

Informe Técnico

Segmentación HVAC entre Campus Norte y Sur mediante OSPF (área NSSA) y ACL en Aruba 6400

Antonio Pérez

20 de noviembre de 2025

1. Objetivo

El objetivo de este diseño es aislar lógicamente las redes **HVAC** de cada campus, de modo que:

- Las VLAN HVAC del **Campus Norte** (192.168.164.0/24) y del **Campus Sur** (192.168.224.0/24) sólo se comuniquen *entre ellas* (Norte ↔ Sur).
- Las redes **LAN** (área OSPF 0.0.0.0) de ambos campus se vean entre sí, pero no tengan acceso a HVAC.
- El tráfico desde cualquier otra subred hacia las redes HVAC sea bloqueado, mientras que se mantiene alta disponibilidad con dos chasis Aruba 6400 en VSX por campus.

Para lograrlo se combinan:

- OSPF con área 1.1.1.1 definida como NSSA `no-summary` para HVAC.
- Redistribución controlada de rutas estáticas mediante `prefix-list` y `route-map`.
- Listas de acceso L3 (`access-list ip`) aplicadas de forma `routed-in/routed-out` sobre las VLAN HVAC.
- Rutas estáticas con distancias administrativas primarias/secundarias para la conectividad HVAC entre campus vía enlaces punto a punto (VLAN 1019) y enlaces A-B internos de cada campus (VLAN 531/731).

2. Topología y direccionamiento

La figura 1 resume la topología lógica entre los cuatro chasis Aruba 6400 (A/B Norte, A/B Sur), las VLAN de tránsito OSPF y las redes HVAC de cada campus.

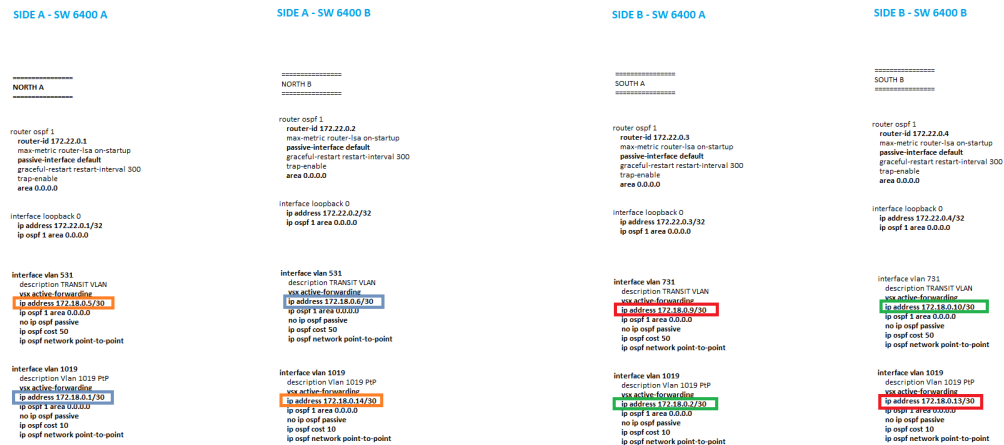


Figura 1: Topología de interconexión LAN/HVAC entre Campus Norte y Sur.

Rangos principales usados:

- **HVAC Norte: 192.168.164.0/24**
- **HVAC Sur: 192.168.224.0/24**
- **Enlace A–A entre Campus (VLAN 1019): 172.18.0.0/30**
 - Norte A: 172.18.0.1/30
 - Sur A: 172.18.0.2/30
- **Enlace B–B entre Campus (VLAN 1019): 172.18.0.12/30**
 - Sur B: 172.18.0.13/30
 - Norte B: 172.18.0.14/30
- **Enlace interno Norte A–B (VLAN 531): 172.18.0.4/30**
 - Norte A: 172.18.0.5/30
 - Norte B: 172.18.0.6/30
- **Enlace interno Sur A–B (VLAN 731): 172.18.0.8/30**
 - Sur A: 172.18.0.9/30
 - Sur B: 172.18.0.10/30

3. Diseño de enrutamiento OSPF

La instancia OSPF (`router ospf 1`) se configura con:

- **Área 0.0.0.0** para las VLAN de tránsito entre chasis y campus (LAN).
- **Área 1.1.1.1 como NSSA no-summary** para las interfaces HVAC (VLAN HVAC Norte y Sur).
- Redistribución de rutas estáticas sólo para prefijos HVAC usando:
 - `ip prefix-list HVAC-ONLY`
 - `route-map REDIST-HVAC`
 - `redistribute static route-map REDIST-HVAC`

Con esto, las redes HVAC se anuncian entre campus de forma controlada, mientras que el resto de las rutas LAN siguen siendo puramente intra-área 0.

4. Políticas de filtrado HVAC (ACL)

Para forzar que sólo haya tráfico HVAC $\leftrightarrow$ HVAC y bloquear accesos desde/hacia otras redes, se define en cada chasis una ACL de capa 3:

- `access-list ip HVAC-IN`:
 - Permite tráfico:
 - `192.168.164.0/24  $\leftrightarrow$  192.168.164.0/24`
 - `192.168.164.0/24  $\leftrightarrow$  192.168.224.0/24`
 - `192.168.224.0/24  $\leftrightarrow$  192.168.224.0/24`
 - `192.168.224.0/24  $\leftrightarrow$  192.168.164.0/24`
 - Deniega y registra:
 - Tráfico desde HVAC hacia cualquier otra red.
 - Tráfico desde cualquier red hacia HVAC.
 - Finalmente permite `ip any any` para no afectar el resto del tráfico de ruteo.
- Esta ACL se aplica como:
 - `apply access-list ip HVAC-IN routed-in`
 - `apply access-list ip HVAC-IN routed-out`

sobre la VLAN HVAC correspondiente.

5. Configuración por chasis

En los ejemplos siguientes, sustituir:

- <VLAN_HVAC_NORTE> por el número real de VLAN HVAC en el Campus Norte.
- <VLAN_HVAC_SUR> por el número real de VLAN HVAC en el Campus Sur.

5.1 SW 6400 A – NORTE

```
conf t
ip prefix-list HVAC-ONLY seq 10 permit 192.168.164.0/24
ip prefix-list HVAC-ONLY seq 20 permit 192.168.224.0/24

route-map REDIST-HVAC permit 10
  match ip address prefix-list HVAC-ONLY

router ospf 1
  router-id 172.22.0.1
  passive-interface default
  graceful-restart restart-interval 300
  trap-enable
  area 0.0.0.0
  area 1.1.1.1 nssa no-summary
  redistribute static route-map REDIST-HVAC

interface loopback 0
  ip address 172.22.0.1/32
  ip ospf 1 area 0.0.0.0

interface vlan 531
  description NORTH-OSPF
  vsx active-forwarding
  ip address 172.18.0.5/30
  ip ospf 1 area 0.0.0.0
  no ip ospf passive
  ip ospf cost 50
  ip ospf network point-to-point

interface vlan 1019
  description PtP-LINK-A
  vsx active-forwarding
  ip address 172.18.0.1/30
  ip ospf 1 area 0.0.0.0
  no ip ospf passive
  ip ospf cost 10
  ip ospf network point-to-point
```

```

access-list ip HVAC-IN
 10 permit ip 192.168.164.0/24 192.168.164.0/24
 20 permit ip 192.168.164.0/24 192.168.224.0/24
 30 permit ip 192.168.224.0/24 192.168.224.0/24
 40 permit ip 192.168.224.0/24 192.168.164.0/24
 90 deny ip 192.168.164.0/24 any log
 91 deny ip 192.168.224.0/24 any log
100 deny ip any 192.168.164.0/24 log
101 deny ip any 192.168.224.0/24 log
200 permit ip any any

interface vlan <VLAN_HVAC_NORTE>
  apply access-list ip HVAC-IN routed-in
  apply access-list ip HVAC-IN routed-out

ip route 192.168.224.0/24 172.18.0.2 distance 5
ip route 192.168.224.0/24 172.18.0.13 distance 25
end
write mem

```

5.2 SW 6400 B – NORTE

```

conf t
ip prefix-list HVAC-ONLY seq 10 permit 192.168.164.0/24
ip prefix-list HVAC-ONLY seq 20 permit 192.168.224.0/24

route-map REDIST-HVAC permit 10
  match ip address prefix-list HVAC-ONLY

router ospf 1
  router-id 172.22.0.2
  passive-interface default
  graceful-restart restart-interval 300
  trap-enable
  area 0.0.0.0
  area 1.1.1.1 nssa no-summary
  redistribute static route-map REDIST-HVAC

interface loopback 0
  ip address 172.22.0.2/32
  ip ospf 1 area 0.0.0.0

interface vlan 531
  description NORTH-OSPF
  vsx active-forwarding

```

```

ip address 172.18.0.6/30
ip ospf 1 area 0.0.0.0
no ip ospf passive
ip ospf cost 50
ip ospf network point-to-point

interface vlan 1019
description PtP-LINK-B
vsx active-forwarding
ip address 172.18.0.14/30
ip ospf 1 area 0.0.0.0
no ip ospf passive
ip ospf cost 10
ip ospf network point-to-point

access-list ip HVAC-IN
10 permit ip 192.168.164.0/24 192.168.164.0/24
20 permit ip 192.168.164.0/24 192.168.224.0/24
30 permit ip 192.168.224.0/24 192.168.224.0/24
40 permit ip 192.168.224.0/24 192.168.164.0/24
90 deny ip 192.168.164.0/24 any log
91 deny ip 192.168.224.0/24 any log
100 deny ip any 192.168.164.0/24 log
101 deny ip any 192.168.224.0/24 log
200 permit ip any any

interface vlan <VLAN_HVAC_NORTE>
apply access-list ip HVAC-IN routed-in
apply access-list ip HVAC-IN routed-out

ip route 192.168.224.0/24 172.18.0.13 distance 5
ip route 192.168.224.0/24 172.18.0.9 distance 25
end
write mem

```

5.3 SW 6400 A – SUR

```

conf t
ip prefix-list HVAC-ONLY seq 10 permit 192.168.164.0/24
ip prefix-list HVAC-ONLY seq 20 permit 192.168.224.0/24

route-map REDIST-HVAC permit 10
match ip address prefix-list HVAC-ONLY

router ospf 1
router-id 172.22.0.3

```

```

passive-interface default
graceful-restart restart-interval 300
trap-enable
area 0.0.0.0
area 1.1.1.1 nssa no-summary
redistribute static route-map REDIST-HVAC

interface loopback 0
ip address 172.22.0.3/32
ip ospf 1 area 0.0.0.0

interface vlan 731
description SOUTH-OSPF
vsx active-forwarding
ip address 172.18.0.9/30
ip ospf 1 area 0.0.0.0
no ip ospf passive
ip ospf cost 50
ip ospf network point-to-point

interface vlan 1019
description PtP-LINK-A
vsx active-forwarding
ip address 172.18.0.2/30
ip ospf 1 area 0.0.0.0
no ip ospf passive
ip ospf cost 10
ip ospf network point-to-point

access-list ip HVAC-IN
10 permit ip 192.168.164.0/24 192.168.164.0/24
20 permit ip 192.168.164.0/24 192.168.224.0/24
30 permit ip 192.168.224.0/24 192.168.224.0/24
40 permit ip 192.168.224.0/24 192.168.164.0/24
90 deny ip 192.168.164.0/24 any log
91 deny ip 192.168.224.0/24 any log
100 deny ip any 192.168.164.0/24 log
101 deny ip any 192.168.224.0/24 log
200 permit ip any any

interface vlan <VLAN_HVAC_SUR>
apply access-list ip HVAC-IN routed-in
apply access-list ip HVAC-IN routed-out

ip route 192.168.164.0/24 172.18.0.1 distance 5
ip route 192.168.164.0/24 172.18.0.14 distance 25
end

```

```
write mem
```

5.4 SW 6400 B – SUR

```
conf t
ip prefix-list HVAC-ONLY seq 10 permit 192.168.164.0/24
ip prefix-list HVAC-ONLY seq 20 permit 192.168.224.0/24

route-map REDIST-HVAC permit 10
  match ip address prefix-list HVAC-ONLY

router ospf 1
  router-id 172.22.0.4
  passive-interface default
  graceful-restart restart-interval 300
  trap-enable
  area 0.0.0.0
  area 1.1.1.1 nssa no-summary
  redistribute static route-map REDIST-HVAC

interface loopback 0
  ip address 172.22.0.4/32
  ip ospf 1 area 0.0.0.0

interface vlan 731
  description SOUTH-OSPF
  vsx active-forwarding
  ip address 172.18.0.10/30
  ip ospf 1 area 0.0.0.0
  no ip ospf passive
  ip ospf cost 50
  ip ospf network point-to-point

interface vlan 1019
  description PtP-LINK-B
  vsx active-forwarding
  ip address 172.18.0.13/30
  ip ospf 1 area 0.0.0.0
  no ip ospf passive
  ip ospf cost 10
  ip ospf network point-to-point

access-list ip HVAC-IN
  10 permit ip 192.168.164.0/24 192.168.164.0/24
  20 permit ip 192.168.164.0/24 192.168.224.0/24
  30 permit ip 192.168.224.0/24 192.168.224.0/24
```

```
40 permit ip 192.168.224.0/24 192.168.164.0/24
90 deny ip 192.168.164.0/24 any log
91 deny ip 192.168.224.0/24 any log
100 deny ip any 192.168.164.0/24 log
101 deny ip any 192.168.224.0/24 log
200 permit ip any any

interface vlan <VLAN_HVAC_SUR>
  apply access-list ip HVAC-IN routed-in
  apply access-list ip HVAC-IN routed-out

ip route 192.168.164.0/24 172.18.0.14 distance 5
ip route 192.168.164.0/24 172.18.0.5 distance 25
end
write mem
```

6. Resultado y validación

Con esta configuración final:

- Las redes **HVAC Norte** y **HVAC Sur** se alcanzan mutuamente vía rutas estáticas preferenciales y OSPF, con redundancia A–A y B–B.
- La ACL HVAC-IN garantiza que:
 - Sólo hay tráfico entre 192.168.164.0/24 y 192.168.224.0/24 (incluyendo tráfico local dentro de cada /24).
 - El resto de las redes (LAN, otras VLAN, etc.) no puede ni iniciar ni recibir tráfico hacia/desde HVAC.
- La lógica de `area 1.1.1.1 nssa no-summary` mantiene a HVAC como un dominio de enrutamiento controlado, mientras que el backbone 0.0.0.0 sigue transportando únicamente las rutas LAN entre campus.