Learn CISCO NETWORK ADMINISTRATION IN A MONTH OF LUNCHES

SAMPLE CHAPTER

BEN PIPER

MANNING

Learn Cisco Network Administration in a Month of Lunches

by Ben Piper

Sample Chapter 5

brief contents

5 Securing ports by using the Port Security feature

In the last chapter you learned how to secure unused ports by disabling them. Disabling unused ports can stop a bad guy from plugging a malicious device into an unused port and getting unauthorized access to the network. It can also help train users—especially those in remote offices—to call IT *before* moving things around. After a few go-rounds of plugging a computer into an empty port and having it not work, most people will take the hint that they need to call IT first.

But although disabling ports is the most secure option for dealing with unused ports, it does nothing to secure in-use ports. And in a live environment, the majority of switch ports *will* be in use.

Port Security is a versatile feature that can mitigate attacks against the network and prevent unauthorized moves, adds, and changes by limiting the number of unique media access control (MAC) addresses that can use a given port. Recall that every device on the network has a unique MAC address that it uses to communicate with other devices in the same broadcast domain. Versatility is crucial because security is not a one-size-fits-all proposition. Some organizations prefer a minimal level of security, whereas others require a level of security that borders on paranoia. Rather than tell you how secure you need to make your network, in this chapter I lay out the specific risks Port Security can mitigate so you can decide for yourself how lax or restrictive you need it to be. Then I'll show you how to configure Port Security to accommodate your requirements.

I'm not going to show you every possible way you can configure Port Security. Instead, I'm going to teach you how to configure it for minimum and maximum levels of security, as shown in table 5.1.

Table 5.1 Port Security levels

Protection level	Attacks mitigated
Minimum	MAC flood attack, denial-of-service attack, traffic sniffing
Maximum	All of the above, plus unauthorized device access and spread of malware

Table 5.1 lists which attacks each level of Port Security can help mitigate. Let's start with the minimum level.

5.1 The minimum Port Security configuration

Although I can't tell you how secure to make your network, I can tell you that you definitely want to enable a minimum Port Security configuration on all end-user ports.

Security is always a tradeoff. You have to consider whether it's worth the time, money, and effort to defend against a particular risk. Port Security is already included in IOS, so there's no additional cost. And the time and effort it takes to configure Port Security to a minimum level is negligible. But what you get in return is peace of mind and protection against a potentially debilitating and costly attack called a MAC flood attack.

5.1.1 Preventing MAC flood attacks

Recall from chapter 2 that a switch maintains a MAC address table containing the MAC address of each device and the port it's connected to. Table 5.2 is an example of the type of information you'd find in a MAC address table. By keeping track of where each device is, the switch avoids flooding every frame to every device.

Table 5.2 Sample MAC address table

Device	MAC address	Switch port
Ben's computer	0800.2700.ec26	FastEthernet0/1

In a MAC flooding attack, a malicious program continually sends frames with fake or spoofed MAC addresses as the source address. Because each frame appears to come from a different MAC address, the switch's MAC address table fills up with these fake addresses, and the switch has no choice but to send every frame to every port. The net effect of this is that the computer running the malicious program effectively becomes a network sniffer that's in a position to capture every frame on the network. Figure 5.1 illustrates how an attacker can use a MAC flooding attack to capture traffic.

In step 1, an attacker sends thousands of frames with bogus source MAC addresses to Switch1. In step 2, Switch1's MAC address table fills up. In step 3, the database

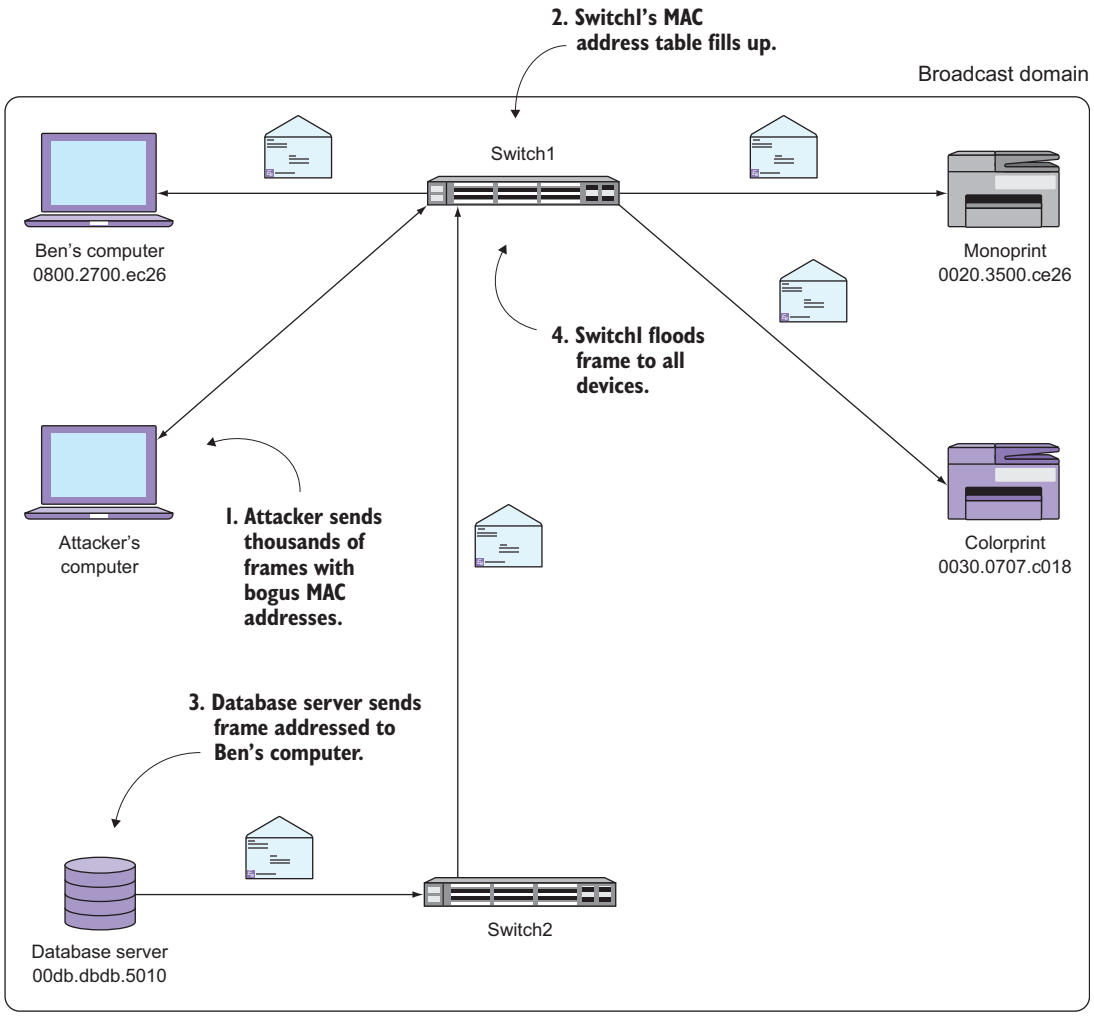

Figure 5.1 MAC flooding attack

server sends a frame addressed to my computer. Switch2 forwards this frame to Switch1. Finally, in step 4, Switch1 floods the frame out all ports, including the one connected to the attacker's computer.

But it's worse than that. A MAC flood can effectively result in a denial of service for all users. Remember the saying from chapter 2: "When everybody talks, nobody listens." MAC flooding severely diminishes network performance to the point of making the network practically unusable. Imagine dozens of customer calls getting dropped all at once because Voice over IP traffic can't traverse the network. Port Security can help ensure that you, as a network administrator, are never put in the unnerving position of

having to deal with such an event. Just one unprotected port is all it takes for a MAC flooding attack to take down your network, which is why it's so important to configure Port Security on every port.

> **NOTE** You can protect against MAC flooding attacks with antivirus software on your PCs and servers and by making sure end users don't have administrative access on their machines. But these methods aren't 100% foolproof. Port Security is the most reliable way to prevent a MAC flood attack even if other security measures fail.

Normally, the switch doesn't care how many different MAC addresses are on the same port. It allows the traffic anyway, regardless of the source MAC address. Remember that MAC addresses were invented to make it possible to plug a device into the network and have it work. But this plug-and-play behavior is the very thing that makes a MAC flooding attack possible.

The obvious solution is to limit the number of source MAC addresses that can simultaneously be associated with a given port. This is exactly what Port Security does. You configure it to permit a specified number of simultaneous MAC addresses, and it allows access on a first-come, first-served basis. Let's look at an example.

Suppose that you have a user with two devices—a PC and a Cisco IP phone—connected to the same port. The phone is physically connected to the switch, and the PC is physically connected to the phone and communicates through it. Table 5.3 shows roughly how they would look in the MAC address table.

Table 5.3 MAC address table

Device	MAC address	Port
PC	0123.4567.8901	FastEthernet0/23
IP phone	0123.4598.7654	FastEthernet0/23

These two devices represent two unique MAC addresses, so you want to limit the maximum number of MAC addresses to two using the `switchport port-security maximum 2` interface command.

Try it now

Locate a port with two devices plugged into it. If you have a PC plugged in behind an IP phone, that's perfect. If you don't, you can still perform the exercise; just change the command to allow only one MAC address.

Issue the following commands to configure the maximum number of allowed MAC addresses on the port to two:

```
interface fa0/1
switchport mode access
switchport port-security maximum 2
```

At this point, nothing should happen. That's because this command doesn't actually enable Port Security. You might find that counterintuitive, but it's actually a blessing. Port Security has the ability to effectively render a port unusable if misconfigured. It's vital that you find out how many MAC addresses should be living on each port *before* enabling Port Security.

If you're not sure about the number of MAC addresses, you can set the number to something high like 10 and then go back and adjust it later. That way, if your boss has a secret workgroup switch under his desk with eight different MACs hanging off it, you'll find out from IOS instead of him.

Try it now

Once you have the maximum number of MAC address set properly, enable Port Security using the `switchport port-security` interface command.

Now verify your configuration with the command `show port-security`.

You should see something similar to the following:

```
Switch1#show port-security
Secure Port   MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)        (Count)
------------------------------------------------------------------------------
    Fa0/1           2              2               0             Shutdown
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)    : 1
Max Addresses limit in System (excluding one mac per port) : 6144
```

The output doesn't provide much detail, but it's enough to figure out what's going on. When you enable Port Security on a port, it notes the MAC addresses that are talking on the port at that time and remembers them, up to the maximum value you specified. That's what the `MaxSecureAddr` column indicates. In this output, the maximum number of MAC addresses allowed on Fa0/1 is `2`.

The `CurrentAddr` column indicates how many MAC addresses the switch has seen on the port since you enabled Port Security. In this output, the number is also `2` because there are only two devices attached.

The `SecurityViolation` column tells you how many times the switch has detected an additional MAC address on the port beyond the allowed maximum. As you might expect, that number is `0`.

The last column, labeled `Security Action`, is arguably the most important one. It lists the action Port Security will take when it detects a *violation*—an additional MAC address beyond the configured maximum. This action is what Cisco calls the *violation mode*.

5.1.2 Violation modes

You're going to configure two violation modes: shutdown and restrict.

SHUTDOWN

In the output, the violation mode is shutdown. This means just what it sounds like. If Port Security detects a security violation—that is, an additional MAC address beyond the maximum two—it shuts down the port altogether. Without warning. No questions asked.

The shutdown behavior is the default. I suspect it's Cisco's way of preventing people from accidentally configuring Port Security and then wondering why things aren't working. When an in-use port abruptly shuts down right after you enable Port Security, it can be pretty dramatic and hard to miss.

RESTRICT

The alternative violation mode—restrict—is a bit more subtle. In this mode, when a violation occurs, Port Security keeps the port up but prevents the new MAC addresses from communicating. In a sense, it's like a dynamic access list that denies MAC addresses beyond the maximum.

You probably don't want Port Security to shut down the port altogether when it detects a violation. In that case, you must manually set the violation mode to restrict using the interface configuration command `switchport port-security violation restrict`.

Try it now

Change the violation mode to restrict using the following command:

```
switchport port-security violation restrict
```

As always, verify using the `show port-security` command.

You should see the violation mode in the last column change from `Shutdown` to `Restrict`. Everything else will stay the same:

```
Switch1#show port-security
Secure Port   MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)         (Count)
------------------------------------------------------------------------------
    Fa0/1          2             2                0             Restrict
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 6144
```

Now when Port Security detects a violation, it won't shut down the port or otherwise affect the first two MAC addresses. They'll continue to communicate normally, and only subsequent addresses will get blocked.

Above and beyond

You may want to use the shutdown violation mode to prevent someone from setting up a rogue wireless access point that uses Power over Ethernet (PoE). When IOS shuts down a port on a PoE switch, it cuts power to whatever device is plugged in. That's also why you don't want to use the shutdown violation mode on ports with IP phones.

5.2 Testing Port Security

One of the most fun aspects of Port Security is testing it. You don't have to launch your very own MAC flooding attack to do this. All you have to do is get one additional MAC address to show up on the same port. There are a couple of ways to do this.

If you're dealing with a PC and IP phone, unplug the PC from the phone and plug in a laptop. Once the switch sees the laptop's MAC address, Port Security will log a security violation and prevent the laptop's MAC address from communicating.

If you just have a single PC, plug a small workgroup switch in between the Cisco switch and the PC. Get a couple of laptops or IP phones and plug those into the workgroup switch. This will give you three MAC addresses on the same port—enough to trigger a Port Security violation.

Try it now

It's important that you keep a close eye on things while you're testing Port Security. IOS can show you real-time information about what Port Security is doing. Just issue the `terminal monitor` command at the enable prompt.

Next, use one of the methods I just listed to test Port Security.

After connecting a third device, you should see a message similar to this:

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by
     MAC address 0800.27ba.dbad on port FastEthernet0/1.
```

The console message leaves little room for interpretation. It gives you the port the violation occurred on and the MAC address that triggered it—good information to know when testing.

Now if you execute another `show port-security` command, you should see the `SecurityViolation` count increase:

```
Switch1#sh port-security
Secure Port   MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)         (Count)
---------------------------------------------------------------------------
    Fa0/1          2             2               18             Restrict
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)    : 1
Max Addresses limit in System (excluding one mac per port) : 6144
```

The number 18 may seem a bit unexpected considering Port Security should be blocking only one MAC address. The `SecurityViolation` counter increments every time an unauthorized MAC address tries to send a frame. If you've configured the maximum number of MAC addresses correctly, this number shouldn't get very high. If it does, it's a clue that you need to investigate the devices on that port.

Above and beyond

You can reset the `SecurityViolation` counter by shutting down the port and re-enabling it. As of this writing, there's no command to clear the counters directly.

5.3 Handling device moves

I mentioned earlier that Port Security is first come, first served. When you physically disconnect a device from a secured port, Port Security forgets all the MAC addresses it saw on that port. That way, if you plug a different device into the same port, Port Security will still allow it. This works well in cases when moving devices always entails physically unplugging something from the switch. For example, when a user moves desks, someone will physically unplug their PC and IP phone from the switch.

But there's another possibility. Suppose that an IT system administrator has a need to simultaneously connect five brand-new computers to the network in order to install software, download updates, and so on to get them ready for new users. But there's a problem: in the office where they're working, there's only one network jack. In order to stay efficient and get the PCs out on time, they plug a small, eight-port workgroup switch into the jack and plugs all the new PCs into that.

5.3.1 Port Security never forgets!

In the network closet, the jack is patched into port FastEthernet0/12 on the switch. You've done your homework, and you know that there should never be more than five simultaneous MAC addresses on the port that the workgroup switch is connected to. So you configure Port Security to allow a maximum of five MACs.

Try it now

It's okay if you don't actually have a small switch plugged in. This is just for practice. Use the following commands to configure Port Security to allow up to five simultaneous MAC addresses on FastEthernet0/12:

```
interface fa0/12
switchport port-security maximum 5
switchport port-security violation restrict
switchport port-security
```

After the system administrator boots up the five computers, each one begins sending traffic with its unique MAC address. Everything works as expected, and the computers can communicate with the network normally. A `show port-security` confirms Port Security is enabled and not blocking anything:

```
Switch1#show port-security
Secure Port   MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)         (Count)
---------------------------------------------------------------------------
    Fa0/1          2             0               0              Restrict
    Fa0/12         5             5               0              Restrict
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)    : 4
Max Addresses limit in System (excluding one mac per port) : 6144
```

When the administrator is finished, they shut down the machines and plug five new ones into the workgroup switch to get them set up. But now there's another problem. None of the machines can get on the network at all. You check Port Security again, and see the following:

```
Switch1#show port-security
Secure Port   MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)         (Count)
---------------------------------------------------------------------------
    Fa0/1          2             0               0              Restrict
    Fa0/12         5             5              30              Restrict
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)    : 4
Max Addresses limit in System (excluding one mac per port) : 6144
```

MAC addresses getting blocked

Port Security hasn't let go of the original five MAC addresses. It still remembers them and consequently doesn't allow the new PCs to communicate.

It's important to understand why this is happening. Port Security has no way of knowing that the original five PCs were unplugged from the network. The eight-port workgroup switch hides that. All Port Security knows is that it saw five unique MAC addresses, and then later on it saw five new ones. In keeping with the configuration, Port Security allowed only the first five MAC addresses and blocked the subsequent ones.

You could tell the system administrator to just unplug or reboot the workgroup switch every time they go through a round of computers, but that's impractical and annoying and would prematurely wear out the switch. You need another way to force Port Security to forget those MAC addresses without any manual intervention.

5.3.2 Aging time

The aging time is a parameter you can set to cause Port Security to periodically forget the MAC addresses it has learned.

After the system administrator finishes up one set of five computers, it takes about 10 minutes to unplug them, move them, and then plug in a new set. During this time,

you want the MAC addresses from the first set to age out so that by the time they get around to the second set, Port Security will have forgotten about the first five.

Try it now

The aging time, like all other Port Security options, is set on a per-port basis. Use the following commands to set the aging time to 10 minutes:

```
interface fa0/12
switchport port-security aging time 10
```

Use the following command to verify your configuration:

```
show port-security interface fa0/12
```

Here's an example of what you should see:

```
Switch1#show port-security interface fa0/12
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 10 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 5
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0800.271c.0b57:1
Security Violation Count   : 30
```

Aging time set to 10 minutes

On the fourth line of the output, you can see the `Aging Time` in minutes. Port Security ages each MAC address *independently* based on when it first saw the address. You can see this with a `show port-security address` command:

```
Switch1#show port-security address
           Secure Mac Address Table
------------------------------------------------------------------------
Vlan   Mac Address       Type                Ports     Remaining Age
                                                          (mins)
----   -----------       ----                -----     -------------
  1    0800.2742.aab8    SecureDynamic       Fa0/12          6
  1    0800.2782.4c93    SecureDynamic       Fa0/12          6
  1    0800.27b8.b488    SecureDynamic       Fa0/12          6
  1    0800.27e4.bb01    SecureDynamic       Fa0/12          6
  1    0800.7200.3131    SecureDynamic       Fa0/12          6
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 4
Max Addresses limit in System (excluding one mac per port) : 6144
```

Notice that each MAC address has the same `Remaining Age` time. This isn't surprising because the system administrator booted each of the five computers at the same time.

Now suppose that they're finished with four of the five computers and shut them down. They still have one left that's giving them trouble, so they leave it plugged in. They bring in four new computers, plug them in, and turn them on. They report that everything still seems to be working.

You run another `show port-security address`:

```
Switch1#show port-security address
           Secure Mac Address Table
------------------------------------------------------------------------
Vlan   Mac Address       Type              Ports     Remaining Age
                                                        (mins)
----   -----------       ----              -----     -------------
   1    0800.2708.e69b    SecureDynamic     Fa0/12          9
   1    0800.27b6.b091    SecureDynamic     Fa0/12          9
   1    0800.27c1.5607    SecureDynamic     Fa0/12          9
   1    0800.27f4.803e    SecureDynamic     Fa0/12          9
   1    0800.7200.3131    SecureDynamic     Fa0/12          8
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 4
Max Addresses limit in System (excluding one mac per port) : 6144
```

This device wasn't swapped out and ages independently of the other addresses.

Notice that the first four MAC addresses are different, and their remaining aging time is 9 minutes. The last address, which belongs to the computer that they did *not* unplug, hasn't changed and has a remaining aging time of 8 minutes. Because the MAC address of this computer was already in the list of allowed MAC addresses, it will still be able to access the network even after the timer expires. Once the timer reaches zero, it will reset to 10 minutes.

Now that you've configured the aging time, you probably won't ever have to mess with Port Security on this particular port. If the system administrator ever has a problem with connectivity, all they have to do is wait a few minutes and try again.

You'll likely have to go through some trial and error to get the aging time just right. If you find that newly connected devices are unable to access the network, you may want to decrease the aging time. Keep the needs of the user in mind, and don't feel like you have to set a long aging time. Even if you set a very short aging time, say 1 minute, the port is still protected against a MAC flood attack. Setting a longer time doesn't buy you any additional security. But if you do require more stringent security, Port Security can give you that as well.

5.4 Preventing unauthorized devices

So far, you've learned how to configure Port Security to prevent a MAC flooding attack without disrupting legitimate user traffic. With some research and maybe a little bit of trial and error, you can configure Port Security on all end-user ports without anyone knowing it's even there.

But although a minimum Port Security configuration may be great for end-user productivity, not all organizations are so lucky. Some have strict security requirements that prohibit non-company devices from connecting to the network. For them, it's not

sufficient to limit the number of MAC addresses on a port; you have to limit which *specific* MAC addresses can use the port. That sounds like a cumbersome task, but as you'll see, Port Security makes it surprisingly easy.

Even if your organization doesn't require such a burdensome level of security, I still strongly suggest reading this section. Here's why: In chapter 4, you learned that one of the reasons for disabling unused ports is to prevent someone from walking in off the street with an infected laptop and plugging it in at an empty desk. But even if you faithfully check and disable unused ports once a day and twice on Sunday, that doesn't stop them from unplugging a work computer and plugging in the infected laptop.

You can probably think of other reasons to restrict a port to a single device. At the beginning of the chapter, I said I'd tell you how to configure Port Security for maximum security. Now that you have some rationale for when you might want to do this, I'm going to teach you how you'd do it.

Above and beyond

Security is all about having layers of protection. Although any organization with an ounce of sense will take measures to physically prevent people from walking in off the street with a malicious device, that doesn't negate the need to take technical measures to protect the network. All security can be broken; the best you can hope for is to slow an attacker down enough that they give up and move on to an easier target. Port Security is one technology that can make an attacker's life more difficult.

5.4.1 Making Port Security maximally secure

Recall that when you enable Port Security, it remembers and allows MAC addresses as it sees them, up to the configured maximum. When the device physically connected to the port gets unplugged, Port Security forgets those MACs. If you have aging configured for, say, 5 minutes, Port Security forgets each MAC address 5 minutes after it first sees it.

In a highly secure environment, you want Port Security to operate a bit differently. First, you want it to allow and remember the specific MAC addresses of the devices that are supposed to be connected. Second, you never want it to forget those MAC addresses—*ever*! Even if someone shuts down the port, disconnects the device, or reboots the switch, you want those MACs to stick to the port like glue as the only MAC addresses authorized to use that port. You can achieve this using what Cisco calls *sticky MAC addresses*.

5.4.2 Sticky MAC addresses

A sticky MAC address is one stored permanently in the startup configuration, under the interface configuration section. The reason it's called *sticky* is that you don't have to manually configure the MAC address. Instead, you let Port Security discover it in the usual way, and IOS will automatically write the MAC address into the running configuration. It's a clever way to achieve a high level of security with a little bit of effort.

Let's say your organization has a PC that sits in a semi-public area, like a lobby or reception area. You want to prevent someone from coming in after hours and plugging a malicious device into the same port. Because only one MAC address should ever be seen on that port, you configure the maximum number of MACs to one. Then you tell Port Security to permanently remember the MAC address using the command `switchport port-security mac-address sticky`.

Try it now

Select a port with only one device connected and configure Port Security to allow one sticky MAC address:

```
interface fa0/1
switchport port-security maximum 1
switchport port-security mac-address sticky
```

This is where the magic happens. As soon as Port Security sees the MAC address, it writes it to the running configuration. You can verify this with a `show run interface fa0/1`:

```
Switch1#show run interface fa0/1
Building configuration...

Current configuration : 233 bytes
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0800.7200.3131
End
```

You issued this command.

Port Security added this sticky MAC address.

Notice that the last two lines of the interface configuration are almost identical except for the MAC address. The first command is the one you issued, and the second is the one Port Security added.

Above and beyond

You may notice that the `switchport port-security maximum 1` command doesn't show up in the configuration. This isn't a mistake, and it doesn't mean you did anything wrong. Sometimes IOS changes or removes certain configuration commands if they're redundant or unnecessary. Port Security defaults to allowing only one MAC address per port, so explicitly setting the maximum to `1` is unnecessary.

Now do a `show port-security address` to compare:

```
Switch1#sh port-security address
          Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type                Ports     Remaining Age
                                                           (mins)
----    -----------       ----                -----     -------------
  1     0800.7200.3131    SecureSticky        Fa0/1           -
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 6144
```

Notice the type is SecureSticky and there is no aging time.

The same address shows up here, and the `Remaining Age` column is blank because the entry will never expire. Until you manually remove the configuration Port Security added, it will remember that MAC.

Try it now

Physically disconnect the PC from the port on which you configured a sticky MAC address and plug in a different device. What happens?

You should see a pattern similar to the following:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
     changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
     changed state to up
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
     caused by MAC address 2c27.d737.9ad1 on port FastEthernet0/1.
```

Disconnect legitimate PC

Connect an unauthorized device.

Port Security blocks the unauthorized device's MAC.

In a real hacking attempt, an intruder might spend a few minutes trying to figure out why they can't get access to the network. They may try tweaking their network settings, rebooting, or connecting to a different port. The important thing is that Port Security thwarts their plug-and-play attempt to gain unauthorized access.

But as good as this configuration is, there's one shortcoming.

Above and beyond

MAC addresses can be spoofed quite easily. A sophisticated attacker can find out the MAC address of the authorized PC and clone it. But that still takes time. Remember, the goal isn't to rely on Port Security as the be-all and end-all of security. Its only job is to make it harder for an attacker to cause trouble.

5.4.3 Caveats about sticky MACs

The additional security of sticky MACs comes with a tradeoff. If you ever need to replace a device, you'll have to manually edit the port configuration to remove the old MAC address so that the new one can take its place. In the earlier example, Port Security added the following line to the running configuration:

```
switchport port-security mac-address sticky 0800.7200.3131
```

The way you'd remove this is to first ensure that that particular MAC address is no longer using that port. Next, you'd enter interface configuration mode and prepend the command with a `no`.

Try it now

Unplug the PC from FastEthernet0/1, or just shut down the port. Then issue the following commands to remove the sticky MAC address. Be sure to change the MAC address to match your particular configuration:

```
int fa0/1
no switchport port-security mac-address sticky 0800.7200.3131
```

Do another `show run int fa0/1`, and the sticky MAC address should be gone.

That's it! Port Security will automatically add the next MAC address it sees as a sticky MAC to the running configuration. Another thing to keep in mind is that after Port Security writes the sticky MAC addresses to the running configuration, you still have to manually save the startup configuration in order for the addresses to persist across switch reboots.

5.5 Commands in this chapter

As you review the list of commands in table 5.4, keep in mind that two ports can be configured with completely different Port Security settings. This makes Port Security versatile, but it also means you have to individually check the port configuration when troubleshooting an issue.

Table 5.4 Commands used in this chapter

Command	Configuration mode	Description
`switchport port-security maximum 5`	Interface	Allows up to five MAC addresses
`switchport port-security violation restrict`	Interface	All MACs beyond the maximum are blocked
`switchport port-security violation shutdown`	Interface	Any MAC beyond the maximum triggers a port shutdown

Table 5.4 Commands used in this chapter *(continued)*

Command	Configuration mode	Description
`switchport port-security`	Interface	Enables Port Security
`switchport port-security mac-address sticky`	Interface	Writes allowed MAC address(es) to the running configuration
`show port-security`	N/A	Displays which ports Port Security is enabled on
`show port-security interface fa0/1`	N/A	Displays detailed Port Security configuration information for a port
`show port-security address`	N/A	Displays the allowed MAC addresses by port
`show run interface fa0/1`	N/A	Displays all interface-level configuration for FastEthernet0/1

5.6 Hands-on lab

Now that you've gotten some practice configuring Port Security on a couple of ports, you're ready to enable Port Security on all end-user ports. Just one unprotected port is all it takes for a MAC flooding attack to take down your network.

As you follow these steps to complete the lab, remember to use the `interface range` command to simultaneously apply the configuration to multiple ports:

1. Start by configuring the maximum number of MAC addresses for each port. If you already have a good handle on how many MAC addresses should be on each port, go ahead and set it using the `switchport port-security maximum` command. Otherwise, if you're not sure, play it safe and set it to a high number like 50. The maximum number of MAC addresses allowed per port is 3,072.
2. Next, set the violation mode on all ports to restrict using the `switchport port-security violation restrict` command. You can go back later and change it to shutdown if you require it, but don't start out with that.
3. Finally, enable Port Security using the `switchport port-security` interface command. If you've done everything correctly, nothing dramatic should happen (unless you're in the middle of a MAC flood attack). Use the `show` commands you learned in this chapter to verify your configuration.

NETWORKING

Learn CISCO NETWORK ADMINISTRATION IN A MONTH OF LUNCHES

BEN PIPER

Cisco's ultrareliable routers and switches are the backbone of millions of networks, but "set and forget" is not an acceptable attitude. Fortunately, you don't have to be an old-time administrator to set up and maintain a Cisco-based network. With a handful of techniques, a little practice, and this book, you can keep your system in top shape.

Learn Cisco Network Administration in a Month of Lunches is designed for occasional and full-time network administrators using Cisco hardware. In 22 bite-sized lessons, you'll learn practical techniques for setting up a Cisco network and making sure that it never fails. Real-world labs start with configuring your first switch and guide you through essential commands, protocols, dynamic routing tricks, and more.

WHAT'S INSIDE

- Understand your Cisco network, including the difference between routers and switches
- Configure VLANs and VLAN trunks
- Secure your network
- Connect and configure routers and switches
- Establish good maintenance habits

This book is written for readers with no previous experience with Cisco networking.

Ben Piper is an IT consultant who holds numerous Cisco, Citrix, and Microsoft certifications including the Cisco CCNA and CCNP. He has created many video courses on networking, Cisco CCNP certification, Puppet, and Windows Server Administration.

Free eBook
SEE INSIDE

"This is one of the best technical books I've ever read. Ben clearly knows his stuff and, more importantly, how to teach it."
—Kent R. Spillner, DRW

"This is the Cisco networking book we've needed for a long time now. Highly recommended if you are looking to get started with Cisco networking."
—Mark Furman
Info-Link Technologies

"A great book to get you up and running in no time."
—Sau Fai Fong, Panda Tech Hub

"If you just want to pass the exam, pick a different book. If you want to configure your Cisco equipment into a working network, this is the place to start."
—David Kerns, Rincon Research

To download their free eBook in PDF, ePub, and Kindle formats, owners of this book should visit manning.com/books/learn-cisco-network-administration-in-a-month-of-lunches

ISBN-13: 978-1-61729-363-4
ISBN-10: 1-61729-363-6
53999
9 781617 293634

MANNING $39.99 / Can $52.99 [INCLUDING eBOOK]