Network Administration/System Administration (NTU CSIE, Spring 2024) Homework #4

B12902110 呂承諺

March 17, 2024

Chapter1: 迷星叫

1.

	可通過的 VLAN 數量	802.1Q 標記
Access Port	1	No
Trunk Port	Many, all in the allowlist	Yes, except for its native VLAN

2. The trunk native VLAN is the VLAN that carries untagged traffic on a trunk port. On the transmitting side, packets with the same VLAN ID as the trunk native VLAN will be sent untagged. On the receiving side, untagged packets are assumed to be in the native VLAN.

3.

封包						
	802.1Q VID 欄位					
傳遞方向	線路 1	線路 2	線路 3	線路 4	線路 5	能否抵達
PC-01/VLAN 10 → PC-02	10	無				可
PC-01/VLAN 20 → PC-02	10	X				否
PC-01/VLAN 10 → PC-04	10		無		X	否
PC-01/VLAN 20 → PC-04	20		20		20	可
PC-01/VLAN 10 → PC-03	10			10		可
PC-01/VLAN 20 → PC-03	20			20		可

4. Suppose the packet has two VLAN tags, the first one with VLAN ID 10 and the second one with VLAN ID 20. When Switch-01 forwards this packet to Switch-02 via link 3, it drops the first tag because VLAN 10 is the native VLAN for this trunk port. Now when Switch-02 receives the frame, it sees the tag with VLAN ID 20 and allows it to flow on link 5, eventually reaching PC-04.

References

- Cisco_Nexus_5000_Series_NX-OS_Software_Configuration_Guide_chapter9.pdf
- Solved: VLAN tagging on Access Port - Cisco Community
- vlan - Aren't Switch Access ports tagged? - Network Engineering Stack Exchange
- VLAN hopping - Wikipedia
- VLAN Attack 虛擬區域網絡攻擊 - Jan Ho 的網絡世界

Chapter2: 春日影

Part 1

Steps

1. Open the backup configuration file, and we see
   `username RiNG privilege 15 password 7 0813435D0C150C16`.
2. According to the web, type 7 encryption is already cracked. We use the Cisco Type 7 Password Decrypt / Decoder / Crack Tool and obtain password `Roselia`.

References

- Catalyst 2960, 2960-S, 2960-C, and 2960-Plus Switches Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later - Configuring Switch-Based Authentication [Cisco Catalyst 2960 Series Switches] - Cisco
- 常見問題 | Intesys 捷赫國際
- Cisco Type 7 Password Decrypt / Decoder / Crack Tool

Part 2

Steps

1. Run the following commands on RiNG-Core:

```
RiNG-Core(config)#no vlan 10

RiNG-Core(config)#vlan 20
RiNG-Core(config-vlan)#name VLAN-MyGO
RiNG-Core(config)#interface range Fa0/1-3
RiNG-Core(config-if-range)#switchport access vlan 20

RiNG-Core(config)#vlan 30
RiNG-Core(config-vlan)#name VLAN-AveMujica
RiNG-Core(config)#interface range Fa0/11-12
RiNG-Core(config-if-range)#switchport access vlan 30

RiNG-Core(config)#interface Po1
RiNG-Core(config-if)#switchport trunk allowed vlan 20,99
```

2. Run the following commands on RiNG-Edge:

```
RiNG-Edge(config)#no vlan 10
RiNG-Edge(config)#vlan 20
RiNG-Edge(config-vlan)#name VLAN-MyGO

RiNG-Edge(config)#interface range Fa0/21-22
RiNG-Edge(config-if-range)#switchport access vlan 20

RiNG-Edge(config)#interface Po1
RiNG-Edge(config-if)#switchport trunk allowed vlan 20,99
```

Part 3

Run the following commands on RiNG-Core:

a.
```
RiNG-Core(config)#no username RiNG
RiNG-Core(config)#username RiNG privilege 15 secret 0 Afterglow
```

Note: `service password-encryption` is already on.

b.
```
RiNG-Core(config)#ip domain-name RiNG
RiNG-Core(config)#crypto key generate rsa
The name for the keys will be: RiNG-Core.RiNG
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 4096
% Generating 4096 bit RSA keys, keys will be non-exportable...[OK]
```

Note: SSH version 2 requires the RSA key size to be at least 768 bits.

c.
```
RiNG-Core(config)#line vty 0 4
RiNG-Core(config-line)#login local
RiNG-Core(config-line)#transport input ssh
```

d.
```
RiNG-Core(config)#line vty 5 15
RiNG-Core(config-line)#transport input none
```

e.
```
RiNG-Core(config)#ip ssh version 2
```

Repeat all commands on RiNG-Edge except for *b. SSH key generation*, because it already has a key.

References

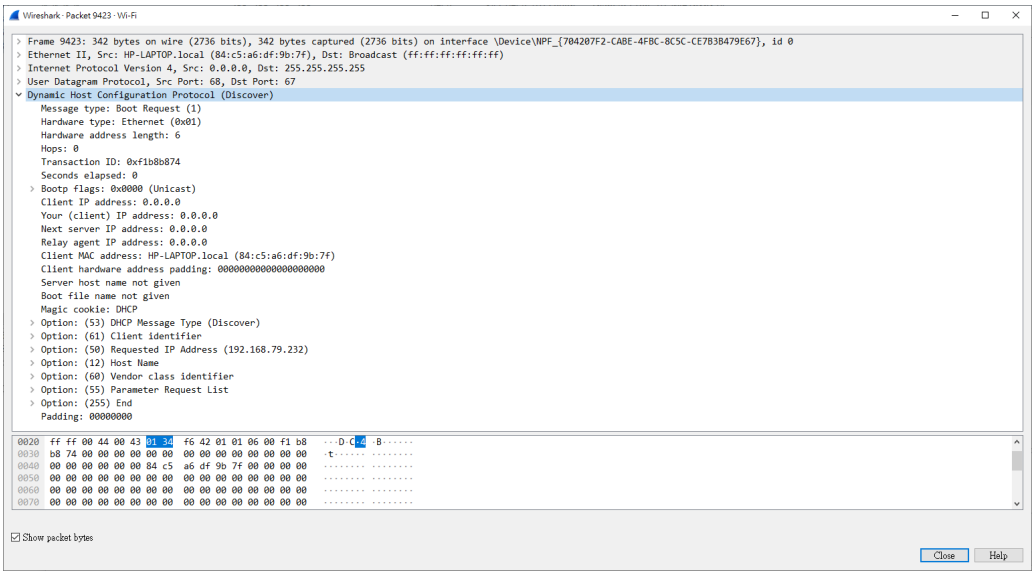
- Catalyst 2960, 2960-S, 2960-C, and 2960-Plus Switches Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later - Configuring Switch-Based Authentication [Cisco Catalyst 2960 Series Switches] - Cisco

Chapter3: 無路矢

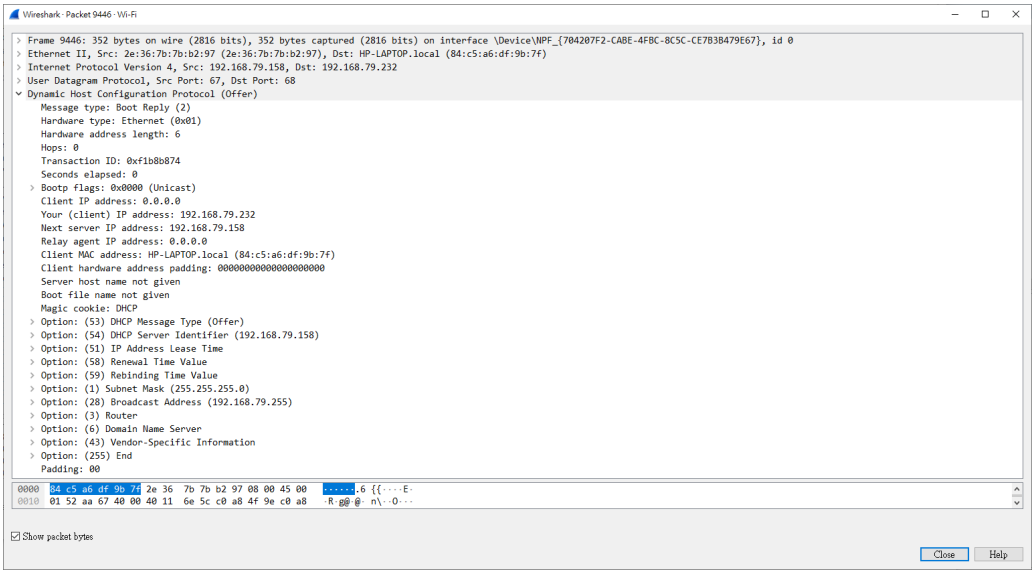
1. dhcp

No.	Time	Source	Destination	Protocol	Length	Info
9423	5.116592	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf1b8b874
9446	5.125337	192.168.79.158	192.168.79.232	DHCP	352	DHCP Offer - Transaction ID 0xf1b8b874
9447	5.125969	0.0.0.0	255.255.255.255	DHCP	358	DHCP Request - Transaction ID 0xf1b8b874
9452	5.139483	192.168.79.158	192.168.79.232	DHCP	352	DHCP ACK - Transaction ID 0xf1b8b874

   - **Discover:** The client sends a broadcast DHCPDISCOVER message to the current local network and hopes for response from a DHCP server.

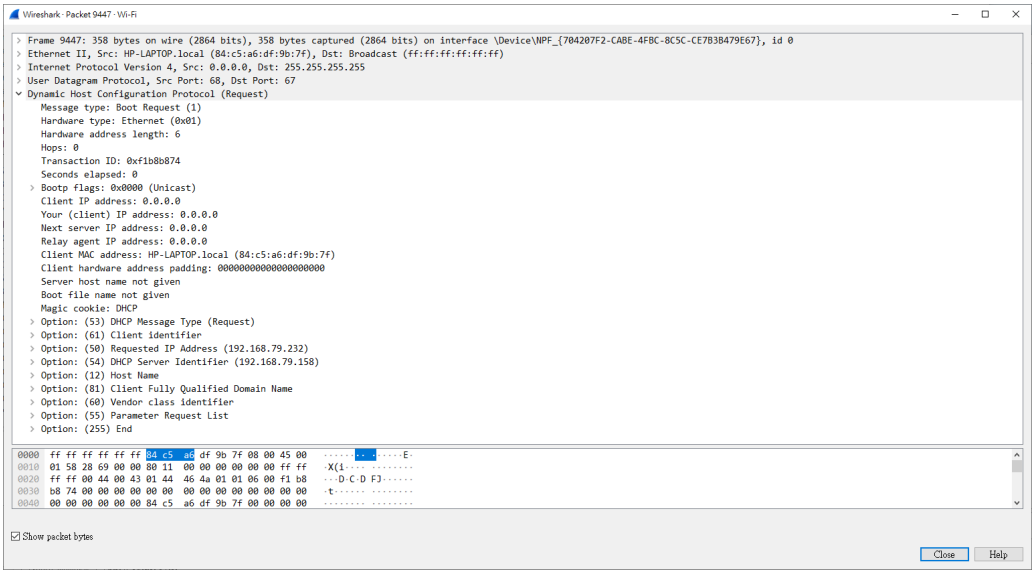


   - **Offer:** The DHCP server reserves an IP address for the client, and then sends a DHCPOFFER message to the client, offering a set of network configuration.



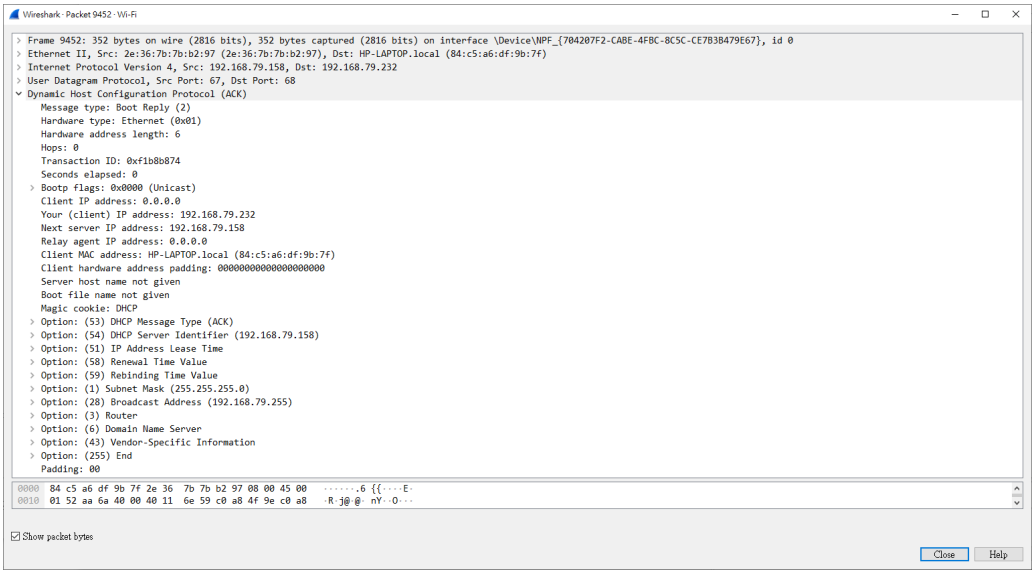
   In this example, the server 192.168.79.158 give us an offer. The offered IP address is 192.168.79.232, subnet mask is 255.255.255.0, and default gateway is 192.168.79.158。

- **Request:** The client sends a broadcast DHCPREQUEST message to the server, requesting the IP address in the offer.



  In this example, that is 192.168.79.232。

- **Acknowledgement:** The server sends a DHCPACK message to the client. This completes the setup.



References

- Dynamic Host Configuration Protocol - Wikipedia

2.
- IP 0.0.0.0
  - 涵義：目前所在的網路。
  - 原因：用戶端還沒有 IP 位址。
- IP 255.255.255.255
  - 涵義：目前網路的廣播位址。目標為 255.255.255.255 的封包不會被路由器轉發到其他網路。
  - 原因：連上網路的最初，用戶端不會知道 DHCP 伺服器的 IP 位址，因此廣播訊息給目前網路的所有裝置，期待有 DHCP 伺服器接收到。

- MAC FF:FF:FF:FF:FF:FF
  - 涵義：廣播 MAC 位址。送往這個位址的封包可以被所有 LAN 上的裝置接受到。
  - 原因：連上網路的最初，用戶端不會知道 DHCP 伺服器的 MAC 位址，因此廣播訊息給目前網路的所有裝置，期待有 DHCP 伺服器接收到。

References

- Reserved IP addresses - Wikipedia
- Broadcast address - Wikipedia

3. Run the following commands to enable DHCP snooping and trust interface `FastEthernet0/22`:

```
RiNG-Core(config)#ip dhcp snooping
RiNG-Core(config)#ip dhcp snooping vlan 1
RiNG-Core(config)#interface Fa0/22
RiNG-Core(config-if)#ip dhcp snooping trust
```

Note: The default setting for an interface is untrusted.

References

- DHCP snooping - Wikipedia
- Catalyst 2960, 2960-S, 2960-C, and 2960-Plus Switches Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later - Configuring DHCP Features and IP Source Guard [Cisco Catalyst 2960 Series Switches] - Cisco