



# cnBNG Installation and Configuration

- [Feature Summary and Revision History, on page 1](#)
- [Feature Description, on page 1](#)
- [Installing cnBNG and Accessing BNG Ops Center, on page 3](#)

## Feature Summary and Revision History

### Summary Data

**Table 1: Summary Data**

|  |                                   |
|--|-----------------------------------|
| Applicable Product(s) or Functional Area | cnBNG                             |
| Applicable Platform(s)                   | SMI                               |
| Feature Default Setting                  | Disabled - Configuration Required |
| Related Changes in this Release          | Not Applicable                    |
| Related Documentation                    | Not Applicable                    |

### Revision History

**Table 2: Revision History**

## Feature Description

This chapter describes cnBNG installation and configuration using the Ultra Cloud Core Subscriber Microservices Infrastructure (SMI) Cluster Manager and the BNG Operations (Ops) Center. The BNG Ops Center is based on the ConfD command line interface (CLI).

To install the SMI Cluster Manager, refer to the "Deploying the SMI Cluster Manager on VMware vCenter" section in the *Ultra Cloud Core Subscriber Microservices Infrastructure - Deployment Guide*.

The SMI Ops Center is the platform to install the cnBNG cluster with the offline or online repository. It is mandatory to install the SMI Ops Center to set up and access the BNG Ops Center.



**Note** To access the offline or online repository, contact your Cisco Account Manager or representative to get access to the offline or online repository.

## BNG Ops Center

The BNG Ops Center is a system-level infrastructure that provides the following functionality:

- A user interface to trigger a deployment of microservices with the flexibility of providing variable helm chart parameters to control the scale and properties of Kubernetes objects (deployment, pod, services, and so on) associated with the deployment.
- A user interface to push application-specific configuration to one or more microservices through Kubernetes configuration maps.
- A user interface to issue application-specific execution commands (such as show and clear commands). These commands:
  - Invoke some APIs in application-specific pods
  - Display the information returned on the user interface application

The following figure shows a sample of the web-based CLI presented to the user.

```

Username: admin
Warning: Permanently added '[localhost]:2024' (RSA) to the list of known hosts.
admin@localhost's password:

Welcome to the bng CLI on unknown
Copyright © 2016–2020, Cisco Systems, Inc.
All rights reserved.

admin connected from 127.0.0.1 using ssh on ops-center-bng-ops-center-68bb45478f-62jwv

Warning!!! Your password will expire in 9 days!

[unknown] bng# show running-config
helm default-repository bng-master
helm repository bng-lac
access-token mgIdatur:AKCpSekcbPUSsIifdwVvxqXjSchQkweH7sD1Xxe9JktjKbpg6Yj9xurfvWn9djkAy8UpZlo
url https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-snapshot/mobile-cnbt-bng/bng-products/dev-bng-lac/ins/
exit
helm repository bng-master
access-token mgIdatur:AKCpSekcbPUSsIifdwVvxqXjSchQkweH7sD1Xxe9JktjKbpg6Yj9xurfvWn9djkAy8UpZlo
url https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-snapshot/mobile-cnbt-bng/bng-products/master/
exit
k8s name unknown
k8s namespace bng
k8s nf-name bng
k8s registry dockerhub.cisco.com/smi-fuse-docker-internal
k8s single-node true
k8s use-volume-claims false
k8s ingress-host-name 10.84.102.189.nip.io
aaa authentication users user admin
uid 117
gid 117
password $1sk7Eytecp$HfM3TJHzjNcfmUmHspB1
ssh_keydir /tmp/admin/.ssh
homedir /tmp/admin
exit
aaa ios level 0
prompt "h> "
exit
aaa ios level 15
prompt "h# "

```

The BNG Ops Center allows you to configure features such as licensing, REST endpoint, and CDL.

# Installing cnBNG and Accessing BNG Ops Center

This section describes how to install cnBNG and access the BNG Ops Center.

The Ultra Cloud Core SMI platform is responsible for setting up and managing the Cloud Native Broadband Network Gateway application.



**Note** The cnBNG installation is tested and qualified on the VMware vCenter 6.7 environment.

## Prerequisites

Before installing cnBNG on the SMI layer in an offline environment:

- Ensure that the SMI Cluster Manager all-in-one (AIO) is installed. This helps orchestrate the K8s Cluster and load the image.
- Ensure that all SMI K8s cluster nodes are in Ready state.
- Run the SMI synchronization operation for the BNG Ops Center and Cloud Native Common Execution Environment (CN-CEE).

For CEE installation, refer to the *Ultra Cloud Core Common Execution Environment- Configuration and Administration Guide*.

- Ensure that the local repositories, which host the product offline TAR ball version, is installed.

### System Requirements

| Feature    | Description   |
|------------|---|
| Disk Space | 2 x 800 GB SSD (RAID 1) or equivalent input/output operations per second (IOPS) and redundancy.   |
| Hardware   | <ul style="list-style-type: none"> <li>• High-performance x86 64-bit chipset</li> <li>• CPU performance Passmark benchmark of 13K rating per chip and 1,365 rating per thread, or better</li> <li>• VMware ESXi-compatible</li> </ul> |

| Feature                | Description  |
|------------------------|--|
|                        | <p><b>Note</b> The following is recommended:</p> <ul style="list-style-type: none"> <li>• Cisco UCSM5 series blade servers to achieve the best performance.</li> <li>• All the host servers should be UCSC-C240-M5SX or UCSC-C220-M5SX.</li> <li>• All the UCS systems should have SSD storage type.</li> <li>• UCS C240M5 servers for better performance and to avoid infrastructure issues.</li> </ul> |
| Platform               | <p>VMware ESXi and VMware vCenter versions 6.5 and 6.7</p> <p><b>Note</b> SMI Cluster Manger support is qualified on the preceding platforms.</p>  |
| Memory                 | <ul style="list-style-type: none"> <li>• At least DDR3-1600 or better than 1600 MT/s</li> <li>• ECC</li> </ul>   |
| Deployment Requirement | <p>Hardware oversubscription, network saturation, or CPU oversubscription reduces application performance and productivity. The Cisco Ultra Cloud Core Subscriber Microservices Infrastructure detects and takes action when infrastructure requirements are not met.</p>  |

## Installing cnBNG in an Offline Environment

Using the SMI Cluster Manager, download the offline TAR ball of the cnBNG, the host and its charts, and corresponding images in the local registries. The SMI Cluster Manager supports the deployment of the BNG Ops Center and all the applications and services associated with it. This section describes the procedures involved in installing cnBNG in an offline environment using the SMI Cluster Manager.

To install cnBNG, complete the following steps:

1. Download the TAR ball from the URL.

```
software-packages download URL
```

**Example:**

```
SMI Cluster Manager# software-packages download
http://<ipv4address>:<port_number>/packages/bng-2021-02-1.tar
```

2. Verify whether the TAR balls are loaded.

```
software-packages list
```

**Example:**

```
BNG Cluster Manager# software-packages list
[ bng-2021-02-1 ]
[ sample ]
```

3. Configure the necessary SMI Ops Center parameters in the cluster to install cnBNG.

```

config
  cluster cluster_name
    ops-centers app_name instance_name
      repository url
      netconf-ip ipv4_address
      netconf-port port
      ssh-ip ipv4_address
      ssh-port port
      ingress-hostname <ipv4_address>.<customer_specific_domain_name>
      initial-boot-parameters use-volume-claims true/false
      initial-boot-parameters first-boot-password password
      initial-boot-parameters auto-deploy true/false
      initial-boot-parameters single-node true/false
      initial-boot-parameters image-pull-secrets
    exit
  exit

```

**Example:**

```

SMI Cluster Manager# config
Entering configuration mode terminal
SMI Cluster Manager(config)# clusters cnbng-smi-cluster-01
SMI Cluster Manager(config-clusters-cnbng-smi-cluster-01)# ops-centers bng bng
SMI Cluster Manager(config-ops-centers-bng/bng)# repository
https://charts.10.10.105.50.nip.io/bng-2021.02.1
SMI Cluster Manager(config-ops-centers-bng/bng)# ingress-hostname 10.10.105.34.nip.io
SMI Cluster Manager(config-ops-centers-bng/bng)# initial-boot-parameters use-volume-claims
true
SMI Cluster Manager(config-ops-centers-bng/bng)# initial-boot-parameters
first-boot-password test123
SMI Cluster Manager(config-ops-centers-bng/bng)# initial-boot-parameters auto-deploy
false
SMI Cluster Manager(config-ops-centers-bng/bng)# initial-boot-parameters single-node
false
SMI Cluster Manager(config-ops-centers-bng/bng)# exit
SMI Cluster Manager(config-clusters-cnbng-smi-cluster-01)# exit
SMI Cluster Manager(config)#

```

**4. Configure the secrets, if your local registry contains secrets.**

```

config
  cluster cluster_name
    secrets docker-registry secret_name
      docker-server server_name
      docker-username username
      docker-password password
      docker-email email
      namespace k8s namespace
    commit
    exit
  exit

```

**Example:**

```

SMI Cluster Manager# config
SMI Cluster Manager(config)# clusters test2
SMI Cluster Manager(config-clusters-test2)# secrets docker-registry secl
SMI Cluster Manager(config-docker-registry-secl)# docker-server serv1
SMI Cluster Manager(config-docker-registry-secl)# docker-username user1

```

```

SMI Cluster Manager(config-docker-registry-sec1)# docker-password Cisco@123
SMI Cluster Manager(config-docker-registry-sec1)# docker-email reg@cisco.com
SMI Cluster Manager(config-docker-registry-sec1)# bng bng
SMI Cluster Manager(config-docker-registry-sec1)# exit
SMI Cluster Manager(config-clusters-test2)# exit
SMI Cluster Manager(config)#

```

##### 5. Run the cluster synchronization.

```
clusters cluster_name actions sync run
```

##### Example:

```
SMI Cluster Manager# clusters cnbng-smi-cluster-01 actions sync run
```

##### Notes:

- **software-packages download** *url*—Specifies the software packages to be downloaded through HTTP/HTTPS.
- **software-packages list**—Specifies the list of available software packages.
- **ops-centers** *app\_name instance\_name*—Specifies the BNG Ops Center and instance. *app\_name* is the application name. *instance\_name* is the name of the instance.
- **repository** *url*—Specifies the local registry URL for downloading the charts.
- **netconf-ip** *ipv4\_address*—Specifies the BNG Ops Center netconf IPv4 address.
- **netconf-port** *port*—Specifies the BNG Ops Center netconf port number.
- **ssh-ip** *ipv4\_address*—Specifies the SSH IPv4 address for the BNG Ops Center.
- **ssh-port** *port*—Specifies the SSH port number for the BNG Ops Center.
- **ingress-hostname** *<ipv4\_address>. <customer\_specific\_domain\_name>*—Specifies the ingress hostname to be set to the BNG Ops Center. *<customer\_specific\_domain\_name>* specifies the domain name of the customer.
- **initial-boot-parameters**—Specifies the initial boot parameters for deploying the helm charts.
  - **use-volume-claims** *true/false*—Specifies the usage of persistent volumes. Set this option to True to use persistent volumes. The default value is true.
  - **first-boot-password** *password*—Specifies the first boot password for the product's Ops Center.
  - **auto-deploy** *true/false*—Auto deploys all the services of the product. Set this option to false to deploy only the product's Ops Center.
  - **single-node** *true/false*— Specifies the product deployment on a single node. Set this option to false for multi node deployments.
  - **image-pull-secrets**—Specifies the docker registry secret name to be used.
- **secrets docker-registry** *secret\_name*—Specifies the secret name for your docker registry.
  - **docker-server** *server\_name*—Specifies the docker server name.
  - **docker-username** *username*—Specifies the docker registry user name.
  - **docker-password** *password*—Specifies the docker registry password.

- **docker-email** *email*—Specifies the docker registry email.
- **namespace** *namespace*—Specifies the docker registry namespace.

### Verifying the cnBNG Installation

Verify the status of the cnBNG installation deployment through the cnBNG CLI. To verify, use the following commands:

1. Log in to the cnBNG product CLI.
2. Verify whether the charts are loaded in the specific instance (verify the namespace).

#### **show helm charts**

##### **Example:**

```
bng# show helm charts
CHART      INSTANCE  STATUS      VERSION  REVISION  RELEASE  NAMESPACE
-----
infra-charts - DEPLOYED 0.0.6-rel-2021-01-0073-210208130850-fac5207 1 bng-bng-infra-charts
  bng-bng
oam-pod - DEPLOYED 0.1.2-rel-2021-01-0144-210122165946-fcb74ed 1 bng-bng-oam-pod bng-bng
bng-dashboard - DEPLOYED 0.0.1-rel-2021-01-0039-210122165311-0d542be 1
bng-bng-bng-dashboard bng-bng
etcd-cluster - DEPLOYED 0.7.0-0-7-0060-210203074532-f118407 1 bng-bng-etcd-cluster bng-bng
ngn-datastore - DEPLOYED 1.3.0-1-3-0782-210125161812-f50a892 1 bng-bng-ngn-datastore
bng-bng
```

3. Verify the status of the system.

#### **show system status**

##### **Example:**

```
bng# show system status
system status deployed true
system status percent-ready 100.0
```

##### **Notes:**

- **show helm charts**—Displays the helm release details.
- **show system status**—Displays the status of the system.

## Accessing BNG Ops Center

You can connect to the BNG Ops Center through SSH or the web-based CLI console.

1. SSH:

```
ssh admin@ops_center_pod_ip -p 2024
```

2. Web-based console:

- a. Log in to the Kubernetes master node.
- b. Run the following command:

```
kubectl get ingress <namespace>
```

The available ingress connections get listed.

- c. Select the appropriate ingress and access the BNG Ops Center.
- d. Access the following URL from your web browser:

```
cli.<namespace>-ops-center.<ip_address>.nip.io
```

By default, the Day 0 configuration is loaded into the cnBNG.

### Day 0 Configuration

To view the Day 0 configuration, run the following command.

```
show running-config
```

The following is a sample Day 0 configuration:

## CP and UP Service Configuration

The CP service requires the basic configuration to process the API calls.




---

**Note** For information about the User Plane service configuration, refer to the *Cloud Native BNG User Plane Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.3.x*

---

### Configuring the CP

The CP configuration is provided using the Ops Center infrastructure.

The following is a sample CP configuration:

```
ipam
 source local
 address-pool Default-Pool
 address-quarantine-timer 60
 vrf-name default
 ipv4
  split-size
  per-cache 131072
  per-dp 131072
  exit
 address-range 13.0.0.1 13.1.255.255
 exit
 ipv6
 address-ranges
  split-size
  per-cache 65536
  per-dp 65536
  exit
  address-range 1:4::1 1:4::ffff
  address-range 1:5::1 1:5::ffff
  address-range 1:6::1 1:6::ffff
  address-range 1:7::1 1:7::ffff
  exit
 prefix-ranges
  split-size
  per-cache 65536
```



```
        per-dp      65536
    exit
    prefix-range 2003:db0:: length 48
    prefix-range 2003:db1:: length 48
    prefix-range 2003:db2:: length 48
    prefix-range 2003:db3:: length 48
    exit
exit
address-pool VRF-Pool
    address-quarantine-timer 60
    vrf-name                it_vrf
    ipv4
        split-size
        per-cache 131072
        per-dp    131072
    exit
    address-range 14.0.0.1 14.1.255.255
    exit
    ipv6
        address-ranges
        split-size
        per-cache 65536
        per-dp    65536
    exit
        address-range 2:4::1 2:4::ffff
        address-range 2:5::1 2:5::ffff
        address-range 2:6::1 2:6::ffff
        address-range 2:7::1 2:7::ffff
    exit
    prefix-ranges
    split-size
    per-cache 65536
    per-dp    65536
    exit
        prefix-range 2004:db0:: length 48
        prefix-range 2004:db1:: length 48
        prefix-range 2004:db2:: length 48
        prefix-range 2004:db3:: length 48
    exit
exit
address-pool pool-ISP
    address-quarantine-timer 60
    vrf-name                default
    ipv4
        split-size
        per-cache 131072
        per-dp    131072
    exit
    address-range 11.0.0.1 11.1.255.255
    exit
    ipv6
        address-ranges
        split-size
        per-cache 65536
        per-dp    65536
    exit
        address-range 4:2::1 4:2::ffff
        address-range 4:3::1 4:3::ffff
        address-range 4:4::1 4:4::ffff
        address-range 4:5::1 4:5::ffff
    exit
    prefix-ranges
```

```

    split-size
      per-cache 65536
      per-dp 65536
    exit
    prefix-range 2001:db0:: length 48
    prefix-range 2001:db1:: length 48
    prefix-range 2001:db2:: length 48
    prefix-range 2001:db3:: length 48
  exit
exit
address-pool pool-st
vrf-name default
static enable user-plane asr9k-2
ipv4
  split-size
    per-cache 262144
    per-dp 262144
  exit
  address-range 12.0.0.1 12.3.255.254 default-gateway 12.0.0.1
exit
ipv6
  address-ranges
    split-size
      per-cache 8192
      per-dp 8192
    exit
    address-range 2:2::1 2:2::ff00
  exit
  prefix-ranges
    split-size
      per-cache 8192
      per-dp 8192
    exit
    prefix-range 3001:db0:: length 48
  exit
exit
address-pool static-pool
vrf-name access-vrf-1
static enable user-plane asr9k-1
ipv4
  split-size
    no-split
  exit
  address-range 20.20.0.0 20.20.0.255 default-gateway 20.20.0.1
exit
exit
cdl node-type session
cdl logging default-log-level error
cdl datastore session
  endpoint replica 2
  endpoint settings slot-timeout-ms 750
  index replica 2
  index map 1
  slot replica 2
  slot map 2
  slot notification limit 300
exit
cdl kafka replica 2
profile dhcp dhcp-server1
ipv4
  mode server

```

```
server
  pool-name pool-ISP
  dns-servers [ 8.8.8.8 ]
  lease hours 6
  lease minutes 40
exit
exit
ipv6
mode server
server
  iana-pool-name pool-ISP
  iapd-pool-name pool-ISP
  lease days 0
  lease hours 4
  lease minutes 2
exit
exit
exit
profile dhcp dhcp-server3
ipv4
mode server
server
  pool-name Default-Pool
  dns-servers [ 8.8.8.8 ]
  lease days 1
  lease hours 6
  lease minutes 3
exit
exit
ipv6
mode server
server
  iana-pool-name Default-Pool
  iapd-pool-name Default-Pool
  lease days 1
  lease hours 6
  lease minutes 3
exit
exit
exit
profile dhcp dhcp-server4
ipv4
mode server
server
  pool-name VRF-Pool
  dns-servers [ 8.8.8.8 ]
  lease hours 6
  lease minutes 40
exit
exit
ipv6
mode server
server
  iana-pool-name VRF-Pool
  iapd-pool-name VRF-Pool
  lease hours 6
exit
exit
exit
profile pppoe bng
ctrl-pkt-priority 7
max-payload deny
service-name [ value]
ac-name 123@acname
```

```

ac-cookie          123@accookie
exit
profile aaa aaa-profl
authorization
  type subscriber method-order [ local ]
  username value <username>
  password <password>
exit
accounting
  method-order [ local ]
exit
exit
profile server-group local
radius-group local
exit
profile subscriber subs-default
dhcp-profile          dhcp-server3
session-type          ipv4v6
activate-feature-templates [ svc1 QOS_HSI QOS_IPTV QOS_VOICE ]
aaa authorize aaa-profl
exit
profile subscriber subs-prof1
dhcp-profile          dhcp-server1
session-type          ipv4v6
activate-feature-templates [ svc1 ]
aaa authorize aaa-profl
exit
profile subscriber subs-prof1-pppoe
dhcp-profile          dhcp-server1
pppoe-profile bng
session-type          ipv4v6
class ppp_cls_map
  activate-feature-templates [ bng_ft_start ]
  matches
    match-type all
    match protocol [ ppp ]
  exit
exit
event session-activate
class ppp_cls_map
  activate-feature-templates [ bng_ft_activate ]
  matches
    match-type all
    match protocol [ ppp ]
  exit
  aaa authenticate aaa-profl
  exit
exit
exit
profile subscriber subs-vrf
dhcp-profile          dhcp-server4
session-type          ipv4v6
activate-feature-templates [ svc3 QOS_VOICE QOS_IPTV QOS_HSI ]
aaa authorize aaa-profl
exit
profile subscriber test-ppp-subscriber
dhcp-profile          dhcp-server3
pppoe-profile          test-ppp-pppoeprofile
session-type          ipv4v6
activate-feature-templates [ svc1 test-ppp-featuretemplate QOS_VOICE QOS_IPTV QOS_HSI ]
aaa authorize aaa-profl
exit
profile feature-template ACL-V4
  ipv4

```

```
    ingress-acl iACL_BNG_IPv4_IN
    egress-acl iACL_BNG_IPv4_OUT
  exit
exit
profile feature-template ACL-V6
  ipv6
    ingress-acl v6-IN
    egress-acl v6-out
  exit
exit
profile feature-template QOS_HSI
  qos
    in-policy QOS_HSI_100B_IN
    out-policy QOS_HSI_100B_OUT
    merge-level 30
  exit
  service-accounting
    enable
    aaa-profile aaa-profl
    periodic-interval 1800
  exit
exit
profile feature-template QOS_VOICE
  qos
    in-policy QOS_VOICE_INGRESS
    out-policy QOS_VOICE_EGRESS
    merge-level 40
  exit
exit
profile feature-template QOS_IPTV
  qos
    in-policy QOS_IPTV_INGRESS
    out-policy QOS_IPTV_EGRESS
    merge-level 50
  exit
exit
profile feature-template QOS
  qos
    in-policy QOS-IN
    out-policy QOS-OUT
    merge-level 10
  exit
  service-accounting
    enable
    aaa-profile aaa-profl
  exit
exit
profile feature-template bng_ft_activate
  ipv4
    mtu 1492
    ingress-acl in4acl3
    disable-unreachables
    verify-unicast-source reachable-via-rx
  exit
  ipv6
    mtu 1492
    ingress-acl match-ipv6-acl
    disable-unreachables
    verify-unicast-source reachable-via-rx
  exit
  session-accounting
    enable
    aaa-profile aaa-profl
    periodic-interval 1200
```

```

exit
ppp
  ipcp dns 8.8.8.8 1.2.3.4
  ipcp peer-address-pool pool-ISP
  ipcp renegotiation ignore
  ipv6cp renegotiation ignore
exit
exit
profile feature-template bng_ft_start
  vrf-name default
  session-accounting
    enable
    aaa-profile      aaa-prof1
    periodic-interval 1200
  exit
ppp
  authentication [ pap ]
  lcp delay seconds 1 milliseconds 0
  lcp renegotiation ignore
  exit
exit
profile feature-template svc1
  vrf-name default
  ipv4
    mtu          1492
    ingress-acl  iACL_BNG_IPv4_IN_1
    egress-acl   iACL_BNG_IPv4_OUT_1
    disable-unreachables
    verify-unicast-source reachable-via-rx
  exit
  ipv6
    mtu          1492
    ingress-acl  ipv6-acl-in-1
    egress-acl   ipv6-acl-out-1
    disable-unreachables
    verify-unicast-source reachable-via-rx
  exit
  session-accounting
    enable
    aaa-profile      aaa-prof1
    periodic-interval 1800
  exit
exit
exit
profile feature-template svc2
  ppp
    ipcp peer-address-pool poolv4
    ipcp renegotiation ignore
    lcp renegotiation ignore
  exit
exit
profile feature-template svc3
  vrf-name it_vrf
  ipv4
    mtu          1492
    ingress-acl  iACL_BNG_IPv4_IN_1
    egress-acl   iACL_BNG_IPv4_OUT_1
    disable-unreachables
    verify-unicast-source reachable-via-rx
  exit
  ipv6
    mtu          1492
    ingress-acl  ipv6-acl-in-1
    egress-acl   ipv6-acl-out-1
    disable-unreachables

```

```
verify-unicast-source reachable-via-rx
exit
session-accounting
enable
aaa-profile      aaa-profl
periodic-interval 1800
exit
exit
profile feature-template svc4
vrf-name default
session-accounting
enable
aaa-profile      aaa-profl
periodic-interval 1800
exit
exit
profile feature-template test-ppp-featuretemplate
vrf-name default
ipv4
mtu 1400
exit
ppp
ipcp peer-address-pool Default-Pool
ipcp renegotiation ignore
ipv6cp renegotiation ignore
lcp renegotiation ignore
exit
exit
profile feature-template uRPF
ipv4
verify-unicast-source reachable-via-rx
exit
ipv6
verify-unicast-source reachable-via-rx
exit
exit
profile radius
algorithm round-robin
deadtime 3
detect-dead-server response-timeout 60
max-retry 1
timeout 5
server 172.16.254.55 1812
type auth
secret <secret_value>
exit
server 172.16.254.55 1813
type acct
secret <secret_value>
exit
server 172.16.254.56 1812
type auth
secret <secret_value>
exit
server 172.16.254.56 1813
type acct
secret <secret_value>
exit
attribute
nas-identifier < any identifier>
nas-ip      172.16.254.86
nas-port-id < add_unique_id>
exit
server-group local
```

```

server auth 172.16.254.55 1812
exit
server auth 172.16.254.56 1812
exit
server acct 172.16.254.55 1813
exit
server acct 172.16.254.56 1813
exit
exit
exit
profile coa
client 172.16.254.55
server-key < key >
exit
client 172.16.254.56
server-key < key >
exit
exit
user-plane <add UP name like asr9k-11>
peer-address ipv4 172.16.247.72
subscriber-profile subs-default
exit
endpoint sm
exit
endpoint nodemgr
exit
endpoint n4-protocol
exit
endpoint dhcp
exit
endpoint radius
replicas 1
vip-ip 172.16.254.86
interface coa-nas
sla response 140000
vip-ip 172.16.254.86 vip-port 2000
exit
exit
endpoint udp-proxy
replicas 1
nodes 2
vip-ip 172.16.254.86 vip-port 3799
interface n4
sla response 150000
exit
interface gtpu
sla response 150000
exit
exit
endpoint charging
exit
logging transaction duplicate enable
logging name bng-dhcp0.bngfsol.collision level application info
logging name bng-dhcp0.bngfsol.collision level transaction info
logging name infra.application.core level application warn
logging name infra.config.core level application error
logging name infra.config.core level transaction error
k8 bng
etcd-endpoint etcd:2379
datastore-endpoint datastore-ep-session:8882
tracing
enable
enable-trace-percent 30
append-messages true

```



```

        endpoint          jaeger-collector:9411
    exit
exit
k8 label protocol-layer key smi.cisco.com/vm-type value protocol
exit
k8 label service-layer key smi.cisco.com/vm-type value service
exit
k8 label cdl-layer key smi.cisco.com/vm-type value session
exit
k8 label oam-layer key smi.cisco.com/vm-type value oam
exit
system mode running
exit

```

## Configuring the UP

The following is a sample UP configuration:

```

user-plane asr9k-11
peer-address ipv4 10.105.247.124
subscriber-profile subs-default
port-id Bundle-Ether2.10
    subscriber-profile subs-vrf
exit
port-id Bundle-Ether2.20
    subscriber-profile subs-vrf
port-id Bundle-Ether2.10
exit
port-id Bundle-Ether2.30
    subscriber-profile subs-vrf
port-id Bundle-Ether2.10
exit
port-id Bundle-Ether2.40
    subscriber-profile subs-vrf
port-id Bundle-Ether2.10
exit
exit

```

## Loading Day1 Configuration

To load the Day 1 configuration for cnBNG, run the following command:

```
ssh admin@ops_center_pod_ip -p 2024 < Day1config.cli
```




---

**Note** The **day1config.cli** file contains the necessary parameters required for the Day 1 configuration.

---

Alternatively, you can copy the configuration and paste it in the BNG Ops Center CLI to load the Day 1 configuration.

```

config
    <Paste the Day 1 configuration here>
commit
exit

```

### Day1config.cli

The **day1config.cli** file contains the Day 1 configuration for cnBNG. For a sample day1 configuration, see [Configuring the CP, on page 8](#).

