Setting Up a Multizone System

The installation of the Cisco Configuration Engine software does not offer the multizone system setup by default. If you require a multizone system setup, you must enable the multizone feature during the system setup. To setup multiple IP addresses on the Cisco Configuration Engine server, you must manually customize the network parameters of the server to have multiple IP addresses. You can configure multiple IP addresses by using IP aliasing on a network interface card or by using multiple network interface cards where each card should have an IP address. This chapter provides a brief overview of the Cisco Configuration Engine multizone setup. It contains the following sections:

- Setup Restrictions, page 4-41
- Typical Deployment of the Multizone System, page 4-41

Setup Restrictions

Two network interfaces are installed in the Cisco Configuration Engine server: **eth0** (Ethernet 0) and **eth1** (Ethernet 1). Both interfaces can be configured and connected to networks. The Cisco Configuration Engine setup has the following restrictions:

1. For both the **eth0** and **eth1** interfaces, the default gateway must be configured on the same network as **eth0**.
2. The primary IP address and hostname should be assigned to **eth0**.
3. The prompt CNS Event Bus Network parameter in the setup of CNS Configuration Engine controls the location of the CNS Event Bus. It should be set as **eth0** hostname.
4. Ethernet 0 is used to connect to the management network. The CPE resides in the management network.

Typical Deployment of the Multizone System

To deploy the Cisco Configuration Engine in a distributed architecture in different security zones, follow these steps:

- Zone 1: Deploy the Cisco Configuration Engine processes which communicate with the network elements through the public network.
- Zone 2: Deploy the Cisco Configuration Engine administrative interfaces, APIs, and the back-end services.
- Zone 3: Deploy the LDAP and the Network File System with the template files.

To deploy one instance of the Cisco Configuration Engine in a distributed architecture, the Cisco Configuration Engine should be in a Demilitarized Zone (DMZ). Figure 4-1 shows a typical deployment of Cisco Configuration Engine server with the Cisco Configuration Engine software in a multi-network environment: private network and public network.

- Private Network—The private network contains the Network Operations Center (NOC), where the provisioning applications connect to the Cisco Configuration Engine through the CNS Event Bus.

- Public Network—The public network is the entry to the management network where CPE connects to the Cisco Configuration Engine through TCP connections.

Figure 4-1   Multizone System
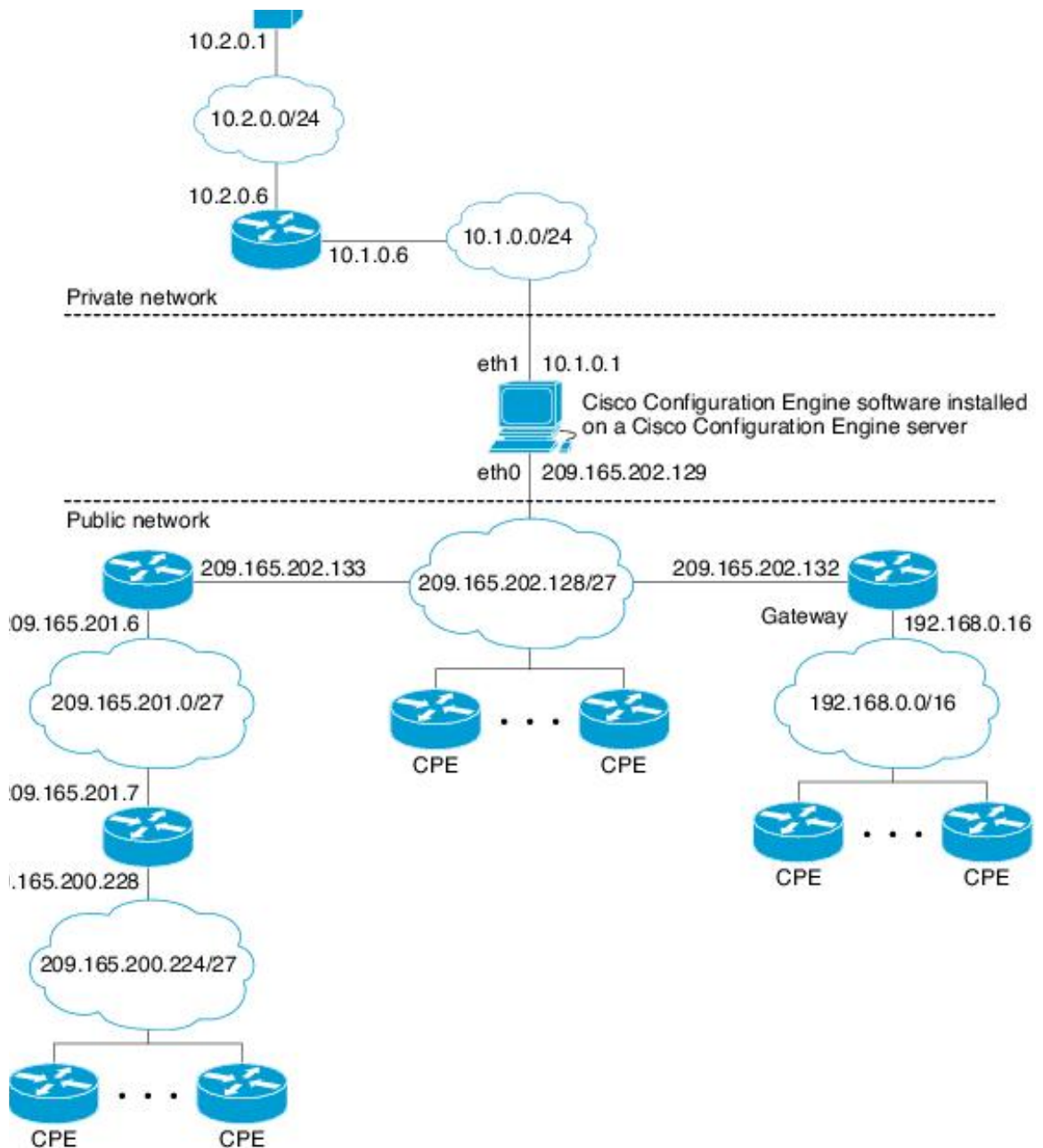
- In Figure 4-1, the public network represents **Zone 1**, private network represents **Zone 3** and the Cisco Configuration Engine resides in **Zone 2** of the DMZ.

- In Cisco Configuration Engine, the server can be configured to block all the administrative requests from the public network. This is done automatically during the setup. The setup program checks if multiple IP addresses are assigned to the Cisco Configuration Engine server. If so, it prompts the user to enable the multi-zone feature.

```
Your box has multiple IP Addresses assigned: 17x.xx.xxx.xx 17x.xx.xxx.xxx You can create
http zones so that http traffic can be limited on the IP Address 17x.xx.xxx.xx. Only
selected URLs can be accessed using IP Address 17x.xx.xxx.xx.
    Do you want to create zones to have limited access to CE from public
    network (y/n)?  [n] y
    Do you want to allow plain-text http access to CE from public network
    (y/n)?  [y] y
```

Typical Deployment of the Multizone System