



1

# UDP数据包分析实验

冯巾松

fengjinsong@tongji.edu.cn

# UDP的概述

- ➡ UDP (User Datagram Protocol) 是传输层的协议，功能即为在IP的数据报服务之上增加了最基本的服务：复用和分用以及差错检测。
- ➡ UDP提供不可靠服务，具有TCP所没有的优势：
- ➡ UDP无连接，时间上不存在建立连接需要的时延。空间上，TCP需要在端系统中维护连接状态，需要一定的开销。此连接装入包括接收和发送缓存，拥塞控制参数和序号与确认号的参数。UDP不维护连接状态，也不跟踪这些参数，开销小。空间和时间上都具有优势

## UDP的应用特点

- DNS如果运行在TCP之上而不是UDP，那么DNS的速度将会慢很多。
- HTTP使用TCP而不是UDP，是因为对于基于文本数据的Web网页来说，可靠性很重要。
- 同一种专用应用服务器在支持UDP时，一定能支持更多的活动客户机。
- 分组首部开销小，TCP首部20字节，UDP首部8字节

# UDP的应用特点

- ➡ UDP没有拥塞控制，应用层能够更好的控制要发送的数据和发送时间，网络中的拥塞控制也不会影响主机的发送速率。某些实时应用要求以稳定的速度发送，能容忍一些数据的丢失，但是不能允许有较大的时延（比如实时视频，直播等）
- ➡ UDP提供尽最大努力的交付，不保证可靠交付。所有维护传输可靠性的工作需要用户在应用层来完成。没有TCP的确认机制、重传机制。如果因为网络原因没有传送到对端，UDP也不会给应用层返回错误信息。

# UDP的应用特点

- UDP是面向报文的，对应用层交下来的报文，添加首部后直接交给交付为IP层，既不合并，也不拆分，保留这些报文的边界。对IP层交上来UDP用户数据报，在去除首部后就原封不动地交付给上层应用进程，报文不可分割，是UDP数据报处理的最小单位。
- 正是如此UDP显得不够灵活，不能控制读写数据的次数和数量。比如要发送100个字节的报文，调用一次sendto函数就会发送100字节，对端也需要用recvfrom函数一次性接收100字节，不能使用循环每次获取10个字节，获取十次这样的做法。



# UDP的应用特点

- ➡ UDP常用一次性传输比较少量数据的网络应用，如DNS,SNMP等，因为对于这些应用，若是采用TCP，为连接的创建，维护和拆除带来不小的开销。UDP也常用于多媒体应用（如IP电话，实时视频会议，流媒体等）数据的可靠传输对它们而言并不重要，TCP的拥塞控制会使它们有较大的延迟，也是不可容忍的。
- ➡ 总之，UDP协议提供不可靠无连接的数据报传输服务

# UDP报文格式

- UDP数据报分为首部和用户数据部分，整个UDP数据报作为IP数据报的数据部分封装在IP数据报中
- UDP数据报文结构图



## UDP的首部格式

➡ UDP首部有8个字节，由4个字段构成，每个字段都是两个字节，

1).源端口：源端口号，需要对方回信时选用，不需要时全部置0.

2).目的端口：目的端口号，在终点交付报文的时候需要用到。

3).长度：UDP的数据报的长度（包括首部和数据）其最小值为8（只有首部）



## UDP的首部格式

- ➡ 4).校验和：检测UDP数据报在传输中是否有错，有错则丢弃。该字段是可选的，当源主机不想计算校验和，则直接令该字段全为0。当传输层从IP层收到UDP数据报时，就根据首部中的目的端口，把UDP数据报通过相应的端口，上交给应用进程。
- ➡ 如果接收方UDP发现收到的报文中的目的端口号不正确（不存在对应端口号的应用进程0），就丢弃该报文，并由ICMP发送“端口不可达”差错报文给对方。

# UDP的校验

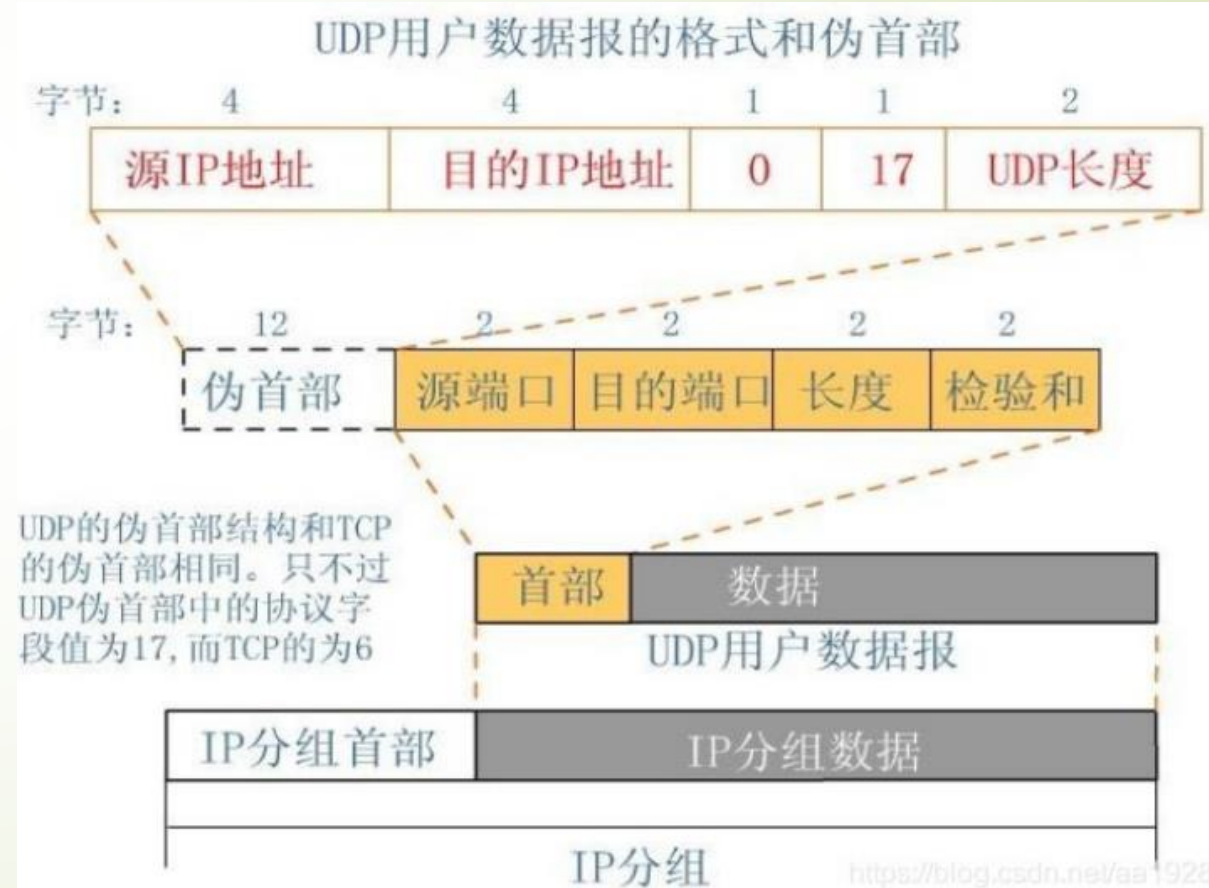
10

➡ 在计算校验和的时候，需要在UDP数据报之前增加12字节的伪首部，伪首部并不是UDP真正的首部。只是在计算校验和，临时添加在UDP数据报的前面，得到一个临时的UDP数据报。校验和就是按照这个临时的UDP数据报计算的。伪首部既不向下传送也不向上递交，仅仅是为了计算校验和。这样的校验和，既检查了UDP数据报，又对IP数据报的源IP地址和目的IP地址进行了检验。

# UDP的校验

➡ UDP校验和的计算方法和IP数据报首部校验和的计算方法相似，都使用二进制反码运算求和再取反。

但不同的是：IP数据报的校验和只检验IP数据报的首部，但UDP的校验和是把首部和数据部分一起校验



# UDP的首部格式

12

➡ 发送方，首先是把全零放入校验和字段并且添加伪首部，然后把UDP数据报看成是由许多16位的子串连接起来，若UDP数据报的数据部分不是偶数个字节，则要在数据部分末尾增加一个全零字节（此字节不发送），接下来就按照二进制反码计算出这些16位字的和。将此和的二进制反码写入校验和字段。在接收方，把收到得UDP数据报加上伪首部（如果不为偶数个字节，还需要补上全零字节）后，按二进制反码计算出这些16位字的和



# UDP的首部格式

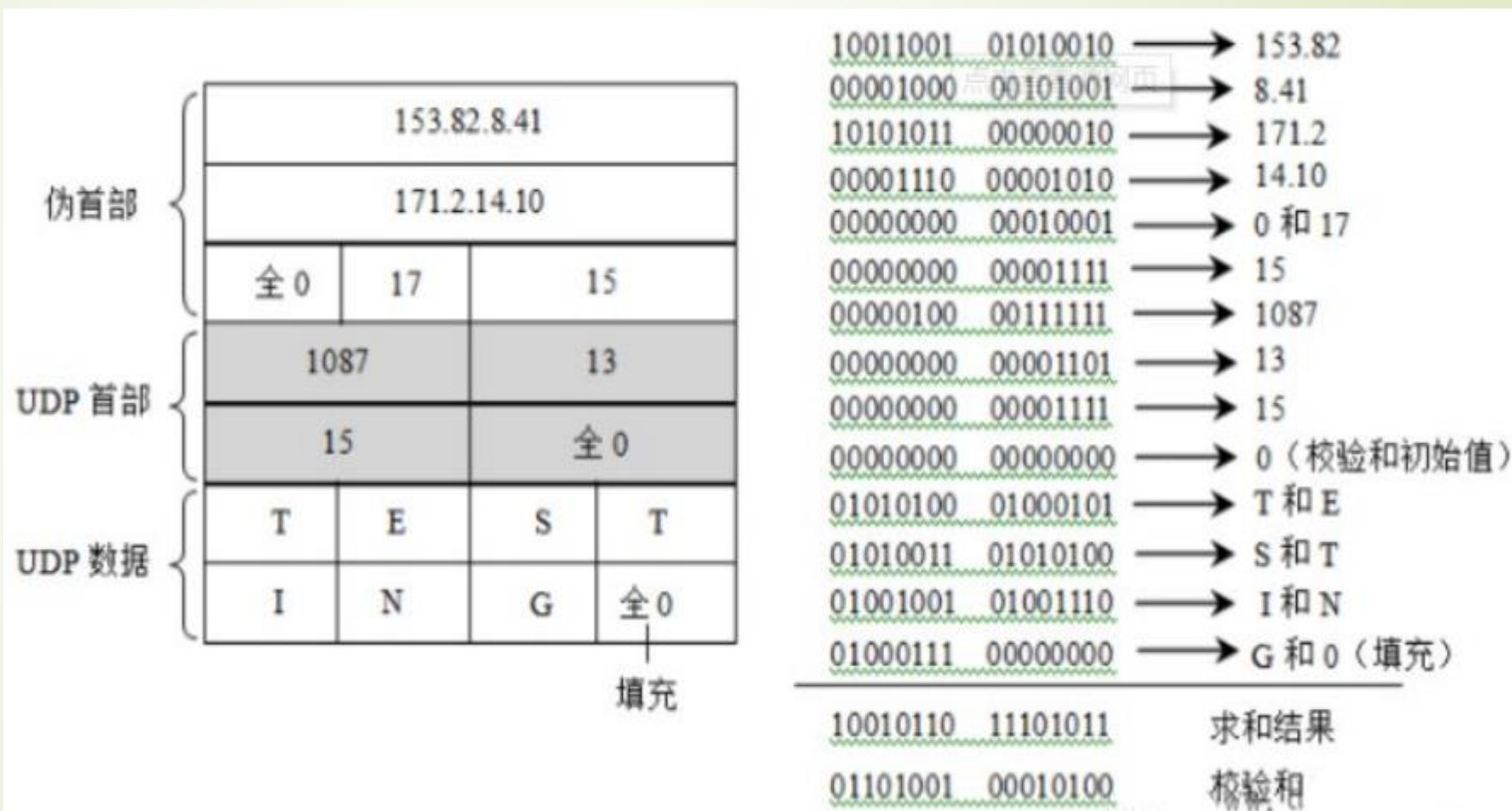
13

- 当无差错时其结果全为1,否则就表明有差错出现,接收方应该丢弃这个UDP数据报。
- 注意: 1). 校验时, 若UDP数据报部分的长度不是偶数个字节, 则需要填入一个全0字节, 但是此字节和伪首部一样, 是不发送的。2). 如果UDP校验和校验出UDP数据报是错误的, 可以丢弃, 也可以交付上层, 但是要附上错误报告, 告诉上层这是错误的的数据报。3). 通过伪首部, 不仅可以检查源端口号, 目的端口号和UDP用户数据报的数据部分, 还可以检查IP数据报的源IP地址和目的地址。这种差错检验的检错能力不强, 但是简单, 速度快。

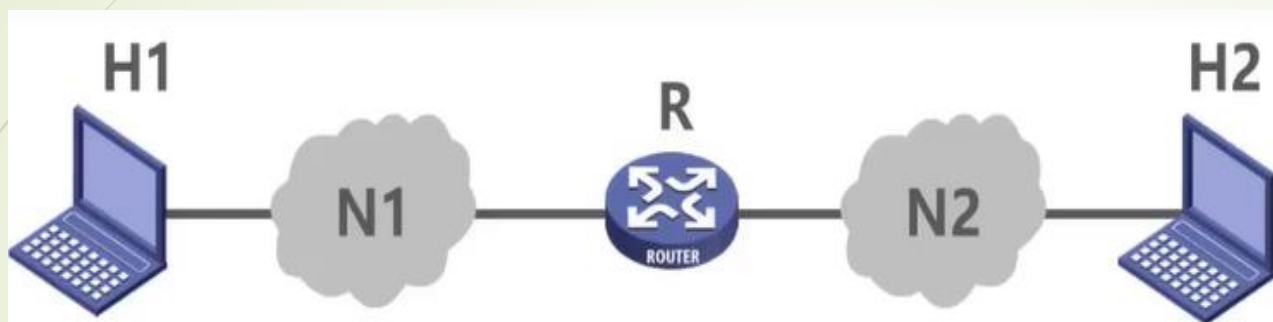


# UDP校验示例

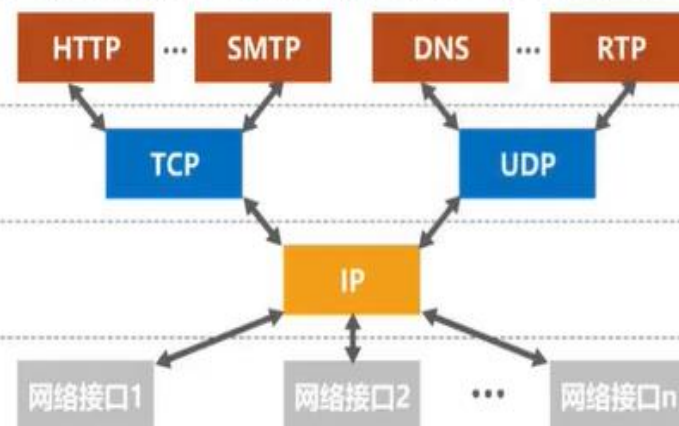
14



# UDP与TCP是TCP/IP体系结构传输层中的2个重要协议



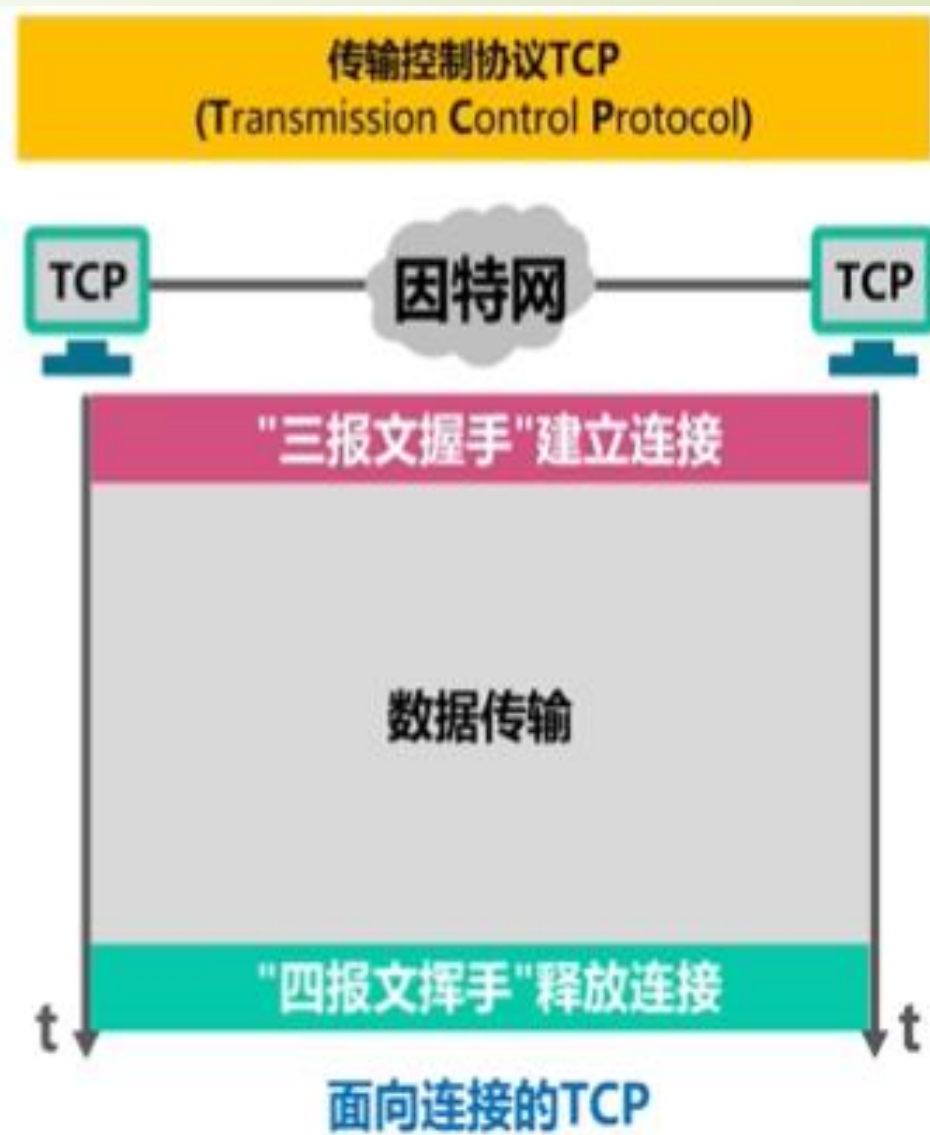
IP协议可以为各种网络应用提供服务  
(Everything over IP)



使用IP协议互连不同的网络接口  
(IP over everything)

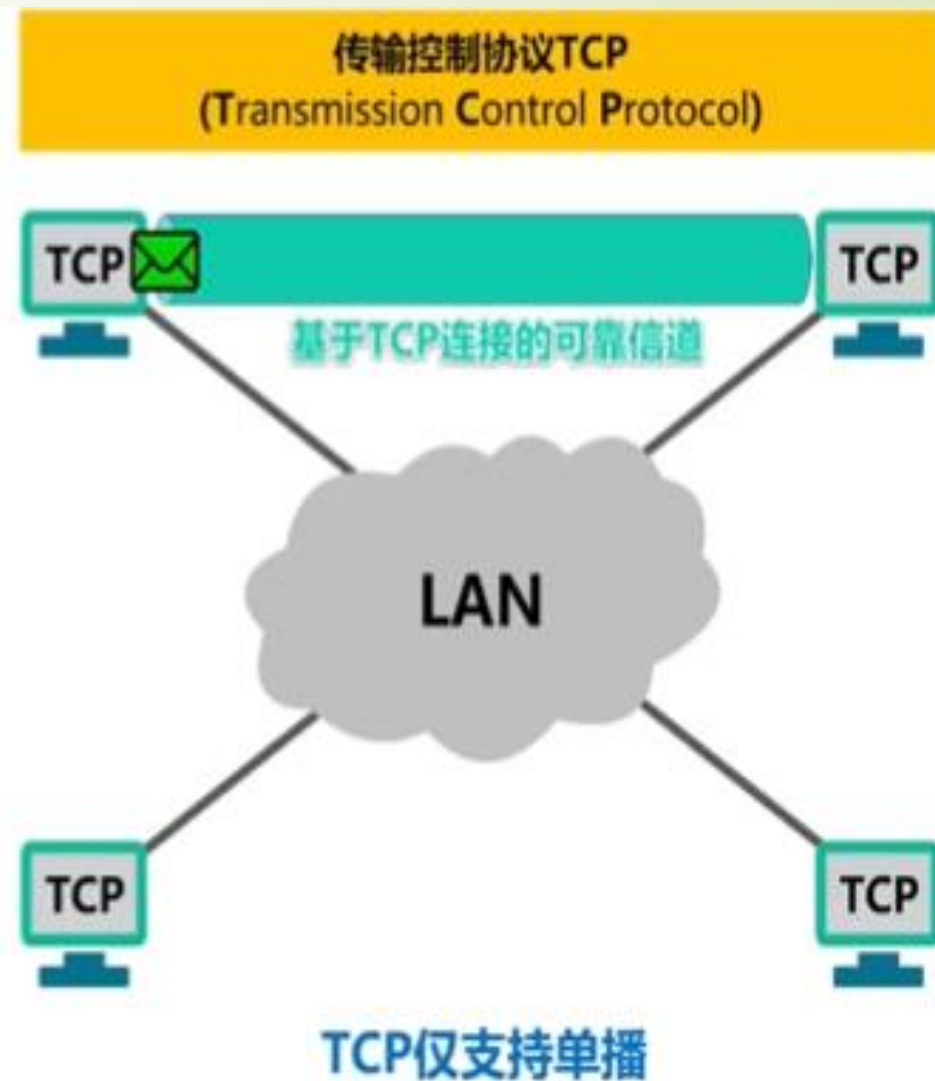
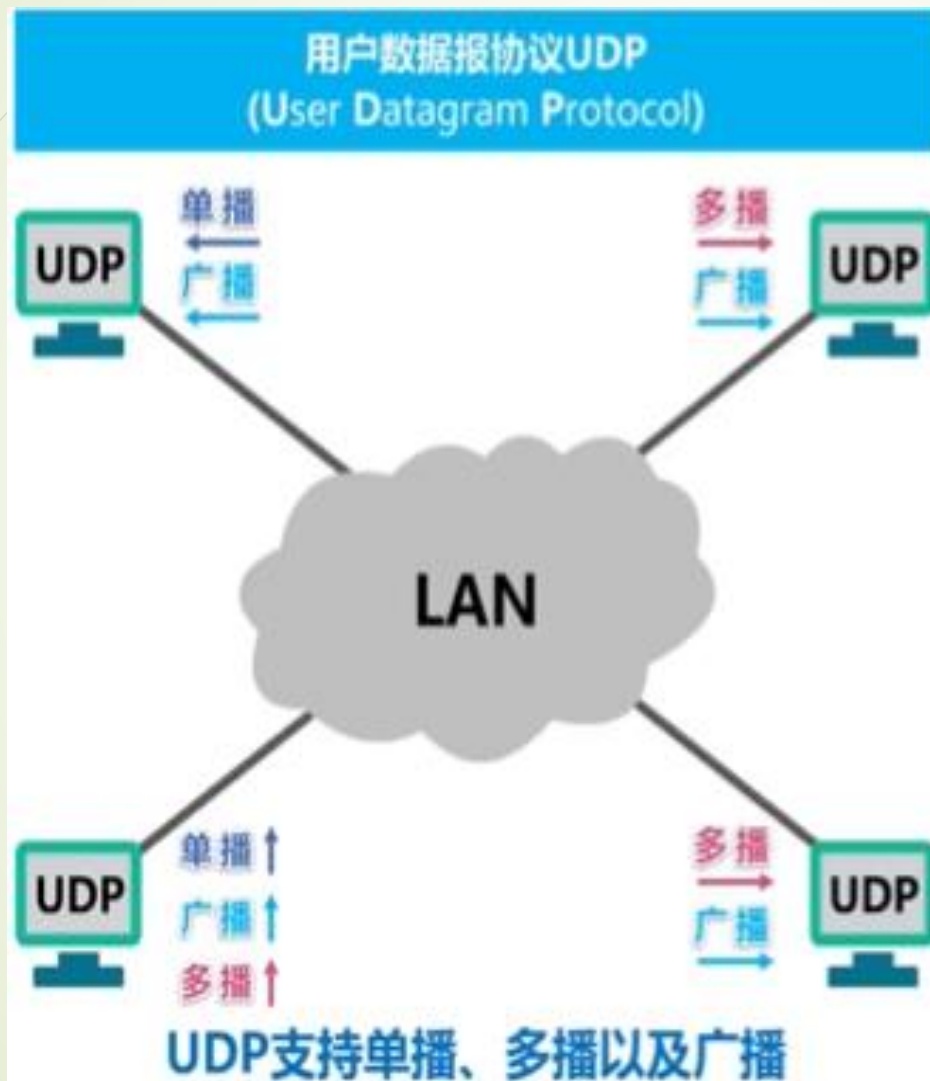
# UDP与TCP的对比

16



# UDP与TCP的对比

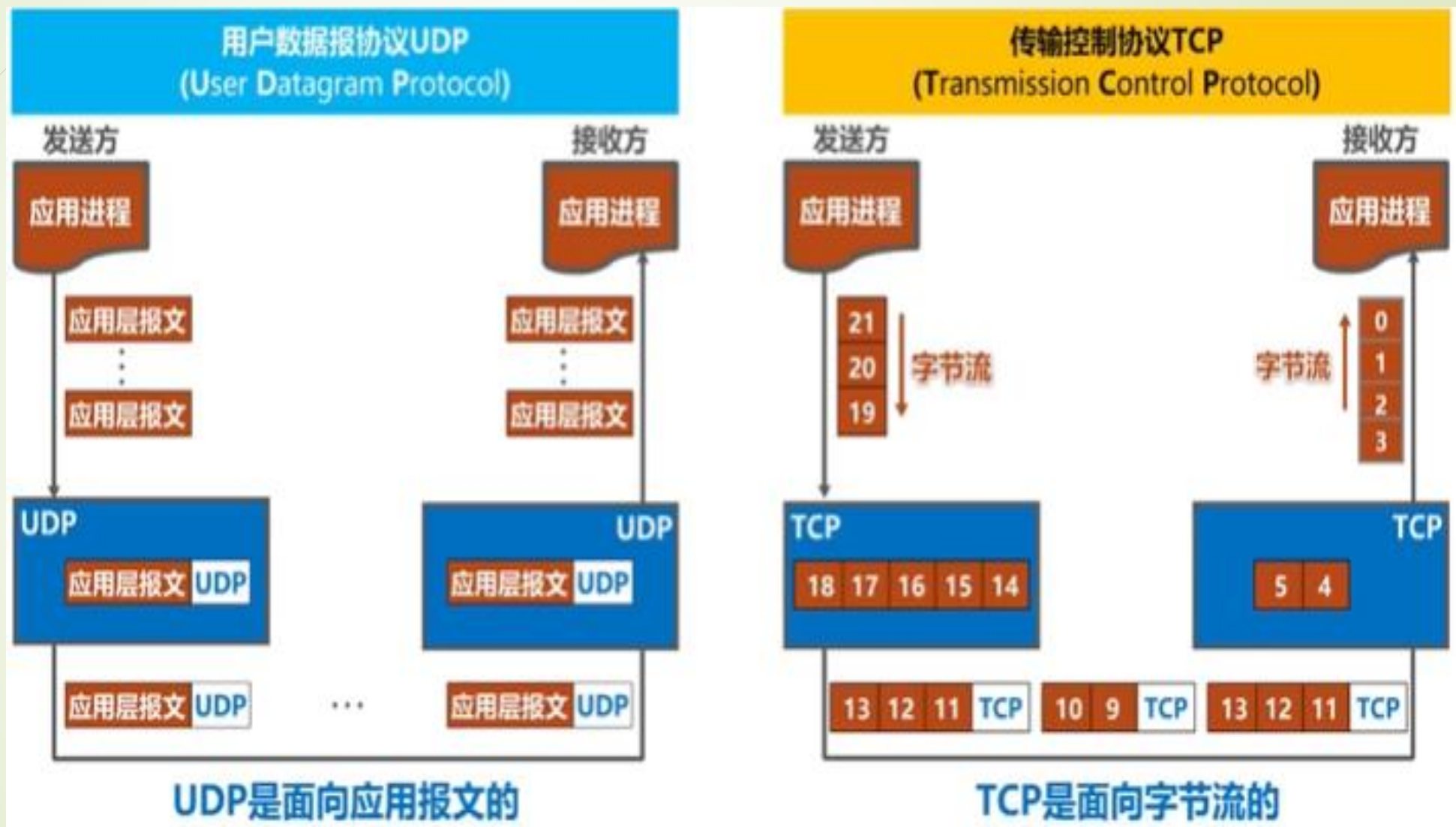
17





# UDP与TCP的对比

18



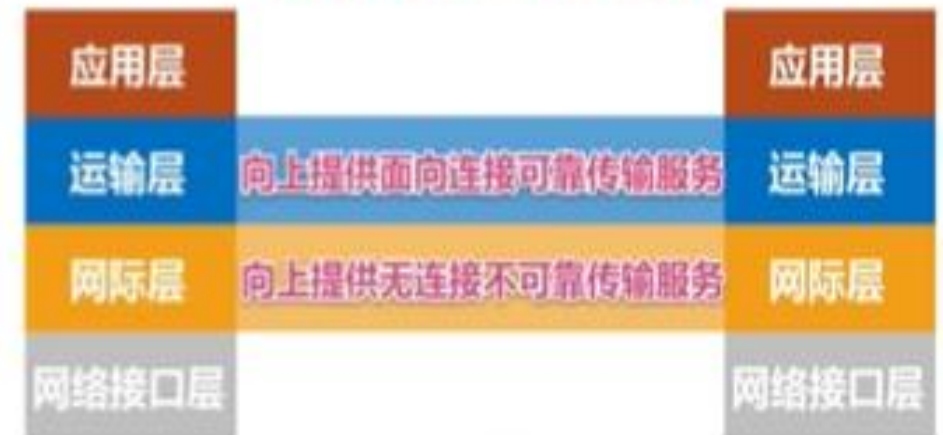


# UDP与TCP的对比

19



**UDP向上层提供无连接不可靠传输服务**  
(适用于IP电话、视频会议等实时应用)

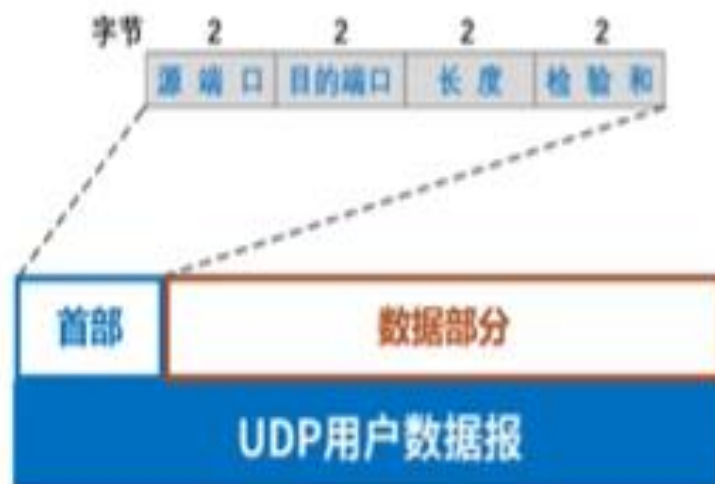


**TCP向上层提供面向连接的可靠传输服务**  
(适用于要求可靠传输的应用，例如文件传输)

# UDP与TCP的对比

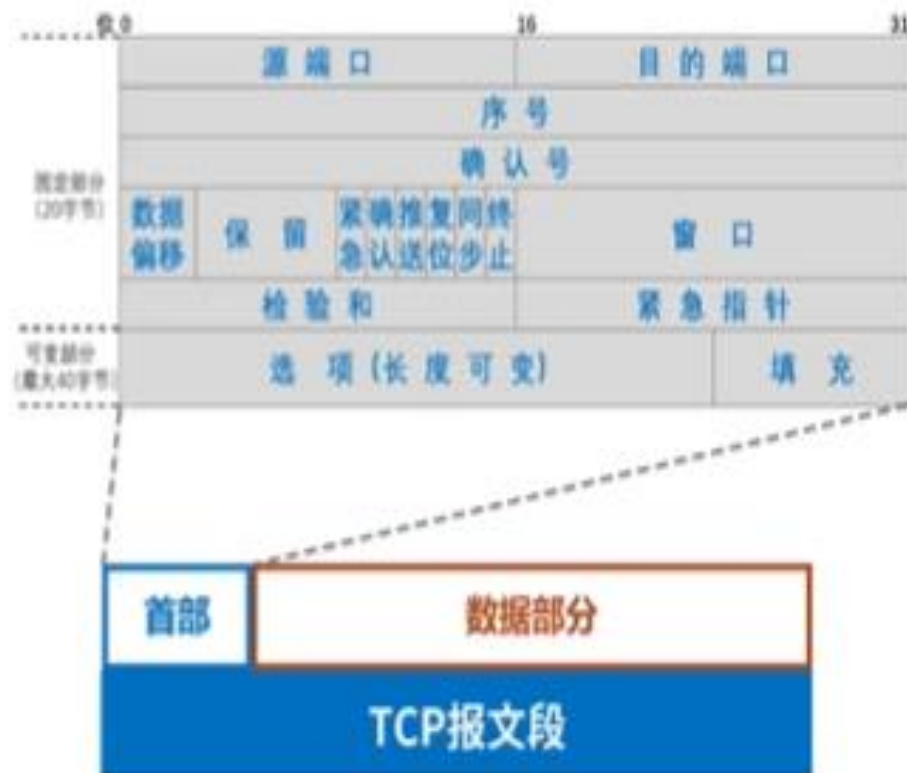
20

## 用户数据报协议UDP (User Datagram Protocol)



UDP用户数据报首部仅8字节

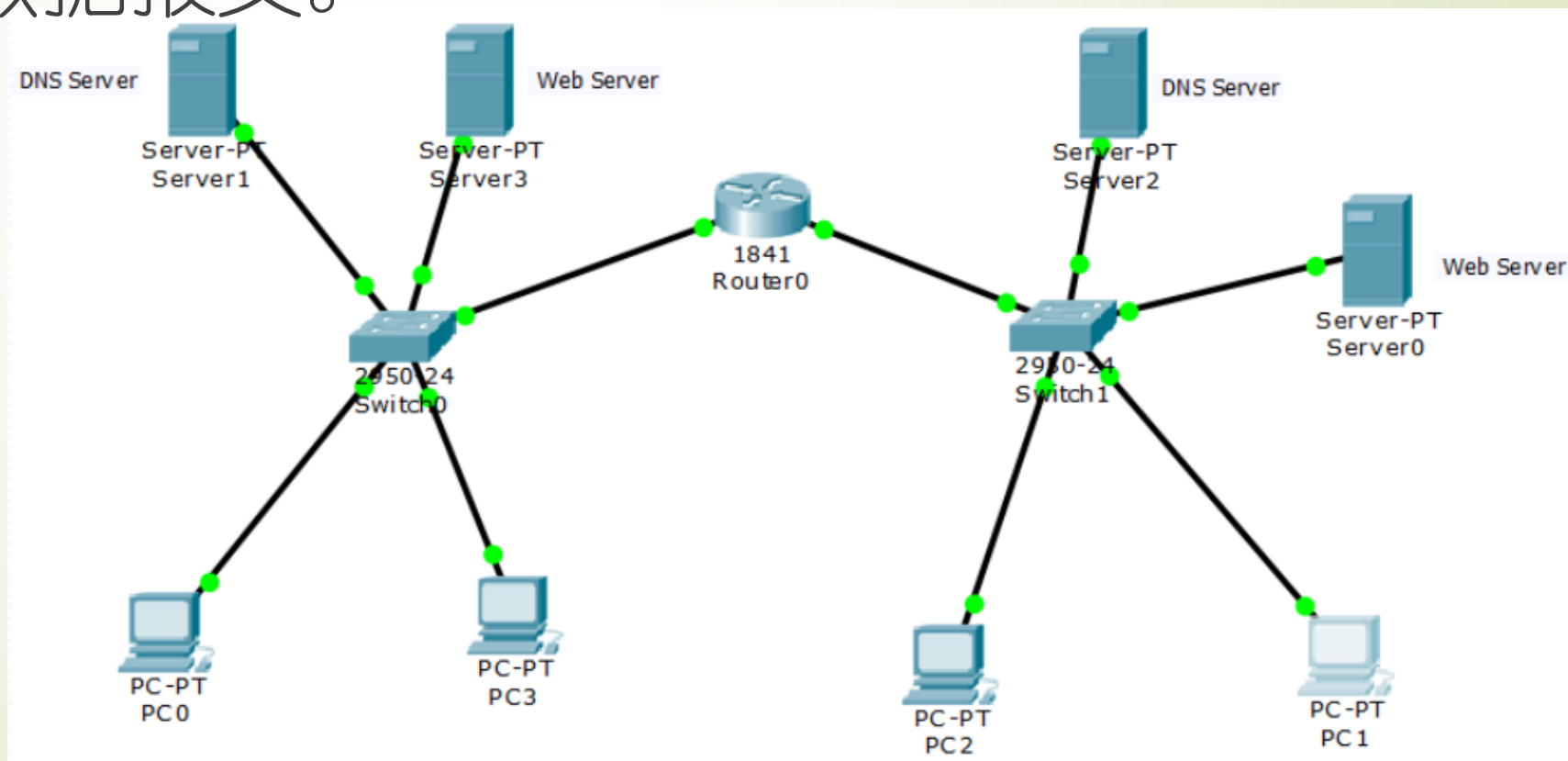
## 传输控制协议TCP (Transmission Control Protocol)



TCP报文段首部最小20字节，最大60字节

# Packet Tracer 分析UDP报文

- ➡ 1) 设置WEB服务器和简单的DNS服务器；
- ➡ 2) 打开PC0浏览器，输入配置Web服务器的Web地址，如www.tongji.edu.cn,产生UDP数据报文。





# Packet Tracer 分析UDP报文

22

PDU Information at Device: PC1

At Device: PC1  
Source: PC1  
Destination: 192.168.2.2

In Layers	Out Layers
Layer7	Layer 7: DNS
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: UDP Src Port: 1034, Dst Port: 53
Layer3	Layer 3: IP Header Src. IP: 192.168.2.12, Dest. IP: 192.168.2.2
Layer2	Layer 2: Ethernet II Header 0050.0F15.515B >> 00D0.BC8E.84D3
Layer1	Layer 1: Port(s): FastEthernet0

1. The DNS client sends a DNS query to the DNS server.

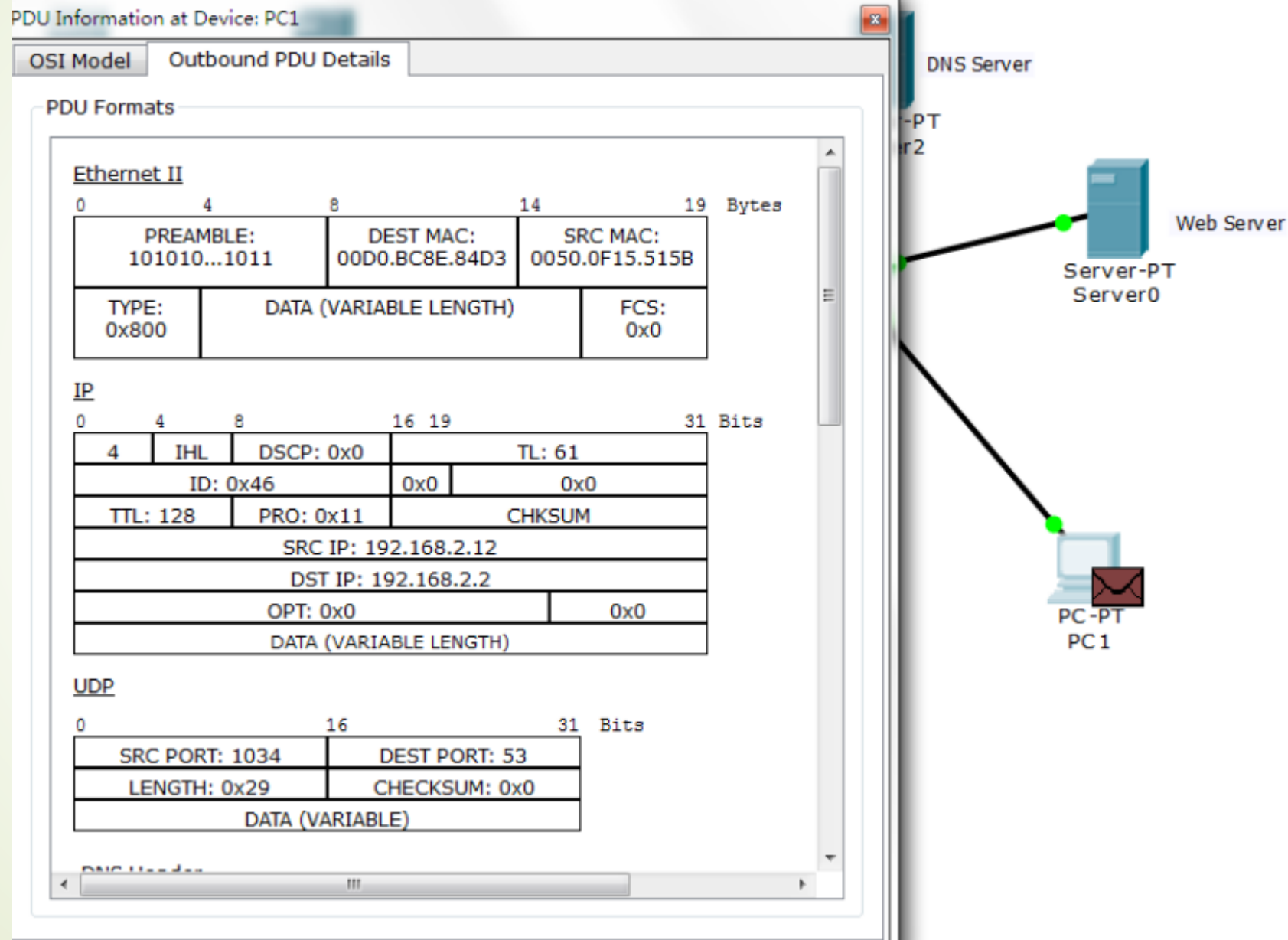
Challenge Me

<< Previous Layer    Next Layer >>

The diagram shows a network topology. On the left, there is a PC labeled 'C-PT PC0'. In the center, there is a server labeled 'Server-PT Server0'. On the right, there is a web server labeled 'Web Server'. A line connects 'C-PT PC0' to 'Server-PT Server0'. Another line connects 'Server-PT Server0' to 'Web Server'. A green dot is visible on the line connecting 'C-PT PC0' to 'Server-PT Server0', indicating the location of the PDU capture.

# Packet Tracer 分析UDP报文

23





# Packet Tracer 分析UDP报文

24

PDU Information at Device: Switch1

OSI Model   Inbound PDU Details   Outbound PDU Details

At Device: Switch1  
Source: PC1  
Destination: 192.168.2.2

**In Layers**

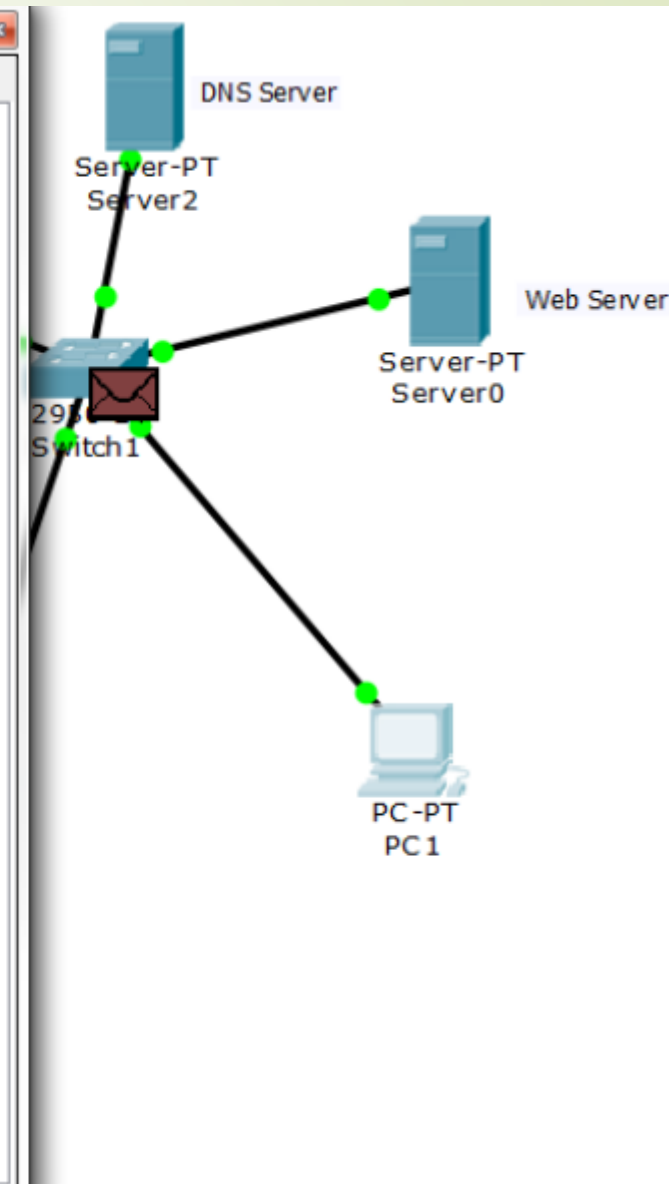
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0050.0F15.515B >> 00D0.BC8E.84D3
Layer 1: Port FastEthernet0/2

**Out Layers**

Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0050.0F15.515B >> 00D0.BC8E.84D3
Layer 1: Port(s): FastEthernet0/1 FastEthernet0/3 FastEthernet0/4 FastEthernet0/5

1. FastEthernet0/2 receives the frame.

Challenge Me   << Previous Layer   Next Layer >>



# Packet Tracer 分析UDP报文

25

The image displays two identical screenshots of the 'PDU Information at Device: Switch1' window in Packet Tracer. The window is divided into three tabs: 'OSI Model', 'Inbound PDU Details', and 'Outbound PDU Details'. The 'Inbound PDU Details' tab is selected, showing the 'PDU Formats' section. This section displays the structure of an Ethernet II, IP, and UDP packet. The Ethernet II section shows a preamble, destination MAC (00D0.BC8E.84D3), source MAC (0050.0F15.515B), type (0x800), and data (variable length). The IP section shows a header with fields like IHL, DSCP, TL, ID, TTL, PRO, and checksum, along with source and destination IP addresses (192.168.2.12 and 192.168.2.2). The UDP section shows source and destination ports (1034 and 53), length, and checksum.

**PDU Information at Device: Switch1**

OSI Model Inbound PDU Details Outbound PDU Details

**PDU Formats**

**Ethernet II**

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 00D0.BC8E.84D3		SRC MAC: 0050.0F15.515B	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

**IP**

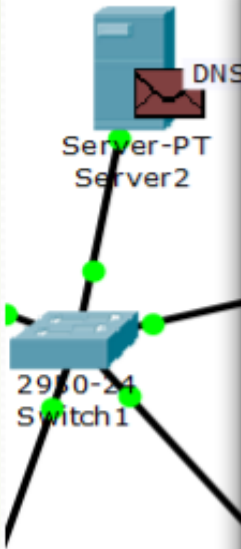
0	4	8	16	19	31	Bits
4		IHL	DSCP: 0x0		TL: 61	
ID: 0x46				0x0		0x0
TTL: 128		PRO: 0x11		CHKSUM		
SRC IP: 192.168.2.12						
DST IP: 192.168.2.2						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

**UDP**

0	16	31	Bits
SRC PORT: 1034		DEST PORT: 53	
LENGTH: 0x29		CHECKSUM: 0x0	
DATA (VARIABLE)			

# Packet Tracer 分析UDP报文

26



Server-PT Server2

2950-24 Switch1

DNS

### PDU Information at Device: Server2

OSI Model   Inbound PDU Details   Outbound PDU Details

At Device: Server2  
Source: PC1  
Destination: 192.168.2.2

In Layers	Out Layers
Layer 7: DNS	Layer 7: DNS
Layer 6	Layer 6
Layer 5	Layer 5
Layer 4: UDP Src Port: 1034, Dst Port: 53	Layer 4: UDP Src Port: 53, Dst Port: 1034
Layer 3: IP Header Src. IP: 192.168.2.12, Dest. IP: 192.168.2.2	Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.2.12
Layer 2: Ethernet II Header 0050.0F15.515B >> 00D0.BC8E.84D3	Layer 2: Ethernet II Header 00D0.BC8E.84D3 >> 0050.0F15.515B
Layer 1: Port FastEthernet0	Layer 1: Port(s): FastEthernet0

1. FastEthernet0 receives the frame.

Challenge Me   << Previous Layer   Next Layer >>

# Packet Tracer 分析UDP报文

27

PDU Information at Device: Server2

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 00D0.BC8E.84D3		SRC MAC: 0050.0F15.515B	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4		IHL		DSCP: 0x0		TL: 61
ID: 0x46				0x0		0x0
TTL: 128		PRO: 0x11		CHKSUM		
SRC IP: 192.168.2.12						
DST IP: 192.168.2.2						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

UDP

0	16	31	Bits
SRC PORT: 1034		DEST PORT: 53	
LENGTH: 0x29		CHECKSUM: 0x0	
DATA (VARIABLE)			

PDU Information at Device: Server2

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 0050.0F15.515B		SRC MAC: 00D0.BC8E.84D3	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

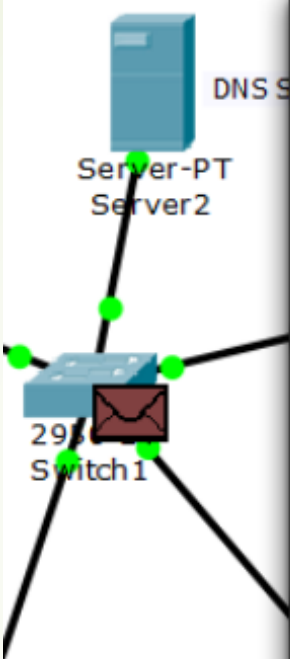
IP

0	4	8	16	19	31	Bits
4		IHL		DSCP: 0x0		TL: 92
ID: 0xc				0x0		0x0
TTL: 128		PRO: 0x11		CHKSUM		
SRC IP: 192.168.2.2						
DST IP: 192.168.2.12						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

UDP

0	16	31	Bits
SRC PORT: 53		DEST PORT: 1034	
LENGTH: 0x48		CHECKSUM: 0x0	
DATA (VARIABLE)			

# Packet Tracer 分析UDP报文



PDU Information at Device: Switch1

OSI Model   Inbound PDU Details   Outbound PDU Details

At Device: Switch1  
Source: PC1  
Destination: 192.168.2.2

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 00D0.BC8E.84D3 >> 0050.0F15.515B	Layer 2: Ethernet II Header 00D0.BC8E.84D3 >> 0050.0F15.515B
Layer 1: Port FastEthernet0/5	Layer 1: Port(s): FastEthernet0/2

1. FastEthernet0/5 receives the frame.

Challenge Me   << Previous Layer   Next Layer >>



# Packet Tracer 分析UDP报文

PDU Information at Device: Switch1

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

PREAMBLE: 101010...1011	DEST MAC: 0050.0F15.515B	SRC MAC: 00D0.BC8E.84D3
TYPE: 0x800	DATA (VARIABLE LENGTH)	FCS: 0x0

IP

0	4	8	16	19	31 Bits
4	4	8	16	19	31
IHL		DSCP: 0x0		TL: 92	
ID: 0xc		0x0		0x0	
TTL: 128		PRO: 0x11		CHKSUM	
SRC IP: 192.168.2.2					
DST IP: 192.168.2.12					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

UDP

0	16	31 Bits
SRC PORT: 53		DEST PORT: 1034
LENGTH: 0x48		CHECKSUM: 0x0
DATA (VARIABLE)		

DNS Header

0	1	5	8	9	12	15 Bits

PDU Information at Device: Switch1

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

101010...1011	0050.0F15.515B	00D0.BC8E.84D3
TYPE: 0x800	DATA (VARIABLE LENGTH)	FCS: 0x0

IP

0	4	8	16	19	31 Bits
4	4	8	16	19	31
IHL		DSCP: 0x0		TL: 92	
ID: 0xc		0x0		0x0	
TTL: 128		PRO: 0x11		CHKSUM	
SRC IP: 192.168.2.2					
DST IP: 192.168.2.12					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

UDP

0	16	31 Bits
SRC PORT: 53		DEST PORT: 1034
LENGTH: 0x48		CHECKSUM: 0x0
DATA (VARIABLE)		

DNS Header

0	1	5	8	9	12	15 Bits

# Packet Tracer 分析UDP报文

30

**PDU Information at Device: PC1**

At Device: PC1  
Source: PC1  
Destination: 192.168.2.2

**In Layers**

Layer 7: DNS
Layer 6
Layer 5
Layer 4: UDP Src Port: 53, Dst Port: 1034
Layer 3: IP Header Src. IP: 192.168.2.2, Dest. IP: 192.168.2.12
Layer 2: Ethernet II Header 00D0.BC8E.84D3 >> 0050.0F15.515B
Layer 1: Port FastEthernet0

**Out Layers**

Layer 7
Layer 6
Layer 5
Layer 4
Layer 3
Layer 2
Layer 1

1. FastEthernet0 receives the frame.

**PDU Information at Device: PC1**

**PDU Formats**

**Ethernet II**

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 0050.0F15.515B		SRC MAC: 00D0.BC8E.84D3	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

**IP**

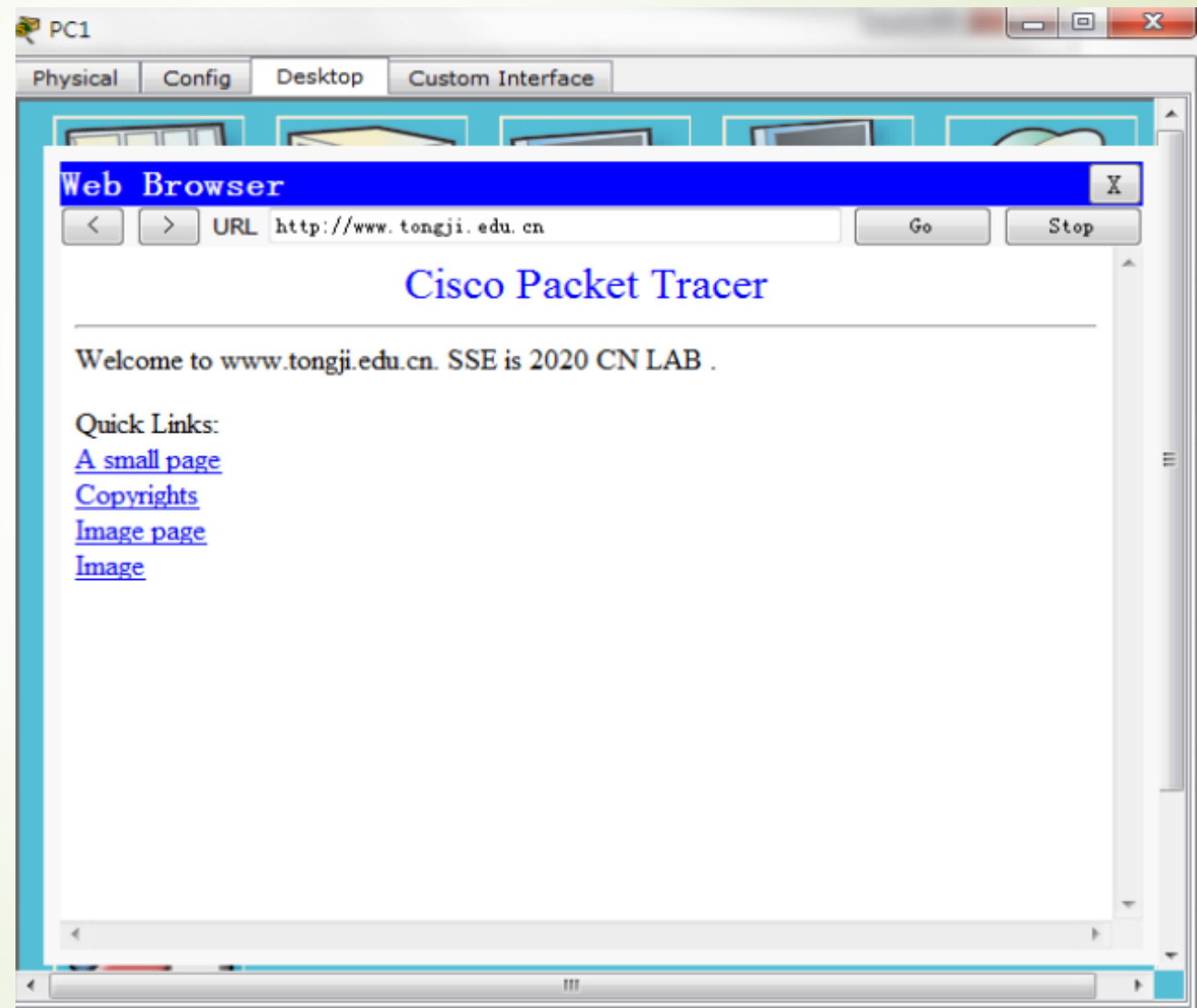
0	4	8	16	19	31	Bits
4		IHL	DSCP: 0x0		TL: 92	
ID: 0xc				0x0	0x0	
TTL: 128		PRO: 0x11		CHKSUM		
SRC IP: 192.168.2.2						
DST IP: 192.168.2.12						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

**UDP**

0	16	31	Bits
SRC PORT: 53		DEST PORT: 1034	
LENGTH: 0x48		CHECKSUM: 0x0	
DATA (VARIABLE)			

# Wireshark UDP报文抓取分析

## ➡ PC1 WEB Browser



# Wireshark UDP报文抓取分析

32

The image displays the Wireshark network protocol analyzer interface. The top pane shows a list of captured packets, filtered by 'udp'. The middle pane shows the details of the selected packet (No. 1498), and the bottom pane shows the raw data in hexadecimal and ASCII.

**Packet List:**

No.	Time	Source	Destination	Protocol	Info
680	25.692414	192.168.1.4	224.0.0.251	MDNS	Standard query PTR _companion-link._tcp.local, "QM" question PTR
681	25.692414	fe80::1c3a:8be:de05:6e6b	ff02::fb	MDNS	Standard query PTR _companion-link._tcp.local, "QM" question PTR
794	30.000639	192.168.1.5	49.65.180.163	UDP	Source port: 15662 Destination port: 15774
918	34.703216	192.168.1.4	224.0.0.251	MDNS	Standard query PTR _companion-link._tcp.local, "QM" question PTR
919	34.703217	fe80::1c3a:8be:de05:6e6b	ff02::fb	MDNS	Standard query PTR _companion-link._tcp.local, "QM" question PTR
1088	40.000865	192.168.1.5	49.65.180.163	UDP	Source port: 15662 Destination port: 15774
1107	40.466340	fe80::65b1:5003:1e0f:6db4	fe80::1	DNS	Standard query A hq.sinajs.cn
1120	40.471969	fe80::1	fe80::65b1:5003:1e0f:6db4	DNS	Standard query response CNAME idc-hq-nfjd.sinajs.cn CNAME idc-hq-n
1122	40.472245	fe80::65b1:5003:1e0f:6db4	fe80::1	DNS	Standard query AAAA hq.sinajs.cn
1124	40.476847	fe80::1	fe80::65b1:5003:1e0f:6db4	DNS	Standard query response CNAME idc-hq-nfjd.sinajs.cn CNAME idc-hq-n
1294	41.857893	192.168.1.5	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
1331	42.858907	192.168.1.5	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
1352	43.858974	192.168.1.5	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
1383	44.858988	192.168.1.5	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
1498	50.001060	192.168.1.5	49.65.180.163	UDP	Source port: 15662 Destination port: 15774

**Packet Details (Frame 1498):**

- Frame 529: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
- Ethernet II, Src: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2), Dst: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)
- Internet Protocol, Src: 192.168.1.5 (192.168.1.5), Dst: 49.65.180.163 (49.65.180.163)
- User Datagram Protocol, Src Port: 15662 (15662), Dst Port: 15774 (15774)
  - Source port: 15662 (15662)
  - Destination port: 15774 (15774)
  - Length: 34
  - Checksum: 0x4344 [validation disabled]
    - [Good checksum: False]
    - [Bad checksum: False]
  - Data (26 bytes)
    - Data: 6f7261790307021800002e3d9e3d01000000000000000000...
    - [Length: 26]

**Packet Details (Frame 529):**

- Frame 529: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
- Ethernet II, Src: ac:fd:ce:3e:9c:a2 (ac:fd:ce:3e:9c:a2), Dst: 90:47:3c:6b:51:29 (90:47:3c:6b:51:29)
- Internet Protocol, Src: 192.168.1.5 (192.168.1.5), Dst: 49.65.180.163 (49.65.180.163)
- User Datagram Protocol, Src Port: 15662 (15662), Dst Port: 15774 (15774)
  - Source port: 15662 (15662)
  - Destination port: 15774 (15774)
  - Length: 34
  - Checksum: 0x4344 [validation disabled]
    - [Good checksum: False]
    - [Bad checksum: False]
  - Data (26 bytes)
    - Data: 6f7261790307021800002e3d9e3d01000000000000000000...
    - [Length: 26]

**Raw Data (Hexadecimal):**

```
0000  90 47 3c 6b 51 29 ac fd ce 3e 9c a2 08 00 45 00  .G<kQ)...>...E.
0010  00 36 13 e9 00 00 80 11 7f 3c c0 a8 01 05 31 41  .6.....<....1A
0020  b4 a3 3d 2e 3d 9e 00 22 43 44 6f 72 61 79 03 07  .=.="" CDoray...
0030  02 18 00 00 2e 3d 9e 3d 01 00 00 00 00 00 00 00  .....=.....
0040  00 00 f6 81
```

## 实验主要分析内容

- 1.配置Web服务器，并从客户端查看；
- 2.配置DNS服务器；
- 3.分析在Packet tracer中UDP报文情况；
- 4.用WireShark抓取UDP数据包；
- 5.查看UDP报文字段内容，并解读