Virtual Device Contexts (VDCs)

What Are VDCs?

- Virtual Device Contexts (VDCs)
  - Layer 1 virtualization of Nexus 7K
  - Loosely analogous to SDRs in IOS XR or Contexts in ASA
- Used to provide separation of…
  - Management plane
  - Control plane
  - Data plane

Virtualization Types in NX-OS

- Virtual LANs (VLANs)
  - Separates layer 2 Ethernet data plane
    - I.e. separate CAM table per VLAN
    - Without routing, no inter-VLAN traffic
  - Separates layer 2 Ethernet control plane
    - I.e. separate STP instances per VLAN
- Virtual SANs (VSANs)
  - Separates Fibre Channel control plane
    - I.e. separate FSPF and fabric services per VSAN
  - Separates Fibre Channel data plane
    - I.e. separate routing table per VLAN

Virtualization Types in NX-OS (Cont.)

- Virtual Routing & Forwarding Instances (VRFs)
  - Separates Layer 3 IPv4/IPv6 data plane
    - Interfaces are separated into different routing tables
    - No inter-VRF routing by default
  - Separates Layer 3 IPv4/IPv6 control plane
    - Separate IGP/BGP instances per VRF

NX-OS Virtualization with VDCs

- VDCs take logic of VLANs, VSANs, & VRFs a step further
- Each VDC has its own…
  - Management plane separation
    - Unique management IP, user database & roles
  - Control plane separation
    - VLANs, VSANs, VRFs & other processes are separate per-VDC
  - Data plane separation
    - Physical ports are a member of a single VDC

Why Use VDCs?

- VDCs allow multiple logical roles per physical chassis
  - Aggregation layer 2 switch
  - Core layer 3 switch
  - OTV Authoritative Edge Device
  - FabricPath/VXLAN Spine switch

Why Use VDCs? (cont.)

- VDCs allow for Multi-Tenancy
  - VDCs as a managed service to customers
  - Customer manages their own layer 2 & layer 3 policies
  - Physical resources are split between multiple customers
  - Reduces space, power, cooling in the datacenter

Why Use VDCs? (cont.)

- VDCs are required to separate certain services on Nexus 7K
  - OTV Authoritative Edge Device and VLAN interfaces (SVIs)
  - F2/F2e modules and M modules
  - FCoE Storage VDC
  - Cisco Nexus 7000 I/O Module Comparison Matrix

Number of Supported VDCs

- Number of supported VDCs depends on Supervisor
  - SUP 1
    - 1 admin VDC
    - 4 user VDCs
  - SUP 2 & SUP 2E
    - 1 admin VDC
    - 8 user VDCs

Admin VDC

- Admin VDC used to control chassis-wide parameters
  - Create and delete other VDCs
  - Allocate ports to VDCs
  - Allocate or limit resources to VDCs
  - Remotely manage the entire chassis

Admin/Default VDC Only Tasks

- Some tasks can only be performed in the admin/default VDC
  - VDC creation/deletion/suspend
  - Resource allocation – interfaces, memory, etc.
  - NX-OS Upgrade across all VDCs
  - ISSU or EPLD Upgrade
  - Ethanalyzer captures
  - Feature-set installation, e.g. FEX, FabricPath, FCoE etc.
  - Control Plane Policing (CoPP)
  - Port Channel load balancing hash
  - Hardware IDS check control
  - ACL Capture feature enable
  - System-Wide QoS

Implementing VDCs

Implementing VDCs

- Create VDC from admin VDC
- Allocate interfaces & resources
- **switchto** VDC to manage it
- Admin users are inherited by user VDC

Creating VDCs

- VDCs are defined in global configuration of admin VDC
  - No separate "admin" mode like IOS XR
- VDC hostname derived from default VDC hostname + VDC name
  - **[no] vdc combined-hostname**
- Each VDC is allocated a separate system MAC address from the backplane sprom
  - E.g. for STP Bridge ID
  - Pool can be verified as **show sprom backplane**

Allocating VDC Interfaces

- Interface allocations must follow line card port group limitations
  - Each line card has different limitations based on ASIC designs
  - NX-OS parser check ensures the entire port group is always allocated for you automatically
- Unallocated or unsupported interface types that are mis-allocated go to VDC 0
  - E.g. an M1 port is allocated into an F2 only VDC

Limiting VDC Resources

- VDC resources can have defined limits
  - VLANs, VRFs, Port Channels, SPAN, ERSPAN, IPv4/IPv6 Unicast Routing Table, IPv4/IPv6 Multicast Routing Table, & Module Type
- Configured as…
  - **limit-resource** under VDC config mode
  - **vdc resource template** in global
    - Template changes do not automatically re-apply

Moving Between VDCs

- Default VDC admin users can **switchto** other VDCs
  - Similar to **changeto context** in ASA
- **switchback** command used to return to admin VDC
- **switchto** needed for initial setup of user VDCs

VDC Management

- Console access lands you in admin VDC
- Physical mgmt0 interface overlaps between all VDCs
  - Separate IP and MAC addresses per VDC
    - Traffic cannot leak between mgmt0 ports
  - **feature telnet** is off by default, **feature ssh** is on
  - Each VDC has its own local user database

VDC User Rights

- Non-default VDC users have two possible default roles
  - **vdc-admin** – all read/write access to only that VDC
  - **vdc-operator** – read only access to only that VDC
  - **vdc-admin** & **vdc-operator** cannot switchback to admin VDC
- Default VDC users inherit read or read/write in non-default VDCs
  - **network-admin** assumes all **vdc-admin** roles
  - **network-operator** assumes all **vdc-operator** roles
  - not vice-versa

VDC High Availability

- HA policy defines what happens when a VDC crashes
  - **Restart** VDC, **Bringdown** VDC, **Reload** SUP, **Switchover** to standby SUP
- HA policy is different depending on single SUP or dual SUP chassis
- Configured as **ha-policy** under VDC config mode

VDC Verification

- What VDCs are configured?
  - show vdc
- How are ports allocated?
  - show vdc membership
- What resources are allocated?
  - show run vdc

Other considerations

- NX-OS ports are disabled by default
  - **shutdown** doesn't show up in the config
  - **show interface status**
  - **show interface brief**
- CDP is enabled by default
  - **no shut** the ports and **show cdp neighbors**