How to configure packet content ACL to mitigate ARP spoofing attack on DGS-3600 series

Created at 2009/1/13

Address Resolution Protocol discover Layer 2 address of an IP neighbor. This protocol doesn't provide authentication and can easily to be fooled. We will discuss and show you how to mitigate the attack: ARP spoofing.

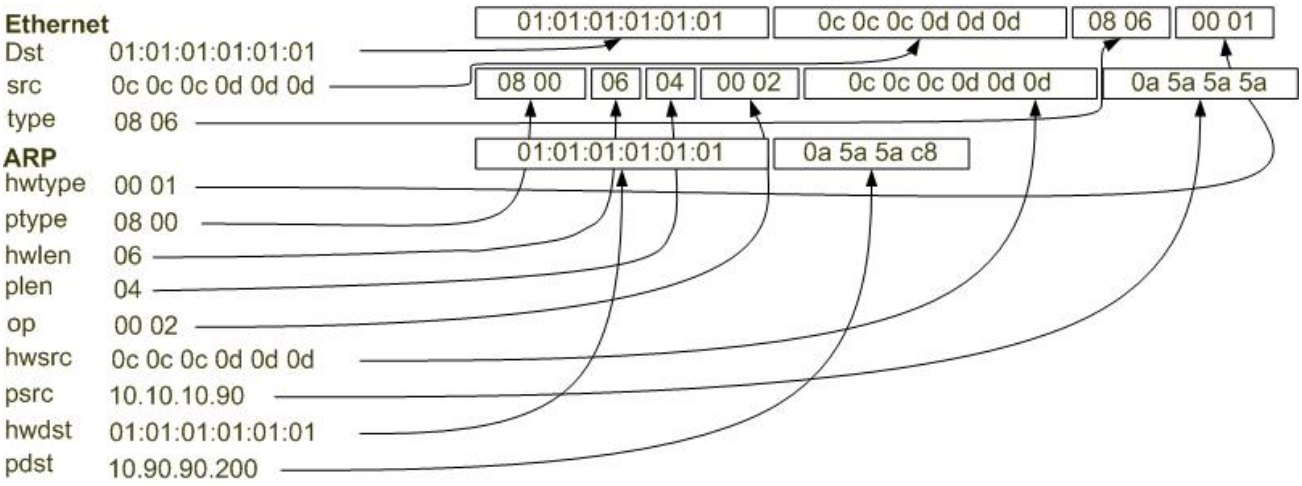
ARP cache poisoning

ARP spoofing is also known as ARP cache poisoning. And I prefer the latter one. This attack consists of inserting false information into the **cache** of the target. Upon receipt the faked ARP. Host will update its ARP table with corrupted information and packet will not go where it should.

Actually, it doesn't matter what type of ARP. This attack can be done by ARP reply, ARP request, or even gratuitous ARP.

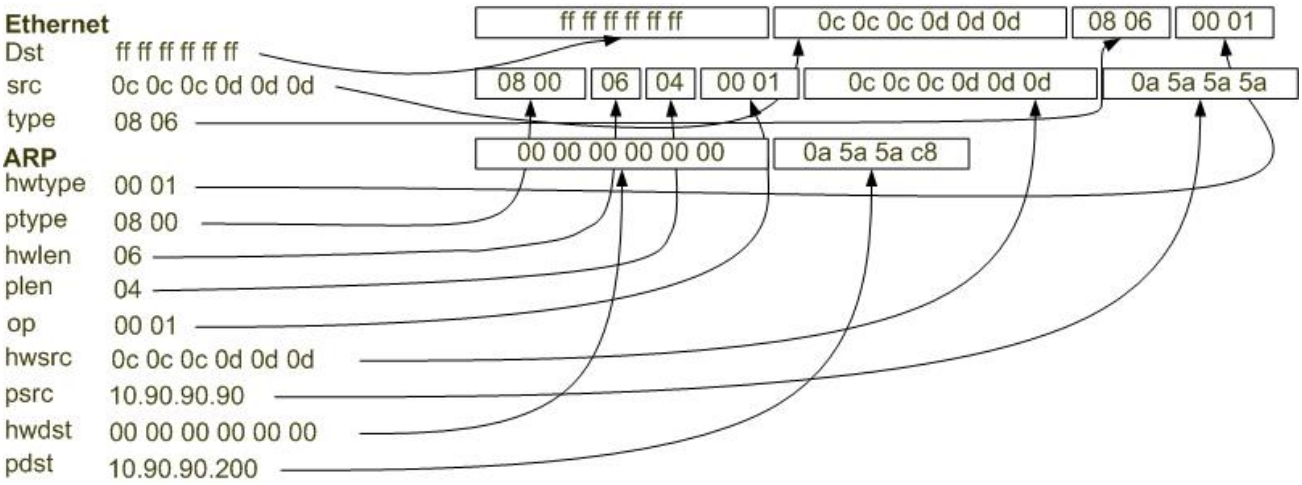
First one, it send ARP reply to a target and binding a victim IP address with an attacker MAC address in the source field of ARP packet.

Figure-1: ARP reply



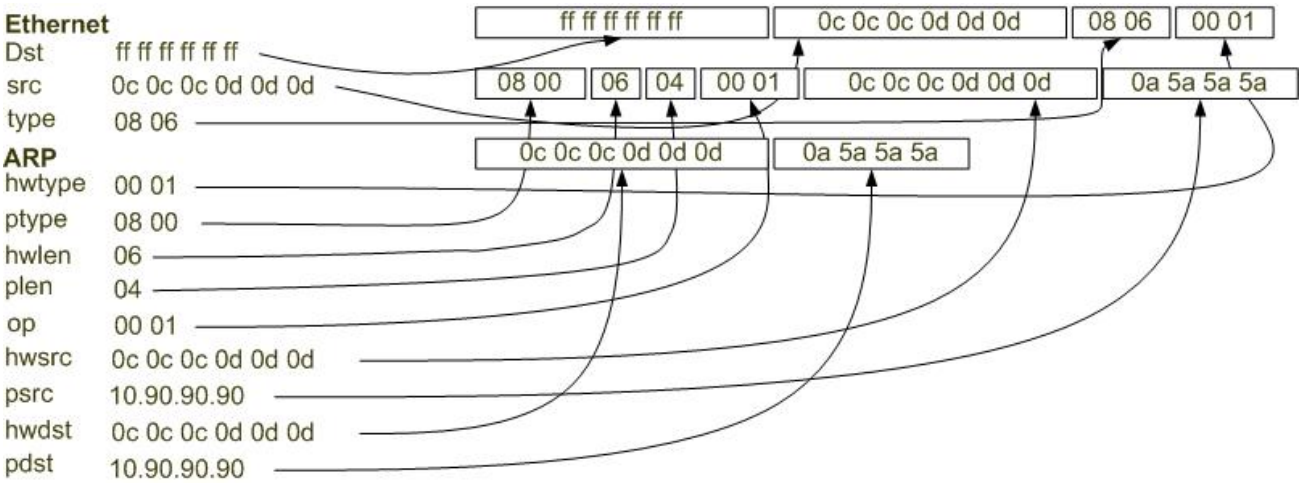
The second one is by sending ARP request to the victim. Many OS will update its ARP table no matter if there is a cache in ARP table.

Figure-2: ARP request



Even more, the attacker can send unsolicited gratuitous ARP to tell hosts changing it ARP table(update).

Figure-3: Gratuitous ARP



Prevent ARP cache poisoning using packet content ACL

Due to the basic ACL can only filter the ARP packet based on packet type, VLAN ID, Source and Destination MAC information. It can not further look into ARP packet. So we will need packet content ACL to help on it.

CAUTION!!!

The packet content ACL in DGS-3600 consists of 4 chunks in each access id. And each chunk is 4 bytes. This means you only have maximum 16 bytes to match in each profile. And also it support only one profile of packet content ACL in whole switch. You must be carefully planning and configuring this ACL due to the valuable chunk.

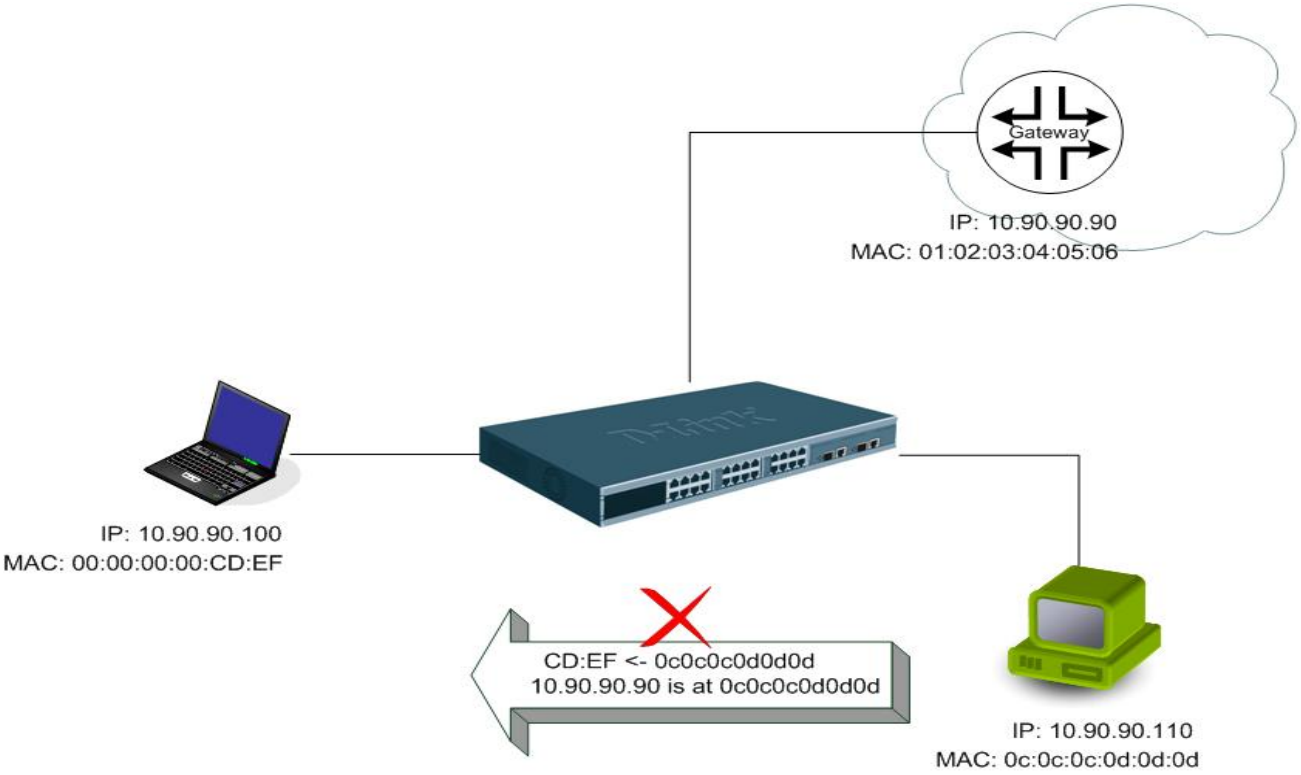
In Figure-4, you will notice that the Chunk0 start from 127th and end at 128th bytes. And also the offset is scratch from **1** not zero!!!

Figure-4: Chunk and packet offset

Chunk	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15
Offset	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
Offset	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
Offset	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
Offset	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Chunk	C16	C17	C18	C19	C20	C21	C22	C23	C24	C25	C26	C27	C28	C29	C30	C31
Offset	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
Offset	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
Offset	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
Offset	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

Example topology



To prevent ARP spoofing attack, we will demonstrate here using packet content ACL to block the invalid ARP packet which contain faked gateway's MAC and IP binding.

In this packet content ACL, We want to have the gateway's ARP packet which can pass thru our switch must match Source MAC address in Ethernet, sender MAC address and sender IP address in ARP protocol. Due to the limited number of chunk we have, we provide a workaround in this issue. First, we will have a normal ACL type that will match the ARP packet and Source MAC. Since ARP spoofing will use sender IP field in ARP protocol to fool the victim. The second one we will use packet content ACL to match the protocol type (ARP) and sender IP field in ARP protocol.

DGS-3600 configuration

	Command	Description
Step1	create access_profile profile_id 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type	Create access profile 1 To match Ethernet type and source MAC address.
Step2	config access_profile profile_id 1 add access_id 1 ethernet source_mac 01-02-03-04-05-06 ethernet_type 0x806 port 1-27 permit	Configure access profile 1 It must be a gateway ARP packet that contains the correct source MAC can pass thru.
Step3	create access_profile profile_id 2 packet_content_mask offset_chunk_1 3 0x0000FFFF offset_chunk_2 7 0x0000FFFF offset_chunk_3 8 0xFFFF0000	Create access profile 2 Chunk 1: mask for protocol type Chunk 2: mask for sender IP in ARP packet Chunk 3: mask for sender IP in ARP packet
Step4	config access_profile profile_id 2 add access_id 1 packet_content offset_chunk_1 0x00000806 offset_chunk_2 0x00000A5A offset_chunk_3 0x5A5A0000 port 1-27 deny	Configure access profile 2 The rest of the ARP packets which sender IP field in ARP protocol is gateway IP with invalid information in other part will be dropped.
Step5	save	Save config