Layer 2

1. **Vlan**
2. 建立vlan

vlan [number]

name [Name]

show vlan

1. 放入vlan

int [interfaces]

switchport access vlan [number]

1. 起Trunk

int [interfaces]

switchport trunk encapsulation dot1q

switchport mode trunk

show interfaces [interface] trunk

1. Allowed VLAN

switchport trunk allowed vlan [number]

switchport trunk allowed vlan add [number]

switchport trunk allowed vlan all [number]

switchport trunk allowed vlan except [number]

switchport trunk allowed vlan remove [number]

switchport trunk allowed vlan none

1. VLAN1

Vlan1是默認vlan，除了擁有vlan的功能以外，還負責傳送Control Plane Traffic，基於資安考量，應避免給Host使用Vlan1。

1. Native VLAN

若收到沒有Vlan tag的封包，則都會往native vlan送。Switch默認native vlan為vlan1。

更改native vlan: switchport trunk native vlan [vlan id](兩邊Interface的Native Vlan必須相同)

若兩台switch的etherchannel互連，兩邊的etherchannel access不同vlan，也會造成Native vlan mismatch error。

1. Vlan internal Usage

在Multilayer Switch使用Layer 3 port的時候，會私自使用vlan。

show vlan internal usage

系統默認由vlan 1006開始遞增私自使用。

更改成由vlan 4094遞減: vlan interenal allocation policy descending

1. **Dynamic Trunking Protocol (DTP)**
2. 設定DTP

switchport mode dynamic [mode] (mode: auto/desirable)

show dtp

1. Static and Dynamic mode

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Static/Dynamic | Access | Trunk | Desirable | Auto |
| Access | Access | unreasonable | Access | Access |
| Trunk | unreasonable | Trunk | Trunk | Trunk |
| Desirable | Access | Trunk | Trunk | Trunk |
| Auto | Access | Trunk | Trunk | Access |

1. Dynamic Desirable vs Static Trunk

預設都會發放DTP message，Static Trunk可使用switchport nonegotiate關掉DTP message，Dynamic Desirable則不行。

1. VTP Domain

不論Static or Dynamic，兩台switches必須有相同的VTP Domain才能Trunk link。

1. **VLAN Trunking Protocol (VTP)**
2. 建立VTP

vtp domain [domain name]

vtp password [password]

show vtp password

show vtp status

1. VTP mode

vtp mode [mode]

mode: Server, Client, Transparent

Transparent: 負責傳送vlan資訊，Configuration Revision永遠是0，可增加vlan至4094。

Configuration Revision: vlan版本流水號，vlan的database被更改，則流水號就+1。如果兩台switch起trunk並在同一個vtp domain，會先比較流水號，流水號小的vlan database會被流水號大的vlan database覆蓋（Ignore mode）。

1. VTP Version

vtp version [version]

Version: 1, 2, 3

1. VTP Pruning

在Server switch enable: vtp pruning

將沒用到的vlan traffic擋下來，節省bandwidth。

1. **EtherChannel(Port channel)**
2. 建立etherchannel

設定etherchannel之後bandwidth會改變，所以STP cost也會改變。

不同的port要設成etherchannel，設定都要一樣。(ex: Protocol, Allowed vlan, rate, STP…)

channel-group [1-256(channel group number)] mode [mode]

no interface port-channel [Group ID]

|  |  |  |
| --- | --- | --- |
| Protocol | Initiative(主動) | Passive(被動) |
| Static on mode | on | on |
| PAGP(Cisco) | desirable | auto |
| LACP | active | passive |

Static on mode: 會假設對方也是on，中間沒有Protocol溝通，所以會有Loop的風險(STP)。

show etherchannel summary

show interfaces port-channel [group number]

1. PAGP vs LACP

PAGP:

|  |  |  |
| --- | --- | --- |
| mode | desirable | auto |
| desirable | Success | Success |
| auto | Success | Fail |

LACP:

|  |  |  |
| --- | --- | --- |
| mode | active | passive |
| active | Success | Success |
| passive | Success | Fail |

Hot standby: 當有active port down時，Hot standby port可以即時補上(Redundancy)，選擇哪個port成為active則是看priority大的，priority相同再看port ID小的。

1. Load Balance

port-channel load-balance [method]

method: 負載平衡的方法。

Layer 3

1. **ACL**
2. ACL types

* Standard ACLs: [list no 1~99, 1300~1999]

Deny or permits source IP address.

(Applied closet to the destination)

access-list [list no.] [permit/deny] [source ip] [wildcard]

access-list [list no.] [permit/deny] [any/host] [source ip]

access-list [list no.] [permit/deny] any

* Extended ACLs: [list no 100~199, 2000~2699]

Deny or permits source IP address.

Deny or permits destination IP address.

Deny or permits port (service).

(Applied closet to the source)

Basic setting:

access-list [list no.] [permit/deny] [source ip] [wildcard] [destination ip] [wildcard]

access-list [list no.] [permit/deny] any(source) any(destination)

* IP Named ACLs(NACL):

ip access-list [standard/extended] [list no]

Named 一個很重要的目的，就是讓 rule pool 階層化。在此階層下，可以隨時移除規則（命令）中的任何一條，即使要更動順序，也只需要動到有變更的後半部分就可以了，不需要整個重新建立。

1. **DHCP**
2. 設定DHCP

ip dhcp pool [name]

network [network ip] [mask]

default-router [default gateway]

domain-name [domain name]

dns-server [ip]

ip dhcp excluded-address [initial ip] [final ip]

show ip dhcp pool

show ip dhcp binding

1. DHCP Relay

|  |  |
| --- | --- |
| Routing | AD |
| RIP | 120 |
| OSPF | 110 |
| EIGRP | 90 |
| Static route | 1 |
| Direct connect | 0 |

interface [interface]

ip helper-address [DHCP IP]

1. **Route Table**

show ip route

show run | include ip route

最常前綴匹配：

最長mask > 最小AD > 最小Metric

1. **Static route**

ip route [destination ad] [mask] [next hop interface ip]

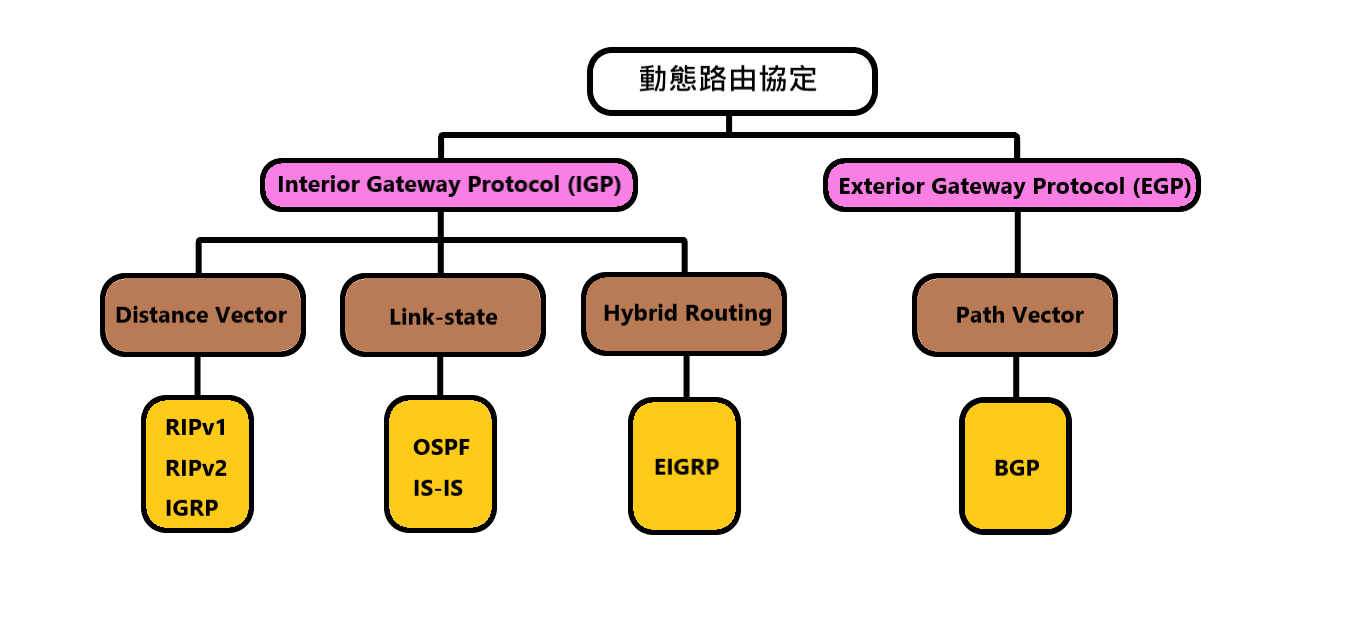
//下個router的ip

ip route [destination ad] [mask] [origin hop interface name] [AD]//本身router的interface名字

Default Route：

ip route 0.0.0.0 0.0.0.0 [next hop interface ip]

ip route 0.0.0.0 0.0.0.0 [origin router interface name]

1. **Dynamic route**

Distance Vector: 透過方向與HOP Counts決定路徑。

Link-state: 透過連結狀態決定路徑，讓所有routers計算出整個網路Topology，再用最短路徑演算法（Shortest Path First, SPF）計算路徑。

Hybrid Routing: 混合型，Distance Vector + Link-state。

Path Vector: 自治系統（Autonomous System, AS）互相溝通。(ISP)

水平分割(Split horizon): 路由器從某個interface收到的更新信息不允許再從這個interface發回去。

路由重分佈(Route Redistribution): 將一個路由協議的路由資訊釋出到另外一個協議中。

1. RIP(Routing Information Protocol) Version2

告訴其他有參與RIP的router自己可以抵達哪些網段。

1. Network cmd

router rip

version 2 (default version 1)

network [network ID]

show ip route rip

1. Passive Interface (被動介面)

只接收RIP封包，不傳送RIP封包。

用於隱藏網路，或節省介面頻寬(EX：將RIP封包送給PC沒有意義，浪費頻寬)。

passive-interface [interface]//使interface不參加RIP

passive-interface [default] //全部interface不參加RIP

no passive-interface [interface]

1. Metric

Metric = Hop counts

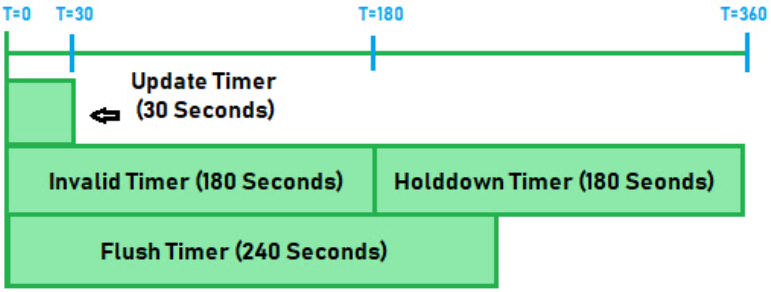
最大15，超過15則unreachable。

透過Standard ACL增加Metric:

offset-list [ACL number] out [increase metric]

1. Timer

* Update Timer: 每次更新route的時間。(default: 30s)
* Invalid Timer: 過多久沒收到某條route更新的時間，這條route被宣告成Invalid，同時Metric會變成16，並且告訴其他router。(default: 180s)
* Hold-down Timer: 被宣告為Invalid route或route的Metric變大時，這條route無法再被更新的時間。(default: 180s)
* Flush Timer: 某條route若沒有再時間內更新，及會被刪除。(default: 240s)

**各timer開始計時的時間：**

timers basic [update] [invalid] [hold-down] [flush]

每一台Router的Timer盡量相同，否則會造成不穩定的問題。

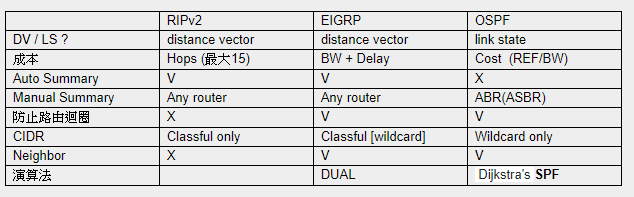
1. Summarization

* auto-summary: 使用預設的classful mask，將子網匯總成一個網段。( 在EIGRP, RIPv2默認開啟，在 OSPF默認關閉。)
* ip summary-address rip [network id] [mask]: 自行定義要匯總成的網段以及遮罩。(下在interface，從此interface發送的路由才會是匯總路由。)
* 兩個功能同時開啟時，auto-summary優先級大於ip summary-address。
* ip summary-address盡量下在接近路由發送的初始interface。
* 不同的路由資訊summary之後，Metric會選最小的。
* 舊的network id route要等到flush timer才會被移除。
* RIP的summary原則是先考慮是否發送路由在考慮是否匯總。
* 盡可能使用ip summary-address，auto-summary盡量關閉。
* 增加路由效率，增強路由穩定性。

1. Default-information Originate

* redistribute static (路由重新分佈): AS的邊界路由器只向外連接一台router的時候適合使用這種設定。
* network 0.0.0.0 (會使所有擁有ip的interface加入protocol): 預設路由只能設interface，建議使用的場合與第一種方式一樣。
* ip default-network [network id] (classful，在全域模式下設定，所以跟rip沒關係。)
* 透過RIP發佈Default route: default-information originate

1. Route Filetering
2. EIGRP(Enhanced Interior Gateway Routing Protocol)
3. OSPF(Open Shortest Path First)
4. Difference



Cisco Memory

|  |  |
| --- | --- |
| Read-Only Memory | bootstrap program、IOS |
| Non-Volatile Random Access Memory | startup-configuration |
| Random Access Memory | running-configuration |
| Flash memory | Configuration備份檔 |

儲存設定：write memory、copy run start

取消目前設定：copy start run

恢復原廠設定：erase startup-configuration

FHRP(First Hop Redundancy Protocol)

1. **HSRP**

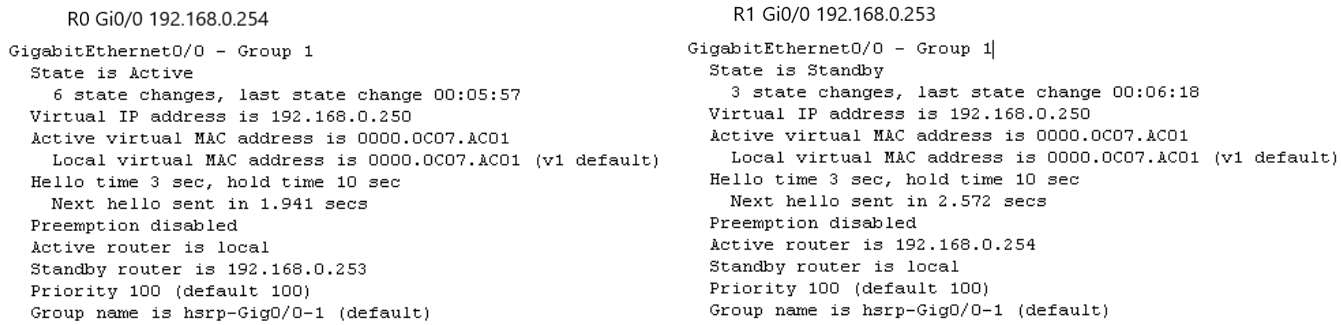
HSRP只有Cisco設備可用，先設定Group ID、VIP(Virtual IP)，參與HSRP的Interface的Group ID要相同，VIP需與Interface的IP處於同一個Subnet中。

1. 建立HSRP

standby [Group ID] ip [VIP]

1. 查看HSRP

show standby可查看HSRP狀態



除了VIP外，還可以看到Virtual MAC，VMAC是自動產生的

更改VMAC : standby [Group ID] mac-address [VMAC]

通常不會更改VMAC

1. 更改Priority

Priority最高的會成為Active(default: 100)

Priority相同，IP大的成為Active。

standby [Group ID] priority [Value]

更改之後state不會立即更換，為了保持穩定性，若突然有更高的Priority出現，不會立即把其升格成Active。

若要立即升格成Active，就要設定preempt(Group裡的interfaces都要設)

standby [Group ID] preempt

1. Track 偵測

standby [Group ID] track [self interface] [minus priority]

ex: standby 1 track GigabitEthernet 0/2 20

//當Gi0/2 down，將priority -20

1. 更改Timer

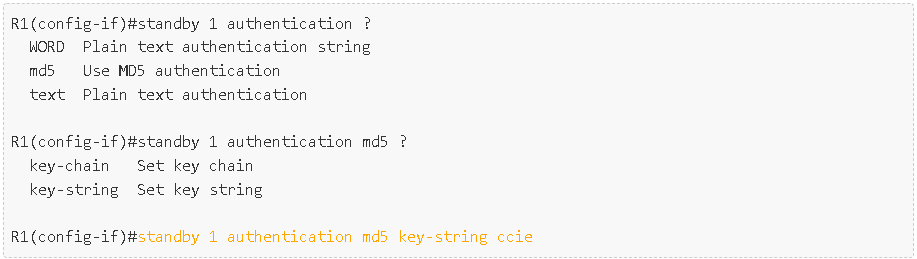
Default: Hello time 3 sec, hold time 10 sec

每3秒聯絡一下Group裡其他的Interface，過10秒之後沒收到Active報平安，則判斷對方掛掉，自己升格成Active。

standby [Group ID] timers [Hello time] [Hold time]

1. 密碼驗證

standby [Group ID] authentication



1. **VRRP**
2. **GLBP**

NAT(Network Address Translation)

1. **Static NAT**

1個private ip對1個public ip

ip nat inside source static ([tcp/udp]) [inside local ip] [inside global ip]

ip nat outside source static ([tcp/udp]) [outside global ip] [outside local ip]

1. **Dynamic NAT / Pooled NAT**

多個private ip對少個public ip

ip nat [inside/outside] source list [list no.] pool [pool name]

ip nat pool [pool name] [initial ip] [final ip] netmask [mask]

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

多個private ip對1個public ip

ip nat [inside/outside] source list [list no.] pool [pool name] overload

ip nat pool [pool name] [initial ip] [final ip] netmask [mask]

1. **Routing Order**

* Cisco:

Traffic from inside: 先看Routing Table，再看NAT Table。

Traffic from outside: 先看NAT Table，再看Routing Table。

SSH(Secure Shell)

1. **Introduction**

Secure Shell (SSH) which provides a feature of secured remote access to network devices. Connection between the client and server is encrypted in both SSH version 1 and 2. Secure Shell (SSH) improves network security by providing a means of establishing secure connection to networking devices for management using Digital Certificates in a Public and Private Key Cryptography. Telnet is used to connect device but the main disadvantage of using Telnet is that it does not encrypt its connections. SSH overcomes this shortcoming.

1. SSH Version 1

SSH v1 provides an encrypted channel to users for logging into remote device. It provides strong host-to-host and user authentication. It also provides secure encrypted communications over the Internet.

1. SSH Version 2

SSH2 is a much more secured, an efficient version of SSH that includes SFTP, which is functionally similar to FTP with addition of SSH2 encryption.

1. Advantages that SSH2 provides over SSH1
2. Eavesdropping

SSH2 encrypts all the data which protects against eavesdropping, making it unreadable to potential eavesdroppers.

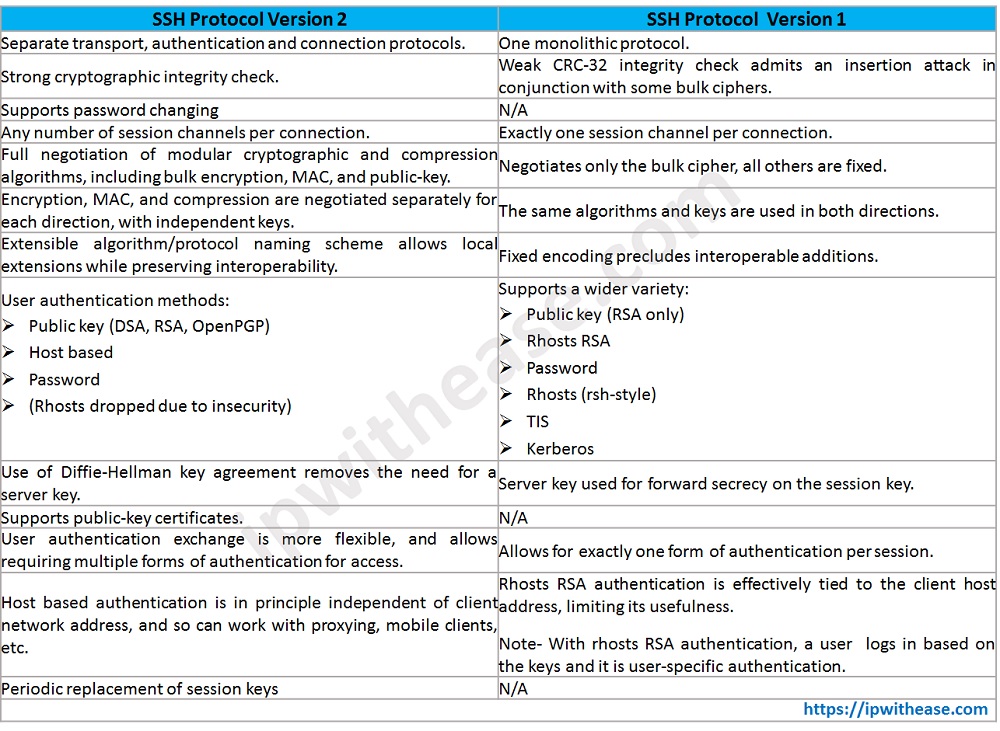
1. DNS and IP Spoofing

SSH2 avoids such attacks by cryptographically authenticating the identity of the server. In session establishment, the SSH client validates the server’s host key against a local list of available keys that are associated with server names and addresses. If the keys mismatch, then an immediate warning is issued.

1. Man in the middle

SSH2 can protect against man-in-the middle attacks by server-host authentication. Because the attacker does not have the server’s private host key, SSH2 provide stronger authentication for the client. Passwords are vulnerable but public keys and certificates are essentially immune to these types of attacks.

1. Difference between SSH Version 1 and 2



1. **Flow**

Hostname

IP Domain Name

Create SSH Key

Enable SSH

Create a User

1. **Command Line Interface**
2. Hostname

hostname [hostname]

1. IP Domain Name

ip domain-name [domain-name]

1. Create SSH Key

crypto key generate rsa

1. Enable SSH

line vty [range of line number]

transport input ssh

login local

1. Create a User

username [username] privilege [level] (password or secret) [password]

password: clear text

secret: password encryption