MAC Address Spoofing

Table of Contents

MAC and IP Spoofing ................................................................................................................................. 2
Controlling Rogue DHCP Servers.................................................................................................................. 3
DHCP Server Snooping – Commands............................................................................................................. 7
MAC Address Spoofing Attack ....................................................................................................................... 9
MAC Address Spoofing Attack ....................................................................................................................... 10
Dynamic ARP inspection ............................................................................................................................... 12
Dynamic ARP Inspection – Configuration ..................................................................................................... 15
ARP ACL for Static IP Addresses .................................................................................................................. 16
Notices ......................................................................................................................................................... 17
**016 Joe Mayes: So MAC and IP spoofing. Is all IP spoofing bad? What do you think? Can somebody give me a good IP spoofing? When is IP spoofing good?

Student: When you mess up your access control list and you've got to try to hack your way into your own stuff.

Joe Mayes: That's part of it. Or another one is NAT, right? NAT is authorized IP spoofing. You took some private address on an inside machine and you spoofed it to be a public address to go out on the internet. Except we don't think of it as spoofing because spoofing's got that bad connotation. But there's no real difference
between NAT and anybody else who changes an address, except that NAT is sponsored. NAT is-- NAT good, right? Spoofing bad, NAT good.

**Controlling Rogue DHCP Servers**

DHCP protocol is not configurable

- DHCP operates on broadcast frames without authentication
- Rogue DHCP servers create DoS and/or MITM attacks
  - Communication fails with incorrect or duplicate IP addresses
  - MITM attacks can be crafted if users connect to false gateways

DHCP can be controlled at the switch

- Switch sets trusted and untrusted DHCP ports
  - Untrusted DHCP ports reject DHCPOFFER, DHCPACK, DHCPNACK

**017 So a number of issues. One of the issues that’s fought people for a long time is rogue DHCP server. And a DHCP server's function is? Anybody know? What’s the DHCP server do?**

Student: To assign IP addresses to machines as they come on the network.

Joe Mayes: Okay. So a machine will request an IP address, DHCP servers will respond, correct?
Student: Mm-hm.

Joe Mayes: And normally the way it's set up is you've got a certain subnet that your broadcast domain's operating on and you expose one or more DHCP servers into that subnet so people all get the same addresses, right? So if I come in with a wireless access point and I jack it into that subnet and that's got its own DHCP server handing out 192.168s on a ten dot network, how do we keep that from mixing up? Generally you don't, right? How do you determine whose address you're going to take in DHCP?

Student: Whoever gets it first.

Joe Mayes: Whoever gets it first, mm-hm. So if that rogue DHCP server was the first one to respond to a DHCP request, that's the address you're going to get. Now, that's the unintentional way to have it happen, somebody actually just buys something and not knowing or not thinking, they put it on the network and all of a sudden people are getting wrong addresses.

When that happens, what's going to happen to a user who gets a 192.168 address on a ten dot network?

Student: They're going to call and complain.

Joe Mayes: And they're going to call and complain because?

Student: They have no internet access, things aren't working.
Joe Mayes: Right. They can’t go anywhere because they can’t route through the router because their address doesn’t match the router addresses.

What if I intentionally put a DHCP server in and let’s say just for fun on that DHCP server, I handed out valid addresses but I gave you a different set of DNS servers and I gave you a different default gateway, and I have a rogue, a whole rogue system now so that I can pass you through my router and capture all your traffic?

Student: You can see every single thing the person’s doing.

Joe Mayes: Then you can see everything somebody’s doing. It’s a way to be a man in the middle, correct?

Student: Mm-hm.

Joe Mayes: So you can do man in the middle with an intentional DHCP attack, or it can just be a mistake from one of your users who doesn’t know any better. Either way, you’ve got a problem. Because DHCP is not controllable. Even in a Windows environment, where you have to register the DHCP servers, all that does is keeps you from turning on Windows DHCP servers, it doesn’t stop anybody else who just jacks one into the network.

So what you can do though is you can turn on DHCP trust at the switch. And what that means is, you can turn on, on a port-by-port basis, and say who gets to send DHCP offers, DHCP acknowledgements, and DHCP negative
acknowledgments into the network. So if I know that I’ve got a DHCP server on port 112 and that’s the only port that I allow those responses to go out, then even if you jack a rogue DHCP server into the network, it can’t respond to DHCP requests because they’ll be blocked. So that’s how you can limit to only authorized DHCP servers.

Student: What we do in the advanced class is we do a TCPdump filter.

Joe Mayes: Mm-hm.

Student: And it’s basically looking for the DHCP offers. So all that’s doing is notifying you that a rogue DHCP server is out there, it’s not necessarily blocking it. So this is kind of-- you can do that blocking of it as well.

Joe Mayes: Yep. Yeah, this is cool because it stops it from happening.

Student: Right.

Joe Mayes: You don’t even have to get notified, you can just get notified that it was blocked, right? You can make it a syslog message that was blocked rather than a syslog message that says you were just violated. Be a little more proactive, right?
DHCP Server Snooping – Commands

DHCP server snooping commands

- **Global config**
  - (enables DHCP snooping globally)
  - `ip dhcp snooping [vlan nnn]`

- **Interface config**
  - (Interfaces are untrusted as DHCP server interfaces by default)
  - `ip dhcp snooping trust`
  - OPTIONAL (protects against DHCP exhaustion attacks)
    - `ip dhcp snooping limit rate nn`
      - `nn = DHCP responses per second`

Configure trusted interfaces first
- untrusted interfaces can errdisable with DHCP server activity

**018 So the commands are, basically you turn on DHCP snooping on the switch. And then on interface, you tell it which interfaces are trusted.

Student: Will Cisco or any other switch that you know of do other protocol snooping besides DHCP? For instance, making sure that maybe DNS, only this port can respond to DNS queries or something like that?

Joe Mayes: Yeah. And actually we'll look at that in a little bit, mm-hm.

Student: Cool.
Joe Mayes: So you can do the snooping trust. And then even when you do a snooping trust, there's another kind of attack. And the other kind of attack is somebody who tries to exhaust your list of DHCP addresses and try to starve your network by putting in, you know, 500 DHCP requests in five seconds so that he uses up every address you have and then nobody else can get on the network, even though it's got DHCP servers.

So what you can do is you can rate limit the number of DHCP responses per second. And anybody who doesn't belong, you've got rogue DHCP servers, you can configure the other interfaces to go error disable. So if somebody does jack in rogue DHCP server, and it'll shut the port down again. It's another port shutdown, another chance for you to go out and find out who just messed up your network. But it's a protection feature. So the DHCP server, not only will it not respond, it'll shut the port down so even when they try to put their regular computer back in, it won't work.
MAC Address Spoofing Attack

**019 So related to this, MAC address spoofing attacks. And if you see here, we've got a MAC address AABBcc and another host over here called-- with a MAC address of 112AbDd. And in this spoofing attack, that person on the right is going to spoof MAC address AABBcc. And what effect will that have on a local network? If I use somebody else's MAC address, what happens to the traffic?

Student: It's starts getting interesting. I don't know. It doesn't know where exactly to send it. If it's got two ports, will it send it to both of them or just randomly pick?

Joe Mayes: It may send it to both of them. Most likely what'll happen is that
machine will go dead because the switch will say, "Oh, you moved." It'll see it on the new interface now and all the traffic you are sending on a switch is controlled by a destination MAC address. It doesn’t matter what it’s IP is. It doesn’t look at the IP, it looks at the destination MAC address. So you will receive the traffic that was meant for the server on the left, the attacker will get it on the right.

**MAC Address Spoofing Attack**

**MAC Address Spoofing Attack**

**020 And that’s what the switch does. I must adjust my MAC address table accordingly.**

Student: So I got a question for you Joe.

Joe Mayes: Mm-hm.
Student: So I get the MAC address spoofing case. I get how port security would protect it, right? So if I come on the switch, the first MAC address is the one that I would get. Say I tried to spoof maybe another port or another machine on another port that did have security enabled?

Joe Mayes: Mm-hm.

Student: How would that work? Do you understand what I'm saying? So like maybe my router is on there and it's MAC address isn't supposed to be changing. And I have port security on that port, will the switch do anything to further protect that port from say, this guy over here trying to use that MAC address on that router? Or do I have to have port security on both ports?

Joe Mayes: Port security won't protect from that. Port security will protect basically for how many MAC addresses you can see on a port. However, next slide. Who knew? Dynamic ARP inspection will protect against that. Your check is in the mail by the way.
Dynamic ARP inspection

Dynamic ARP Inspection controls ARP spoofing

- ARP spoofing supports MITM exploits

Dynamic ARP Inspection works from DHCP binding table

- Table created by DHCP server snooping
- ARP replies entering ports are compared to DHCP binding table
  - Binding table entries are trusted
- ARP replies that don’t match table entries are dropped
  - Ports receiving spoofed ARP replies go to errdisable mode
    - Default mode inspects for invalid MAC address advertisements
    - Can also check for invalid IP addresses

Dynamic ARP Inspection can support static IP addresses

- Uses static `arp access-list acl-name`

**021 So dynamic ARP inspection controls ARP spoofing. So dynamic ARP inspection works with DHCP binding tables. So what happens is, if you think of it most machines end up with two tables where they keep track of stuff. One is going to be an ARP table. And on the ARP table you’re going to have a list of IP addresses to MAC addresses. Then if you have the MAC address table or the CAM table on the switch, that’s going to have MAC addresses to ports.

What if that was put into one database instead, where you knew the relationship between port and MAC address and IP address? Now you could test every packet that went through the switch to
that table. Now, how’s it going to know that those are trusted addresses, right? And that it wasn’t spoofed to begin with?

Well, if you run everything by DHCP and you already have the DHCP server ports identified, then when the request goes into the DHCP server and comes out again with an IP address, that creates a table entry because now it’s seen a MAC, an IP and a port. And it says, "Okay, now I know where all those are. That’s real, everything else is fake." So now if it sees a false MAC address to IP relationship or false IP to MAC, if it sees a false port for the MAC or the IP, in all those cases now can be used to kill it. So anytime the traffic is wrong, the system will look back to the table, say, "That doesn’t match what I saw when the DHCP set this up, therefore that’s a spoof, therefore I’m killing it."

Now, the question that comes up then is what do you do about static IP addresses? There’s two ways to do it. One way to do it is there is a static command. And you can actually create a list and list all the MAC addresses per report. Or another way you could do it that’s a little bit easier sometimes, a little bit more scalable, is you can go into your DHCP server and have reserved addresses, where for a certain MAC address you can reserve a given IP. Then you can take your servers even and put them on DHCP. But they’re going to get the same address every time, so it’s just as if they were static.

And matter of fact, in some ways, it’s even better. One of the problems with static addressing is let’s say I change my
DNS server. All the dynamic machines, all the machines running DHCP, will just get the new DNS server next time their address changes or next time their address updates. Static machines won’t, I’ve got to go change them all manually. But if I put machines with reserved MAC addresses, then they are also running DHCP, even though the IP address will never change. The other feature is the DNS server is the default gateway, and those numbers can all be updated just by the change in the DHCP.

Student: Question. What happens when you do have to move a machine to a new port or something like that when you have this turned on? How do you do that without it saying, "Oh, that’s wrong, you’re not on the right port anymore."

Joe Mayes: You can either plug it in, get the violation and then clear the violation, and that’ll change the table. Or you could go in manually and type a big long statement that takes out one address and allows you to put it back in again. Most people just let it violate and then clear the violation, because it’s basically shut and no shut and it’s back on.

Student: Okay.

Joe Mayes: Good question though. So that’s what it does. By default, it doesn’t check for IP addresses, it looks for MAC to port. As an option, you can turn on the IP address checking.
Dynamic ARP Inspection – Configuration

Global configuration

ip arp inspection vlan nnn

Interface configuration

• Sets trusted interfaces for ARP entries
  — Links from other switches also performing DAI
    o without this, all traffic from other switches will be dropped
  ip arp inspection trust

Additional inspections

ip arp inspection validate [src-mac] [dst-mac] [ip]

**022 So IP ARP inspection and then IP ARP inspection trust for the trusted interfaces. And then validate source MAC, destination MAC, IP address. So the top two is what we've seen already for the ARP inspection and the new line then is the validated MAC address and IP address. Questions?
ARP ACL for Static IP Addresses

**Arp ACL for Static IP Addresses**

1. Create the ARP ACL in global config
   
   ```
   arp access-list ACLNAME permit ip host sender-ip  
   mac sender-mac
   ```

   - For multiple static IP addresses, create multiple lines in the ARP  
   ACL

2. Apply the ACL to the VLAN where it’s needed
   
   ```
   ip arp inspection filter ARP ACLNAME vlan VLAN-ID
   ```

**OPTION:** For some static IP addresses, it might be easier to administer them as reserved DHCP addresses and avoid the need for ARP ACL entries.

**023** So what you're getting out of this is, you're getting a really busy switch.
Everybody thought you just took switches out of the box and just, you know, stuck them in the rack, put four screws in and you were happy. There really is a reason that you got that configuration jack on the switch, because some of this stuff is pretty cool.

So if you want to create an access list in the global config, this is where you put the name of the MAC addresses in for static. And that's why you say in the options on the bottom, it might be easier just to administer them as reserved DHCP addresses. Either way works, you get the same result. The result is that they're in the table
Notices

© 2016 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.