EVPN With NAC Configuration Guide

In this configuration example we will examine the EVPN with NAC use case. As shown in Figure 1 below, we have two Pica8 switches in this topology. Switch R1 has a Cisco IP phone connected with it. Switch1 is also connected with our management network that gives it access to Cisco ISE network access controller. Similarly switch R2 is also connected with a host and an IP phone.

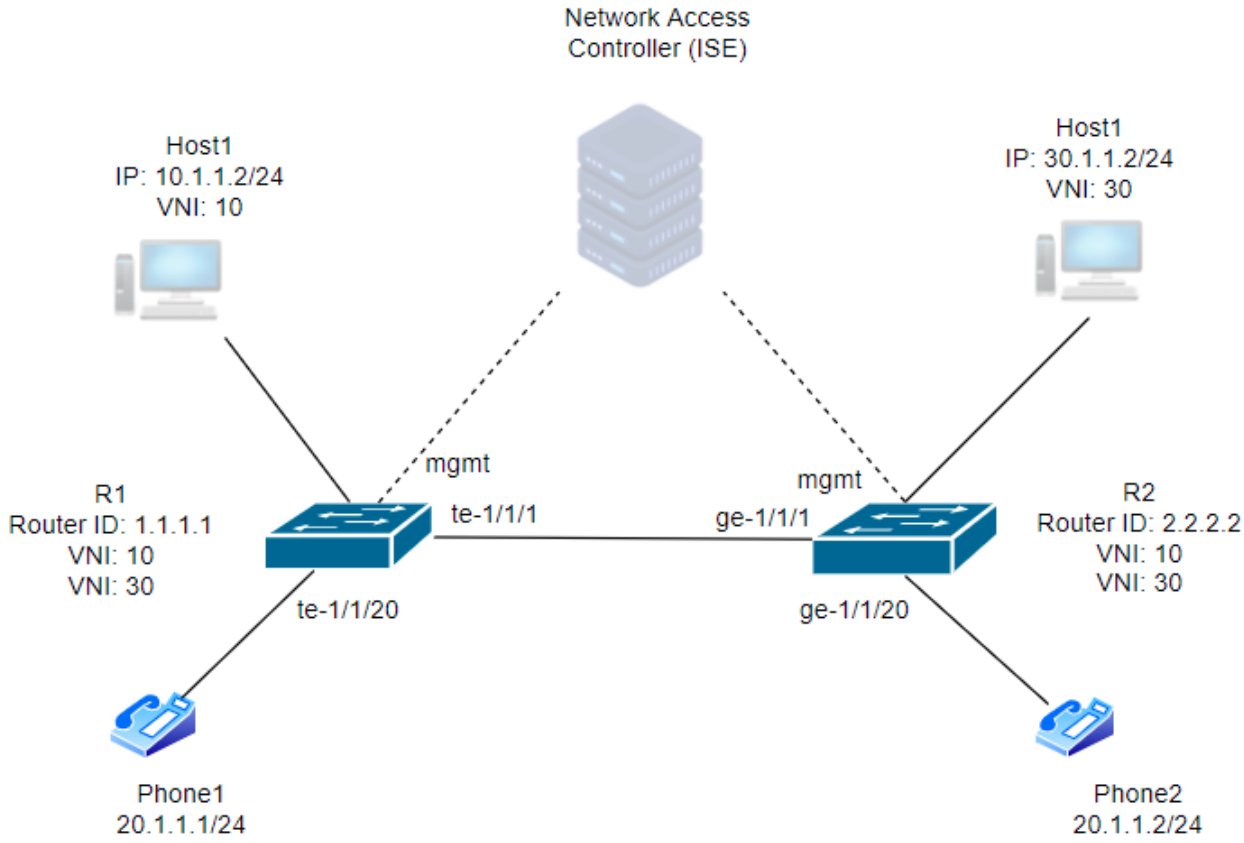

Figure 1. EVPN with NAC Topology

The general idea in this use case is that we will first program ISE to recognize any MAB authentication requests for this IP phone device and assign it a dynamic VLAN through the Access-Accept message. This will cause the switch to put the physical port connecting the IP phone into a VLAN which is part of the VXLAN network through VLAN to VNI mapping. Once part of that VNI, the IP phone can then be accessible throughout the VXLAN network. The communication between the IP phone and other devices will pass through the VXLAN tunnel if the devices are physically located on different switches. The phone can then be managed by some kind of phone management or call manager software to establish phone connectivity throughout the network however, such configuration details are beyond the scope of this document.

The routing model used in this topology for the host computers is the EVPN Asymmetric routing model in which, when two communicating devices reside in two different VNIs, routing will take place locally on the device from one VNI to the target VNI and then data packets are bridged from one switch to the other switch and forwarded to the destination device. Since ISE will usually profile IP phone devices and put them all into a single VLAN or voice VLAN, hence such devices will belong to the same VNI even if they are connected to different switches. In this example topology, ISE will assign the dynamic VLAN ID 20 to both the IP phone devices.

Switch Configuration

This section details the configuration of the two switch devices in this topology.

R1 Switch Configuration

Step 1: Configure VLAN ID, L3 VLAN interfaces loopback interfaces and IP addressing. The MTU value of layer 3 interfaces is set to 1450 to ensure there is enough space for the overlay VXLAN header. The switch will complain and refuse to commit the configuration if MTU size is not set to 1450. Interface te-1/1/10 connects to PC1 and interface te-1/1/20 connects to the IP phone.

```
admin@R1# set interface gigabit-ethernet te-1/1/1 family ethernet-switching native-vlan-id 4094
admin@R1# set interface gigabit-ethernet te-1/1/20 family ethernet-switching port-mode trunk
admin@R1# set interface gigabit-ethernet te-1/1/2 family ethernet-switching native-vlan-id 10
admin@R1# set interface gigabit-ethernet te-1/1/10 family ethernet-switching native-vlan-id 10
admin@R1# set l3-interface loopback lo address 1.1.1.1 prefix-length 32
admin@R1# set l3-interface loopback vrf1 address 201.201.201.201 prefix-length 32
admin@R1# set l3-interface vlan-interface vlan4094 mtu 1450
admin@R1# set l3-interface vlan-interface vlan4094 address 40.94.0.2 prefix-length 24
admin@R1# set l3-interface vlan-interface vlan10 vrf vrf1
admin@R1# set l3-interface vlan-interface vlan20 vrf vrf1
admin@R1# set l3-interface vlan-interface vlan30 vrf vrf1
admin@R1# set l3-interface vlan-interface vlan10 mtu 1450
admin@R1# set l3-interface vlan-interface vlan20 mtu 1450
admin@R1# set l3-interface vlan-interface vlan10 address 10.1.1.201 prefix-length 24
admin@R1# set l3-interface vlan-interface vlan20 address 20.1.1.201 prefix-length 24
admin@R1# set l3-interface vlan-interface vlan1111 vrf vrf1
admin@R1# set l3-interface vlan-interface vlan1111 router-mac 00:16:16:16:16:16
admin@R1# set l3-interface vlan-interface vlan1111 mtu 1450
admin@R1# set vlans vlan-id 20 l3-interface vlan20
admin@R1# set vlans vlan-id 10 l3-interface vlan10
admin@R1# set vlans vlan-id 30 l3-interface vlan30
admin@R1# set vlans vlan-id 1111 l3-interface vlan1111
admin@R1# set vlans vlan-id 4094 l3-interface vlan4094
```

Step 2: Configure VXLAN VNI and map VNI IDs to VLAN IDs.

```
admin@R1# set vxlans source-interface lo address 1.1.1.1
admin@R1# set vxlans vni 100 vlan 1111
admin@R1# set vxlans vni 10 vlan 10
admin@R1# set vxlans vni 30 vlan 30
admin@R1# set vxlans vni 20 vlan 20
admin@R1# set vxlans vrf vrf1 l3-vni 100 prefix-routes-only
admin@R1# set vxlans source-interface lo address 1.1.1.1
admin@R1# set vxlans vni 100 vlan 1111
admin@R1# set vxlans vni 10 vlan 10
admin@R1# set vxlans vni 30 vlan 30
```

Step 3: Enable IP routing and configure VRF and hostname.

```
admin@R1# set ip routing enable true
admin@R1# set ip vrf vrf1
```

Step 4: Configure BGP and OSPF related configuration

```
admin@R1# set protocols bgp local-as 65001
admin@R1# set protocols bgp router-id 1.1.1.1
admin@R1# set protocols bgp neighbor 2.2.2.2 remote-as "internal"
admin@R1# set protocols bgp neighbor 2.2.2.2 update-source "1.1.1.1"
admin@R1# set protocols bgp neighbor 2.2.2.2 evpn activate
admin@R1# set protocols bgp ipv4-unicast
admin@R1# set protocols bgp evpn advertise-all-vni
admin@R1# set protocols bgp evpn advertise ipv4-unicast
admin@R1# set protocols bgp vrf vrf1 local-as 65001
admin@R1# set protocols bgp vrf vrf1 router-id 1.1.1.1
admin@R1# set protocols bgp vrf vrf1 evpn advertise ipv4-unicast
admin@R1# set protocols ospf router-id 1.1.1.1
admin@R1# set protocols ospf network 40.94.0.0/24 area 0.0.0.0
admin@R1# set protocols ospf network 1.1.1.1/32 area 0.0.0.0
```

Step 5: Configure 802.1X and NAC. Specify the NAS IP, the authentication server IP which is the IP address of the ISE server in this case and authentication mode.

```
admin@R1# set protocols dot1x interface te-1/1/20 host-mode multiple
admin@R1# set protocols dot1x interface te-1/1/20 auth-mode mac-radius
admin@R1# set protocols dot1x aaa radius authentication server-ip 10.10.50.65 shared-key test
admin@R1# set protocols dot1x aaa radius nas-ip 10.10.51.201
```

Step 6: Enable POE for interface te-1/1/20. We need this step to power up the phone device using the switch's' POE feature without needing an external power source.

```
admin@R1# set poe interface te-1/1/20
```

R2 Configuration

Step 1: Configure VLAN ID, L3 VLAN interfaces, loopback interfaces and IP addresses. Interface ge-1/1/10 connects to PC2 and interface ge-1/1/20 connects to the IP phone.

```
root@R2# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching native-vlan-id 4094
root@R2# set interface gigabit-ethernet ge-1/1/10 family ethernet-switching native-vlan-id 30
root@R2# set interface gigabit-ethernet ge-1/1/20 family ethernet-switching port-mode trunk
root@R2# set l3-interface loopback lo address 2.2.2.2 prefix-length 32
root@R2# set l3-interface loopback vrf1 address 134.134.134.134 prefix-length 32
root@R2# set l3-interface vlan-interface vlan1111 vrf vrf1
root@R2# set l3-interface vlan-interface vlan1111 mtu 1450
root@R2# set l3-interface vlan-interface vlan30 vrf vrf1
root@R2# set l3-interface vlan-interface vlan20 vrf vrf1
root@R2# set l3-interface vlan-interface vlan30 mtu 1450
root@R2# set l3-interface vlan-interface vlan20 mtu 1450
root@R2# set l3-interface vlan-interface vlan30 address 30.1.1.134 prefix-length 24
root@R2# set l3-interface vlan-interface vlan20 address 20.1.1.134 prefix-length 24
root@R2# set l3-interface vlan-interface vlan4094 mtu 1450
root@R2# set l3-interface vlan-interface vlan4094 address 40.94.0.1 prefix-length 24
root@R2# set vlans vlan-id 10 l3-interface vlan10
root@R2# set vlans vlan-id 20 l3-interface vlan20
root@R2# set vlans vlan-id 30 l3-interface vlan30
```

Step 2: Configure VXLAN VNI and map VNI IDs to VLAN IDs.

```
root@R2# set vlans vlan-id 1111 l3-interface "vlan1111"
root@R2# set vlans vlan-id 4094 l3-interface "vlan4094"
root@R2# set vxlans source-interface lo address 2.2.2.2
root@R2# set vxlans vni 100 vlan 1111
root@R2# set vxlans vni 10 vlan 10
root@R2# set vxlans vni 20 vlan 20
root@R2# set vxlans vni 30 vlan 30
```

Step 3: Enable IP routing and configure VRF and hostname.

```
root@R2# set system hostname "R2"
root@R2# set ip routing enable true
root@R2# set ip vrf vrf1
```

Step 4: Configure BGP and OSPF related configuration

```
root@R2# set protocols bgp local-as 65001
root@R2# set protocols bgp router-id 2.2.2.2
root@R2# set protocols bgp neighbor 1.1.1.1 remote-as "internal"
root@R2# set protocols bgp neighbor 1.1.1.1 update-source "2.2.2.2"
root@R2# set protocols bgp neighbor 1.1.1.1 evpn activate
root@R2# set protocols bgp evpn advertise-all-vni
root@R2# set protocols bgp evpn advertise ipv4-unicast
root@R2# set protocols bgp vrf vrf1 local-as 65001
root@R2# set protocols bgp vrf vrf1 router-id 2.2.2.2
root@R2# set protocols bgp vrf vrf1 evpn advertise ipv4-unicast
root@R2# set evpn vrf vrf1 vni 100 prefix-routes-only
root@R2# set protocols ospf router-id 2.2.2.2
root@R2# set protocols ospf network 40.94.0.0/24 area 0.0.0.0
root@R2# set protocols ospf network 2.2.2.2/32 area 0.0.0.0
```

Step 5: Configure 802.1X and NAC. Specify the NAS IP, the authentication server IP which is the IP address of the ISE server in this case and the authentication mode.

```
admin@R2# set protocols dot1x interface ge-1/1/20 host-mode multiple
admin@R2# set protocols dot1x interface ge-1/1/20 auth-mode mac-radius
admin@R2# set protocols dot1x aaa radius authentication server-ip 10.10.50.65 shared-key test
admin@R2# set protocols dot1x aaa radius nas-ip 10.10.51.134
```

Step 6: Enable POE for interface ge-1/1/20. We need this step to power up the phone device using the switch's' POE feature.

```
admin@R2# set poe interface ge-1/1/20
```

Note: In a more realistic network environment, DHCP access needs to be allowed in the VLAN connecting the IP phone devices to automatically assign IP address and other basic network information like DNS and gateway details. Such configurations are not implemented in this example topology.

Verify Configuration

After successful authentication from the ISE server, the switch port is assigned the dynamic VLAN as shown below in the output of the show command on R1.

```
admin@R1# run show dot1x interface gigabit-ethernet ge-1/1/20
Interface ge-1/1/20:
============================================================
Client MAC : cc:98:91:4e:c9:a7
Status : authorized
Success Auth Method : MAB
Traffic Class : Other
Dynamic VLAN ID : 20 (active)
============================================================
```

On R1 run the command **run show route vrf vrf1** to display the routes. Notice below that there is a route to subnet 30.1.1.0/24.

```
admin@R1# run show route vrf vrf1
show ip route vrf vrf1
=======================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route


VRF vrf1:
K>* 0.0.0.0/0 [255/8192] unreachable (ICMP unreachable), 04:07:17
C>* 10.1.1.0/24 is directly connected, vlan10, 04:06:28
C>* 20.1.1.0/24 is directly connected, vlan20, 04:05:33
B>* 11.11.11.147/32 [200/0] via 2.2.2.2, vlan1111 onlink, weight 1, 04:05:30
C>* 30.1.1.0/24 is directly connected, vlan30, 04:06:28
C>* 201.201.201.201/32 is directly connected, vrf1, 04:07:17



show ipv6 route vrf vrf1
========================
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route


VRF vrf1:
C * fe80::/64 is directly connected, vlan1111, 04:06:27
C * fe80::/64 is directly connected, vlan30, 04:06:28
C>* fe80::/64 is directly connected, vlan10, 04:06:28
```

```
admin@R2# run show route vrf vrf1
show ip route vrf vrf1
=======================
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route


VRF vrf1:
K>* 0.0.0.0/0 [255/8192] unreachable (ICMP unreachable), 00:12:12
C>* 10.1.1.0/24 is directly connected, vlan10, 00:11:23
C>* 20.1.1.0/24 is directly connected, vlan10, 00:11:33
C>* 30.1.1.0/24 is directly connected, vlan30, 00:11:23


show ipv6 route vrf vrf1
========================
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route


VRF vrf1:
C * fe80::/64 is directly connected, vlan1111, 00:11:22
C * fe80::/64 is directly connected, vlan30, 00:11:22
C * fe80::/64 is directly connected, vlan10, 00:11:22
C>* fe80::/64 is directly connected, vlan40, 00:11:22
```

Run the command **run show vxlan evpn route** on either R1 or R2 to check the VXLAN EVPN routes.

```
admin@R1#  run show vxlan arp
IP-ADDRESS       MAC-ADDRESS        VNI       REMOTE-VTEP      Interface   Status   Age
---------------  -----------------  --------  ---------------  ----------  -------  ----
10.1.1.2         18:5a:58:3c:42:a1  10                         te-1/1/10   Dynamic  249
20.1.1.1         17:54:56:ac:42:22  20                         te-1/1/20   Dynamic  250
10.1.1.1         18:5a:58:03:35:81  10      2.2.2.2                       Static
30.1.1.1         18:5a:58:03:35:81  30      2.2.2.2                       Static
30.1.1.2         1c:72:1d:c9:1b:e1  30      2.2.2.2                        Static
```

To check the VXLAN tunnels on either devices, run the command **run show vxlan tunnel.**

```
admin@R2# run show vxlan tunnel
Total number of tunnels: 3

VNI 10, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:2.2.2.2, dst addr:1.1.1.1, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:40.94.0.2
  output ports:ge-1/1/1

VNI 20, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:2.2.2.2, dst addr:1.1.1.1, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:40.94.0.2
  output ports:ge-1/1/1

VNI 30, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:2.2.2.2, dst addr:1.1.1.1, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:40.94.0.2
  output ports:ge-1/1/1

VNI 100, Encap:service-vlan-delete, Decap:service-vlan-add-replace
  src addr:2.2.2.2, dst addr:1.1.1.1, state:UP
  traffic type:all
  Vtep type:EVPN
  nexthops:40.94.0.2
  output ports:ge-1/1/1
```