# 1. NANO-GUIDE TCP/IP et tcpdump

Fichier PDF

## 1.1. Acronymes

**Acronyms**

| | | | |
|---|---|---|---|
| AH | Authentication Header (RFC 2402) | ISAKMP | Internet Security Association & Key Management Protocol (RFC 2408) |
| ARP | Address Resolution Protocol (RFC 826) | | |
| BGP | Border Gateway Protocol (RFC 1771) | L2TP | Layer 2 Tunneling Protocol (RFC 2661) |
| CWR | Congestion Window Reduced (RFC 2481) | NNTP | Network News Transfer Protocol (RFC 977) |
| DF | Don't Fragment bit (IP) | OSPF | Open Shortest Path First (RFC 1583) |
| DHCP | Dynamic Host Configuration Protocol (RFC 2131) | POP3 | Post Office Protocol v3 (RFC 1460) |
| DNS | Domain Name System (RFC 1035) | RFC | Request for Comments |
| ECN | Explicit Congestion Notification (RFC 3168) | RIP | Routing Information Protocol (RFC 2453) |
| EIGRP | Extended IGRP (Cisco) | LDAP | Lightweight Directory Access Protocol (RFC 2251) |
| ESP | Encapsulating Security Payload (RFC 2406) | SKIP | Simple Key-Management for Internet Protocols |
| FTP | File Transfer Protocol (RFC 959) | SMTP | Simple Mail Transfer Protocol (RFC 821) |
| GRE | Generic Routing Encapsulation (RFC 2784) | SNMP | Simple Network Management Protocol (RFC 1157) |
| HTTP | Hypertext Transfer Protocol (RFC 1945) | SSH | Secure Shell |
| ICMP | Internet Control Message Protocol (RFC 792) | SSL | Secure Sockets Layer (Netscape) |
| IGMP | Internet Group Management Protocol (RFC 2236) | TCP | Transmission Control Protocol (RFC 793) |
| IGRP | Interior Gateway Routing Protocol (Cisco) | TFTP | Trivial File Transfer Protocol (RFC 1350) |
| IMAP | Internet Message Access Protocol (RFC 2060) | TOS | Type of Service field (IP) |
| IP | Internet Protocol (RFC 791) | UDP | User Datagram Protocol (RFC 768) |

***All RFCs can be found at http://www.rfc-editor.org***

## 1.2. tcpdump

**tcpdump Usage**

```
tcpdump  [-aenStvx]  [-F file]
[-i int]  [-r file]  [-s snaplen]
[-w file]  ['filter_expression']

-e  Display data link header.
-F  Filter expression in file.
-i  Listen on int interface.
-n  Don't resolve IP addresses.
-r  Read packets from file.
-s  Get snaplen bytes from each packet.
-S  Use absolute TCP sequence numbers.
-t  Don't print timestamp.
-v  Verbose mode.
-w  Write packets to file.
-x  Display in hex.
-X  Display in hex and ASCII.
```

## 1.3. DNS

## DNS

Bit Number

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ID. | | | | | | | | | | | | | | | |
| QR | Opcode | | | | AA | TC | RD | RA | Z | | | | RCODE | | |
| QDCOUNT | | | | | | | | | | | | | | | |
| ANCOUNT | | | | | | | | | | | | | | | |
| NSCOUNT | | | | | | | | | | | | | | | |
| ARCOUNT | | | | | | | | | | | | | | | |
| Question Section | | | | | | | | | | | | | | | |
| Answer Section | | | | | | | | | | | | | | | |
| Authority Section | | | | | | | | | | | | | | | |
| Additional Information Section | | | | | | | | | | | | | | | |

### DNS Parameters

**Query/Response**
0 Query
1 Response

**Opcode**
0 Standard query (QUERY)
1 Inverse query (IQUERY)
2 Server status request (STATUS)

**AA**
(1 = Authoritative Answer)

**TC**
(1 = TrunCation)

**RD**
(1 = Recursion Desired)

**RA**
(1 = Recursion Available)

**Z**
(Reserved; set to 0)

**Response code**
0 No error
1 Format error
2 Server failure
3 Non-existant domain (NXDOMAIN)
4 Query type not implemented
5 Query refused

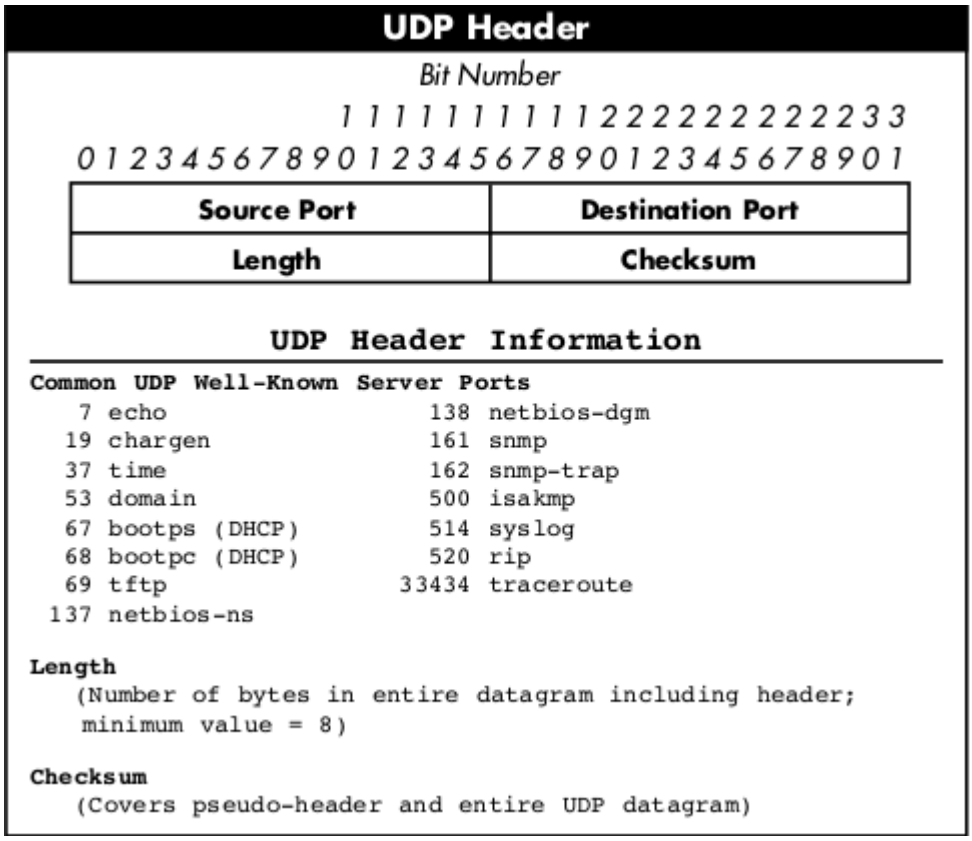
**QDCOUNT**
(No. of entries in Question section)

**ANCOUNT**
(No. of resource records in Answer section)

**NSCOUNT**
(No. of name server resource records in Authority section)

**ARCOUNT**
(No. of resource records in Additional Information section.

## 1.4. Entête UDP



**UDP Header**

Bit Number

1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

| Source Port | Destination Port |
|---|---|
| Length | Checksum |

**UDP Header Information**

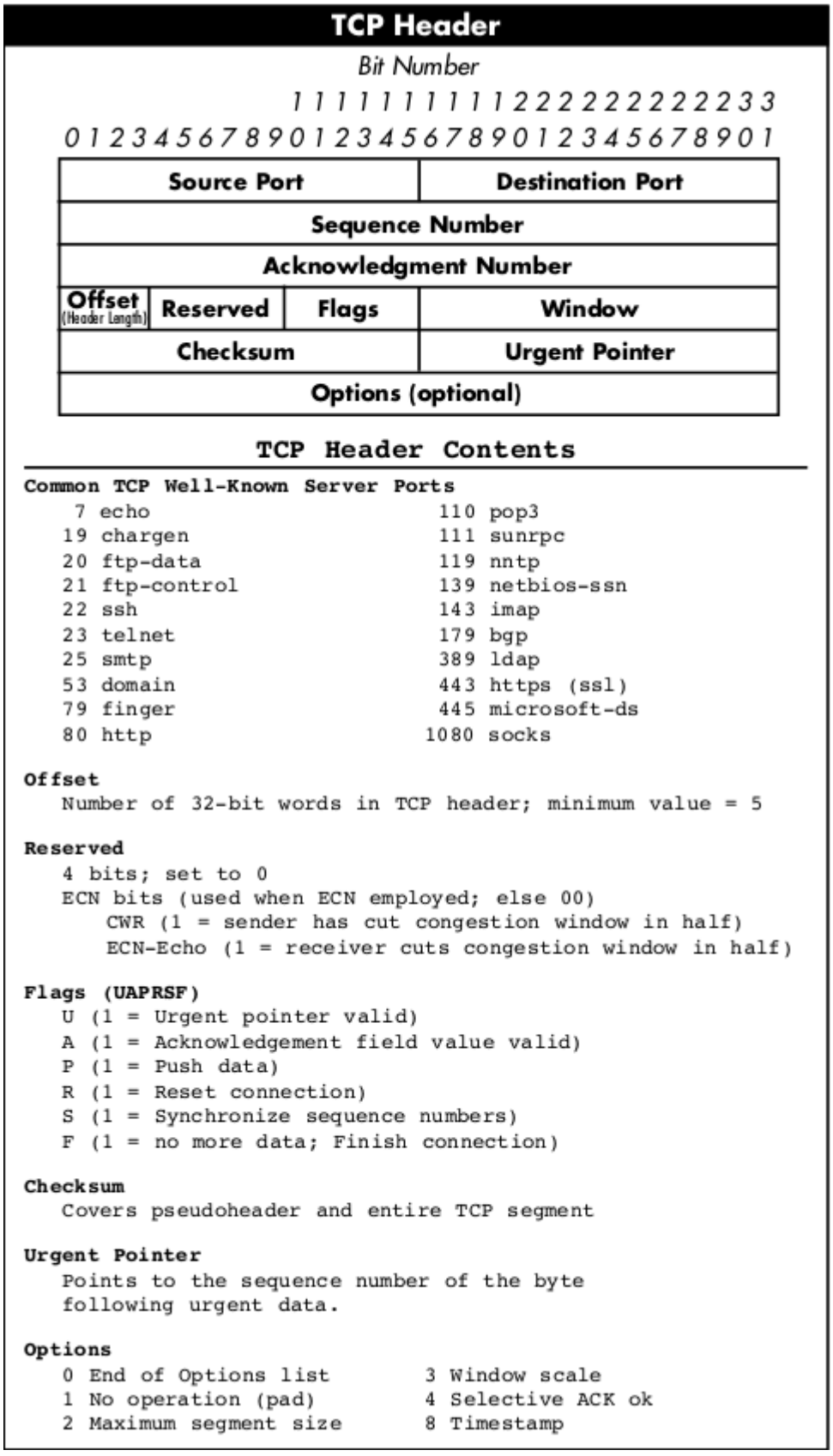
**Common UDP Well-Known Server Ports**

| | | | |
|---|---|---|---|
| 7 | echo | 138 | netbios-dgm |
| 19 | chargen | 161 | snmp |
| 37 | time | 162 | snmp-trap |
| 53 | domain | 500 | isakmp |
| 67 | bootps (DHCP) | 514 | syslog |
| 68 | bootpc (DHCP) | 520 | rip |
| 69 | tftp | 33434 | traceroute |
| 137 | netbios-ns | | |

**Length**
(Number of bytes in entire datagram including header; minimum value = 8)

**Checksum**
(Covers pseudo-header and entire UDP datagram)

## 1.5. Entête TCP



**TCP Header**

*Bit Number*

*1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3*
*0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1*

| Source Port | | | Destination Port |
|---|---|---|---|
| Sequence Number | | | |
| Acknowledgment Number | | | |
| Offset (Header Length) | Reserved | Flags | Window |
| Checksum | | | Urgent Pointer |
| Options (optional) | | | |

**TCP Header Contents**

**Common TCP Well-Known Server Ports**

```
  7 echo                      110 pop3
 19 chargen                   111 sunrpc
 20 ftp-data                  119 nntp
 21 ftp-control               139 netbios-ssn
 22 ssh                       143 imap
 23 telnet                    179 bgp
 25 smtp                      389 ldap
 53 domain                    443 https (ssl)
 79 finger                    445 microsoft-ds
 80 http                     1080 socks
```

**Offset**
Number of 32-bit words in TCP header; minimum value = 5

**Reserved**
4 bits; set to 0
ECN bits (used when ECN employed; else 00)
CWR (1 = sender has cut congestion window in half)
ECN-Echo (1 = receiver cuts congestion window in half)

**Flags (UAPRSF)**
U (1 = Urgent pointer valid)
A (1 = Acknowledgement field value valid)
P (1 = Push data)
R (1 = Reset connection)
S (1 = Synchronize sequence numbers)
F (1 = no more data; Finish connection)

**Checksum**
Covers pseudoheader and entire TCP segment

**Urgent Pointer**
Points to the sequence number of the byte following urgent data.

**Options**

```
0 End of Options list        3 Window scale
1 No operation (pad)         4 Selective ACK ok
2 Maximum segment size       8 Timestamp
```

## 1.6. Entête IP

## TCP Header

Bit Number

1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

| Source Port | | | Destination Port |
|---|---|---|---|
| Sequence Number | | | |
| Acknowledgment Number | | | |
| Offset (Header Length) | Reserved | Flags | Window |
| Checksum | | | Urgent Pointer |
| Options (optional) | | | |

### TCP Header Contents

**Common TCP Well-Known Server Ports**

```
  7 echo                      110 pop3
 19 chargen                   111 sunrpc
 20 ftp-data                  119 nntp
 21 ftp-control               139 netbios-ssn
 22 ssh                       143 imap
 23 telnet                    179 bgp
 25 smtp                      389 ldap
 53 domain                    443 https (ssl)
 79 finger                    445 microsoft-ds
 80 http                     1080 socks
```

**Offset**
Number of 32-bit words in TCP header; minimum value = 5

**Reserved**
4 bits; set to 0
ECN bits (used when ECN employed; else 00)
CWR (1 = sender has cut congestion window in half)
ECN-Echo (1 = receiver cuts congestion window in half)

**Flags (UAPRSF)**
U (1 = Urgent pointer valid)
A (1 = Acknowledgement field value valid)
P (1 = Push data)
R (1 = Reset connection)
S (1 = Synchronize sequence numbers)
F (1 = no more data; Finish connection)

**Checksum**
Covers pseudoheader and entire TCP segment

**Urgent Pointer**
Points to the sequence number of the byte following urgent data.

**Options**

```
0 End of Options list        3 Window scale
1 No operation (pad)         4 Selective ACK ok
2 Maximum segment size       8 Timestamp
```

## 1.7. ICMP et PING

## ICMP

Bit Number

1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

| Type | Code | Checksum |
|---|---|---|
| Other message-specific information... | | |

**Type Name/Codes (Code=0 unless otherwise specified)**

```
 0  Echo Reply
 3  Destination Unreachable
     0 Net Unreachable
     1 Host Unreachable
     2 Protocol Unreachable
     3 Port Unreachable
     4 Fragmentation Needed & DF Set
     5 Source Route Failed
     6 Destination Network Unknown
     7 Destination Host Unknown
     8 Source Host Isolated
     9 Network Administratively Prohibited
    10 Host Administratively Prohibited
    11 Network Unreachable for TOS
    12 Host Unreachable for TOS
    13 Communication Administratively Prohibited
 4  Source Quench
 5  Redirect
    0 Redirect Datagram for the Network
    1 Redirect Datagram for the Host
    2 Redirect Datagram for the TOS & Network
    3 Redirect Datagram for the TOS & Host
 8  Echo
 9  Router Advertisement
10  Router Selection
11  Time Exceeded
    0 Time to Live exceeded in Transit
    1 Fragment Reassembly Time Exceeded
12  Parameter Problem
    0 Pointer indicates the error
    1 Missing a Required Option
    2 Bad Length
13  Timestamp
14  Timestamp Reply
15  Information Request
16  Information Reply
17  Address Mask Request
18  Address Mask Reply
30  Traceroute
```

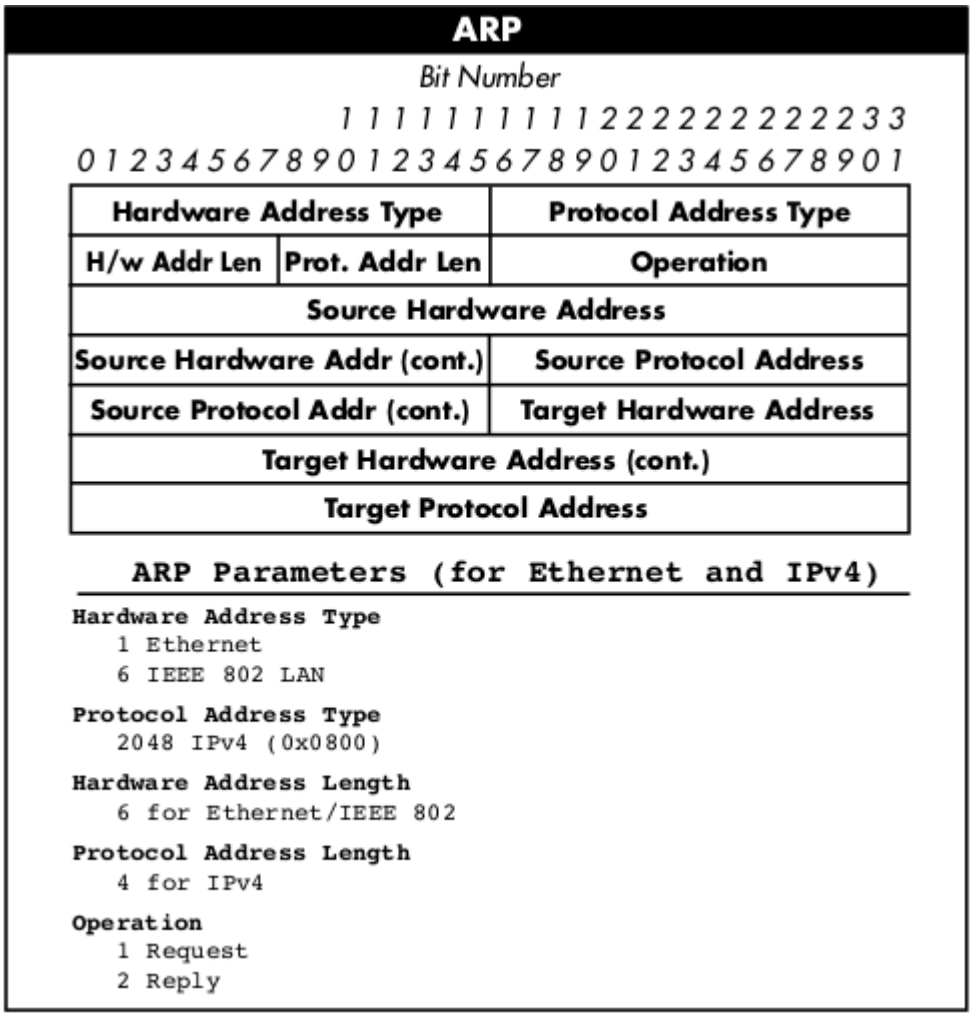
## PING (Echo/Echo Reply)

Bit Number

1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

| Type (8 or 0) | Code (0) | Checksum |
|---|---|---|
| Identifier | | Sequence Number |
| Data... | | |

## 1.8. ARP




From:
https://siocours.lycees.nouvelle-aquitaine.pro/ - **Les cours du BTS SIO**

Permanent link:
**https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/tcpip/accueil**

Last update: **2013/11/28 11:24**