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 trunk

1. Allowed VLAN

switchport trunk allowed vlan [number]

1. Ether-channel
2. 建立ether-channel

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

|  |  |  |
| --- | --- | --- |
| Protocol | SW1 | SW2 |
| Static on mode | On | on |
| PAGP | desirable | auto |
| LACP | active | passive |

show etherchannel summary

show interfaces port-channel [group number]

port-channel load-balance [method]

Layer 3

1. Route Table

show ip route

show run | include ip route

1. Static route

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

預設：

Ip route 0.0.0.0 0.0.0.0 [next hop interface]

1. Dynamic route

FHRP(First Hop Redundancy Protocol)

1. HSRP

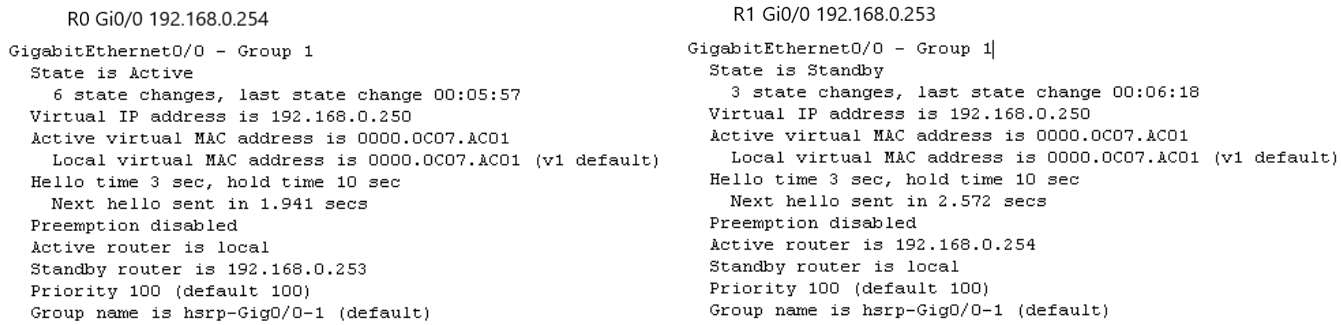
HSRP只有Cisco設備可用，先設定Group ID、VIP(Virtual IP)，參與HSRP的Interface的Group ID要相同，VIP需與Interface的IP處於同一個Subnet中。

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)

standby [Group ID] priority [Value]

更改之後state不會立即更換，為了保持穩定性，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

standby [Group ID] preempt

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. VRRP
2. GLBP

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.

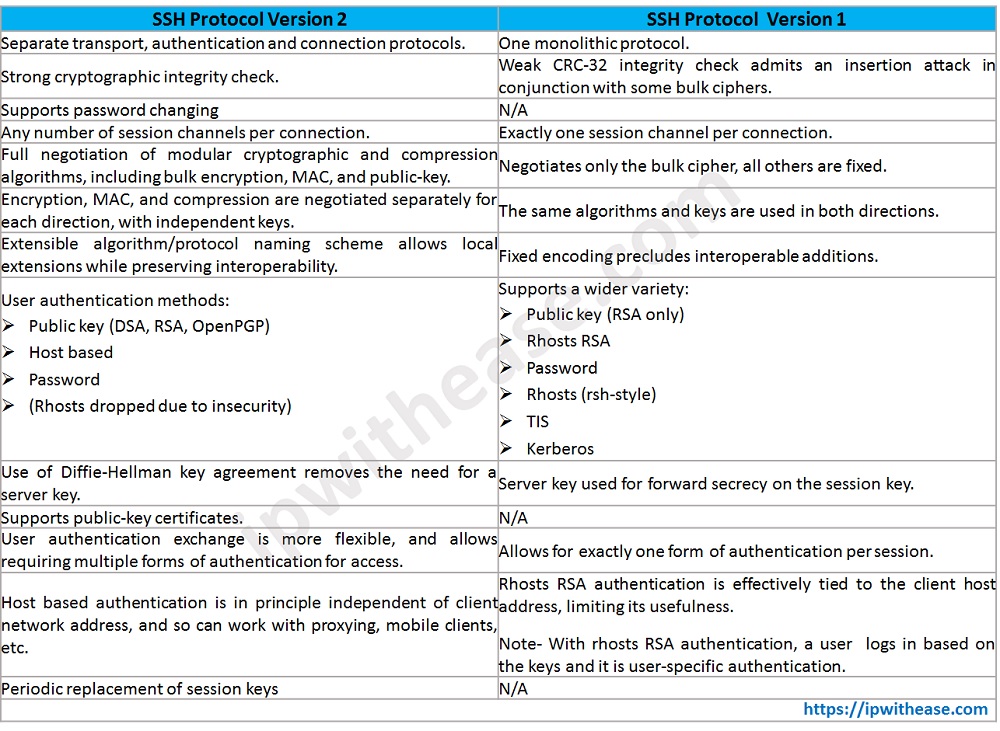
1. DNS and IP Spoofing

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