



## Appendix

- [NFVIS Deployment in Sites with Low WAN Bandwidth, on page 1](#)
- [Single IP Address Sharing Between NFVIS and the Router VM, on page 2](#)

### NFVIS Deployment in Sites with Low WAN Bandwidth

The VNF images are downloaded from Cisco SD-WAN Manager onto NFVIS device during provisioning. Across low bandwidth WAN uplinks, the image download can be time consuming. In this case, there is an option to make the large image files available in the local repository of NFVIS device and the device is instructed to use the local image during provisioning.

The following steps shows how you can create and upload VNF images in NFVIS.

1. Upload the image package in Cisco SD-WAN Manager image repository.

For example:

```
vEdge_20.3.904-9_vBranch_Cisco_ENB_Viptela_monitor_EFT.tar.gz
```

2. SCP copy the VNF image onto NFVIS device. Cisco SD-WAN Manager then skips downloading the package. Ensure that you rename the package when you SCP and upload the same package into Cisco SD-WAN Manager.

```
scp<username>@<SCP_SERVER_IP>:/<package_name>  
intdatastore:<vnf_typ>_<name>_<version>_<package_name>
```

Example:

```
scp admin@172.19.156.240:/vEdge_20.3.904-9_vBranch_Cisco_ENB_Viptela_monitor_EFT.tar.gz  
intdatastore:/ROUTER_vEdge_20.3.904-9_vEdge_20.3.904-9_vBranch_Cisco_ENB_Viptela_monitor_EFT.tar.gz
```

Add <vnf\_typ>\_<name>\_<version>\_ prefix in front of the original package name which is based on the information from the image\_properties.xml file inside the package.

```
<image_properties>  
  <vnf_type>ROUTER</vnf_type>  
  <name>vEdge</name>  
  <version>20.3.904-9</version>
```

```
.....  
.....
```

```
.....
</image_properties>
```

3. Use the **show system:system file-list** command to verify that the image is copied successfully.

You can then go ahead with the rest of the Network Design template workflow and Cisco SD-WAN Manager skips the download VNF step. Ensure that you select the correct package in the Network Design template.

## Single IP Address Sharing Between NFVIS and the Router VM

This topic contains the end-to-end configuration example to configure the single IP address sharing feature between NFVIS and the router VM.

### Step 1: Configure HTTP Host for Day 0 Configuration

The following examples show how to set up the HTTP server to host the day 0 configuration file for Cisco Catalyst 8000V and Cisco vEdge devices respectively.

#### Example: Host Day 0 Configuration File for Cisco Catalyst 8000V

```
Content-Type: multipart/mixed; boundary="=====2587222130433519110=="
MIME-Version: 1.0
-----2587222130433519110==
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config"
#cloud-config
vinitparam:
- otp : ${EX_OTP}
- vbond : ${EX_VBOND}
- org : ${EX_ORGNAME}
- uuid : ${EX_UUID}

-----2587222130433519110==
Content-Type: text/cloud-boothook; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment;
  filename="config-default.txt"
#cloud-boothook
system
  host-name          ${EX_HOSTNAME}
  system-ip          ${EX_SYSTEM_IP}
  overlay-id         1
  site-id            ${EX_SITE_ID}
  port-offset        0
  control-session-pps 300
  admin-tech-on-failure
  sp-organization-name "${EX_ORGNAME}"
  organization-name  "${EX_ORGNAME}"
  port-hop
  track-transport
  track-default-gateway
  console-baud-rate  115200
  vbond ${EX_VBOND} port 12346
  logging
  disk
  enable
  !
```

```
!
!
bfd app-route multiplier 6
bfd app-route poll-interval 600000
sslproxy
no enable
rsa-key-modulus      2048
certificate-lifetime 730
eckey-type           P256
ca-tp-label          PROXY-SIGNING-CA
settings expired-certificate drop
settings untrusted-certificate drop
settings unknown-status drop
settings unsupported-protocol-versions drop
settings unsupported-cipher-suites drop
settings failure-mode close
settings minimum-tls-ver TLSv1
!
no tcpproxy enable
!
sdwan
interface GigabitEthernet2
 tunnel-interface
  encapsulation ipsec weight 1
  no border
  color default
  no last-resort-circuit
  no low-bandwidth-link
  no vbond-as-stun-server
  vmanage-connection-preference 5
  port-hop
  carrier default
  nat-refresh-interval 5
  hello-interval 1000
  hello-tolerance 12
  no allow-service all
  no allow-service bgp
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  no allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
  no allow-service snmp
  exit
exit
appqoe
no tcptopt enable
!
omp
no shutdown
send-path-limit 4
ecmp-limit 4
graceful-restart
no as-dot-notation
timers
  holdtime 60
  advertisement-interval 1
  graceful-restart-timer 43200
  eor-timer 300
exit
```

```

    address-family ipv4
      advertise connected
      advertise static
    !
    address-family ipv6
      advertise connected
      advertise static
    !
  !
!
security
  ipsec
    rekey          86400
    replay-window  512
    authentication-type sha1-hmac ah-sha1-hmac
  !
!
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
no service tcp-small-servers
no service udp-small-servers
username admin privilege 15 secret 0 admin
vrf definition Mgmt-intf
  description Transport VPN
  rd          1:512
  address-family ipv4
    route-target export 1:512
    route-target import 1:512
    exit-address-family
  !
  address-family ipv6
    exit-address-family
  !
!
vrf definition 500
  address-family ipv4
    exit-address-family
  !
  address-family ipv6
    exit-address-family
  !
!
vrf definition ${EX_DATA_VPN_NUMBER}
!
  address-family ipv4
    exit-address-family
  !
  address-family ipv6
    exit-address-family
  !
!
vrf definition ${EX_MGMT_VPN_NUMBER}
!
  address-family ipv4
    exit-address-family
  !
  address-family ipv6
    exit-address-family
  !
!
hostname ${EX_HOSTNAME}
username ${EX_SSH_USERNAME} privilege 15 secret 0 ${EX_SSH_PASSWORD}
enable password ${EX_ENABLE_PASSWORD}
!
ip name-server ${EX_DNS_IP}

```

```
!  
ip arp proxy disable  
no ip finger  
no ip rcmd rcp-enable  
no ip rcmd rsh-enable  
no ip dhcp use class  
ip multicast route-limit 2147483647  
ip bootp server  
no ip source-route  
no ip http server  
no ip http secure-server  
no ip http ctc authentication  
no ip igmp ssm-map query dns  
interface GigabitEthernet1  
  vrf forwarding 500  
  description MGMT  
  no shutdown  
  arp timeout 1200  
  ip address ${NICID_0_IP_ADDRESS} ${NICID_0_NETMASK}  
  ip redirects  
  ip mtu 1500  
  mtu 1500  
  negotiation auto  
exit  
interface GigabitEthernet2  
  description Transport  
  no shutdown  
  arp timeout 1200  
  ip address ${EX_VPN0_WAN_IP_ADDRESS} ${EX_VPN0_WAN_NETMASK}  
  ip nat outside  
  ip redirects  
  ip mtu 1500  
  mtu 1500  
  negotiation auto  
exit  
interface GigabitEthernet3  
  vrf forwarding ${EX_MGMT_VPN_NUMBER}  
  ip address ${EX_MGMT_IP_ADDRESS} ${EX_MGMT_NETMASK}  
  no shutdown  
  exit  
!  
interface GigabitEthernet4  
  vrf forwarding ${EX_DATA_VPN_NUMBER}  
  ip address ${EX_LAN_IP_ADDRESS} ${EX_LAN_NETMASK}  
  no shutdown  
  exit  
!  
interface Tunnel2  
  no shutdown  
  ip unnumbered GigabitEthernet2  
  no ip redirects  
  ipv6 unnumbered GigabitEthernet2  
  no ipv6 redirects  
  tunnel source GigabitEthernet2  
  tunnel mode sdwan  
exit  
clock timezone UTC 0 0  
logging persistent size 104857600 filesize 10485760  
logging buffered 512000  
no logging rate-limit  
logging persistent  
aaa authentication login default local  
aaa authorization exec default local  
aaa session-id common
```

```

no crypto ikev2 diagnose error
no crypto isakmp diagnose error
snmp-server ifindex persist
line con 0
  login authentication default
  speed 115200
  stopbits 1
!
line vty 0 4
  transport input ssh
!
line vty 5 80
  transport input ssh
!
lldp run
nat64 translation timeout tcp 60
nat64 translation timeout udp 1
!
!
ip route 0.0.0.0 0.0.0.0 ${EX_VPN0_WAN_GATEWAY}
!
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
ip nat route vrf 500 0.0.0.0 0.0.0.0 global
!
-----2587222130433519110==

```

### Example: Host Day 0 Configuration File for a Cisco vEdge Device for version 20.5

```

#cloud-config
write_files:
- path: /etc/viptela/otp
  content: "${OTP}"
- path: /etc/viptela/uuid
  content: "${UUID}"
- path: /etc/default/personality
  content: "vedge"
- path: /etc/default/inited
  content: "1"
- path: /etc/viptela/cdb_init_done
  content: "1"
- path: /etc/viptela/vdaemon_gen_id
  content: "0"
- path: /etc/confd/init/cloud-init.xml
  content: |
    <config xmlns="http://tail-f.com/ns/config/1.0">
      <omp xmlns="http://viptela.com/omp">
        <advertise>
          <protocol>ospf</protocol>
          <route>external</route>
        </advertise>
        <advertise>
          <protocol>connected</protocol>
        </advertise>
        <advertise>
          <protocol>static</protocol>
        </advertise>
      </omp>
      <security xmlns="http://viptela.com/security">
        <ipsec>
          <authentication-type>ah-sha1-hmac</authentication-type>
          <authentication-type>sha1-hmac</authentication-type>
        </ipsec>
      </security>
      <system xmlns="http://viptela.com/system">

```

```

<personality>vedge</personality>
<rootcert-installed>>true</rootcert-installed>
<host-name>${HOSTNAME}</host-name>
<system-ip>${SYSTEM_IP}</system-ip>
<site-id>${SITE_ID}</site-id>
<organization-name>${ORGNAME}</organization-name>
<vbond>
  <remote>${VBOND}</remote>
</vbond>
<aaa>
  <auth-order>local</auth-order>
  <auth-order>radius</auth-order>
  <auth-order>tacacs</auth-order>
  <usergroup>
    <name>basic</name>
    <task>
      <mode>system</mode>
      <permission>read</permission>
      <permission>write</permission>
    </task>
    <task>
      <mode>interface</mode>
      <permission>read</permission>
      <permission>write</permission>
    </task>
  </usergroup>
  <usergroup>
    <name>netadmin</name>
  </usergroup>
  <usergroup>
    <name>operator</name>
    <task>
      <mode>system</mode>
      <permission>read</permission>
    </task>
    <task>
      <mode>interface</mode>
      <permission>read</permission>
    </task>
    <task>
      <mode>policy</mode>
      <permission>read</permission>
    </task>
    <task>
      <mode>routing</mode>
      <permission>read</permission>
    </task>
    <task>
      <mode>security</mode>
      <permission>read</permission>
    </task>
  </usergroup>
  <user>
    <name>admin</name>
  </user>
</aaa>
</system>
<vpn xmlns="http://viptela.com/vpn">
  <vpn-instance>
    <vpn-id>0</vpn-id>
    <dns>
<password>${$siwKBQ=SwT21Ua9BSreDPI6gB8s14E6PAJoVXgMogv/wHJ8F1C6sWdRazdxorYYTLrL6syiG6qnIABInrE96HJiKF6Qrql</password>

```

```

    <dns-addr>${DNS_IP}</dns-addr>
  </dns>
  <interface>
    <if-name>ge0/0</if-name>
    <ip>
      <dhcp-client>>true</dhcp-client>
    </ip>
    <nat/>
    <tunnel-interface>
      <encapsulation>
        <encap>ipsec</encap>
      </encapsulation>
      <allow-service>
        <all>>true</all>
      </allow-service>
    </tunnel-interface>
    <shutdown>>false</shutdown>
  </interface>
  <interface>
    <if-name>ge0/3</if-name>
    <ip>
      <address>${NICID_4_IP_ADDRESS}/${NICID_4_CIDR_PREFIX}</address>
    </ip>
    <shutdown>>false</shutdown>
  </interface>
</vpn-instance>
<vpn-instance>
  <vpn-id>${DATA_VPN_NUMBER}</vpn-id>
  <interface>
    <if-name>ge0/2</if-name>
    <ip>
      <address>${SERVICE_IP}/${SERVICE_MASK_LENGTH}</address>
    </ip>
    <shutdown>>false</shutdown>
  </interface>
</vpn-instance>
<vpn-instance>
  <vpn-id>${MANAGEMENT_VPN_NUMBER}</vpn-id>
  <interface>
    <if-name>ge0/1</if-name>
    <ip>
      <address>${MGMT_IP}/${MGMT_MASK_LENGTH}</address>
    </ip>
    <shutdown>>false</shutdown>
  </interface>
</vpn-instance>
<vpn-instance>
  <vpn-id>512</vpn-id>
  <interface>
    <if-name>eth0</if-name>
    <shutdown>>false</shutdown>
  </interface>
</vpn-instance>
</vpn>
</config>

```

## Step 2: Configure Single IP Address Sharing

This example shows how to configure single IP address sharing between NFVIS and the router VMs using the CLI Add-on feature template in Cisco SD-WAN Manager.

### Sample Configuration for Cisco Catalyst 8000V Using CLI Add-on Feature Template

In this example NFVIS uses the int-mgmt-net-br interface in VPN 0 to establish control connection with Cisco SD-WAN Manager. The configuration also includes the VM lifecycle configuration for the day 0 configuration. NFVIS gets this information from HTTP server included in the configuration.

```

vm_lifecycle tenants tenant admin
  description      "Built-in Admin Tenant"
  managed_resource true
  vim_mapping      true
  deployments deployment deployment-ROUTER_1
  vm_group deployment-ROUTER_1
  image
ROUTER_C8000V_V175-Serial_C8Kv_175_LATEST_20201115_122120-serial_vBranch_Ubaid_Sdwan3.tar.gz

  flavor          ROUTER_1
  vim_vm_name     ROUTER_1
  bootup_time     900
  recovery_wait_time 5
  recovery_policy action_on_recovery REBOOT_ONLY
  !
  config_data configuration ciscosdwan_cloud_init.cfg
  file "http://172.25.221.219/config/UBAID_SDWAN_CLOUD_INITnew.cfg"
  variable EX_UUID
    val [ {{EX_UUID}} ]
  !
  variable EX_OTP
    val [ {{EX_OTP}} ]
  !
  variable EX_ORGNAME
    val [ "{{EX_ORGNAME}}" ]
  !
  variable EX_VBOND
    val [ {{EX_VBOND}} ]
  !
  variable EX_SYSTEM_IP
    val [ {{EX_SYSTEM_IP}} ]
  !
  variable EX_SITE_ID
    val [ {{EX_SITE_ID}} ]
  !
  variable EX_VPN0_WAN_GATEWAY
    val [ {{EX_VPN0_WAN_GATEWAY}} ]
  !
  variable EX_VPN0_WAN_IP_ADDRESS
    val [ {{EX_VPN0_WAN_IP_ADDRESS}} ]
  !
  variable EX_VPN0_WAN_NETMASK
    val [ {{EX_VPN0_WAN_NETMASK}} ]
  !
  variable EX_DNS_IP
    val [ {{EX_DNS_IP}} ]
  !
  variable EX_SSH_USERNAME
    val [ {{EX_SSH_USERNAME}} ]
  !
  variable EX_SSH_PASSWORD
    val [ "{{EX_SSH_PASSWORD}}" ]
  !
  variable EX_ENABLE_PASSWORD
    val [ "{{EX_ENABLE_PASSWORD}}" ]
  !
  variable EX_HOSTNAME
    val [ {{EX_HOSTNAME}} ]
  !
  variable EX_LAN_IP_ADDRESS

```

```

        val [ {{EX_LAN_IP_ADDRESS}} ]
        !
        variable EX_LAN_NETMASK
        val [ {{EX_LAN_NETMASK}} ]
        !
        variable EX_MGMT_IP_ADDRESS
        val [ {{EX_MGMT_IP_ADDRESS}} ]
        !
        variable EX_MGMT_NETMASK
        val [ {{EX_MGMT_NETMASK}} ]
        !
        variable EX_DATA_VPN_NUMBER
        val [ {{EX_DATA_VPN_NUMBER}} ]
        !
        variable EX_MGMT_VPN_NUMBER
        val [ {{EX_MGMT_VPN_NUMBER}} ]
        !
    !
!
!
single-ip-mode vm-name deployment-ROUTER_1.deployment-ROUTER_1
!
vpn 0
interface int-mgmt-net-br
    no shutdown
    tunnel-interface
    color bronze
    no allow-service bgp
    allow-service dhcp
    allow-service dns
    allow-service icmp
    no allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service ospf
    no allow-service stun
    allow-service https
    encapsulation ipsec
!
!

```

### Sample Configuration for a Cisco vEdge Cloud Router Using CLI Add-on Feature Template

In this example NFVIS uses the int-mgmt-net-br interface in VPN 0 to establish control connection with Cisco SD-WAN Manager. The configuration also includes the VM lifecycle configuration for the day 0 configuration. NFVIS gets this information from HTTP server included in the configuration.

```

vm_lifecycle tenants tenant admin
description      "Built-in Admin Tenant"
managed_resource true
vim_mapping      true
deployments deployment-ROUTER_1
vm_group deployment-ROUTER_1
    bootup_time      600
    recovery_wait_time 5
    recovery_policy action_on_recovery REBOOT_ONLY
    !
    kpi_data kpi VM_ALIVE
        metric_collector type ICMPping
        metric_collector nicid 4
    !

config_data configuration /openstack/latest/user_data

```

```

file "http://172.25.221.219/config/20.5-vedge-single-ip-dhcp.cfg"
variable EX_UUID
  val [ {{EX_UUID}} ]
!
variable EX_OTP
  val [ {{EX_OTP}} ]
!
variable EX_ORGNAME
  val [ "{{EX_ORGNAME}}" ]
!
variable EX_VBOND
  val [ {{EX_VBOND}} ]
!
variable EX_SYSTEM_IP
  val [ {{EX_SYSTEM_IP}} ]
!
variable EX_SITE_ID
  val [ {{EX_SITE_ID}} ]
!
variable EX_DNS_IP
  val [ {{EX_DNS_IP}} ]
!
variable EX_SSH_USERNAME
  val [ {{EX_SSH_USERNAME}} ]
!
variable EX_SSH_PASSWORD
  val [ "{{EX_SSH_PASSWORD}}" ]
!
variable EX_ENABLE_PASSWORD
  val [ "{{EX_ENABLE_PASSWORD}}" ]
!
variable EX_HOSTNAME
  val [ {{EX_HOSTNAME}} ]
!
variable EX_SERVICE_IP
  val [ {{EX_SERVICE_IP}} ]
!
variable EX_SERVICE_MASK_LENGTH
  val [ {{EX_SERVICE_MASK_LENGTH}} ]
!
variable EX_MGMT_IP
  val [ {{EX_MGMT_IP}} ]
!
variable EX_MGMT_MASK_LENGTH
  val [ {{EX_MGMT_MASK_LENGTH}} ]
!
variable EX_DATA_VPN_NUMBER
  val [ {{EX_DATA_VPN_NUMBER}} ]
!
variable EX_MANAGEMENT_VPN_NUMBER
  val [ {{EX_MANAGEMENT_VPN_NUMBER}} ]
!
!
!
single-ip-mode vm-name deployment-ROUTER_1.deployment-ROUTER_1
!
vpn 0
interface int-mgmt-net-br
  no shutdown
  tunnel-interface
  color bronze
  no allow-service bgp

```

```
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
encapsulation ipsec
!
!
```