Technical Report

HVAC Segmentation between North and South Campus using OSPF (NSSA Area) and ACL on Aruba 6400

Antonio Pérez
Network Engineer – Saint Francis School

November 20, 2025

1. Objective

The objective of this design is to logically isolate the **HVAC** networks in each campus so that:

- The HVAC VLANs in the **North Campus** (`192.168.164.0/24`) and the **South Campus** (`192.168.224.0/24`) only communicate *with each other* (North ↔ South).
- The **LAN** networks (OSPF area `0.0.0.0`) of both campuses see each other, but have no access to HVAC.
- Traffic from any other subnet to the HVAC networks is blocked, while maintaining high availability with two Aruba 6400 chassis in VSX per campus.

To achieve this, the following mechanisms are combined:

- OSPF with area `1.1.1.1` defined as `NSSA no-summary` for HVAC.
- Controlled redistribution of static routes using `prefix-list` and `route-map`.
- Layer 3 access lists (`access-list ip`) applied as `routed-in`/`routed-out` on the HVAC VLANs.
- Static routes with primary/secondary administrative distances for HVAC connectivity between campuses via point-to-point links (`VLAN 1019`) and internal A–B links in each campus (`VLAN 531/731`).

2. Topology and addressing

Figure **??** summarizes the logical topology among the four Aruba 6400 chassis (A/B North, A/B South), the OSPF transit VLANs, and the HVAC networks in each campus.

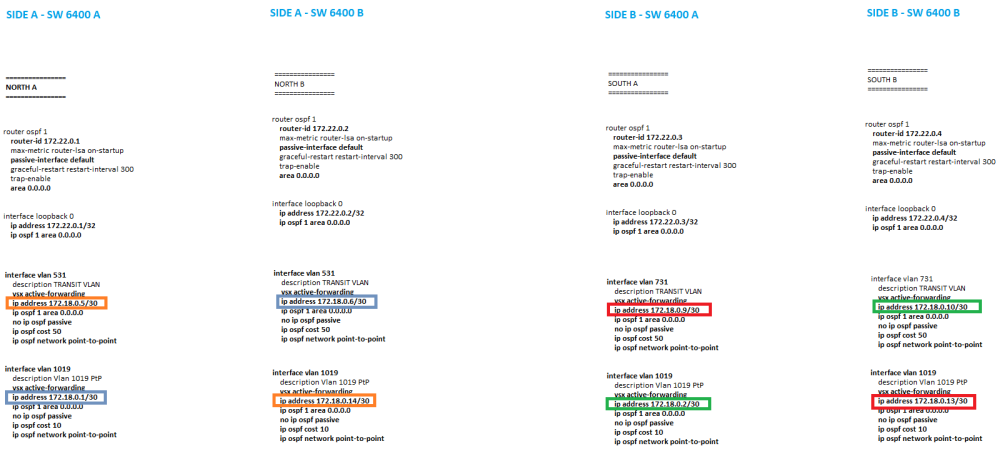

Figure 1: LAN/HVAC interconnection topology between North and South Campus.

Main ranges used:

- **HVAC North**: `192.168.164.0/24`
- **HVAC South**: `192.168.224.0/24`
- **A–A Inter-campus link** (VLAN 1019): `172.18.0.0/30`
  - North A: `172.18.0.1/30`
  - South A: `172.18.0.2/30`
- **B–B Inter-campus link** (VLAN 1019): `172.18.0.12/30`
  - South B: `172.18.0.13/30`
  - North B: `172.18.0.14/30`
- **Internal link North A–B** (VLAN 531): `172.18.0.4/30`
  - North A: `172.18.0.5/30`
  - North B: `172.18.0.6/30`
- **Internal link South A–B** (VLAN 731): `172.18.0.8/30`
  - South A: `172.18.0.9/30`
  - South B: `172.18.0.10/30`

3. OSPF routing design

The OSPF instance (`router ospf 1`) is configured as follows:

- **Area `0.0.0.0`** for all transit VLANs between chassis and campuses (LAN).
- **Area `1.1.1.1` as `NSSA no-summary`** for HVAC interfaces (HVAC VLANs North and South).
- Redistribution of static routes only for HVAC prefixes using:
  - `ip prefix-list HVAC-ONLY`
  - `route-map REDIST-HVAC`
  - `redistribute static route-map REDIST-HVAC`

With this approach, the HVAC networks are advertised between campuses in a controlled way, while all LAN routes remain within OSPF area 0 only.

4. HVAC filtering policies (ACL)

To enforce that only HVAC ↔ HVAC traffic is allowed and that access from/to other networks is blocked, a Layer 3 ACL is defined on each chassis:

- `access-list ip HVAC-IN`:
  - Allows traffic:
    - `192.168.164.0/24` ↔ `192.168.164.0/24`
    - `192.168.164.0/24` ↔ `192.168.224.0/24`
    - `192.168.224.0/24` ↔ `192.168.224.0/24`
    - `192.168.224.0/24` ↔ `192.168.164.0/24`
  - Denies and logs:
    - Traffic from HVAC towards any other network.
    - Traffic from any network towards HVAC.
  - Finally allows `ip any any` so that non-HVAC routing traffic is not impacted.
- This ACL is applied as:
  - `apply access-list ip HVAC-IN routed-in`
  - `apply access-list ip HVAC-IN routed-out`

  on the corresponding HVAC VLAN interface.

5. Configuration per chassis

In the following examples, replace:

- `<VLAN_HVAC_NORTE>` with the actual HVAC VLAN ID in the North Campus.
- `<VLAN_HVAC_SUR>` with the actual HVAC VLAN ID in the South Campus.

5.1 SW 6400 A – NORTH

```
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 – NORTH

```
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 – SOUTH

```
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 – SOUTH

```
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. Result and validation

With this final configuration:

- The **HVAC North** and **HVAC South** networks reach each other via static routes with preferred/backup paths and OSPF, with redundancy through A–A and B–B links.
- The `HVAC-IN` ACL ensures that:
  - Only traffic between `192.168.164.0/24` and `192.168.224.0/24` (including local traffic within each /24) is allowed.
  - All other networks (`LAN`, other VLANs, etc.) can neither initiate nor receive traffic to/from HVAC.
- The `area 1.1.1.1 nssa no-summary` logic keeps HVAC as a controlled routing domain, while the `0.0.0.0` backbone continues to carry only the LAN routes between campuses.