

Linux Networking: udp

David Morgan

© David Morgan 2003-2013

UDP

- Stateless, unreliable transport protocol with no delivery guarantee
- performance over reliability
- well suited to broadcast and discovery type messaging
- RFC 768 and RFC 1122 (STD 6)

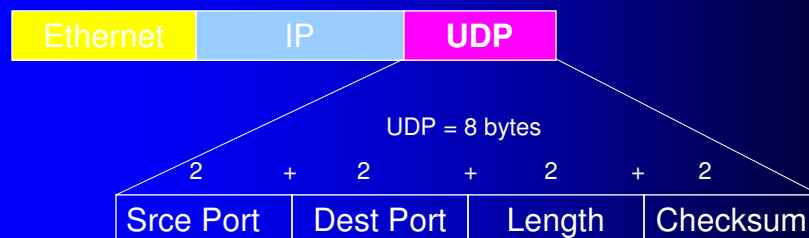
© David Morgan 2003-2013

UDP Ports

- UDP multiplexes among various upper layer protocols by using PORTS
- 16 bit port numbers are assigned to specific applications by UDP
- Some UDP ports use "Well Known" numbers (53 DNS, 69 TFTP etc)

© David Morgan 2003-2013

UDP header



© David Morgan 2003-2013

UDP Header

- Source Port - originator of the data
 - Not required can legally be 0
- Destination Port - destination application
- Length - length of the UDP header and following data
- Checksum - over IP "pseudo header", UDP header and data
 - Optional - can be left 0xFFFF

© David Morgan 2003-2013

UDP checksum

- To detect errors (sent-vs-received mismatch)
- Sender algorithm
 - sum all 16-bit words in packet
 - take binary 1's-complement
 - place in checksum field
- Receiver algorithm
 - sum all 16-bit words in packet
 - add to that the checksum
 - result should be 1111111111111111

© David Morgan 2003-2013

Algorithm example

data:
in ASCII- A B C D
in binary- 01000001 01000010 01000011 01000100

sum: 01000001 01000010
 01000011 01000100
 10000100 10000110

1's-comp: 01111011 01111001
(checksum)

**these add to
11111111 11111111
so had better sum of
received data plus
received checksum**

© David Morgan 2003-2013

Who uses UDP instead of TCP?

- streaming applications
- discovery tools
- certain application protocols
 - DNS
 - TFTP
 - traceroute

© David Morgan 2003-2013

UDP Trace (traceroute -m1 www.ucla.edu)

The screenshot displays a network capture in Wireshark. The packet list pane shows the following entries:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	66.159.240.70	66.51.205.100	DNS	Standard query A www.ucla.edu
2	0.023184	66.51.205.100	66.159.240.70	DNS	Standard query response A 169.232.56.135[Short Frame]
3	0.026552	66.159.240.70	169.232.56.135	UDP	Source port: 1048 Destination port: 33435
4	0.045266	66.159.240.1	66.159.240.70	ICMP	Time-to-live exceeded
5	0.076306	66.159.240.70	169.232.56.135	UDP	Source port: 1048 Destination port: 33436
6	0.094790	66.159.240.1	66.159.240.70	ICMP	Time-to-live exceeded
7	0.095518	66.159.240.70	169.232.56.135	UDP	Source port: 1048 Destination port: 33437
8	0.114716	66.159.240.1	66.159.240.70	ICMP	Time-to-live exceeded

The packet details pane for the selected packet (Frame 1) shows the following structure:

- Ethernet II
- Internet Protocol Version 4, Src: 66.159.240.70 (66.159.240.70), Dst Addr: 66.51.205.100 (66.51.205.100)
- User Datagram Protocol, Src Port: 1048 (1048), Dst Port: 33 (33)
- Source port: 1048 (1048)
- Destination port: 33 (33)
- Length: 38
- Checksum: 0x202f (correct)
- Domain Name System (query)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 10 67 00 d3 72 00 60 08 96 ab b2 08 00 45 00  .g..r. ....E.  
0010 00 3a 13 0b 40 00 40 11 85 2a 42 9f f0 46 42 33  .:..B..B..FB3  
0020 cd 64 00 00 00 00 00 00 00 00 00 00 00 00 00  .g.....m..  
0030 00 00 00 00 00 00 03 77 77 77 04 75 63 6c 61 03  .....w www.ucla.  
0040 65 64 75 00 00 01 00 01  .edu.....
```