Cisco Switch Layer2 Layer3 Design and Configuration

Layer2 and Layer3 switches are the foundation of any network. After all, any network devices (routers, firewalls, computers, servers etc) have to be connected to a switch. Sooner or later, as a network engineer you will be faced with the task of deploying a switch network for a customer or for your own company. Therefore, learning about some basic switch design and configuration principles will prove beneficial for your professional career.

One simple and popular switch design scenario will be shown in the following tutorial. This scenario will fit most SMB networks (or even bigger ones) that have a few layer 2 VLANs and consequently a few layer3 network subnets. It is a good design principle to separate network hosts by department or by similar group of users.

Network Scenario

In our network scenario below we have segmented the network into 7 Layer2 VLANs (and hence 7 Layer3 subnets), as listed below:

- VLAN10: Network devices management VLAN (10.10.10.0/24)
- VLAN20: Callcenter Department (10.10.20.0/24)
- VLAN30: Sales Department (10.10.30.0/24)
- VLAN40: Accounting & Financial Department (10.10.40.0/24)
- VLAN50: Support Department (10.10.50.0/24)
- VLAN60: Company Servers (10.10.60.0/24)
- VLAN100: Company Managers (10.10.100.0/24)

As far as the design goes I will try to use Cisco’s hierarchical internetworking model (Distribution, Aggregation and Access Layers) with some modifications. For the proposed scenario the distribution and aggregation layer will be combined on the same layer 3 switch to keep the design simple and for better understanding.
The diagram above shows one Layer 3 switch used for Aggregation, three Layer 2 switches used for access purposes and one router for Internet connectivity.

Company X has several departments grouped on several levels in a building. The departments are Callenter, Sales, Accounting, Support and Management. The only department allowed access to the internet is the Management department. Each of the departments has been allocated a Layer2 VLAN and an IPv4 Class C private address range. All the switches are connected over port-channel links for higher bandwidth and better redundancy.
Configuration

Configuration of Layer3 Aggregation Switch

Switch model used: Cisco ME-C3750-24TE (IOS image c3750me-i5k91-mz.122-55.SE6.bin)

Step1: Access, management and logging configuration

```
username admin privilege 15 secret Strongpasshere       \-- creates user admin with highest privilege 15
logging buffered 1024000 debugging                      \-- enables logging using the local storage. The log file will be max 1024000 bits and will record debugging logs
service password-encryption                            \-- Make all passwords secure
enable secret Strongpasshere                            \-- create the enable password
line vty 0 4                                           \-- enables remote network login
transport input telnet ssh                              \-- enables telnet & ssh on the switch
login local                                             \-- uses local database credentials for login

line console 0
password Strongpasshere
login
```

Step2: Layer2 VLAN Configuration

```
vlan 10
  name Device_Management
!
vlan 20
  name Callcenter
!
vlan 30
  name Sales
!
vlan 40
  name Accounting&Finance
!
vlan 50
  name Support
!
vlan 60
  name Servers
!
vlan 100
  name Company_Management
```
Step3: Layer 3 VLAN Configuration

```
ip routing
!
interface Vlan10
description Device_Management
  ip address 10.10.10.1 255.255.255.0
!
interface Vlan20
description Callcenter
  ip address 10.10.20.1 255.255.255.0
!
interface Vlan30
description Sales
  ip address 10.10.30.1 255.255.255.0
!
interface Vlan40
description Accounting&Finance
  ip address 10.10.40.1 255.255.255.0
!
interface Vlan50
description Support
  ip address 10.10.50.1 255.255.255.0
!
interface Vlan60
description Servers
  ip address 10.10.60.1 255.255.255.0
!
interface Vlan100
description Company_Management
  ip address 10.10.100.1 255.255.255.0
```

Step4: Port-Channel configuration

```
interface GigabitEthernet1/1/1
  description downlink Link 1 to Switch Management&support&servers
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan add 10,50,60,100
  switchport mode trunk
  channel-group 1 mode on

interface GigabitEthernet1/1/2
  description downlink Link 2 to Switch Management&support&servers
  switchport
  switchport trunk encapsulation dot1q
```
switchport trunk allowed vlan add 10,50,60,100
switchport mode trunk
channel-group 1 mode on

interface GigabitEthernet1/1/3
description downlinkLink 1 to Switch Accounting&Finance
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 10,40
switchport mode trunk
channel-group 2 mode on

interface GigabitEthernet1/1/4
description downlink Link 2 to Switch Accounting&Finance
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 10,40
switchport mode trunk
channel-group 2 mode on

interface GigabitEthernet1/1/5
description downlink Link 1 to Switch Callcenter&Sales
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 10,20,30
switchport mode trunk
channel-group 3 mode on

interface GigabitEthernet1/1/6
description downlink Link 2 to Switch Callcenter&Sales
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 10,20,30
switchport mode trunk
channel-group 3 mode on
Interface to Router

```plaintext
interface GigabitEthernet1/1/7
  description To Router
  switchport
  switchport access vlan 10
  switchport mode access
```

Default route to the router

```plaintext
ip route 0.0.0.0 0.0.0.0 10.10.10.5
```

Configuration of Layer2 Access Switches

Switch models used: Cisco WS-C2960G-48TC-L (IOS Image: c2960-lanbase-mz.122-35.SE5.bin)

1) Switch Management&suport&servers configuration

NOTE: Configuration for device management and logging remain the same as Layer3 switch above.

Step1: Layer2 VLAN Configuration

We only add the vlans needed on this switch.

```plaintext
vlan 10
  name Device_Management
!
vlan 50
  name Support
!
vlan 60
  name Servers
!
vlan 100
  name Company_Management
```

Step2: Port-Channel Configuration

```plaintext
interface GigabitEthernet1/1
  description uplink Link 1 to Switch AGGREGATION
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan add 10,50,60,100
```
switchport mode trunk
cchannel-group 1 mode on

interface GigabitEthernet1/2
description uplink Link 2 to Switch AGGREGATION
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 10,50,60,100
switchport mode trunk
channel-group 1 mode on

Step 3: Management interface

interface Vlan10
description Device_Management
ip address 10.10.10.2 255.255.255.0

Step 4: Configure Access interfaces to users

Only one interface per vlan is shown for brevity

interface GigabitEthernet0/3
description Server
switchport access vlan 60
switchport mode access
spanning-tree portfast – allows immediate transition of the port into forwarding state
spanning-tree bpduguard enable – if a BPDU is received on the port it transitions to errdisable

interface GigabitEthernet0/4
description Management
switchport access vlan 100
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable

interface GigabitEthernet0/5
description Support
switchport access vlan 50
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
2) **Switch Accounting&Finance configuration**

NOTE: Configuration for device management and logging remain the same as Layer3 switch above.

**Step1: Layer2 VLAN Configuration**

We only add the vlans needed on this switch.

```
vlan 10
  name Device_Management
!
vlan 40
  name Accounting&Finance
```

**Step2: Port-Channel Configuration**

```
interface GigabitEthernet1/1
  description uplink Link 1 to Switch AGGREGATION
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan add 10,40
  switchport mode trunk
  channel-group 1 mode on

interface GigabitEthernet1/2
  description uplink Link 2 to Switch AGGREGATION
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan add 10,40
  switchport mode trunk
  channel-group 1 mode on
```

**Step3: Management interface**

```
interface Vlan10
  description Device_Management
  ip address 10.10.10.3 255.255.255.0
```
Step4: Configure Access interfaces to users

Only one interface per vlan is shown for brevity

```bash
interface GigabitEthernet0/3
description  Accounting
switchport access vlan 40
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
```

3) Switch Callcenter&Sales configuration

NOTE: Configuration for device management and logging remain the same as Layer3 switch above.

Step1: Layer2 VLAN Configuration

We only add the vlans needed on this switch.

```bash
vlan 10
  name Device_Management
!
vlan 20
  name Callcenter
!
vlan 30
  name Sales
```

Step2: Port-Channel Configuration

```bash
interface GigabitEthernet1/1
description Link 1 to Switch AGGREGATION
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 10,20,30
switchport mode trunk
channel-group 1 mode on
!
interface GigabitEthernet1/2
description Link 2 to Switch AGGREGATION
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 10,20,30
```
switchport mode trunk
channel-group 1 mode on

**Step3: Management interface**

interface Vlan10
description Device_Management
ip address 10.10.10.4 255.255.255.0

**Step4: Configure Access interfaces to users**

Only one interface per vlan is shown for brevity

interface GigabitEthernet0/3
description Callcenter
switchport access vlan 20
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet0/4
description Sales
switchport access vlan 30
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable

**Configuration of Router for Internet Access**

Only relevant configuration is shown

**Step1: Internal Vlan Configuration connected to Layer3 Switch**

vlan 10
  name Device_Management
!
interface FastEthernet0
switchport mode access
switchport access vlan 10

**Step2: Layer3 Interfaces Configuration**

interface GigabitEthernet1
description WAN
ip address 1.1.1.10 255.255.255.0
```
no ip proxy-arp
ip nat outside
!
interface Vlan10
description Management
   ip address 10.10.10.5 255.255.255.0
ip nat inside

Step3: Configure NAT for providing access only to Management Users

!NAT ACL is matching only the company management subnet
!
ip access-list extended NAT
   permit ip 10.10.100.0 0.0.0.255 any
!
ip nat inside source list NAT interface GigabitEthernet1 overload
!

Step4: Other config

!A default route to the internet is needed
ip route 0.0.0.0 0.0.0.0 1.1.1.1

!A static route to the management subnet is needed
ip route 10.10.100.0 255.255.255.0 10.10.10.1

At this point only the Company Management has access to the internet and nobody else.
```

About the Author

Harris Andrea is a Cisco Certified Professional with more than 18 years of experience working with Cisco network technologies. He is the author of two Cisco Books (“Cisco ASA Firewall Fundamentals” and “Cisco VPN Configuration Guide”) which have been embraced by thousands of Cisco professionals all over the world. You can find more Cisco configuration guides and tutorials on his blog here
http://www.networkstraining.com