

# UDP数据包分析实验

同济大学软件学院

# UDP数据报(用户数据报协议)

## 1. UDP的概述 (User Datagram Protocol, )

UDP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数据报(用户数据报协议)

## 2. 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数据报(用户数据报协议)

## 2. 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数据报(用户数据报协议)

## 2. 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数据报(用户数据报协议)

## 2. UDP的应用特点

UDP是面向报文的，对应用层交下来的报文，添加首部后直接乡下交付为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。比如我们要发送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数据报(用户数据报协议)

## 2. 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）数据的可靠传输对他们而言并不重要，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数据报(用户数据报协议)

## 3. UDP报文格式

### UDP的首部格式

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数据报文结构如图所示：





# UDP数据报(用户数据报协议)

## 3. UDP报文格式

### 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数据报(用户数据报协议)

## 3. UDP报文格式

### 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数据报(用户数据报协议)

## 3. UDP报文格式

### UDP校验

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，而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。

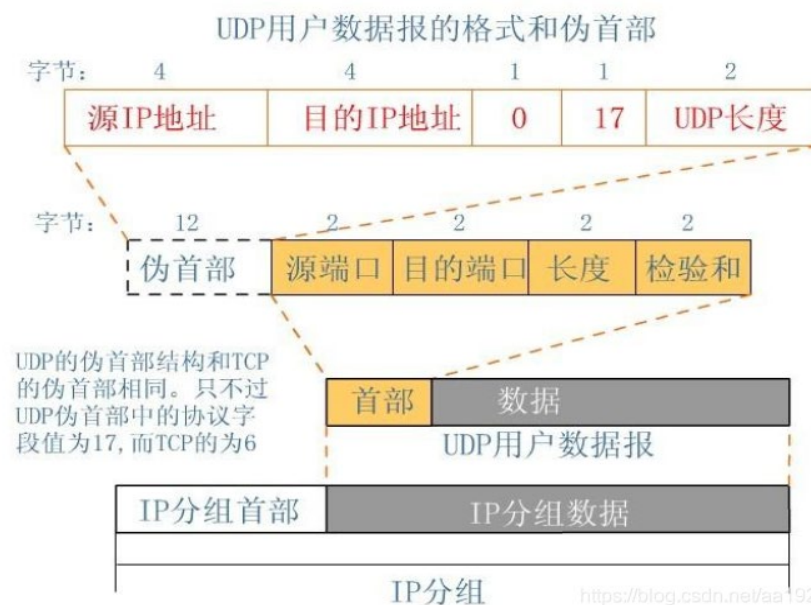


# UDP数据报(用户数据报协议)

## 3. UDP报文格式

### UDP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数据报(用户数据报协议)

## 3. UDP报文格式

### UDP校验

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数据报(用户数据报协议)

## UDP校验

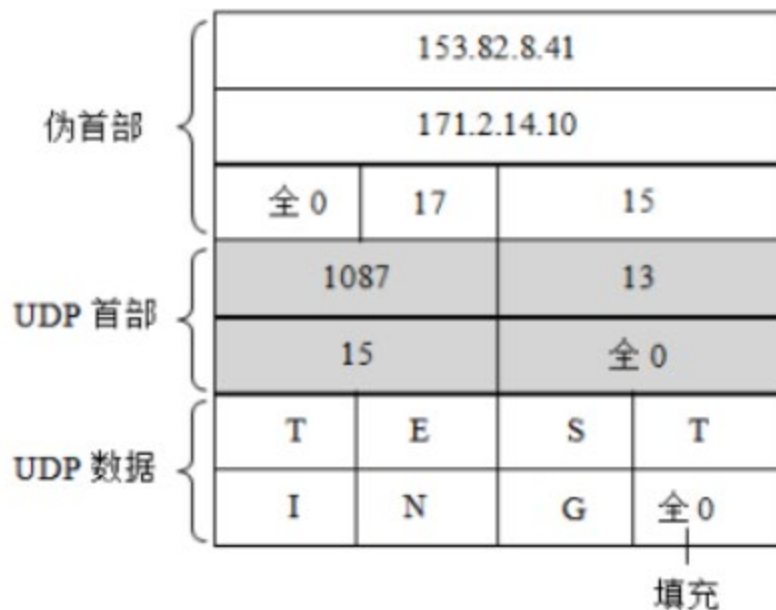
当无差错时其结果全为1,。否则就表明有差错出现,接收方应该丢弃这个UDP数据报。注意: 1). 校验时,若UDP数据报部分的长度不是偶数个字节,则需要填入一个全0字节,但是此字节和伪首部一样,是不发送的。2).如果UDP校验和校验出UDP数据报是错误的,可以丢弃,也可以交付上层,但是要附上错误报告,告诉上层这是错误的的数据报。3).通过伪首部,不仅可以检查源端口号,目的端口号和UDP用户数据报的数据部分,还可以检查IP数据报的源IP地址和目的地址。这种差错检验的检错能力不强,但是简单,速度快。



# UDP数据报(用户数据报协议)

## UDP校验示例

### 计算UDP校验和的例子



10011001 01010010 → 153.82  
00001000 00101001 → 8.41  
10101011 00000010 → 171.2  
00001110 00001010 → 14.10  
00000000 00010001 → 0 和 17  
00000000 00001111 → 15  
00000100 00111111 → 1087  
00000000 00001101 → 13  
00000000 00001111 → 15  
00000000 00000000 → 0 (校验和初始值)  
01010100 01000101 → T 和 E  
01010011 01010100 → S 和 T  
01001001 01001110 → I 和 N  
01000111 00000000 → G 和 0 (填充)

10010110 11101011 求和结果

01101001 00010100 校验和

www.jiangon.com

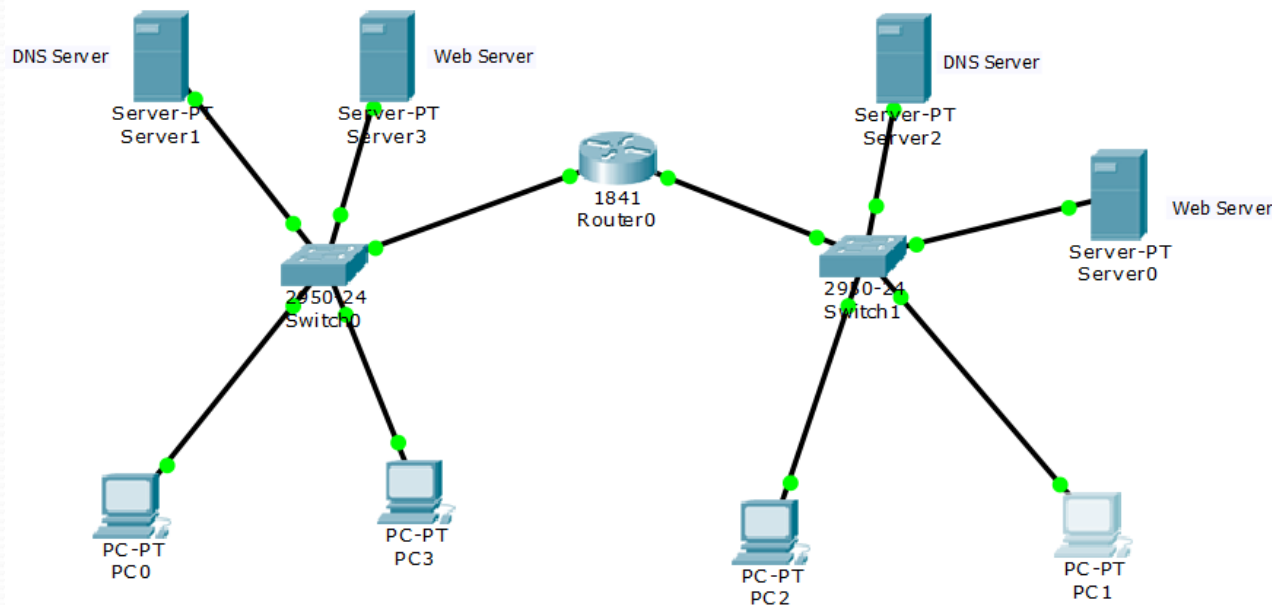
<https://blog.csdn.net/aa1928992772>

# UDP数据报(用户数据报协议)

## 4.Packet Tracer 分析UDP报文

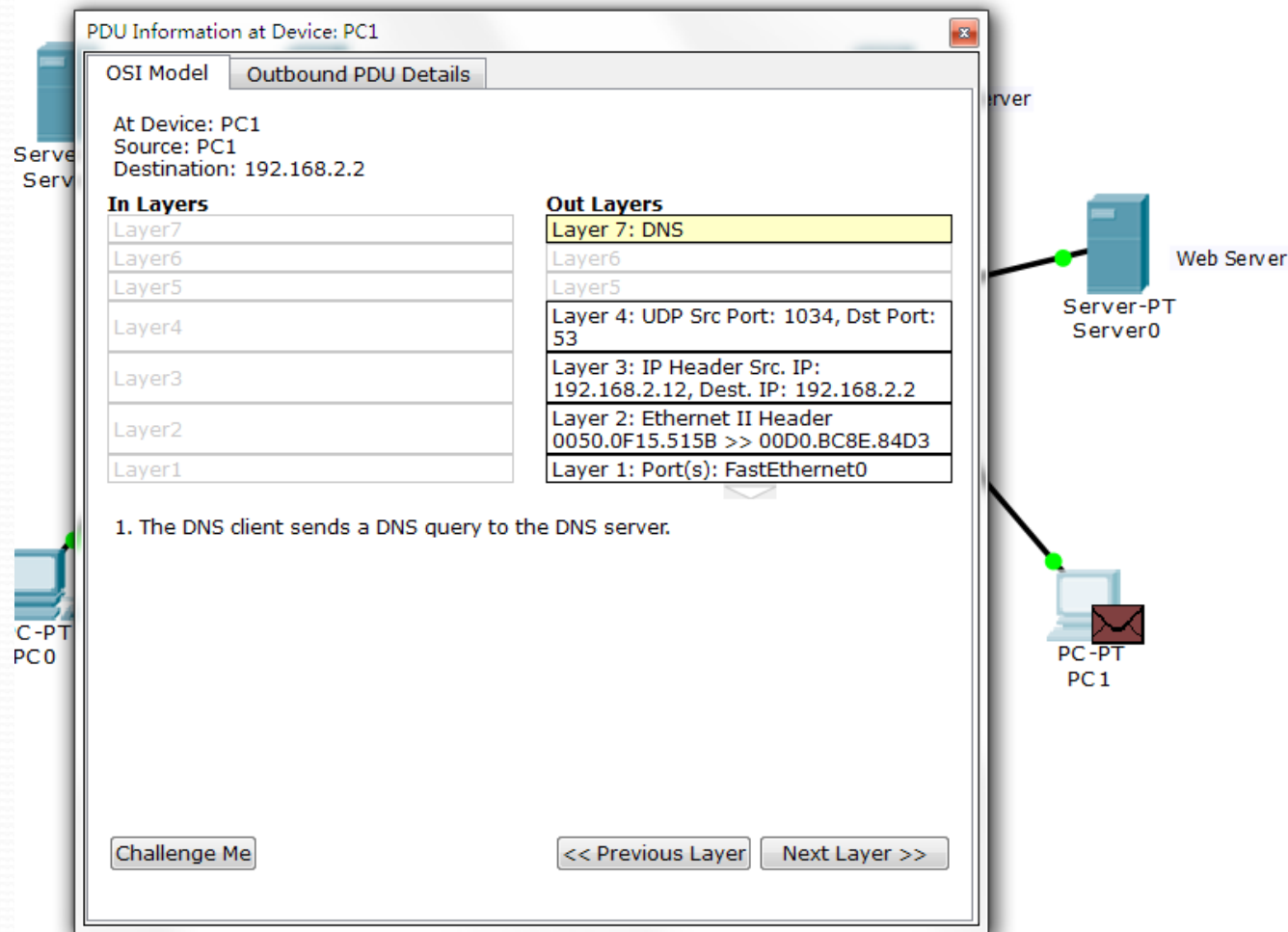
### 网络结构图

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。



# UDP协议

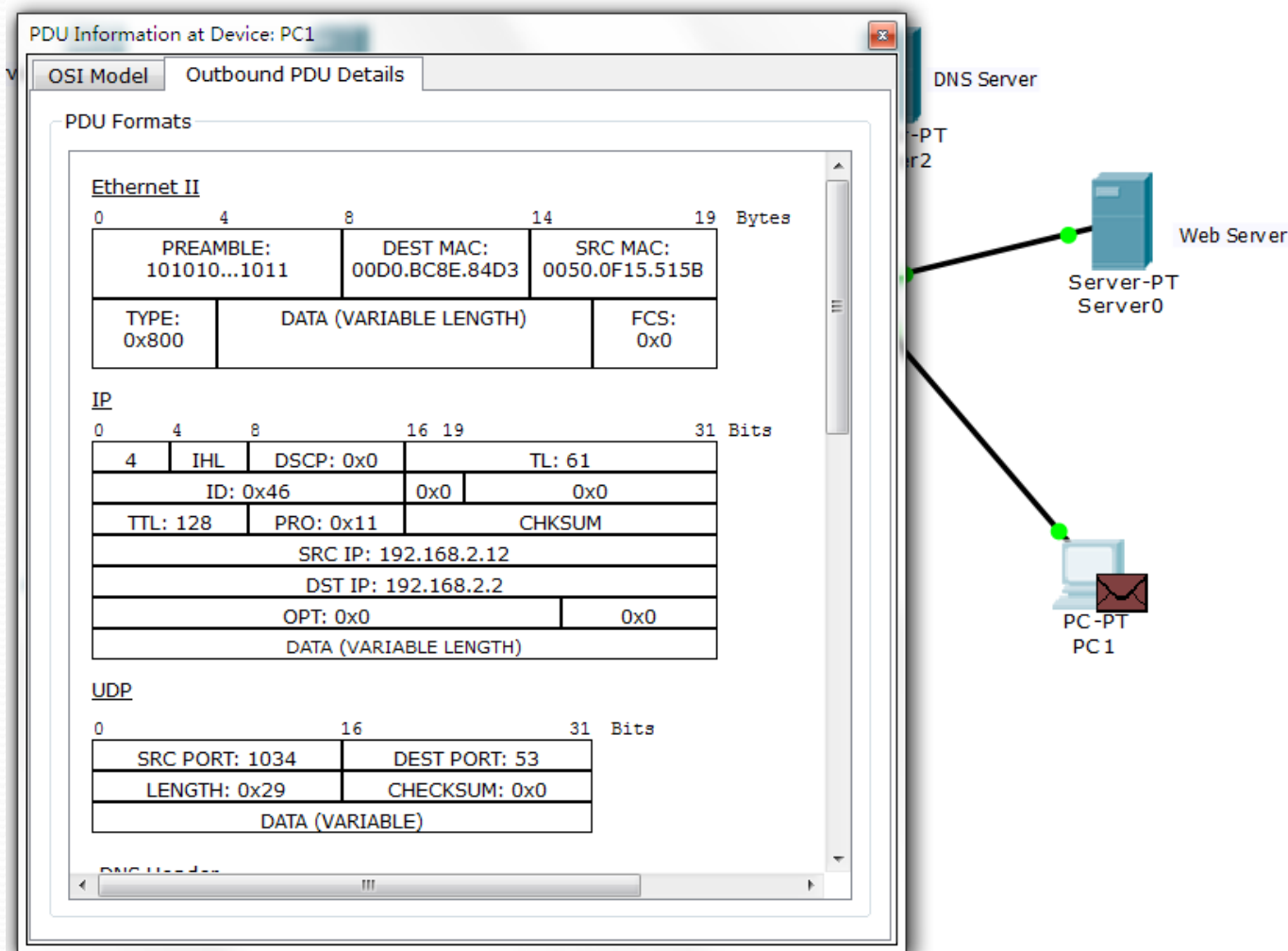
## 4 .Packet Tracer 分析UDP报文





# UDP协议

## 4 .Packet Tracer 分析UDP报文



# UDP协议

## 4 .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**

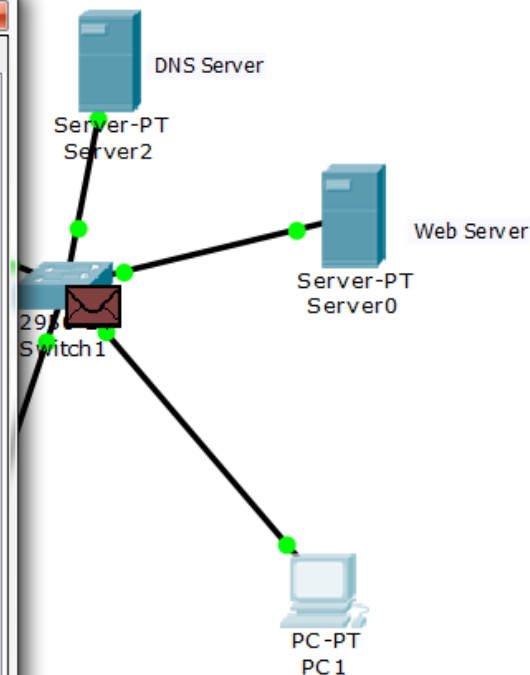
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 0050.0F15.515B >> 00D0.BC8E.84D3
Layer 1: Port FastEthernet0/2

**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 >>



## 4 .Packet Tracer 分析UDP报文

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)							

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)												

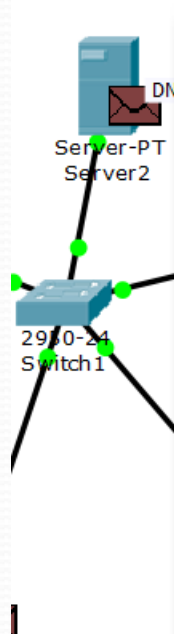
UDP

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



# UDP协议

## 4 .Packet Tracer 分析UDP报文



**PDU Information at Device: Server2**

At Device: Server2  
Source: PC1  
Destination: 192.168.2.2

OSI Model	Inbound PDU Details	Outbound PDU Details
<b>In Layers</b>		<b>Out Layers</b>
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 >>

## 4 .Packet Tracer 分析UDP报文

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

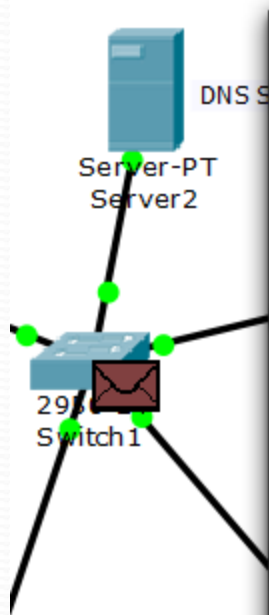
0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 92			
ID: 0xc		0x0	0x0			
TTL: 128		PRO: 0x11	CHKSUM			
SRC IP: 192.168.2.2						
DST IP: 192.168.2.12						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

UDP

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

# UDP协议

## 4 .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 >>



## 4 .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	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

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	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

# UDP协议

## 4 .Packet Tracer 分析UDP报文

PDU Information at Device: PC1

OSI Model Inbound PDU Details

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.

Challenge Me << Previous Layer Next Layer >>

Server-PT Server0

PC-PT PC1

PDU Information at Device: PC1

OSI Model Inbound 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**

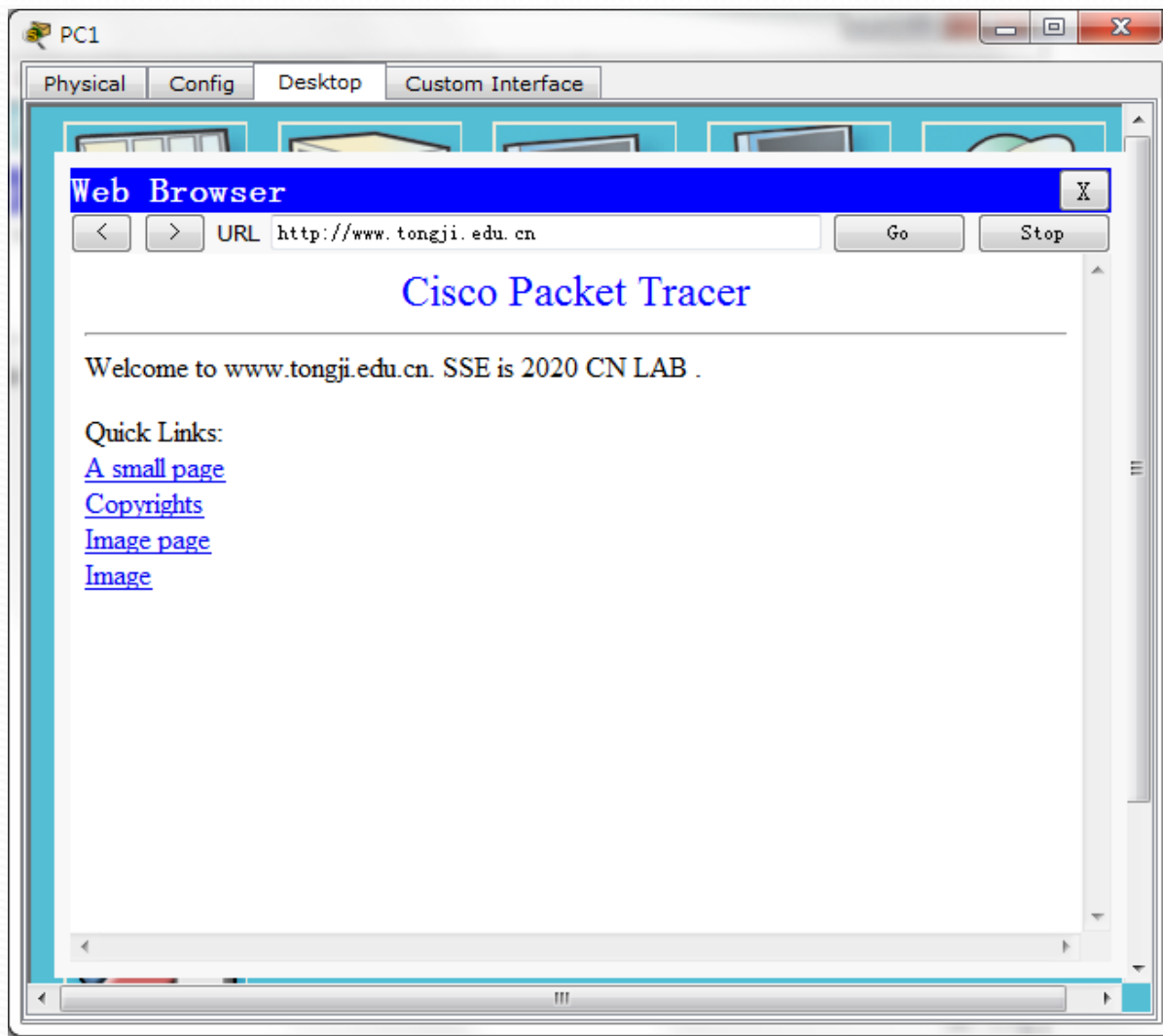
0 4 8 16 19 31 Bits		
IHL: 4	DSCP: 0x0	TL: 92
ID: 0xc	0x0	0x0
TTL: 128	PRO: 0x11	CHKSUM
SRC IP: 192.168.2.2		
DST IP: 192.168.2.12		
OPT: 0x0		0x0
DATA (VARIABLE LENGTH)		

**UDP**

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

# UDP协议

## 4. Packet Tracer 分析报文 PC1 WEB Browser





# 5. Wireshark UDP报文抓取分析

Capturing from Microsoft - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: udp Expression... Clear Apply

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

- 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: 6f7261790307021800002e3d9e3d010000000000000000...
  - [Length: 26]

529 20.000427 192.168.1.5 49.65.180.163 UDP Source port: 15662 Destination port: 15774

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: 6f7261790307021800002e3d9e3d010000000000000000...
  - [Length: 26]

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；