

Ethernet specification

Table of Contents

- 1. TERMINOLOGY 1
- 2. Ethernet protocol list 1
- 3. ARP 1
 - 3.1. introduce 1
 - 3.2. Operating scope 2
 - 3.3. Message..... 2
- 4. VLAN 3
 - 4.1. introduce 3
 - 4.2. vlan distribution 3
 - 4.3. Frame format 3
 - 4.4. Double tagging 3
- 5. ICMP 4
 - 5.1. introduce 4
 - 5.2. Ip address of ASDM. 4
 - 5.3. Echo or Echo Reply Message 4
 - 5.4. Message formats 5
- 6. IPCP..... 6
 - 6.1. introduce 6
 - 6.2. Protocol Header Overview 6
 - 6.3. message list 6
 - 6.4. implementation 7
- 7. IPLM 7
 - 7.1. introduce 7
 - 7.2. Protocol Header Overview 7
 - 7.3. implementation 8
- 8. example for test ARP/ICMP 8
 - 8.1. Tools 8
 - 8.2. Connection..... 8
 - 8.3. test step 9
 - 8.4. test result 11

1. TERMINOLOGY

- *MAC* Media Access Control
- *ARP* Address Resolution Protocol
- *IP* Internet Protocol
- *ICMP* Media Access Control
- *VLAN* Virtual Local Area Network
- *UDP* User Datagram protocol
- *TCP* Transmission Control Protocol
- *IPCP* Ip Command protocol
- *IPLM* Ip link Manager

2. Ethernet protocol list

- Layer 2
 - ARP
 - VLAN
- Layer 3
 - ICMP
- Layer 4
 - UDP
 - UDP socket<use for IPCp and IPLM>
- Layer 5
 - IPCP
 - IPLM

3. ARP

3.1. introduce

The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite. ARP was defined in 1982 by RFC 826, which is Internet Standard STD 37.

3.2. Operating scope

The Address Resolution Protocol is a request-response protocol whose messages are encapsulated by a link layer protocol. It is communicated within the boundaries of a single network, never routed across internetworking nodes. This property places ARP into the link layer of the Internet protocol suite

3.3. Message

- Arp request. The Ip address of ASDM is 192.18.36.1/255.255.0.0 The MAC address of ASDM is 02:00:00:00:14:01
- Internet Protocol (IPv4) over Ethernet ARP packet

Octet offset	0	1
0	Hardware type (HTYPE)	
2	Protocol type (PTYPE)	
4	Hardware address length (HLEN)	Protocol address length (PLEN)
6	Operation (OPER)	
8	Sender hardware address (SHA) (first 2 bytes)	
10	(next 2 bytes)	
12	(last 2 bytes)	
14	Sender protocol address (SPA) (first 2 bytes)	
16	(last 2 bytes)	
18	Target hardware address (THA) (first 2 bytes)	
20	(next 2 bytes)	
22	(last 2 bytes)	
24	Target protocol address (TPA) (first 2 bytes)	
26	(last 2 bytes)	

4. VLAN

4.1. introduce

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2)

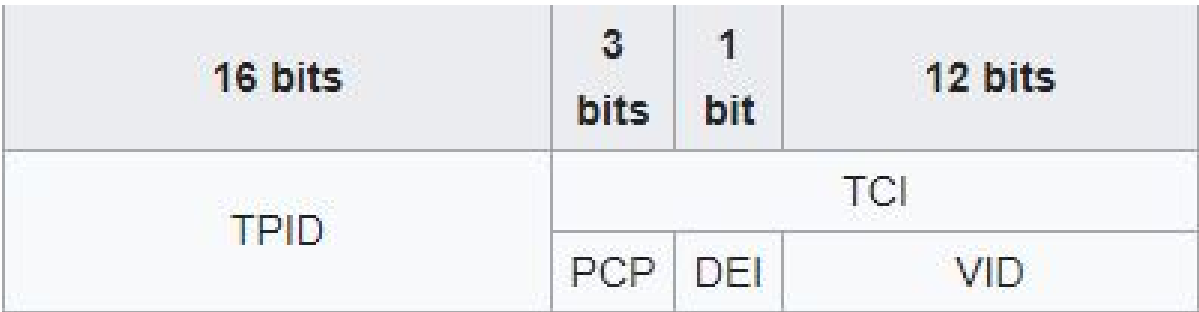
The protocol most commonly used today to support VLANs is IEEE 802.1Q

4.2. vlan distribution

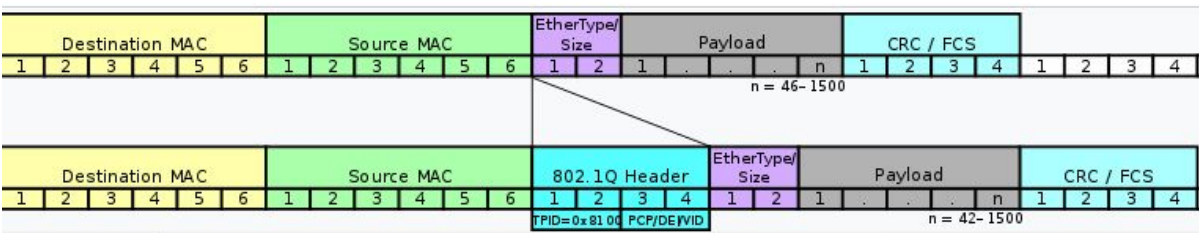
vlan ID	node name	function
2	VGM-ASDM	ipcp
5	VGM-ASDM	Traffic Jam Pilot
6	VGM-ASDM	IPLM
12	VGM-ASDM	ICMP

4.3. Frame format

- 802.1Q tag format



- Frame format

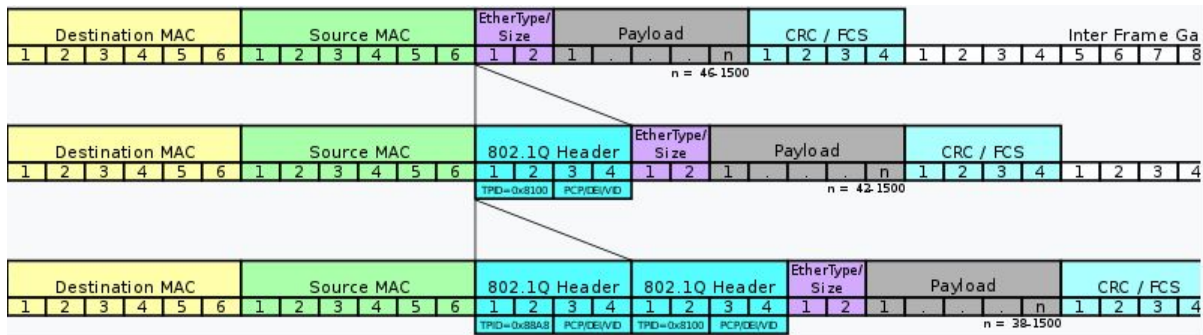


4.4. Double tagging

- GEELY asked us to discard the Double tagging messages.
- All ECUs (including the switches) shall drop frames with more than one outer VLAN Tag with TPID

0x8100.

- All ECUs (including the switches) shall drop frames with an outer VLAN Tag with TPID 0x9100 or 0x88a8.



5. ICMP

5.1. introduce

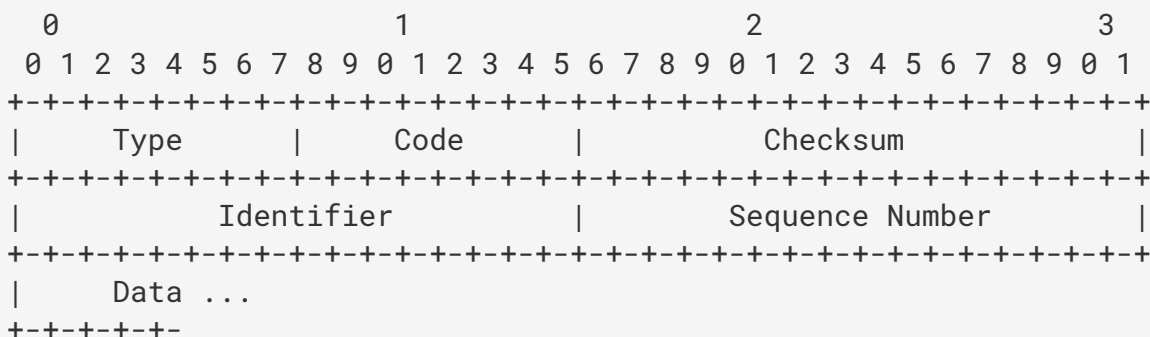
The Internet Protocol (IP) is used for host-to-host datagram service in a system of interconnected networks called the Catenet

ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route.

5.2. Ip address of ASDM

The Ip address of ASDM is 192.18.36.1/255.255.0.0

5.3. Echo or Echo Reply Message



- IP Fields:
 - Addresses: The address of the source in an echo message will be the destination of the echo reply message. To form an echo reply message, the source and destination addresses are simply

reversed, the type code changed to 0, and the checksum recomputed.

- IP Fields:
 - Type
 - 8 for echo message
 - 0 for echo reply message
 - Code
 - 0
 - Checksum
 - The checksum is the 16-bit ones' complement of the one's complement sum of the ICMP message starting with the ICMP Type. For computing the checksum, the checksum field should be zero. If the total length is odd, the received data is padded with one octet of zeros for computing the checksum. This checksum may be replaced in the future.
 - Identifier
 - If code = 0, an identifier to aid in matching echos and replies, may be zero.
 - Sequence Number
 - If code = 0, a sequence number to aid in matching echos and replies, may be zero
 - Description
 - The data received in the echo message must be returned in the echo reply message.

The identifier and sequence number may be used by the echo sender to aid in matching the replies with the echo requests. For example, the identifier might be used like a port in TCP or UDP to identify a session, and the sequence number might be incremented on each echo request sent. The echoer returns these same values in the echo reply.

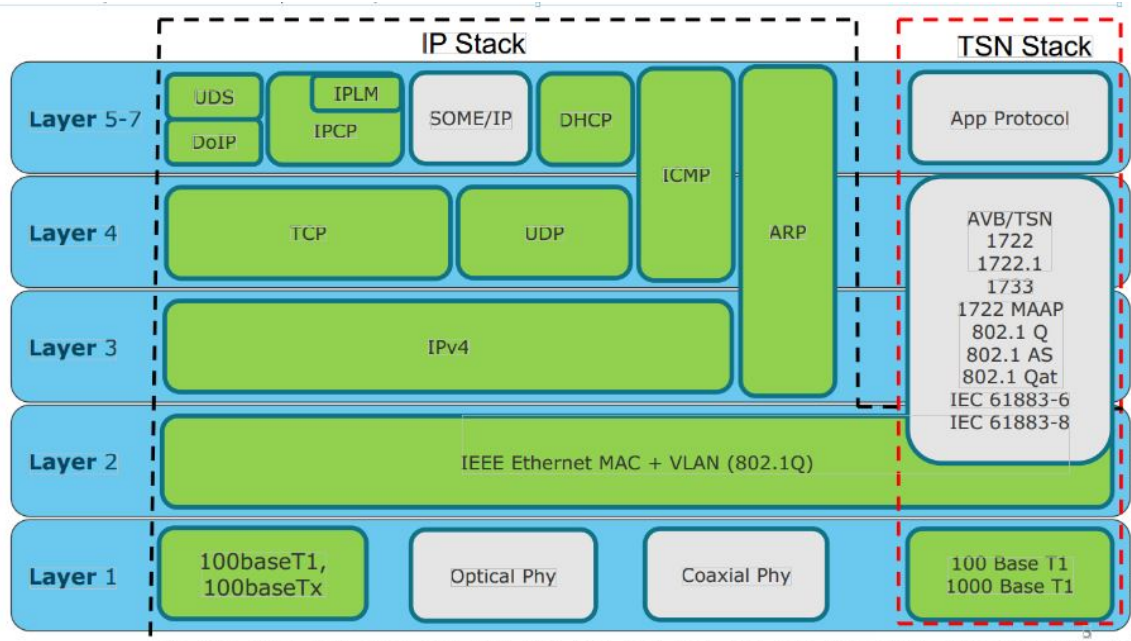
Code 0 may be received from a gateway or a host.

5.4. Message formats

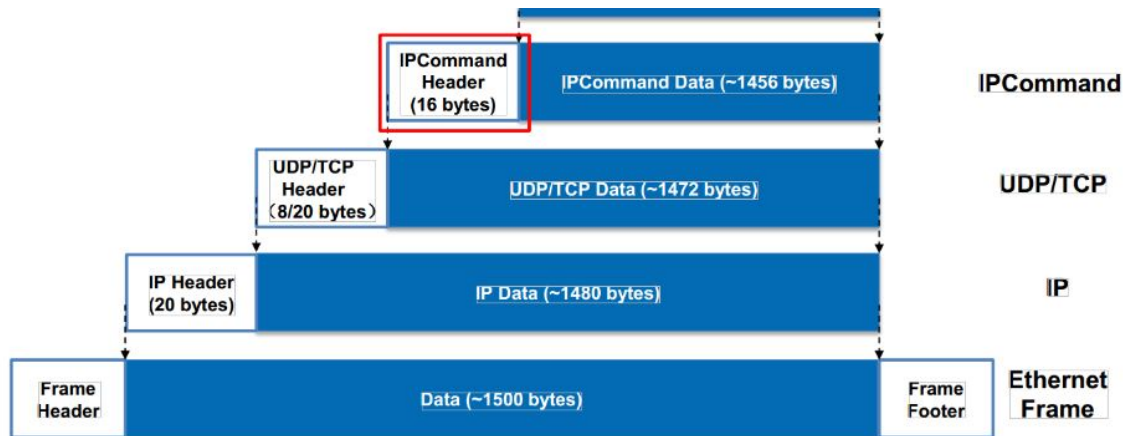
ICMP messages are sent using the basic IP header. The first octet of the data portion of the datagram is a ICMP type field; the value of this field determines the format of the remaining data. Any field labeled "unused" is reserved for later extensions and must be zero when sent, but receivers should not use these fields (except to include them in the checksum).

6. IPCP

6.1. introduce



6.2. Protocol Header Overview



6.3. message list

Unique Identifier(16 bit)	operationID name
0x0001	GlobalDataMessage
0x0002	PathControlMessage
0x0003	PositionMessage

0x0004	ProfileMessage
0x0005	ProfileControlMessage

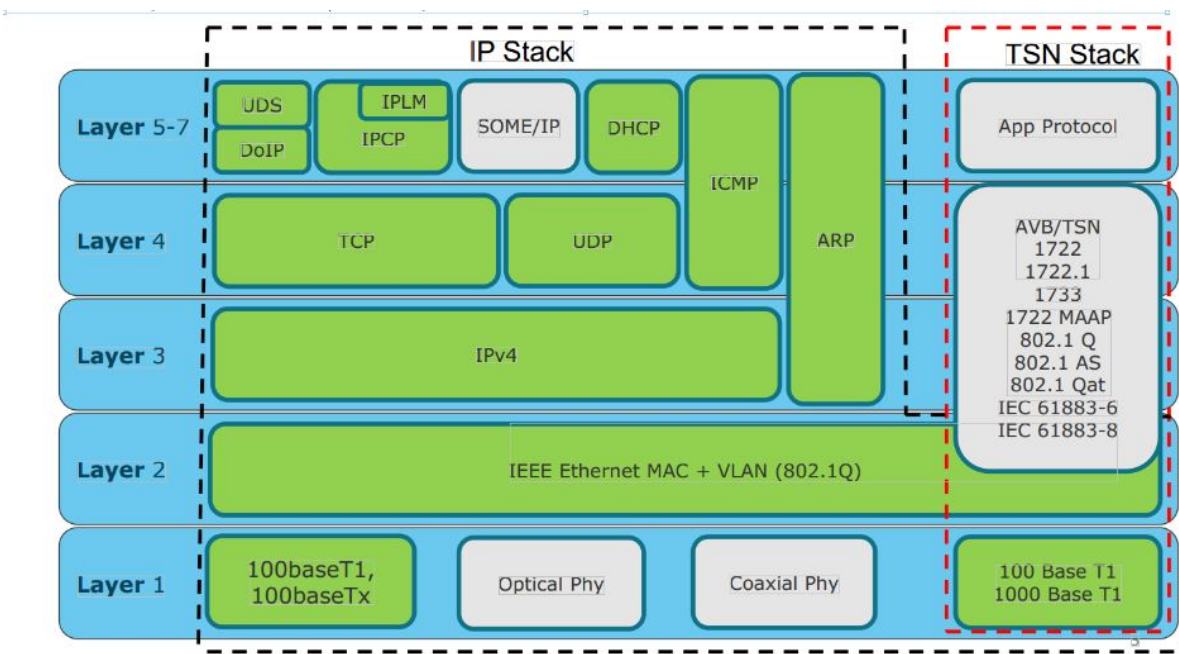
6.4. implementation



IPCP requires a script to emulate the IHU server and I think this could be done by Sarvesh

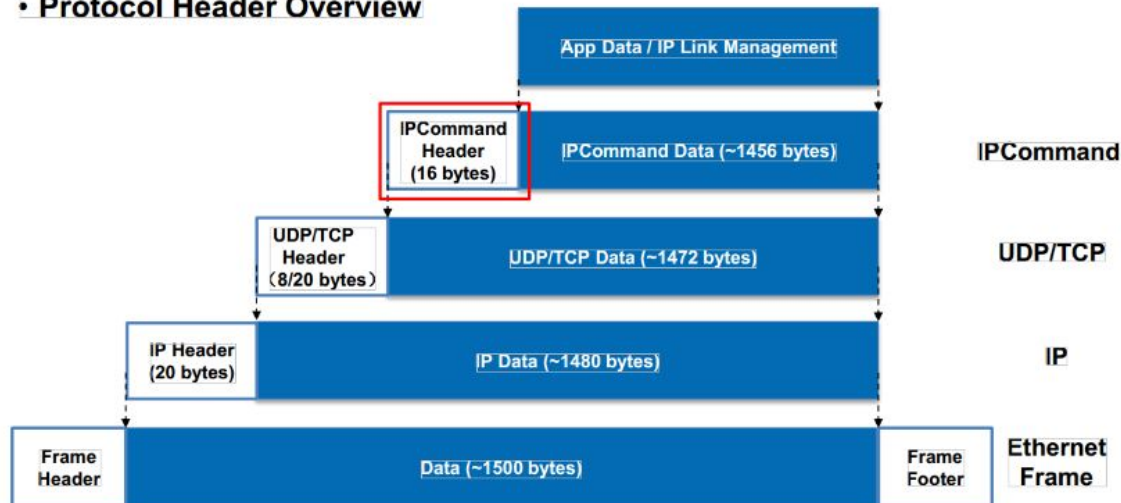
7. IPLM

7.1. introduce



7.2. Protocol Header Overview

• Protocol Header Overview



7.3. implementation



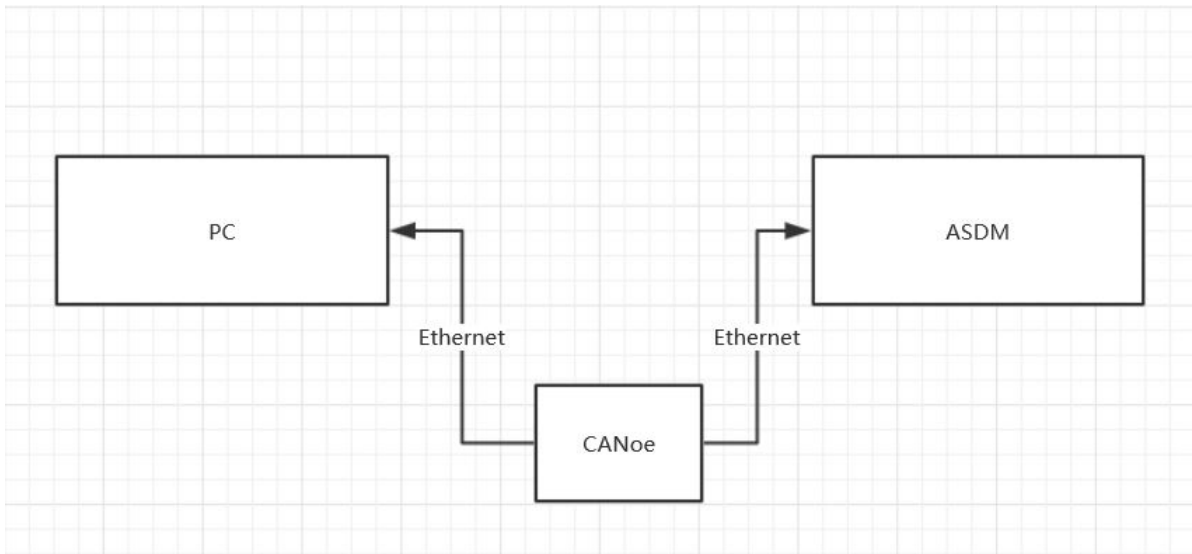
IPLM requires a script to emulate the IHU server and I think this could be done by Sarvesh

8. example for test ARP/ICMP

8.1. Tools

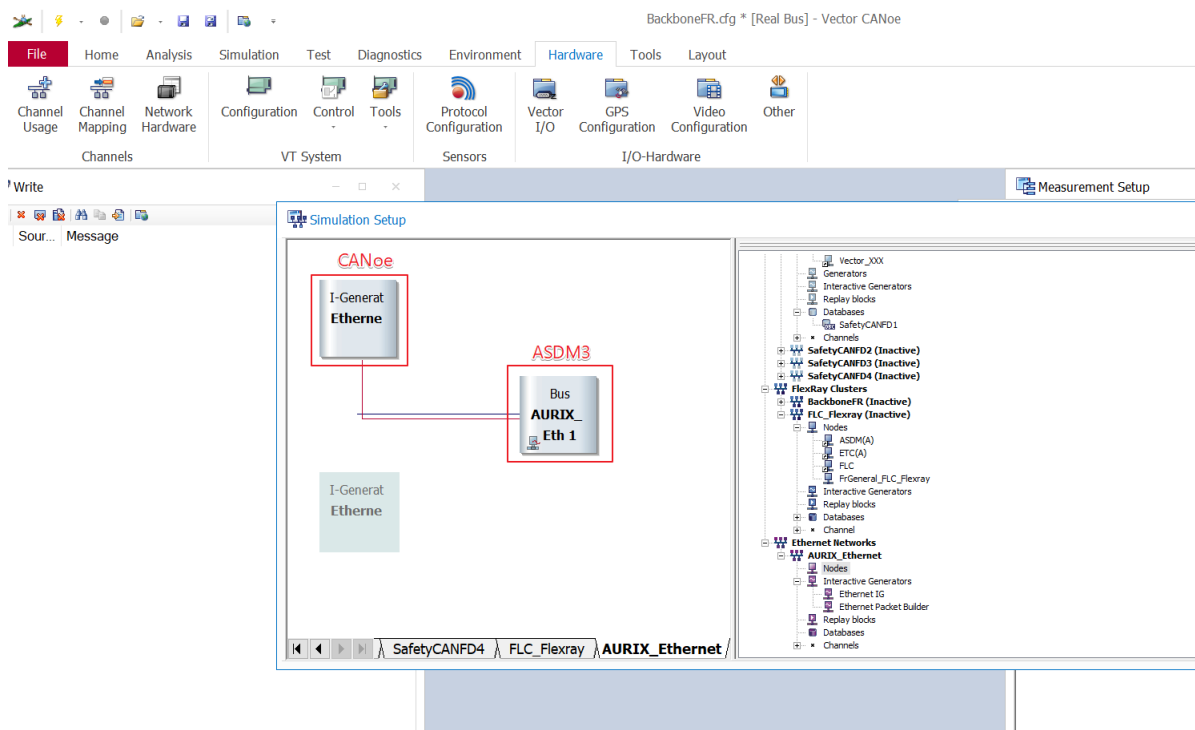
- Vector VN5610A
- ASDM boards
- PC
- power supply

8.2. Connection



8.3. test step

- Open the software for VN5610A, Power on the ASDM3



- Config VN5610A and send A arp packet

Ethernet Packet Builder

Add Packet	Delete	Configuration...	Send	Packet Description	Source	Destination	Protocol	Packet Length	Payload Length
				Packet 1	00:16:81:02:6E:CE	FF:FF:FF:FF:FF:FF	ARP	60	0
				Packet 2	02:00:00:00:00:00	00:A0:C9:00:00:00	ICMPv4	60	18
				Packet 4	00:16:81:02:71:A0	02:00:00:00:14:11	ICMPv4	60	18
				Packet 4	00:16:81:02:71:A0	FF:FF:FF:FF:FF:FF	ARP	60	0

▼ Packet Information

▼ Ethernet

Destination	FF:FF:FF:FF:FF:FF	[0/6]	Manual configured MAC address
Source	00:16:81:02:6E:CE	[6/6]	Use MAC Id of adapter from Current Channel
Type	0x0806	[12/2]	ARP

▼ ARP

Hardware Type	1	[14/2]	Ethernet [10Mb]
Protocol Type	0x0800	[16/2]	IPv4
Hardware Size	6	[18/1]	Byte length of each hardware address
Protocol Size	4	[19/1]	Byte length of each protocol address
Operation	1	[20/2]	ARP Request
Sender Hardware Address	00:16:81:02:72:A0	[22/6]	Hardware address of the sender
Sender Protocol Address	198.18.32.1	[28/4]	Protocol address of the sender
Target Hardware Address	00:00:00:00:00:00	[32/6]	Hardware address of the intended receiver
Target Protocol Address	198.18.36.11	[38/4]	Protocol address of the intended receiver

ARP header

▼ Raw Frame

Bytes per line: Auto Current byte pos: - Packet length: 60

```

0x00000000 FF FF FF FF FF FF 16 81 02 6E CE 08 06 00 01 08 00 06 04 00 01 .....n.....
0x00000016 00 16 81 02 72 A0 C6 12 20 01 00 00 00 00 00 C6 12 24 0B 00 00 .....I.....$...
0x0000002c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

- config the VN5610A and send a icmp packet

Ethernet Packet Builder

Add Packet	Delete	Configuration...	Send	Packet Description	Source	Destination	Protocol	Packet Length	Payload Length
				Packet 1	00:16:81:02:6E:CE	FF:FF:FF:FF:FF:FF	ARP	60	0
				Packet 2	02:00:00:00:00:00	00:A0:C9:00:00:00	ICMPv4	60	18
				Packet 4	00:16:81:02:71:A0	02:00:00:00:14:11	ICMPv4	60	18
				Packet 4	00:16:81:02:71:A0	FF:FF:FF:FF:FF:FF	ARP	60	0

▼ Packet Information

▼ Ethernet

Destination	02:00:00:00:14:11	[0/6]	Manual configured MAC address
Source	00:16:81:02:71:A0	[6/6]	Manual configured MAC address
Type	0x0800	[12/2]	IPv4

▼ IPv4

Version	4	[14/1]	Version information (4 Bit) IPv4
Header Length	5	[14/1]	Internet Header Length (4 Bit) = 20 Byte
DS Field	0000 0000	[15/1]	Differentiated Service Field
Total Length	46	[16/2]	Total Length Field (Byte)
Identification	0	[18/2]	Identification Field
Control Flags	000	[20/1]	Control Flags (3 Bit)
Fragment Offset	0	[20/2]	Fragmentation Offset Field (13 Bit)
Time to Live	64	[22/1]	Time to Live
Protocol	1	[23/1]	Protocol Field
Checksum	0xAA9E	[24/2]	IP Header Checksum [Checksum is correct]
Source	198.18.32.1	[26/4]	IP Source Address
Destination	198.18.36.11	[30/4]	IP Destination Address

ICMP header

▼ ICMPv4

Type	8	[34/1]	Echo Request (PING)
Code	0	[35/1]	Code of service
Checksum	0xF7FF	[36/2]	Checksum [Checksum is correct]
Identifier	0x0000	[38/2]	Identifier field
Sequence Number	0	[40/2]	Sequence Number

▼ Payload

Current byte pos: - Payload length: 18

```

0x00000000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

payload

▼ Raw Frame

Bytes per line: Auto Current byte pos: - Packet length: 60

```

0x00000000 02 00 00 00 14 11 02 71 A0 08 00 45 00 00 2E 00 00 00 40 01 AA 9E C6 12 20 01 C6 12 24 0B 08 00 F7 FF 00 00 .....q...E.....
0x00000028 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

8.4. test result

- The VN5610A receive the arp reply from ASDM

The screenshot shows a Wireshark capture of an ARP reply packet. The packet list on the right shows three packets: a link up event, an ARP request from 198.18.32.1, and an ARP reply from 198.18.36.11. The selected packet is the ARP reply, which is highlighted in blue. The packet details pane on the left shows the following information:

- Frame Checksum: DFED965A
- Packet Length: 60 bytes
- Direction: Rx
- Ethernet II, Src: Ethernet, Dst: 00:16:81:02:72:A0
- ARP, Operation: ARP Reply, Sender Hardware Address: 02:00:00:00:14:11, Sender Protocol Address: 198.18.36.11, Target Hardware Address: 00:16:81:02:72:A0, Target Protocol Address: 00:16:81:02:72:A0

Time	Chn	VLAN...	Dir	Source MAC	Destination ...	Etherne...	Packet L...	Prot...	Protocol Info
0.000628	Eth 1								Link up, 100 Mbit/s
7.195286	Eth 1		Tx	00:16:81:02:6...	FF:FF:FF:FF:FF:0806	60	arp	ARP: 198.18.32.1 asks for MAC address of 198.18.36.11	
7.195376	Eth 1		Rx	02:00:00:00:1...	00:16:81:02:7...	0806	60	arp	ARP: 198.18.36.11 has MAC address 02:00:00:00:14:11

- The VN5610A receive the icmp reply from ASDM

The screenshot shows a Wireshark capture of an ICMPv4 echo reply packet. The packet list on the right shows four packets: two ARP requests, an ICMPv4 echo request, and an ICMPv4 echo reply. The selected packet is the ICMPv4 echo reply, which is highlighted in blue. The packet details pane on the left shows the following information:

- Type: Ethernet Packet
- Channel: Eth 1
- Frame Checksum: C918E72A
- Packet Length: 60 bytes
- Direction: Rx
- Ethernet II, Src: Ethernet, Dst: 00:16:81:02:72:A0
- IPv4, Version: 4, Header Length: 20 bytes
- Differentiated Service Field: DSCP=0 ECN=Not-ECT
- Total Length: 46 bytes
- Identification: 2
- Control Flags: Don't Fragment

Time	Chn	VLAN...	Dir	Source MAC	Destination ...	Etherne...	Packet L...	Prot...	Protocol Info
142.374436	Eth 1		Tx	00:16:81:02:6...	FF:FF:FF:FF:FF:0806	60	arp	ARP: 198.18.32.1 asks for MAC address of 198.18.36.11	
142.374506	Eth 1		Rx	02:00:00:00:1...	00:16:81:02:7...	0806	60	arp	ARP: 198.18.36.11 has MAC address 02:00:00:00:14:11
144.745367	Eth 1		Tx	00:16:81:02:7...	02:00:00:00:1...	0800	60	icmpv4	Type 08
144.745558	Eth 1		Rx	02:00:00:00:1...	00:16:81:02:7...	0800	60	icmpv4	Type 00