Module 7: DHCPv4

1. DHCPv4 Concepts (DHCPv4 Server and Client)

-Giao thức cấu hình máy chủ động v4 (DHCPv4) chỉ định động địa chỉ IPv4 và thông tin cấu hình mạng khác. Vì các máy khách trên máy tính để bàn thường tạo nên phần lớn các nút mạng, DHCPv4 là một công cụ cực kỳ hữu ích và tiết kiệm thời gian cho các quản trị viên mạng.

-Máy chủ DHCPv4 tự động gán hoặc cho thuê địa chỉ IPv4 từ nhóm địa chỉ trong một khoảng thời gian giới hạn do máy chủ chọn hoặc cho đến khi máy khách không cần địa chỉ đó nữa.

-DHCP Request (DHCPREQUEST):

+Trước khi hợp đồng thuê hết hạn, máy khách sẽ gửi trực tiếp thông báo DHCPREQUEST đến máy chủ DHCPv4 đã cung cấp địa chỉ IPv4 ban đầu. Nếu không nhận được DHCPACK trong một khoảng thời gian nhất định, máy khách sẽ phát một DHCPREQUEST khác để một trong các máy chủ DHCPv4 khác có thể gia hạn hợp đồng thuê.

-DHCP Acknowledgment (DHCPACK):

+Khi nhận được thông báo DHCPREQUEST, máy chủ xác minh thông tin cho thuê bằng cách trả về một DHCPACK.

-Steps to Configure a Cisco IOS DHCPv4 Server:

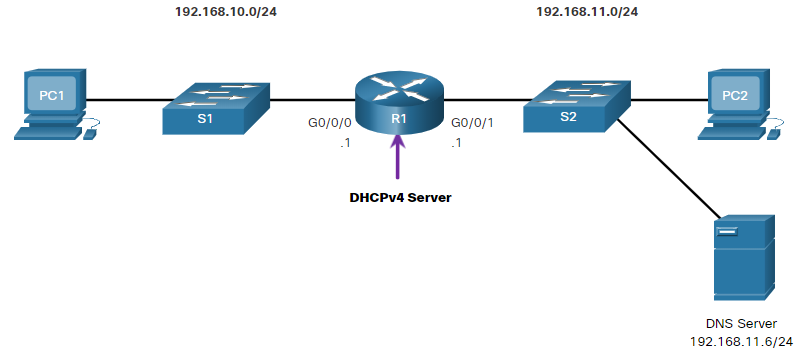
+Bước 1: Loại trừ địa chỉ ipv4. Có thể loại trừ một địa chỉ đơn lẻ hoặc một dải địa chỉ bằng cách chỉ định địa chỉ thấp và địa chỉ cao của dải. Địa chỉ bị loại trừ phải là những địa chỉ được gán cho bộ định tuyến, máy chủ,…. Lệnh *ip dhcp excluded-address* **low-address[high-address]**.

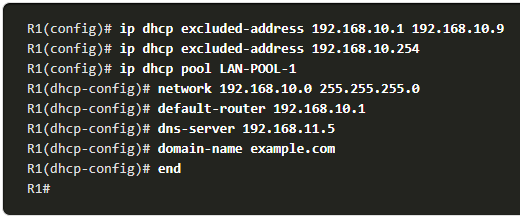
+Bước 2: Đặt tên nhóm DHCPv4. Lệnh *ip dhcp pool* **pool-name**.

+Bước 3: Cấu hình DHCPv4 pool:

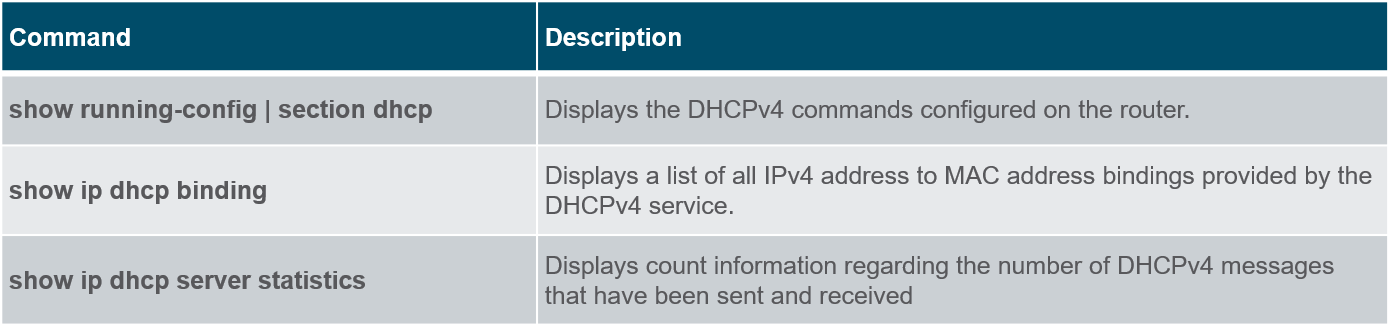
* Xác định nhóm địa chỉ: *network* **network-number[mask| prefix-length]**
* Xác định router mặc định hay default: *default router* **address**
* Xác định DNS server: *dns-server* **address**
* Xác định tên miền: *domain-name* **domain**

VD minh hoạ:

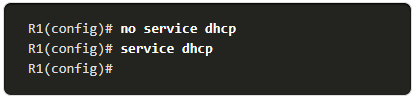




-Sử dụng các lệnh để xác minh máy chủ đang hoạt động



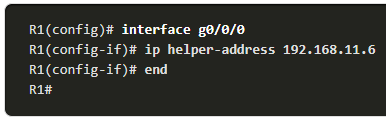
-Tắt Máy chủ Cisco IOS DHCPv4: Dịch vụ DHCPv4 được bật theo mặc định. Để tắt dịch vụ hãy sử dụng lệnh dưới đây



1. DHCPv4 Relay

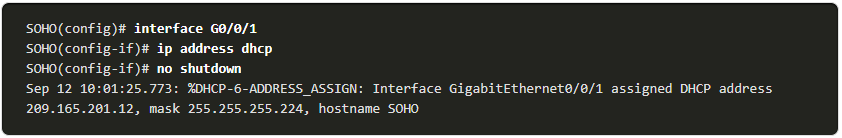
-Cấu hình R1 bằng lệnh cấu hình giao diện địa chỉ địa chỉ *ip helper-address*. Điều này sẽ khiến R1 chuyển tiếp các chương trình phát sóng DHCPv4 đến máy chủ DHCPv4.

-VD minh hoạ:



1. Cisco Router as a DHCPv4 Client

-Để định cấu hình giao diện Ethernet làm máy khách DHCP, hãy sử dụng lệnh chế độ cấu hình giao diện dhcp địa chỉ ip, như được hiển thị trong ví dụ



1. Tổng kết

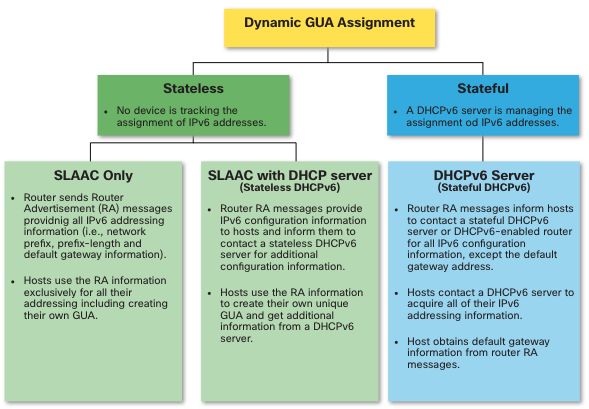
* **ip dhcp excluded-address low-address [high-address]**
* **ip dhcp pool name**
* **network network-number [mask | /prefix-length]**
* **default-router address [address2 ... address8]**
* **dns-server address [address2 ... address8]**
* **domain-name domain**
* **lease {days [hours [minutes]] | infinite}**
* **netbios-name-server address [address2 ... address8]**
* **show running-config | section dhcp**
* **show ip dhcp binding**
* **show ip dhcp server statistics**
* **[no] service dhcp**
* **ip helper-address address**
* **ip address dhcp**

Module 8: SLAAC and DHCPv6

1. IPv6 GUA Assignment

-Trên một bộ định tuyến, địa chỉ IPv6 toàn cục (GUA) được định cấu hình theo cách thủ công bằng cách sử dụng lệnh cấu hình giao diện địa chỉ ipv6 ipv6-address / prefix-length.

-Theo mặc định, bộ định tuyến hỗ trợ IPv6 gửi ICMPv6 RA định kỳ giúp đơn giản hóa cách máy chủ có thể tự động tạo hoặc có được cấu hình IPv6 của nó.

-Một máy chủ có thể được chỉ định động một GUA bằng cách sử dụng các dịch vụ stateful và stateless.

-Tất cả các phương thức stateless và stateful trong mô-đun này sử dụng thông báo ICMPv6 RA để đề xuất cho máy chủ lưu trữ cách tạo hoặc lấy cấu hình IPv6 của nó.

-ICMPv6 RA bao gồm 3 flags sau:

+A flag: flag tự động định cấu hình địa chỉ biểu thị sử dựng tự động định cấu hình địa chỉ stateless(SLAAC) để tạo IPV6 GUA.

+O flag: flag cấu hình biểu thị rằng thông tin bổ sung có sẵn từ máy chủ DHCPv6 stateless.

+M flag: flag cấu hình địa chỉ được quản lí biểu thị sử dụng máy chủ DHCPv6 stateful để lấy IPv6 GUA.

Module 9: FHRP Concepts

1. First Hop Redundancy Protocols

-Thiết bị cuối thường được định cấu hình bằng một địa chỉ IPv4 cổng mặc định duy nhất.

Nếu giao diện bộ định tuyến cổng mặc định không thành công, các máy chủ LAN sẽ mất kết nối mạng LAN bên ngoài.

-Điều này xảy ra ngay cả khi một bộ định tuyến dự phòng hoặc bộ chuyển mạch Lớp 3 có thể đóng vai trò như một cổng mặc định tồn tại.

-Giao thức dự phòng bước đầu tiên (FHRP) là cơ chế cung cấp các cổng mặc định thay thế trong mạng chuyển mạch nơi hai hoặc nhiều bộ định tuyến được kết nối với cùng một VLAN.

1. HSRP

HSRP Overview: Cisco cung cấp HSRP và HSRP cho IPv6 như một cách để tránh mất quyền truy cập mạng bên ngoài nếu bộ định tuyến mặc định của bạn bị lỗi. HSRP là FHRP độc quyền của Cisco được thiết kế để cho phép chuyển đổi dự phòng một cách rõ ràng đối với thiết bị IP bước đầu tiên.

Module 10: LAN Security Concepts

1. Endpoint Security

-Các phương tiện truyền thông tin tức thường đưa tin về các cuộc tấn công vào mạng doanh nghiệp. Chỉ cần tìm kiếm “các cuộc tấn công mạng mới nhất” trên internet để tìm thông tin cập nhật về các cuộc tấn công hiện tại. Nhiều khả năng, những cuộc tấn công này sẽ liên quan đến một hoặc nhiều điều sau đây:

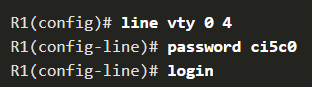
-Từ chối dịch vụ phân tán (DDoS) - Đây là một cuộc tấn công phối hợp từ nhiều thiết bị, được gọi là thây ma, với mục đích làm suy giảm hoặc ngăn chặn quyền truy cập công khai vào trang web và tài nguyên của tổ chức.

-Vi phạm dữ liệu - Đây là một cuộc tấn công trong đó máy chủ hoặc máy chủ dữ liệu của một tổ chức bị xâm nhập để lấy cắp thông tin bí mật.

-Phần mềm độc hại - Đây là cuộc tấn công trong đó máy chủ của tổ chức bị nhiễm phần mềm độc hại gây ra nhiều sự cố. Ví dụ, ransomware như WannaCry mã hóa dữ liệu trên máy chủ và khóa quyền truy cập vào nó cho đến khi trả tiền chuộc.

1. Access Control

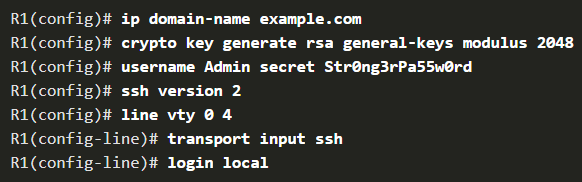
-Phương pháp xác thực truy cập từ xa đơn giản nhất là cấu hình tổ hợp đăng nhập và mật khẩu trên bảng điều khiển, dòng vty và cổng aux.



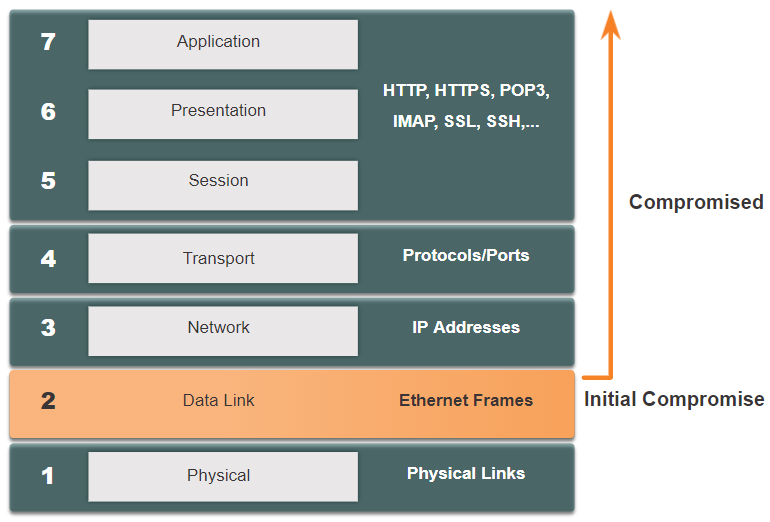
-SSH là một hình thức truy cập từ xa an toàn hơn:

Nó yêu cầu tên người dùng và mật khẩu.

Tên người dùng và mật khẩu có thể được xác thực cục bộ.



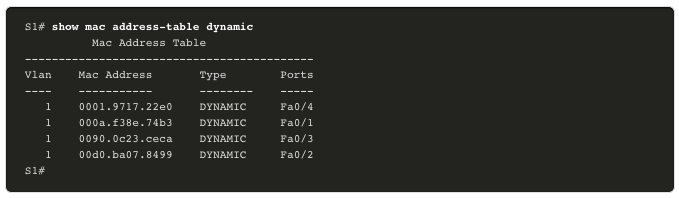
1. Layer 2 Security Threats

-Nhớ lại rằng mô hình tham chiếu OSI được chia thành bảy lớp hoạt động độc lập với nhau. Hình cho thấy chức năng của từng lớp và các yếu tố cốt lõi có thể được khai thác.

-Quản trị viên mạng thường xuyên triển khai các giải pháp bảo mật để bảo vệ các phần tử từ Lớp 3 đến Lớp 7. Họ sử dụng VPN, tường lửa và thiết bị IPS để bảo vệ các phần tử này

1. MAC Address Table Attack

-Nhớ lại rằng để đưa ra quyết định chuyển tiếp, thiết bị chuyển mạch LAN Lớp 2 xây dựng một bảng dựa trên các địa chỉ MAC nguồn trong các khung đã nhận. Đây được gọi là bảng địa chỉ MAC. Bảng địa chỉ MAC được lưu trữ trong bộ nhớ và được sử dụng để chuyển đổi khung hiệu quả hơn.



Module 11: Switch Security Configuration

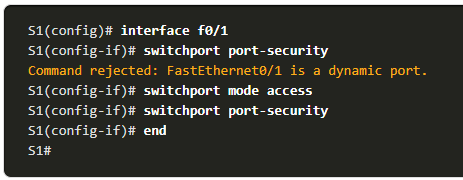
1. Implement Port Security

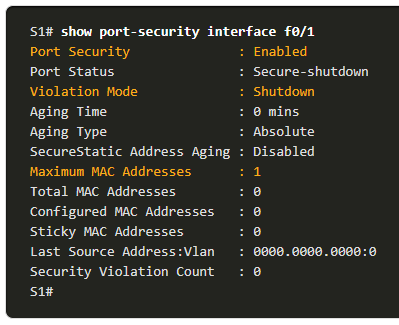
-Các cuộc tấn công Lớp 2 là một trong những cách dễ dàng nhất để tin tặc triển khai nhưng những mối đe dọa này cũng có thể được giảm thiểu bằng một số giải pháp Lớp 2 phổ biến.

-Các cuộc tấn công Lớp 2 là một trong những cách dễ dàng nhất để tin tặc triển khai nhưng những mối đe dọa này cũng có thể được giảm thiểu bằng một số giải pháp Lớp 2 phổ biến. Để định cấu hình một loạt các cổng, hãy sử dụng lệnh phạm vi giao diện.

Switch(config)# **interface range** *type module/first-number – last-number*

1. Enable Port Security

-Bảo mật cổng được kích hoạt bằng lệnh cấu hình giao diện cổng-bảo mật cổng chuyển đổi.

-Lưu ý trong ví dụ, lệnh bảo mật cổng switchport đã bị từ chối. Điều này là do bảo mật cổng chỉ có thể được cấu hình trên các cổng truy cập được cấu hình thủ công hoặc các cổng trung kế được cấu hình thủ công. Theo mặc định, các cổng chuyển đổi Lớp 2 được đặt thành tự động động (bật trung kế)

-Sử dụng lệnh hiển thị giao diện bảo mật cổng để hiển thị cài đặt bảo mật cổng hiện tại cho FastEthernet 0/1.

-Sau khi bật bảo mật cổng, có thể định cấu hình các chi tiết cụ thể về bảo mật cổng khác, như được minh họa trong ví dụ.

-Để đặt số lượng địa chỉ MAC tối đa được phép trên một cổng, hãy sử dụng lệnh sau:

Switch(config-if)# **switchport port-security maximum** *value*

Switch có thể được định cấu hình để tìm hiểu về địa chỉ MAC trên một cổng an toàn theo một trong ba cách:

1. Manually Configured: Quản trị viên định cấu hình (các) địa chỉ MAC tĩnh theo cách thủ công bằng cách sử dụng lệnh sau cho từng địa chỉ MAC an toàn trên cổng:

Switch(config-if)# **switchport port-security mac-address** *mac-address*

1. Dynamically Learned: Khi nhập lệnh bảo mật cổng cổng chuyển đổi, MAC nguồn hiện tại cho thiết bị được kết nối với cổng sẽ tự động được bảo mật nhưng không được thêm vào cấu hình đang chạy. Nếu công tắc được khởi động lại, cổng sẽ phải tìm hiểu lại địa chỉ MAC của thiết bị.
2. Dynamically Learned – Sticky: Quản trị viên có thể bật công tắc để học động địa chỉ MAC và “gắn” chúng vào cấu hình đang chạy bằng cách sử dụng lệnh sau:

Switch(config-if)# **switchport port-security mac-address sticky**