootz Bootstrap Server:** A Bootz Bootstrap server is any gRPC server used as a source of Bootz bootstrapping data and shoul a gRPC server. Example: Google Proto

Note Bootz only supports single name-server. When the DHCP server has more than one server address configured, Bootz fails to apply the server configuration.

The Bootz server contains the following artifacts:

- Cisco IOS XR software images: You can download Cisco images, SMU, and patches using the Cisco Support & Downloads page.
- Bootstrapping Data

- **Bootstrapping Data:** It is the collection of data that the router obtains from the Bootz server during the provisioning process. You must create and upload the bootstrapping data in the Bootz server.
  - **Signed Bootstrap Response:** Each bootstrap response contains the onboarding information for a single control card or line card. For the response message format, see the Bootstrap Response Message for a single card.
  - **Owner Certificate:** The owner certificate is installed on the router with the public key of your organization. The router uses the owner certificate to verify the signature in the signed bootstrap response artifact using the public key that is available in the owner certificate.
  - **Ownership Voucher:** Ownership Voucher is used to identify the owner of the device by verifying the owner certificate that is stored in the device. Cisco supplies Ownership Voucher in response to your request. You must submit the Pinned Domain Certificate and device serial numbers with the request. Cisco generates and provides the Ownership Voucher to you.
- **Report Progress:** When the device obtains the onboarding information from a Bootz server, the router reports the bootstrapping progress to the Bootz server using the API calls.

  Each bootstrap request to the gRPC server (bootstrap server) contains the following artificats:
  - Serial number of the control card
  - Software image to download and install
  - Bootloader Password for the device
  - Certificate used to validate the bootstrap server
  - Bootstrap server configuration information such as server credentials, path information, authentication information, and certificates

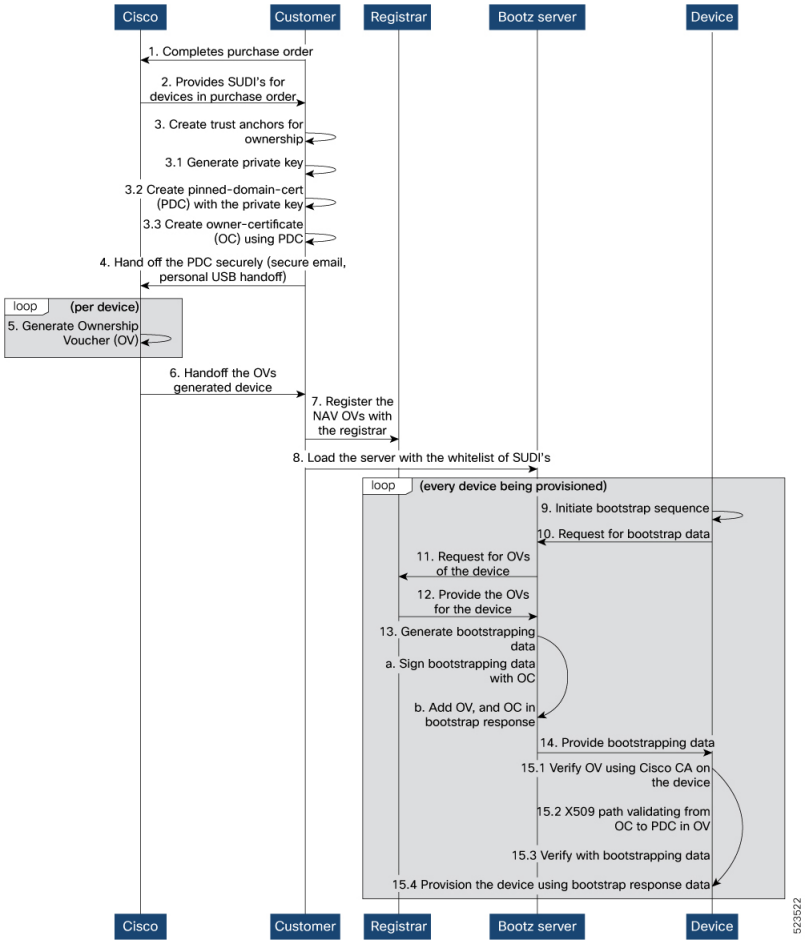
  For the request message format, see the Bootstrap Request Message.

Provision Bootz Using DHCP Server

When you boot the device, the Bootz process initiates automatically on a device without prior configuration. During the process, the router receives the details of the configuration file from the DHCP server.

The following figure illustrates the end-to-end sequence of the Bootz process:

Figure 1: End-to-end sequence of the Bootz process



Before you begin

The network administrator performs the following tasks as part of the initial setup for secure ZTP:

- Ensure to enable secure ZTP on the router using the **ztp secure-mode enable** command and then reload the router.
- Contact Cisco Support to obtain a voucher. Provide the following details to request for ownership voucher certificate:
  - Order details with the Serial numbers of the routers

  For example,

```
{
        "expires-on": "2016-10-21T19:31:42Z",
        "assertion": "verified",
        "serial-number": "JADA123456789",
        "idevid-issuer": "base64encodedvalue==",
        "pinned-domain-cert": "base64endvalue==",
        "last-renewal-date": "2017-10-07T19:31:42Z"
    }
```

Step 1 Upload the following bootstrapping data to the Bootz server. Steps to upload may vary depending on the server that you are using, refer to the documentation provided by your vendor.

- Cisco IOS XR software images: You can download Cisco images, SMU, and patches using the Cisco Support & Downloads page.
- Serial numbers of the routers you plan to onboard using Bootz
- Owner certificates
- Pinned Domain Certificate (PDC)
- Ownership vouchers

Step 2 Set up the DHCP server to provide the redirect URL to the router:

Before triggering the secure ZTP process, configure the DHCP server to provide the location of the IOS-XR image to the router. For information on how to configure the DHCP server, see your DHCP server documentation.

Configure the following parameters in the DHCP server:

- `option-code`: The DHCP SZTP redirect Option has the following parameters:
  - OPTION_V4_SZTP_REDIRECT (143): Use this DHCP v4 code for IPV4.
  - OPTION_V6_SZTP_REDIRECT (136): Use this DHCP v4 code for IPV6.

  For example, `option dhcp6.bootstrap-servers code 136 = text;`
- `option-length`: The option length in octets
- `bootstrap-servers`: A list of servers for the onboarding device to contact the servers for the bootstrapping data.

  `"bootz://<ip-address-or-hostname>[:<port>]<endpoint>"`

Step 3 Power on the router.

Here is the high-level workflow of the Bootz process:

a. When you boot the device with an IOS-XR image, the secure ZTP process verifies if the secure ZTP mode (`secure-ztp mode`) is enabled. If not enabled, the device boots normally.

Note When `secure-ztp mode` is enabled, the ZTP process accepts only the `secure-redirect-URL` and ignores the presence of the boot file name option from the DHCP response.

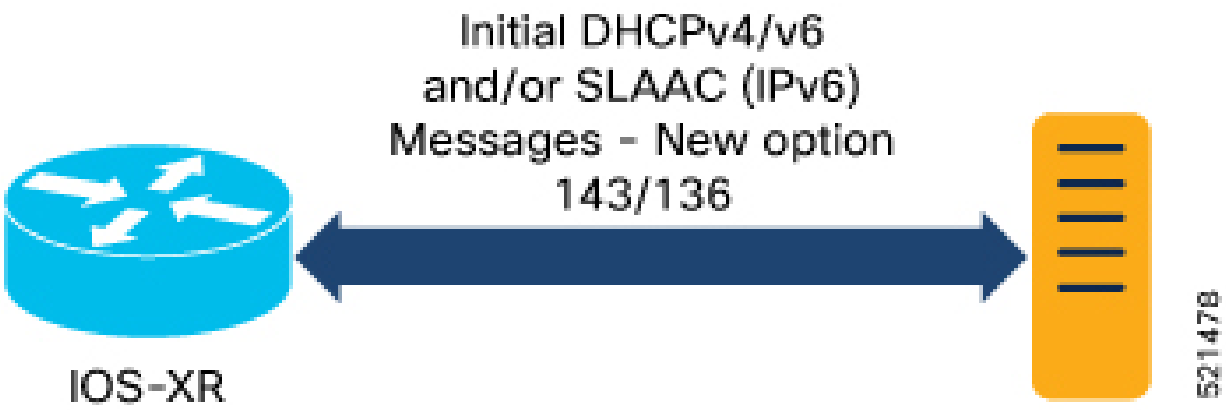
b. **DHCP discovery**:

1. The router initiates a DHCP request to the DHCP server.

2. The DHCP server responds with a DHCPv4 143 address option (for IPv4 addressing) or a DHCPv6 136 option (for IPv6 addressing).

Note URLs to access bootstrap servers for further configuration is listed in options 136 and 143.

Figure 2: DHCP discovery



c. Router validation:

1. After receiving the URL from the DHCP server, the router initiates a gRPC connection to the Bootz server. The address of the Bootz server is obtained from the DHCP response from server.
2. After the onboarding device is authenticated, the web server sends the required artifacts along with the bootstrap response data to the onboarding device.

d. Server validation:

The router receives the bootstrap response data that contains Owner Certificate, Ownership Voucher, and the details of the image upgrade, if any.

Bootstrap response data includes the following:

- Image path
- Image version
- Trust anchor
- Boot configuration
- GNSI artifacts

These artifacts come from the Bootz server as a bootstrap response gRPC message. The router verifies the ownership voucher by validating its signature to one of its preconfigured trust anchors and downloads the image. When the router obtains the onboarding information, it reports the bootstrapping progress to the Bootz server.

e. Artifact Validation:

The router validates the artifact received from the Bootz server.

1. The device extracts the `pinned-domain-cert` node, an X.509 certificate from the ownership voucher to verify the owner certificate.

2. The device authenticates the owner certificate by performing the X.509 certificate path verification process on the trusted certificate.
3. Finally, the device verifies whether the conveyed information artifact is signed by the validated owner certificate.

f. Provision the device:

1. The device first processes the boot image information.
2. Executes the script and then onboards the artifacts received from the gRPC server.

g. After the onboarding process is completed, the network device is operational.