TCP/IP Quick Guide

OSI MODEL

Layer 7: Application Layer
- Defines interface to user processes
- Provides standardized network services

Layer 6: Presentation Layer
- Specifies architecture-independent data transfer format
- Encodes and decodes data; Encrypts and decrypts data; Compresses and decompresses data

Layer 5: Session Layer
- Manages user sessions and dialogues
- Controls establishment and termination of logical links between users

Layer 4: Transport Layer
- Provides reliable and sequential end-to-end packet delivery
- Provides connectionless oriented packet delivery

Layer 3: Network Layer
- Routes packets according to unique network addresses

Layer 2: Data Link Layer
- Defines procedures for operating the communication link
- Provides framing and sequencing

Layer 1: Physical Layer
- Defines physical means of sending data over network devices

Security
- TCP/IP Quick Guide
- OSI Model
- Layer 7: Application Layer
- Layer 6: Presentation Layer
- Layer 5: Session Layer
- Layer 4: Transport Layer
- Layer 3: Network Layer
- Layer 2: Data Link Layer
- Layer 1: Physical Layer
- TCP/IP Quick Guide
- OSI Model
- Layer 7: Application Layer
- Layer 6: Presentation Layer
- Layer 5: Session Layer
- Layer 4: Transport Layer
- Layer 3: Network Layer
- Layer 2: Data Link Layer
- Layer 1: Physical Layer
- TCP/IP Quick Guide
- OSI Model
- Layer 7: Application Layer
- Layer 6: Presentation Layer
- Layer 5: Session Layer
- Layer 4: Transport Layer
- Layer 3: Network Layer
- Layer 2: Data Link Layer
- Layer 1: Physical Layer
- TCP/IP Quick Guide
- OSI Model
- Layer 7: Application Layer
- Layer 6: Presentation Layer
- Layer 5: Session Layer
- Layer 4: Transport Layer
- Layer 3: Network Layer
- Layer 2: Data Link Layer
- Layer 1: Physical Layer
- TCP/IP Quick Guide
- OSI Model
- Layer 7: Application Layer
- Layer 6: Presentation Layer
- Layer 5: Session Layer
- Layer 4: Transport Layer
- Layer 3: Network Layer
- Layer 2: Data Link Layer
- Layer 1: Physical Layer
**IP: Internet Protocol**

### IPv4: Internet Protocol version 4

**IPv4 Packet Format**

<table>
<thead>
<tr>
<th>4</th>
<th>8</th>
<th>16</th>
<th>32bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>IHL</td>
<td>Type of Service</td>
<td>Total length</td>
</tr>
<tr>
<td>Identification</td>
<td>Flags</td>
<td>Fragment offset</td>
<td></td>
</tr>
<tr>
<td>Time to live</td>
<td>Protocol</td>
<td>Header checksum</td>
<td></td>
</tr>
</tbody>
</table>

- **Version** - the version of IP (4 for IPv4).
- **IHL** – number of 32-bit words that points to the beginning of the data. It is between 5 (20 bytes) to 15 (60 bytes).
- **Type of Service** – indicates the quality of service desired.
  - **Precedence (000 to 111)**
  - **Differentiated Services**
- **Flags** – includes bit settings for fragment handling.
  - **MF (More Fragment)**
  - **MF (More Fragment)**
- **Fragment Offset** – indicates the offset of the fragments relative to the beginning of the data in the original datagram.
- **Protocol** - indicates which upper-layer protocol receives incoming packets.
  - **ICMP**
  - **IGMP**
  - **TCP**
  - **UDP**
  - **ESP**
  - **AH**
  - **GRE**
  - **ESP**
  - **AH**
- **Header Checksum** – ensures IP header integrity.
- **Source Address** – 32-bit field specifies the sending node.
- **Destination Address** – 32-bit field specifies the receiving node.

**IPv4 Address Classes**

<table>
<thead>
<tr>
<th>Bits</th>
<th>Class</th>
<th>Network</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>A</td>
<td>0</td>
<td>Host</td>
</tr>
<tr>
<td>24</td>
<td>B</td>
<td>10</td>
<td>Host</td>
</tr>
<tr>
<td>16</td>
<td>C</td>
<td>110</td>
<td>Host</td>
</tr>
</tbody>
</table>

**IPv4 Address Format**

```
<table>
<thead>
<tr>
<th>Network-Prefix</th>
<th>Subnet-Number</th>
<th>Host-Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>127</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>128-191</td>
<td>128-191</td>
<td>1</td>
</tr>
<tr>
<td>192-223</td>
<td>192-223</td>
<td>1</td>
</tr>
<tr>
<td>224-239</td>
<td>224-239</td>
<td>1</td>
</tr>
<tr>
<td>240-247</td>
<td>240-247</td>
<td>1</td>
</tr>
</tbody>
</table>
```

**CIDR**

```
CIDR: Classless and Subnet Address Extensions and Supernetting

<table>
<thead>
<tr>
<th>Network</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.0.0.0</td>
<td>255.255.255.248</td>
</tr>
<tr>
<td>172.16.0.0</td>
<td>255.255.255.240</td>
</tr>
<tr>
<td>192.168.0.0</td>
<td>255.255.255.224</td>
</tr>
</tbody>
</table>
```

### IPv6: Internet Protocol version 6

**IPv6 Packet Format**

<table>
<thead>
<tr>
<th>4</th>
<th>12</th>
<th>16</th>
<th>24</th>
<th>32bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Traffic Class</td>
<td>Flow label</td>
<td>Payload length</td>
<td>Next header type</td>
</tr>
<tr>
<td>Source address (128 bits)</td>
<td>Destination address (128 bits)</td>
<td>Extension Header Information (optional and variable length)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Version** - Internet Protocol Version number (IPv6 is 6).
- **Traffic Class** – enables a source to identify the desired delivery priority of the packets.
- **Flow label** - used by source to label packets for special handling by the IPv6 router.
- **Payload length** – the length of the data portion of the packet.
- **Next header type** – identifies the type of header immediately following the IPv6 header. It is similar to the “protocol” field in IPv4.
- **Hop limit** – specifies the maximum number of routers (hops) through which a packet can traverse before discarded.
- **Source address** – 128-bit address of the originator of the packet.
- **Destination address** – 128-bit address of the intended recipient of the packet.
- **Extension Header Information** – an optional field (not included in the basic header) with variable length.
  - **Routing**
  - **Fragmentation**
  - **Authentication**
  - **Encapsulating**
  - **Hop-by-Hop Option**
  - **Destination Options**

**IPv6 Address Format**

```
<table>
<thead>
<tr>
<th>16bits</th>
<th>16bits</th>
<th>16bits</th>
<th>16bits</th>
<th>16bits</th>
<th>16bits</th>
<th>16bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Routing Prefixes (N bits)</td>
<td>Subnet ID (64-N bits)</td>
<td>Interface ID (64 bits)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**IPv6 Address Types**

**IPv6 address is classified in three types: Unicast, Multicast and Anycast.**

- **Unicast Address**: applied to one network interface.
- **Multicast Address**: applied for multiple network interfaces, and communication is conducted with all hosts with the same address.
- **Anycast Address**: applied for multiple network interfaces, but actual communication is conducted with one of them. It has the same format as the Unicast address.

© Javvin Technologies Inc. All rights reserved. www.javvin.com
### IPv4 vs. IPv6

<table>
<thead>
<tr>
<th>Subjects</th>
<th>IPv4</th>
<th>IPv6</th>
<th>IPv6 Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Space</td>
<td>4 Billion Addresses</td>
<td>$3.4 \times 10^{38}$ addresses</td>
<td>79 Octillion times the IPv4 address space</td>
</tr>
<tr>
<td>Configuration</td>
<td>Manual or use DHCP</td>
<td>Universal Plug and Play (UPnP) with or without DHCP</td>
<td>Lower Operation Expenses and reduce error</td>
</tr>
<tr>
<td>Broadcast / Multicast</td>
<td>Uses both</td>
<td>No broadcast and has different forms of multicast</td>
<td>Better bandwidth efficiency</td>
</tr>
<tr>
<td>Anycast support</td>
<td>Not part of the original protocol</td>
<td>Explicit support of anycast</td>
<td>Allows new applications in mobility, data center</td>
</tr>
<tr>
<td>Routing efficiency</td>
<td>Need to process Option and Checksum fields by every router</td>
<td>No checksum; Extended header for options.</td>
<td>Improved support for extensions and options and better routing efficiency.</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>Mostly manual and labor intensive</td>
<td>Facilitate the re-numbering of hosts and routers</td>
<td>Lower operation expenses and facilitate migration</td>
</tr>
<tr>
<td>QoS support</td>
<td>ToS using Diffserv</td>
<td>Flow classes and flow labels</td>
<td>More Granular control of QoS</td>
</tr>
<tr>
<td>Security</td>
<td>Uses IPv6 for Data packet protection</td>
<td>IPv6 becomes the key technology to protect data and control packets</td>
<td>Unified framework for security and more secure computing environment</td>
</tr>
<tr>
<td>Mobility</td>
<td>Uses Mobile IPv4</td>
<td>Mobile IPv6 provides fast handover, better router optimization and hierarchical mobility</td>
<td>Better efficiency and scalability; Work with latest 3G mobile technologies and beyond</td>
</tr>
</tbody>
</table>

### TCP/IP Utilities

- **TCPdump**
  
  tcpdump -dump traffic on a network

  **-a** Convert network and broadcast addresses to names
  **-c** Exit after receiving count packets
  **-f** Filter expression in file
  **-l** Listen on interface
  **-L** Don't convert IPv6 addresses to numbers
  **-p** Read packets from file
  **-r** Get snapshot bytes from each packet
  **-s** Don't print timestamp
  **-t** Verbose mode
  **-v** Write packets to file
  **-w** Display in hex
  **-x** Display in hex and ASCII
  **-w file** ["filter_expression"]
  **-W timeout** Time to wait for a response (seconds).
  **-w deadline** Specify a timeout (seconds) before ping exits.
  **-V** Show version and exit.
  **-U** Print full user-to-user latency.
  **-M hint** Select Path MTU Discovery strategy.
  **-T timestamp option** Set special IP timestamp options
  **-t ttl** Set the IP Time to Live.
  **-S sndbuf** Set socket sndbuf.
  **-r** Bypass routing tables and send to a host on an attached interface.
  **-R** Record route.
  **-q** Quiet output.
  **-p pattern** Specify (up to 16) "pad" bytes to fill out the packet.
  **-L** Suppress loopback of multicast packets.
  **-b** Numeric output only.
  **-p pattern** Specify (up to 16) "pad" bytes to fill out the packet.
  **-q** Quiet output.
  **-r** Record route.
  **-s** Bypass routing tables and send to a host on an attached interface.
  **-w socketsize** Specify the number of bytes to be sent.
  **-s sndbuf** Set socket sndbuf.
  **-e mt** Set the IP Time to Live.
  **-c timestamp option** Set special IP timestamp options
  **-M hint** Select Path MTU Discovery strategy.
  **-e** Print full user-to-user latency.
  **-v** Verbose output.
  **-v** Show version and exit.
  **-w deadline** Specify a timeout (seconds) before ping exits.
  **-w timeout** Time to wait for a response (seconds).

### TCP: Transmission Control Protocol

#### TCP Header Format

- **Source port** – Identifies points at which upper-layer source process receives TCP services.
- **Destination port** – Identifies points at which upper-layer Destination process responds to TCP services.
- **Sequence number** – Specifies the number assigned to the first byte of data in the current message.
- **ACKnowledgment number** – Contains the sequence number of the next byte of data the sender wishes to receive.
- **Offset** – Indicates where the data begins.
- **Reserved** – Reserved for future use. Must be zero.
- **Control bits** (Flags) – Carry a variety of control information.
- **Window** – Specifies the size of the sender’s receive window.
- **Data** – Contains upper-layer information.

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Echo</td>
<td>Reply</td>
</tr>
<tr>
<td>3</td>
<td>Destination Unreachable</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Protocol Unreachable</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Fragmentation Needed &amp; DF Set</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>Destination Network Unknown</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>Source Host Isolated</td>
<td>9</td>
</tr>
<tr>
<td>10</td>
<td>11</td>
<td>Communication Administratively Prohibited</td>
</tr>
<tr>
<td>12</td>
<td>13</td>
<td>Host Unreachable for TO</td>
</tr>
<tr>
<td>14</td>
<td>Source Quench</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Redirect</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>Echo</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>Route Advertisement</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>Router Selection</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>Parameter Problem</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>Timestamp</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>Timestamp Reply</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>Information Reply</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>Address Mask</td>
<td>0</td>
</tr>
<tr>
<td>30</td>
<td>Traceroute</td>
<td>0</td>
</tr>
</tbody>
</table>

### ICMP

- **ICMP Header Format**
  
  ICMP: Internet Message Control Protocol. ICMP for IPv4 is defined in IETF RFC 792 and ICMP for IPv6 is defined in IETF RFC 2463.

- **Type**
  - **0** Echo Reply
  - **3** Destination Unreachable
  - **8** Echo
  - **9** Route Advertisement
  - **10** Router Selection
  - **11** Time Exceeded
  - **12** Parameter Problem
  - **13** Timestamp
  - **14** Timestamp Reply
  - **15** Information Request
  - **16** Information Reply
  - **17** Address Mask Request
  - **18** Address Mask Reply
  - **30** Traceroute

- **Code**
  - **0** Echo Reply
  - **0** Net Unreachable
  - **1** Source Quench
  - **2** Routable
  - **3** Redirect Datagram for the TOS & Host
  - **4** Redirect Datagram for the Network
  - **5** Redirect Datagram for the Host
  - **6** Redirect Datagram for the TOS & Network
  - **7** Redirect Datagram for the TOS & Host
  - **8** Echo
  - **9** Route Advertisement
  - **10** Router Selection
  - **11** Time Exceeded
  - **12** Parameter Problem
  - **13** Timestamp
  - **14** Timestamp Reply
  - **15** Information Request
  - **16** Information Reply
  - **17** Address Mask Request
  - **18** Address Mask Reply
  - **30** Traceroute

- **Checksum**
  - **0** End of Option List

- **Checksum**
  - **0** Pointer indicates the error

- **Data**
  - **0** Acknowledgment number
  - **3** Destination Address
  - **5** Source Address
  - **8** Header Length
  - **10** Identifier
  - **16** Sequence number

- **Type**
  - **0** Echo Reply
  - **3** Destination Unreachable
  - **8** Echo
  - **9** Route Advertisement
  - **10** Router Selection
  - **11** Time Exceeded
  - **12** Parameter Problem
  - **13** Timestamp
  - **14** Timestamp Reply
  - **15** Information Request
  - **16** Information Reply
  - **17** Address Mask Request
  - **18** Address Mask Reply
  - **30** Traceroute

### UDP: User Datagram Protocol

UDP is defined by IETF RFC 768.

#### UDP Header Format

- **Source port** – Identifies points at which upper-layer source process sends UDP services.
- **Destination port** – Identifies points at which upper-layer Destination process receives UDP services.
- **Length** – The length in octets of the user datagram, including the header and the data (Minimum is 8).
- **Checksum** – Indicates whether the header was damaged in transit.
- **Data** – Contains upper-layer information.

- **Source port** – An optional field indicates the port of the sending process.
- **Destination port** – Identifies points at which upper-layer Destination process receives UDP services.
- **Length** – The length in octets of the user datagram, including the header and the data. (Minimum is 8).
- **Checksum** – Indicates whether the header was damaged in transit.
- **Data** – Contains upper-layer information.
TCP/UDP Port Numbers

Well Known Ports: from 0 through 1023
Registered Ports: from 1024 through 49151
Dynamic and/or Private Ports: from 49152 through 65535

---

The Mostly Used TCP/UDP Port Numbers

<table>
<thead>
<tr>
<th>Port No.</th>
<th>Protocol</th>
<th>Service Name</th>
<th>Aliases</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TCP</td>
<td>tcpmux</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>TCP/UDP</td>
<td>compressnet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>TCP/UDP</td>
<td>compressnet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>TCP/UDP</td>
<td>echo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>TCP/UDP</td>
<td>daytime</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>TCP/UDP</td>
<td>chargen</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>TCP</td>
<td>ftp-data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>TCP</td>
<td>ftp-control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>TCP</td>
<td>ssh</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>TCP</td>
<td>telnet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>TCP</td>
<td>smtp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>TCP/UDP</td>
<td>snmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>UDP</td>
<td>rLP</td>
<td>resource</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>TCP/UDP</td>
<td>nameserver</td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>TCP</td>
<td>nicname</td>
<td>whois</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>UDP</td>
<td>TACACS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>TCP/UDP</td>
<td>domain</td>
<td>DNS</td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>UDP</td>
<td>bootps</td>
<td>dhtps</td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>UDP</td>
<td>bootps</td>
<td>dhtps</td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>TCP/UDP</td>
<td>TF/TP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>TCP</td>
<td>gopher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>79</td>
<td>TCP/UDP</td>
<td>finger</td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>TCP/UDP</td>
<td>http</td>
<td>www,</td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>TCP/UDP</td>
<td>kerberos</td>
<td>krb5</td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>TCP</td>
<td>hostname</td>
<td>hostnames</td>
<td></td>
</tr>
<tr>
<td>102</td>
<td>TCP</td>
<td>iso-tsap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>107</td>
<td>TCP</td>
<td>rlogin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>TCP/UDP</td>
<td>pop3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>111</td>
<td>TCP/UDP</td>
<td>snmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>113</td>
<td>TCP</td>
<td>auth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>117</td>
<td>TCP</td>
<td>snmp-path</td>
<td></td>
<td></td>
</tr>
<tr>
<td>118</td>
<td>TCP</td>
<td>sqlserv</td>
<td></td>
<td></td>
</tr>
<tr>
<td>119</td>
<td>TCP/UDP</td>
<td>smtp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>ntp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>135</td>
<td>TCP/UDP</td>
<td>snmp</td>
<td>loc-srv</td>
<td></td>
</tr>
<tr>
<td>137</td>
<td>TCP/UDP</td>
<td>netbios-ns</td>
<td>sname</td>
<td></td>
</tr>
<tr>
<td>138</td>
<td>UDP</td>
<td>netbios-dgm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>139</td>
<td>TCP</td>
<td>netbios-ns</td>
<td></td>
<td></td>
</tr>
<tr>
<td>143</td>
<td>TCP</td>
<td>imap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>158</td>
<td>TCP</td>
<td>pcmail-srv</td>
<td></td>
<td></td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>smap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>162</td>
<td>UDP</td>
<td>smtp-trap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>170</td>
<td>TCP</td>
<td>print-srv</td>
<td></td>
<td></td>
</tr>
<tr>
<td>179</td>
<td>TCP</td>
<td>bgp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>194</td>
<td>TCP</td>
<td>irc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>213</td>
<td>UDP</td>
<td>ipx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>389</td>
<td>TCP</td>
<td>ldap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>401</td>
<td>TCP/UDP</td>
<td>UPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>TCP/UDP</td>
<td>https</td>
<td>M.com</td>
<td></td>
</tr>
<tr>
<td>445</td>
<td>TCP/UDP</td>
<td>cIFS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>464</td>
<td>TCP/UDP</td>
<td>kpassword</td>
<td></td>
<td></td>
</tr>
<tr>
<td>500</td>
<td>UDP</td>
<td>skey</td>
<td>ike</td>
<td></td>
</tr>
<tr>
<td>513</td>
<td>TCP</td>
<td>login</td>
<td></td>
<td></td>
</tr>
<tr>
<td>513</td>
<td>UDP</td>
<td>who</td>
<td>whod</td>
<td></td>
</tr>
<tr>
<td>514</td>
<td>TCP</td>
<td>cmd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>514</td>
<td>UDP</td>
<td>syslog</td>
<td></td>
<td></td>
</tr>
<tr>
<td>515</td>
<td>TCP</td>
<td>printer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>517</td>
<td>UDP</td>
<td>tals</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TCP/UDP Ports

Process X
---
Port N
UDP datagrams TCP connection
TCP/UDP

Process Y
---
Port M
TCP/UDP

Sockets

IP Addresses

Well Known Ports: from 0 through 1023
Registered Ports: from 1024 through 49151
Dynamic and/or Private Ports: from 49152 through 65535

Host A
unreliable
IP datagrams

Host B

---

RAMABERD
Amoursh o Ajarai Tخصص
دوزه های شبکه

WWW.RAHBORDCO.NET