计算机网络实验报告

警示

1.实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2.当次小组成员成绩只计学号、姓名登录在下表中的。
3.在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计。
4.实验报告文件以 PDF 格式提交。

院系	计算机学院	班 级	人工智能与大数据	组长	陈欣宇
学号	21307347	21307350	21307100		
学生	陈欣宇	高宇	陈华清		
实验分工					
陈欣宇	负责一台路由器配置以及交换机的端口镜像配置，使用主机 C 抓取数据包，完成实验报告	陈华清	辅助完成路由器配置和其他实验任务，辅助编写实验报告		
高宇	完成主机 A 的配置和路由器 2 的部分配置，进行实验并完成部分实验报告				

【实验题目】VPN 实验

【实验目的】理解 VPN 的工作原理及配置方法。

【实验内容】

(1) 完成实验教程第 10 章实验 10-1 的实验，回答实验提出的问题及实验思考。（P335）

(2) 假设你是恶意监听者,希望捕获路由器 R1 和路由器 R2 之间的通信数据包,应该如何实现?请尝试实现,并根据路由器之间采集到的数据包，观察并讨论分析采用了 IPSec 和不采用 IPSec 的区别.

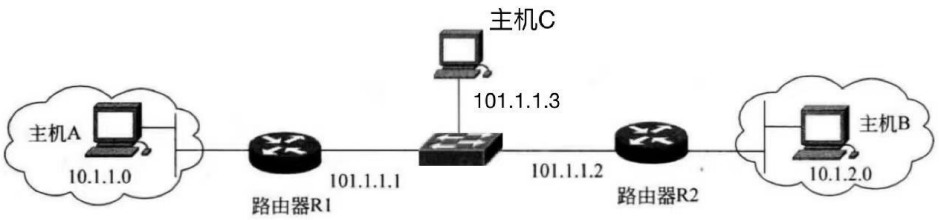
【实验要求】

一些重要信息信息需给出截图，注意实验步骤的前后对比。

【实验记录】(如有实验拓扑请自行画出,)

一、实验 10-1

改变拓扑如图：



分析：能否捕获 VPN 数据包以分析其安全性？在完成基本配置后测试通信的安全性，在启用 IPSec 协议后设法捕获数据包，通过实验前后数据安全性的对比，验证 IPSec 的安全性。

步骤 1：根据已知条件，IPSec 加密策略信息细节如表 10-1 所示。

表 10-1 IPSec 加密策略信息细节

策　略	主 机 A	主 机 B
变换集	ESP-DES 隧道模式	ESP-DES 隧道模式
对等体主机名	路由器 R2	路由器 R1
对等体 IP 地址	101.1.1.2	101.1.1.1
要加密来自哪些主机的数据流	10.1.1.1	10.1.2.1
要加密的分组类型	TCP	TCP
SA 建立方式	IPSEC-ISAKMP	IPSEC-ISAKMP

步骤 2：路由器基本配置

R1：

```
26-RSR20-1(config)#show ip interface brief
Interface                IP-Address(Pri)      IP-Address(Sec)      Status          Protocol
Serial 2/0               101.1.1.1/30         no address           up              up
Serial 2/1               no address           no address           down            down
GigabitEthernet 0/0      no address           no address           down            down
GigabitEthernet 0/1      10.1.1.1/24          no address           up              up
GigabitEthernet 0/2      no address           no address           down            down
GigabitEthernet 0/3      no address           no address           down            down
```

R2：

```
26-RSR20-2(config)#show ip interface brief
Interface                IP-Address(Pri)      IP-Address(Sec)      Status          Protocol
Serial 2/0               101.1.1.2/30         no address           up              up
Serial 2/1               no address           no address           down            down
GigabitEthernet 0/0      no address           no address           down            down
GigabitEthernet 0/1      10.1.2.1/24          no address           up              up
GigabitEthernet 0/2      no address           no address           down            down
GigabitEthernet 0/3      no address           no address           down            down
```

步骤 3：配置默认路由

R1：

```
26-RSR20-1(config)#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 101.1.1.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 101.1.1.2
C     10.1.1.0/24 is directly connected, GigabitEthernet 0/1
C     10.1.1.1/32 is local host.
C     101.1.1.0/30 is directly connected, Serial 2/0
C     101.1.1.1/32 is local host.
```

R2：

```
S*    0.0.0.0/0 [1/0] via 101.1.1.1
C     10.1.2.0/24 is directly connected, Loopback 0
C     10.1.2.1/32 is local host.
C     101.1.1.0/30 is directly connected, Serial 2/0
C     101.1.1.2/32 is local host.
```

```
26-RSR20-2(config)#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 101.1.1.1 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 101.1.1.1
C     10.1.2.0/24 is directly connected, GigabitEthernet 0/1
C     10.1.2.1/32 is local host.
C     101.1.1.0/30 is directly connected, Serial 2/0
C     101.1.1.2/32 is local host.
```

(1) 验证网络连通情况

```
PS C:\Users\D502> ping 10.1.1.2

正在 Ping 10.1.1.2 具有 32 字节的数据:
来自 10.1.1.2 的回复: 字节=32 时间=1960ms TTL=126
来自 10.1.1.2 的回复: 字节=32 时间=2032ms TTL=126
来自 10.1.1.2 的回复: 字节=32 时间=2039ms TTL=126
来自 10.1.1.2 的回复: 字节=32 时间=2226ms TTL=126

10.1.1.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1960ms, 最长 = 2226ms, 平均 = 2064ms
```

```
PS C:\Users\D502> ping 10.1.2.2

正在 Ping 10.1.2.2 具有 32 字节的数据:
来自 10.1.2.2 的回复: 字节=32 时间=2690ms TTL=126
来自 10.1.2.2 的回复: 字节=32 时间=2544ms TTL=126
来自 10.1.2.2 的回复: 字节=32 时间=2744ms TTL=126

10.1.2.2 的 Ping 统计信息:
    数据包: 已发送 = 3, 已接收 = 3, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 2544ms, 最长 = 2744ms, 平均 = 2659ms
```

(2) 捕获通信数据包，测试数据包的安全性

在路由器之间的交换机上配置端口镜像，捕获路由器之间传递数据包

```
26-s5750-2(config)#show monitor
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
GigabitEthernet 0/15          frame-type Both
dest-intf:
GigabitEthernet 0/21
```

成功在主机 C 上抓到 A ping B 的包，可见当前通信数据包安全性不高

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:88:99:00:12:de	LLDP_Multicast	LLDP	58	MA/00:88:99:00:12:de MA/00:88:99:00:12:de 3601
2	1.242501	10.1.1.2	10.1.2.2	ICMP	74	Echo (ping) request id=0x0001, seq=158/40448, ttl=127 (reply in 3)
3	1.242501	10.1.2.2	10.1.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=158/40448, ttl=127 (request in 2)
4	2.245398	10.1.1.2	10.1.2.2	ICMP	74	Echo (ping) request id=0x0001, seq=159/40704, ttl=127 (reply in 5)
5	2.245398	10.1.2.2	10.1.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=159/40704, ttl=127 (request in 4)
6	3.252692	10.1.1.2	10.1.2.2	ICMP	74	Echo (ping) request id=0x0001, seq=160/40960, ttl=127 (reply in 7)
7	3.252692	10.1.2.2	10.1.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=160/40960, ttl=127 (request in 6)
8	4.265530	10.1.1.2	10.1.2.2	ICMP	74	Echo (ping) request id=0x0001, seq=161/41216, ttl=127 (reply in 9)
9	4.265530	10.1.2.2	10.1.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=161/41216, ttl=127 (request in 8)
10	7.240278	101.1.1.3	101.255.255.255	UDP	1482	51507 → 1689 Len=1440

步骤 4：配置 IPSec VPN

步骤 5：定义需要的数据流以及应用 VPN

步骤 6：验证测试

以上配置完成后，路由器 R1 和 R2 之间的安全隧道建立完成。子网 10.1.1.x 与子网 10.1.2.x 之间的数据流将被加密传输

(1) 显示所有尝试协商的策略以及最后的默认策略设置

#show crypto isakmp policy

路由器 R1：

```
26-RSR20-1(config-if-Serial 2/0)#show crypto isakmp policy
Protection suite of priority 10
   encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
   hash algorithm:         Message Digest 5
   authentication method:  Pre-Shared Key
   Diffie-Hellman group:   #2 (1024 bit)
   lifetime:               86400 seconds
Default protection suite
   encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
   hash algorithm:         Secure Hash Standard
   authentication method:  Rsa-Sig
   Diffie-Hellman group:   #1 (768 bit)
   lifetime:               86400 seconds
```

路由器 R2：

```
26-RSR20-2(config-if-Serial 2/0)#show crypto isakmp policy
Protection suite of priority 10
   encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
   hash algorithm:         Message Digest 5
   authentication method:  Pre-Shared Key
   Diffie-Hellman group:   #2 (1024 bit)
   lifetime:               86400 seconds
Default protection suite
   encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
   hash algorithm:         Secure Hash Standard
   authentication method:  Rsa-Sig
   Diffie-Hellman group:   #1 (768 bit)
   lifetime:               86400 seconds
```

显示了安全联盟和密钥交换策略（策略编号为 10）的各项参数和默认策略的各项参数

(2) 显示在路由器上设置的 transform-set

#show crypto ipsec transform-set

路由器 R1：

```
26-RSR20-1(config-if-Serial 2/0)#show crypto ipsec transform-set
transform set vpn: { ah-md5-hmac,esp-md5-hmac,esp-des,}
        will negotiate = {Tunnel,}
```

路由器 R2：

```
26-RSR20-2(config-if-Serial 2/0)#show crypto ipsec transform-set
transform set vpn: { ah-md5-hmac,esp-md5-hmac,esp-des,}
        will negotiate = {Tunnel,}
```

配置了 IPsec 的传输模式，模式名称为 vpn，AH 验证为 ah-md5-hmac,ESP 加密为 esp-des，ESP 验证为 esp-md5-hamc，工作模式是隧道模式

(3) 显示当前安全联盟使用到设置

show crypto ipsec sa

```
26-RSR20-1(config)#show crypto ipsec sa


Interface: Serial 2/0
        Crypto map tag:vpnmap
        local ipv4 addr 101.1.1.1
        media mtu 1500


        ================================
        sub_map type:static, seqno:10, id=0
        local  ident (addr/mask/prot/port): (10.1.1.0/0.0.0.255/0/0))
        remote  ident (addr/mask/prot/port): (10.1.2.0/0.0.0.255/0/0))
        PERMIT
        #pkts encaps: 34, #pkts encrypt: 34, #pkts digest 68
        #pkts decaps: 30, #pkts decrypt: 30, #pkts verify 60
        #send errors 0, #recv errors 0

        Inbound esp sas:
             spi:0x2d35a072 (758489202)
              transform: esp-des esp-md5-hmac
              in use settings={Tunnel Encaps,}
              crypto map vpnmap 10
              sa timing: remaining key lifetime (k/sec): (4607991/3377)
              IV size: 8 bytes
              Replay detection support:Y


        Inbound ah sas:
             spi:0xdc164967 (3692448103)
              transform: ah-null ah-md5-hmac
              in use settings={Tunnel Encaps,}
              crypto map vpnmap 10
              sa timing: remaining key lifetime (k/sec): (4607991/3377)
              IV size: 0 bytes
              Replay detection support:Y


        Outbound esp sas:
             spi:0x327b8a93 (846957203)
              transform: esp-des esp-md5-hmac
              in use settings={Tunnel Encaps,}
              crypto map vpnmap 10
              sa timing: remaining key lifetime (k/sec): (4607991/3377)
              IV size: 8 bytes
              Replay detection support:Y


        Outbound ah sas:
             spi:0x95e12d20 (2514562336)
              transform: ah-null ah-md5-hmac
              in use settings={Tunnel Encaps,}
              crypto map vpnmap 10
              sa timing: remaining key lifetime (k/sec): (4607991/3377)
              IV size: 0 bytes
              Replay detection support:Y
```

```
26-RSR20-2(config-if-Serial 2/0)#show crypto ipsec sa


Interface: Serial 2/0
        Crypto map tag:vpnmap
        local ipv4 addr 101.1.1.2
        media mtu 1500


        ================================
        sub_map type:static, seqno:10, id=0
        local  ident (addr/mask/prot/port): (10.1.2.0/0.0.0.255/0/0))
        remote  ident (addr/mask/prot/port): (10.1.1.0/0.0.0.255/0/0))
        PERMIT
        #pkts encaps: 22, #pkts encrypt: 22, #pkts digest 44
        #pkts decaps: 26, #pkts decrypt: 26, #pkts verify 52
        #send errors 0, #recv errors 0

        Inbound esp sas:
             spi:0x327b8a93 (846957203)
              transform: esp-des esp-md5-hmac
              in use settings={Tunnel Encaps,}
              crypto map vpnmap 10
              sa timing: remaining key lifetime (k/sec): (4606993/3428)
              IV size: 8 bytes
              Replay detection support:Y


        Inbound ah sas:
             spi:0x95e12d20 (2514562336)
              transform: ah-null ah-md5-hmac
              in use settings={Tunnel Encaps,}
              crypto map vpnmap 10
              sa timing: remaining key lifetime (k/sec): (4606993/3428)
              IV size: 0 bytes
              Replay detection support:Y


        Outbound esp sas:
             spi:0x2d35a072 (758489202)
              transform: esp-des esp-md5-hmac
              in use settings={Tunnel Encaps,}
              crypto map vpnmap 10
              sa timing: remaining key lifetime (k/sec): (4606993/3428)
              IV size: 8 bytes
              Replay detection support:Y


        Outbound ah sas:
             spi:0xdc164967 (3692448103)
              transform: ah-null ah-md5-hmac
              in use settings={Tunnel Encaps,}
              crypto map vpnmap 10
              sa timing: remaining key lifetime (k/sec): (4606993/3428)
              IV size: 0 bytes
              Replay detection support:Y
```

显示建立的 IPSec SA

(4) 显示所有配置在路由器上的 crypto map

Show crypto map

R1:

```
26-RSR20-1(config-if-Serial 2/0)#show crypto map

Crypto Map:"vpnmap" 10 ipsec-isakmp, (Complete)
        Extended IP access list 110
        Security association lifetime: 4608000 kilobytes/3600 seconds(id=3)
        PFS (Y/N): N
        Transform sets = { vpn,  }

        Interfaces using crypto map vpnmap:
                Serial 2/0
```

R2:

```
26-RSR20-2(config-if-Serial 2/0)#show crypto map

Crypto Map:"vpnmap" 10 ipsec-isakmp, (Complete)
        Extended IP access list 110
        Security association lifetime: 4608000 kilobytes/3600 seconds(id=3)
        PFS (Y/N): N
        Transform sets = { vpn,  }

        Interfaces using crypto map vpnmap:
                Serial 2/0
```

显示 crypto map，名称为 vpnmap，优先级为 10，transform set 为 vpn，使用的端口为 serial 2/0

(5) 进行数据加密传输验证

从左网发 ping 命令，逐级验证到右网。记录验证结果。

逐级结果都能够 ping 通

```
26-RSR20-1#ping
Protocol [ip]:
Target IP address: 101.1.1.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address:10.1.1.1
Time to Live [1, 64]:
Type of service [0, 31]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data Pattern [0xABCD]:
Sending 5, 100-byte ICMP Echoes to 101.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/48/50 ms
```

```
26-RSR20-1#ping
Protocol [ip]:
Target IP address: 10.1.2.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address:10.1.1.1
Time to Live [1, 64]:
Type of service [0, 31]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data Pattern [0xABCD]:
Sending 5, 100-byte ICMP Echoes to 10.1.2.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/66/70 ms
```

从右网发 ping 命令至左网。记录验证结果。

逐级结果都能够 ping 通

```
26-RSR20-2#ping
Protocol [ip]:
Target IP address: 101.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address:10.1.2.1
Time to Live [1, 64]:
Type of service [0, 31]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data Pattern [0xABCD]:
Sending 5, 100-byte ICMP Echoes to 101.1.1.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 50/50/50 ms
```

```
26-RSR20-2#ping
Protocol [ip]:
Target IP address: 10.1.1.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address:10.1.2.1
Time to Live [1, 64]:
Type of service [0, 31]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data Pattern [0xABCD]:
Sending 5, 100-byte ICMP Echoes to 10.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/62/70 ms
```

(6) 捕获 VPN 数据包，分析 AH、ESP 报文头；分析数据流的加密情况（提示：重点解决 VPN 数据包的捕获问题，可增加设备或适当改变拓扑结构）

根据之前路由器间数据包的通过端口镜像的捕获方法，捕获到 ESP 包，且捕获不到原先的 ICMP 包，数据被加密，只能观察到两个路由器地址，无法观察主机 A、B 的 IP 地址。

1	0.000000	101.1.1.3	101.255.255.255	UDP	1482 51507 → 1689 Len=1440
2	1.907191	RuijieNe_77:17:86	LLDP_Multicast	LLDP	391 MA/14:14:4b:77:17:86 MA/14:14:4b:77:17:86 121
3	2.655925	101.1.1.1	101.1.1.2	ESP	150 ESP (SPI=0x603ac3ec)
4	2.656423	101.1.1.2	101.1.1.1	ESP	150 ESP (SPI=0x07a528b9)
5	3.659082	101.1.1.1	101.1.1.2	ESP	150 ESP (SPI=0x603ac3ec)
6	3.659540	101.1.1.2	101.1.1.1	ESP	150 ESP (SPI=0x07a528b9)
7	4.683120	101.1.1.2	101.1.1.1	ESP	150 ESP (SPI=0x07a528b9)
8	4.683166	101.1.1.1	101.1.1.2	ESP	150 ESP (SPI=0x603ac3ec)
9	5.705011	101.1.1.1	101.1.1.2	ESP	150 ESP (SPI=0x603ac3ec)
10	5.705378	101.1.1.2	101.1.1.1	ESP	150 ESP (SPI=0x07a528b9)
11	8.523339	101.1.1.3	101.255.255.255	UDP	1482 51507 → 1689 Len=1440
12	9.900173	00:88:99:00:12:de	Broadcast	ARP	42 Who has 101.1.1.1? Tell 101.1.1.3
13	10.905331	00:88:99:00:12:de	Broadcast	ARP	42 Who has 101.1.1.1? Tell 101.1.1.3
14	11.899798	00:88:99:00:12:de	Broadcast	ARP	42 Who has 101.1.1.1? Tell 101.1.1.3
15	17.051386	101.1.1.3	101.255.255.255	UDP	1482 51507 → 1689 Len=1440

```
> Frame 3: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface \Device\NPF_{93CAEBF1-6A0E-4568-A292-53DB46A8E4ED}, id 0
> Ethernet II, Src: RuijieNe_b4:f3:8d (00:74:9c:b4:f3:8d), Dst: RuijieNe_47:2c:37 (80:05:88:47:2c:37)
v Internet Protocol Version 4, Src: 101.1.1.1, Dst: 101.1.1.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 136
    Identification: 0x0228 (552)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 254
    Protocol: Authentication Header (51)
    Header Checksum: 0xee15 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 101.1.1.1
    Destination Address: 101.1.1.2
v Authentication Header
    Next header: Encap Security Payload (50)
    Length: 4 (24 bytes)
    Reserved: 0000
    AH SPI: 0x9043f3df
    AH Sequence: 42
    AH ICV: 17d7bbe4a3562fac210b0a78
v Encapsulating Security Payload
    ESP SPI: 0x603ac3ec (1614463980)
    ESP Sequence: 42
```

AH 可对整个数据包提供身份验证、完整性与抗重播保护，在捕获数据包可见 Authentication Header：Next header 表示下一个报头，表示被 AH 包含的那个协议类型；Length 表示 AH 报头的长度；Reserved 为保留字段；AH SPI 表示安全参数索引，用于确定数据包使用哪一安全关联标识。Sequence 表示序数 ：表示通过通信的安全关联所发送的数据包数，为该数据包提供抗重播保护。ICV 为消息身份验证码，用于验证消息身份验证与完整性。

ESP 提供机密性、数据起源验证、无连接的完整性、抗重播服务和有限业务流机密性。

SPI 为安全参数索引，和 IP 头之前的目标地址以及协议结合在一起，用来标识用于处理数据包的特

定的那个安全关联；Sequence 为序列号，是插在 ESP 头的一个号码，使 ESP 具有了抵抗重播攻击的能力。

二、假设你是恶意监听者,希望捕获路由器 R1 和路由器 R2 之间的通信数据包,应该如何实现?请尝试实现,并根据路由器之间采集到的数据包，观察并讨论分析采用了 IPSec 和不采用 IPSec 的区别.

参考本实验拓扑结构，在路由器之间的交换机上配置端口镜像，即可捕获路由器间的通信数据包，使用 IPSec 和不采用 IPSec 的区别已经展示。区别如下：ICMP 包在使用 IPSec 后被加密为 VPN 包

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:88:99:00:12:de	LLDP_Multicast	LLDP	58	MA/00:88:99:00:12:de MA/00:88:99:00:12:de 3601
2	1.242501	10.1.1.2	10.1.2.2	ICMP	74	Echo (ping) request id=0x0001, seq=158/40448, ttl=127 (reply in 3)
3	1.242501	10.1.2.2	10.1.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=158/40448, ttl=127 (request in 2)
4	2.245398	10.1.1.2	10.1.2.2	ICMP	74	Echo (ping) request id=0x0001, seq=159/40704, ttl=127 (reply in 5)
5	2.245398	10.1.2.2	10.1.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=159/40704, ttl=127 (request in 4)
6	3.252692	10.1.1.2	10.1.2.2	ICMP	74	Echo (ping) request id=0x0001, seq=160/40960, ttl=127 (reply in 7)
7	3.252692	10.1.2.2	10.1.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=160/40960, ttl=127 (request in 6)
8	4.265530	10.1.1.2	10.1.2.2	ICMP	74	Echo (ping) request id=0x0001, seq=161/41216, ttl=127 (reply in 9)
9	4.265530	10.1.2.2	10.1.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=161/41216, ttl=127 (request in 8)
10	7.240278	101.1.1.3	101.255.255.255	UDP	1482	51507 → 1689 Len=1440

1	0.000000	101.1.1.3	101.255.255.255	UDP	1482	51507 → 1689 Len=1440
2	1.907191	RuijieNe_77:17:86	LLDP_Multicast	LLDP	391	MA/14:14:4b:77:17:86 MA/14:14:4b:77:17:86 121
3	2.655925	101.1.1.1	101.1.1.2	ESP	150	ESP (SPI=0x603ac3ec)
4	2.656423	101.1.1.2	101.1.1.1	ESP	150	ESP (SPI=0x07a528b9)
5	3.659082	101.1.1.1	101.1.1.2	ESP	150	ESP (SPI=0x603ac3ec)
6	3.659540	101.1.1.2	101.1.1.1	ESP	150	ESP (SPI=0x07a528b9)
7	4.683120	101.1.1.2	101.1.1.1	ESP	150	ESP (SPI=0x07a528b9)
8	4.683166	101.1.1.1	101.1.1.2	ESP	150	ESP (SPI=0x603ac3ec)
9	5.705011	101.1.1.1	101.1.1.2	ESP	150	ESP (SPI=0x603ac3ec)
10	5.705378	101.1.1.2	101.1.1.1	ESP	150	ESP (SPI=0x07a528b9)
11	8.523339	101.1.1.3	101.255.255.255	UDP	1482	51507 → 1689 Len=1440
12	9.900173	00:88:99:00:12:de	Broadcast	ARP	42	Who has 101.1.1.1? Tell 101.1.1.3
13	10.905331	00:88:99:00:12:de	Broadcast	ARP	42	Who has 101.1.1.1? Tell 101.1.1.3
14	11.899798	00:88:99:00:12:de	Broadcast	ARP	42	Who has 101.1.1.1? Tell 101.1.1.3
15	17.051386	101.1.1.3	101.255.255.255	UDP	1482	51507 → 1689 Len=1440

学号	学生	自评分
21307347	陈欣宇	95
21307350	高宇	93
21307100	陈华清	93

本次实验完成后，请根据组员在实验中的贡献，请实事求是，自评在实验中应得的分数。（按百分制）