在做網路規劃時, 一些重要的 Physical Switch 設定觀念

Jing, mqjing@gmail.com

在 Data Center 裡面, 可能存在著不同的 networks 負責不同的工作, 例如 storage network 專門負責 Ceph storage 封包, private network 負責處理每個不同私有網路的封包, Management network 負責管理每個 node 時的封包. 而其中的每個 network 都是用 VLAN 隔開以確保封包只會流向正確的 networks. 在 Data Center 裡無論是 GRE 或 OpenStack VLAN 網路模式, 裡面的每個 network 都是透過 VLAN 來區隔 traffic. 若沒有 router 做轉換封包的工作, 某一個 network 上的封包絕對不會流到另外一條 network 上, 因此, 在自己 network 上的 VM 絕對不會收到其他 network 的封包.

可是, 對於這樣的多重網路的觀念, 要如何 physical switch 上做設定呢? 在虛擬網路頻繁交通的封包, 終究需要透過 physical 上的 port 做交通往來或者是接往 Internet 取得對外的通訊. 我們要如何設定 Physical Switch 的 port 呢? 使得我們能放心的規劃 Data Center 裡面的多項 VLAN 網路, 又不會影響外面的網路.

這份文章主要是針對一個簡單的案例, 介紹 Physical Switch Port 設定參數對於網路的實際意義, 做一個說明. 如果我們了解 Physical Switch Port 參數對於 network 的意義, 我們才會有能力設計或部屬出想要的網路架構.

重要名詞定義

1. External port: 是一個 physical switch 的 port. 是 Data Center 裡的 VM 通往 Internet, ADSL 或 其他外網的孔道
2. External network: 是我們設計 Data Center 內的所規劃的對外網路, 若有 VM 要連到外面, 那就必須要透過 router, 把封包轉到 external network, 然後透過 external port 連到外面.

Physical Switch 的 port 有三個參數: 分別是 PVID, VID, port type.
重要觀念:

1. 定義 external network
   External port 的 PVID 定義了 external network. Data Center 內可能有一堆 network, 但只有一條是 external network.
2. 定義只接受某些 network
   一般 Port 的 VID 定義了我們是否要接收某個 VLAN network 的封包
3. 去除 Data Center 的網路設定, 連到外面 Internet
   Port type 為 UNTAG, 就會把所有流出這個 port 的封包, 全部去掉 tag, 通常我們為了要讓 external network 接到外面 Internet 去, 所以會把 external port 的 port type 設為 UNTAG.

靈活運用

4. 要接受 external network 封包的 port, 就只要在自己 port 的 VID 集合中, 加入 external port 的 PVID 號碼即可. 讓自己接受來自 external network package.
5. 對於不想接受 external network 封包的 port, 只要自己 port 的 VID 集合中, 沒有 external

network 的 ID 就可以了.

應用:

你可以利用 physical switch port 的 PVID 與 VID 的觀念，設計出可以讓你限定某些集合 A 的 port, 可以接受/傳送外面 External network 的封包。某些集合 B的 port 的 traffic 不會流出去影響到外面。

設定細節

<External port: 連接到外面的 physical switch port>

- 設定 **PVID:** 定義了我們內部的 external network. 把外面流進來沒有 tag 的封包，一律加上我們設計的 external network VLAN ID.
- 設定 **port type**: 因為要與外面交換封包，所以一定是設定為 UNTAG (出去一律把封包的 tag 拿到掉) 或者 (1) 你也可以設定指定把 external network VLAN ID 拿掉後，再流出去 Internet. 作法為設定 UNTAG 你的 external network ID 或者是 (2) 設定 port type = TAG 搭配 PVID = external network VLAN ID, 把 VLAN ID 的 tag 拿掉後，再流出 Internet (其實 external port 的 PVID 本來就會設成 external network ID)
- 設定 **VID:** 為 external network VLAN ID, 限定只有 external network 的封包可以出到 Internet.

<可收外面封包的 port 群組 A>

一群 physical switch 上的 port , 可能承載著許多 VLAN networks, 但其中有一個 network 是對外的 external network.

- **port type**: TAG
- 設定 **VID**: 是一個集合，指定這個 port 只接受的內部 VLAN network ID 集合與 external network VLAN ID.
- 設定 **PVID**: default 1 (對於沒有 tag 的封包會加 tag, 但不能設定與我們交流的 network ID 一樣，否則會拆封包裹的 tag)

<完全隔絕外面封包的 port 群組 B>

一群 physical switch 上的 port , 可能承載著許多 VLAN network, 但不處理 external network.

- **port type**: TAG
- 設定 **VID**: 是一個集合，指定了這個 port只接受的 VLAN network ID 集合，但因為獨立於來自 external network 的封包，所以 這個 VID 集合裏不包含 external network VLAN ID)。
- 設定 **PVID**: default 1 (對於沒有 tag 的封包會加 tag, 但不能設定與我們交流的 network ID 一樣，否則會拆封包裹的 tag)