# How to bind MAC addresses to core switches

Article Overview

MAC addresses can be bound to core switches using static, sticky, or DHCP-based methods to control device access and enhance network security.

1. Static MAC Address Binding

Static binding involves manually assigning a MAC address to a specific switch port. This ensures that only the designated device can communicate through that port. On Cisco switches, this can be configured using port security commands:

Switch(config)# interface FastEthernet0/1Switch(config-if)# switchport port-securitySwitch(config-if)# switchport port-security mac-address 00AA.BBCC.DDEESwitch(config-if)# switchport port-security maximum 1Switch(config-if)# switchport port-security violation restrict
This method is highly secure but administratively intensive, especially in large networks, because each MAC must be manually entered and updated if devices move .

2. Sticky MAC Address Binding

Sticky MAC binding allows the switch to learn MAC addresses dynamically and then save them in the running configuration. This combines the convenience of dynamic learning with the security of static binding:

Switch(config-if)# switchport port-security mac-address sticky
Once learned, the MAC addresses are retained across reboots if saved to the startup configuration. This method is useful for environments where devices may occasionally move but still require port-level security .

3. DHCP-Based MAC Binding

For larger deployments, especially with IP phones or hundreds of devices, binding MAC addresses via DHCP reservations is more scalable. The DHCP server assigns a specific IP address to a device based on its MAC address. On Cisco core switches acting as DHCP servers:

ip dhcp pool VOIP host 172.16.10.10 255.255.254.0 client-identifier 01:00:50:54:xx:xx:xx hardware-address 5405.db39.f302
This ensures that only the specified MAC address receives the reserved IP, preventing unauthorized devices from obtaining network access .

4. Considerations for Core Switch Deployment

o Port Security Limits: Core switches often handle uplinks and multiple VLANs; binding too many MAC addresses per port can impact performance.
o Device Mobility: Sticky or DHCP-based binding is preferable in environments with mobile devices.
o Security Enforcement: Combine MAC binding with VLAN segmentation and access control lists (ACLs) for enhanced security.
o Monitoring and Maintenance: Regularly audit MAC tables and DHCP reservations to prevent stale entries and ensure network integrity . By combining these methods, network administrators can securely control which devices connect to the network, reduce unauthorized access, and maintain efficient IP address management.

Actually, I make a core switch vtp server and other are client and configure a core switch as a DHCP server. All ip

Switch port and MAC address binding (based on Cisco Simulator), Programmer All, we have been working hard to make a technical

Understand how to manage MAC addresses on your network switch. Easy steps for finding, adding, and deleting MAC

A MAC address entry includes a destination MAC address, an outgoing interface, and a VLAN ID. When the device receives a frame,

Hello We would like to control who can connect to our network. How do I create a list of ALLOWED mac addresses

S2750, S5700, and S6700 V200R005 (C00, C01, C02, and C03) Configuration Guide - Security How Do I Bind an IP

CBS350 (config-if-range)# end You should now have mapped MAC-based VLAN groups to the VLANs on your switch

Bind MAC to VLAN Use the Bind MAC to VLAN page to map a MAC address to a VLAN. After the source MAC address and the

A switch supports the binding of one MAC address and multiple IP addresses. If you need to bind non-contiguous IP addresses to a

# How to bind MAC addresses to core switches

The following example shows how to limit the number of MAC addresses to 100 in VLAN 10, and configure the switch to drop packets

Overview MAC address entries are automatically generated when the switch learns the source MAC addresses of

Huawei Technical Support

To prevent IP address theft or employee IP address tampering in a Cisco switch, you can take the following measures: binding an IP

About MAC Addresses The Media Access Control (MAC) address is a unique value that is associated with a network device. Layer 2

Ip bind with mac commands enable: ip dhcp snooping ip dhcp snooping vlan (no.) ip source binding (mac address)

For security and convenience management, you need to bind the MAC address to the port, that is, the MAC address is bound to the

Web: https://in-au.co.za