Technische Universität Berlin

IPv4 - TCP, UDP, Ports

Training for Afghan System Administrators

TCP and UDP

Both TCP and UDP are protocols on the transport layer of the Internet model. Both protocols have advantages and disadvantages. Which protocol is better for a specific application depends on many factors (but this is outside of the scope of our training). Some brief differences:

- The Transmission Control Protocol (TCP) provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating over an IP network. TCP is the protocol that major Internet applications such as the World Wide Web, email, remote administration and file transfer rely on.

- Applications that do not require reliable data stream service may use the User Datagram Protocol (UDP), which provides a connectionless datagram service that emphasizes reduced latency over reliability. However, UDP does not provide error checking, does not always deliver packets in the right order, and is therefore generally less reliable. Typical uses for UDP are e.g. streaming.

Ports

A port is a software construct serving as a communications endpoint in a computer's host operating system. The purpose of ports is to uniquely identify different applications or processes running on a single computer and thereby enable them to share a single physical connection to a packet-switched network like the Internet; they were unnecessary until computers became capable of executing more than one program at the same time.

A port is always associated with an IP address of a host and the protocol type of the communication, and thus completes the destination or origination address of a communications session. A port is identified for each address and protocol by a 16-bit number, commonly known as the port number.

When specifying a complete address including the port number, the port is usually appened with a colon / ":" at the end of the address, e.g.:

- 123.123.123.123:22 # port number 22 (sshd) on the host 123.123.123.123

Some important services and their port numbers

A list of services and the protocols and ports they use can also be found in the file “/etc/services”. Ports below 1024 are reserved, from 1025 - 65535 you can choose freely. Here is a short list of important services:

- 20 & 21: File Transfer Protocol (FTP)
- 22: Secure Shell (SSH)
- 23: Telnet remote login service
- 25: Simple Mail Transfer Protocol (SMTP)
- 53: Domain Name System (DNS) service
- 80: Hypertext Transfer Protocol (HTTP) used in the World Wide Web
- 110: Post Office Protocol (POP3)
- 143: Internet Message Access Protocol (IMAP)
- 161: Simple Network Management Protocol (SNMP)
- 194: Internet Relay Chat (IRC)
- 443: HTTP Secure (HTTPS)
- 465: SMTP Secure (SMTPS)

Some more tools for network testing / troubleshooting

General tools:

- ping # check if host is reachable (won't work if ICMP blocked by firewall)
- traceroute # check if reachable hop by hop
- tracepath # same as traceroute but also shows MTU and more
- telnet # connect to arbitrary port on any host
- netstat # check open connections and listening services
- netcat # “Network Swiss Army Knife”

DNS – related tools:

- host # simple and fast DNS lookups
- dig # check any nameservers and record types
- nslookup # has an interactive mode; also available on Windows
- whois # find out who registered a domain

Advanced tools:

- nmap # scan entire networks, very sophisticated (obey local laws!!!)
- wireshark # graphical network protocal analyzer