Agenda

[Agenda 1](#_Toc102339052)

[SPI模式(aas: as a Service) 2](#_Toc102339053)

[壹、 SaaS (軟體及服務) 2](#_Toc102339054)

[貳、 PaaS (平台及服務) 2](#_Toc102339055)

[參、 IaaS (基礎架構及服務) 2](#_Toc102339056)

[雲 3](#_Toc102339057)

[壹、 公有雲 3](#_Toc102339058)

[貳、 私有雲 3](#_Toc102339059)

[參、 混合雲 3](#_Toc102339060)

[Network Layer 4](#_Toc102339061)

[QoS(Quality of Service) 4](#_Toc102339062)

[壹、 用途 4](#_Toc102339063)

[貳、 頻寬優先權分級 4](#_Toc102339064)

[參、 模式 4](#_Toc102339065)

[NAT(Network Address Translation) 6](#_Toc102339066)

[壹、 Static NAT 6](#_Toc102339067)

[貳、 Dynamic NAT/Pooled NAT 6](#_Toc102339068)

[參、 Port Address Translation NAT(PAT NAT) / Network Address Port Translation (NAPT) 6](#_Toc102339069)

[肆、 內網穿透(NAT traversal) 7](#_Toc102339070)

[SNMP 8](#_Toc102339071)

[NETCONF(升級版的SNMP) 8](#_Toc102339072)

[壹、 NETCONF協議架構 8](#_Toc102339073)

[RESTCONF 10](#_Toc102339074)

[Paramiko vs Netmiko vs Napalm 10](#_Toc102339075)

[Ansible vs Ansible Tower 10](#_Toc102339076)

[Streaming Telemetry 11](#_Toc102339077)

[IPsec(Internet Protocol Security) 11](#_Toc102339078)

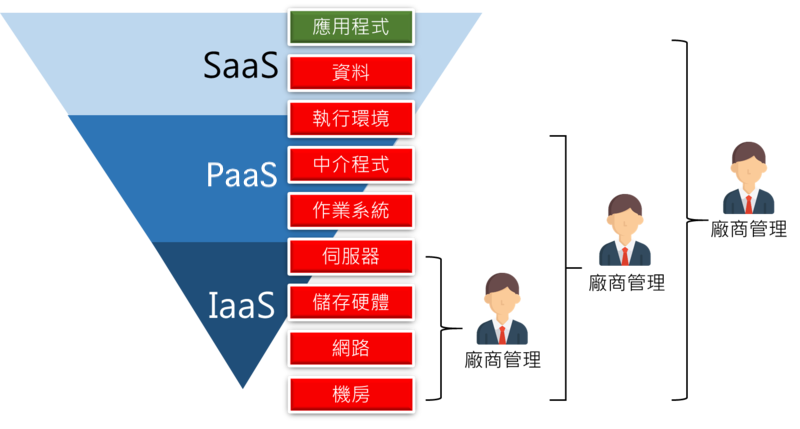
SPI模式(aas: as a Service)

1. SaaS (軟體及服務)

安裝在雲端伺服器的軟體，客戶透過連網連到伺服器並使用伺服器裡的軟體。(ex: Gmail, google map, fb)

1. PaaS (平台及服務)
2. IaaS (基礎架構及服務)

Ex: 雲端硬碟



雲

1. 公有雲

伺服器架設給很多人使用。

1. 私有雲

伺服器只架設給自己使用。

1. 混合雲

公有雲+私有雲

Network Layer

https://www.itread01.com/hkcxqey.html

QoS(Quality of Service)

1. 用途

主要用來做資源的分配，流量的分配，router的cpu的處理，避免網路擁塞以及封包遺失等問題。依據每個應用程式的需求來分配頻寬或優先權。

1. 頻寬優先權分級

根據Bandwidth、Delay、Jitter、Loss四種參數定義資料流量標準。

Bandwidth：頻寬。

Delay：封包來回的時間。

Jitter(抖動、斷斷續續)：封包傳輸時間的間距(間距要平均)。

Loss：封包遺失。

1. 模式

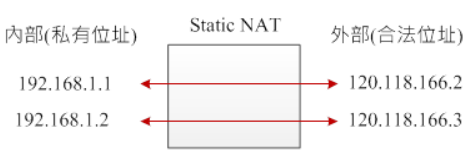
* Best-effort：資料盡量送，沒有針對bandwidth、delay、jitter、loss 做保證，無QoS機制。(類似UDP)
* Integrated services(IntServ)：QoS的保證是從source到destination中間的routers都要能確保有足夠的資源保留給QoS後，才允許傳輸資料封包。要如何確定經過的routers保留的資源符合QoS參數要求，就需要透過Resource Reservation Protocol(RSVP)來詢問每台Routers。(缺點：在WAN中經過的routers多，且routers不是歸我們管理，所以InterServ不好實作。)
* Differentiated services(DiffServ)：從source到destination中間會經過的第一台router開始，先對封包進行class與mark，並進行QoS分級直到最後，所以每台router的QoS參數不太一樣，每台router根據各自封包中的mark來做QoS的行為稱為PHB(Per Hop Behavior)。(目前最常用)

NAT(Network Address Translation)

私有IP與公有IP之間轉換。為了應對Classful IP的不足。

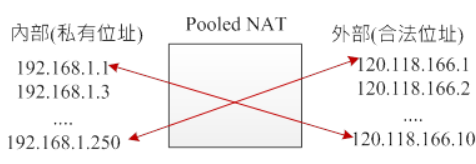
1. Static NAT

公有IP與私有IP是一對一。沒有減少使用公有IP，著重於隱藏私有IP。



1. Dynamic NAT/Pooled NAT

公有IP與私有IP是多對多。在運作當中也是一對一。將若干個公有IP做成「Pool」，宣告某一網段內的主機可從Pool索取公有IP，使用完後還給Pool。圖示：10個公有IP被250主機輪流使用。



1. Port Address Translation NAT(PAT NAT) / Network Address Port Translation (NAPT)

一般常用的NAT設定，公有IP與私有IP是一對多，使用連接埠的方式使其同一時間，一個公有IP可以對應多個私有IP，「IP + port」

1. 內網穿透(NAT traversal)

因為NAT只能由內網主機發起連接，若要在其他網路的主機連接至內網主機就需要NAT traversal。

SNMP

https://codingnote.cc/zh-tw/p/329134/

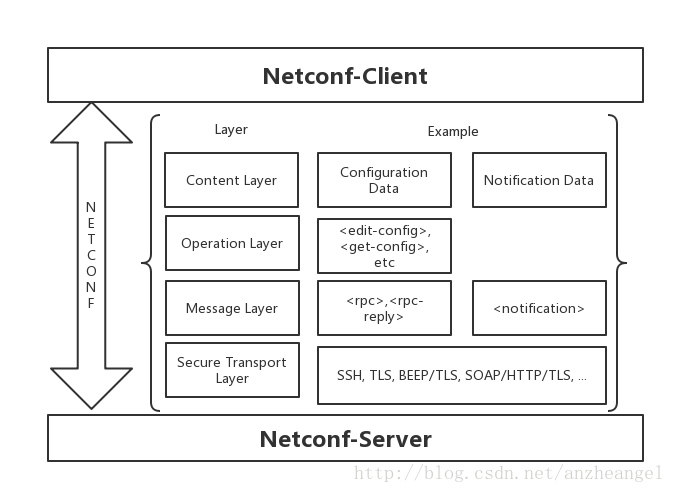
NETCONF(升級版的SNMP)

The Network Configuration Protocol

SDN用軟件去配置網路

<https://www.twblogs.net/a/5b899a0f2b71775d1ce2b15d>

1. NETCONF協議架構



1. Netconf-server

Netconf agent installed on network devices.

1. Netconf-client

Manage network devices.

Receive event notification.

1. Datastores

Startup configuration datastore: 保存設備啟動時的configuration。

Candidate configuration datastore: 保存想要運行的configuraion，修改該datastore時，不會影響目前設備的配置。

Running configuration datastore: 保存當前設備正在運行的configuration，修改該datastore時，會影響目前設備的配置。

1. Secure Transport Layer

Encrypted communication paths. (e.g., SSH, TLS)

Netconf Communications steps:

1. Manager請求建立連接。
2. Manager與Agent互相發送<hello>。
3. Manager發送RPC操作請求。
4. Agent回復RPC請求的結果。
5. Message Layer

|  |  |
| --- | --- |
| RPC invocations | <rpc> messages |
| RPC results | <rpc-reply> messages |
| Event notifications | <notification> messages |

1. Operation Layer

Operation Layer is only carried on <rpc> and <rpc-reply>.

<get>

<get-config>

<edit-config>

<copy-config>

<delete-config>

<lock>

<unlock>

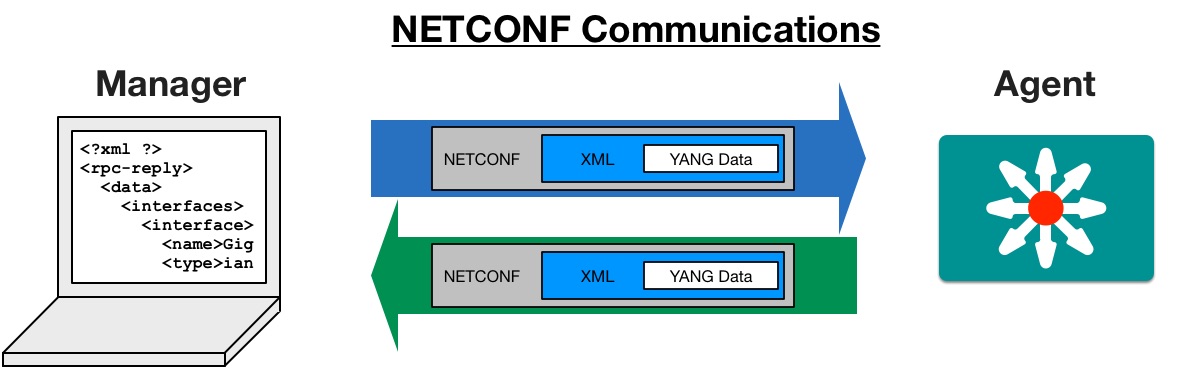
<close-session>

<kill-session>



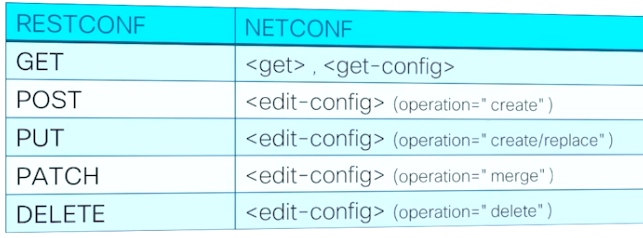
1. Content Layer

建模語言：YANG、Schema (類似於SNMP的MIB)



RESTCONF

|  |  |  |
| --- | --- | --- |
|  | NETCONF | RESTCONF |
| 客戶端 | NETCONF client | HTTP client |
| 配置格式約束 | YANG module / XSD | YANG module |
| 發送內容格式 | XML | XML/JSON |
| 交互方式 | RPC | HTTP |
| 傳輸協議 | SSH | HTTP(s) |
| 服務端 | NETCONF server | HTTP server |



Paramiko vs Netmiko vs Napalm

<https://www.techtarget.com/searchnetworking/tip/Network-automation-with-Python-Paramiko-Netmiko-and-NAPALM>

Ansible vs Ansible Tower

Streaming Telemetry

IPsec (Internet Protocol Security)

1. 介紹

IPSec是IETF(Internet Engineering Task Force)制定的一組開放的網路安全協議，同時支援IPv4、IPv6，只對IP流量進行保護，為一種安全框架結構。

IPSec 提供的三個特性：

1. 保證來源的驗證：接收方驗證發送方身分是否合法。
2. 數據加密：以密文的方式在網路上傳輸。
3. 數據的完整性：接收方對數據進行驗證，判斷封包是否被竄改過。
4. 防重放：接收方拒絕舊的封包，防止中間人通過重複發送捕獲到的數據包進行攻擊。
5. 應用場景

IPSec VPN 實現 branch site 與 headquarters site 的互聯，類似一種路由技術，網路的擴展，使branch與headquarters能夠共享資源，和實現遠程訪問(Ex: 可以從家裡透過VPN連到公司的網域)。

1. IPSec框架

IKE(Internet Key Exchange)協議：提供密鑰協商，建立和維護安全聯盟SA等服務。

安全聯盟SA(Security Alliance)：

建立IPSec隧道時，雙方對隧道參數的約定，主要包括隧道兩端的IP地址、驗證方式、驗證算法、驗證密鑰、加密算法、共享密鑰、以及生命週期等參數。

SA有兩種，IKE/ISAKMP SA 與 IPSec SA。

* IKE/ISAKMP SA：雙向，保護IKE協議協商時的流量。
* IPSec SA：單向，保護2個sites之間網路通訊時，實際感興趣的流量，而2個sites之間的雙向通訊至少需要2個SA，比如 site A 到 site B 要1個SA，site B 到 site A 也要一個SA。

