Network Ports and Protocols

ACADEMY OF BLACKHAT

What is protocol?

Internet protocols are a set of rules and conventions that govern how data is transmitted and received over the internet. They define the standards for communication between devices and networks.

What is network port?

- A network port is a communication endpoint in a computer network. It is a software construct that allows networked devices or applications to send and receive data.
- Network ports are identified by a number, and each number is associated with a specific protocol or service.
- These port numbers are 16-bit unsigned integers, which means they can range from 0 to 65,535.

What do you mean by port number?

- When a network communication from the internet or another source arrives at a server, its port number can be used to identify the particular process to which it should be passed.
- Every device connected to a network has a set of standardised ports with a unique number.

- These are reserved numbers for specific protocols and the functions that go along with them. For instance, communications sent over the Hypertext Transfer Protocol (HTTP) always end up on port 80, which is one of the most frequently used ports.

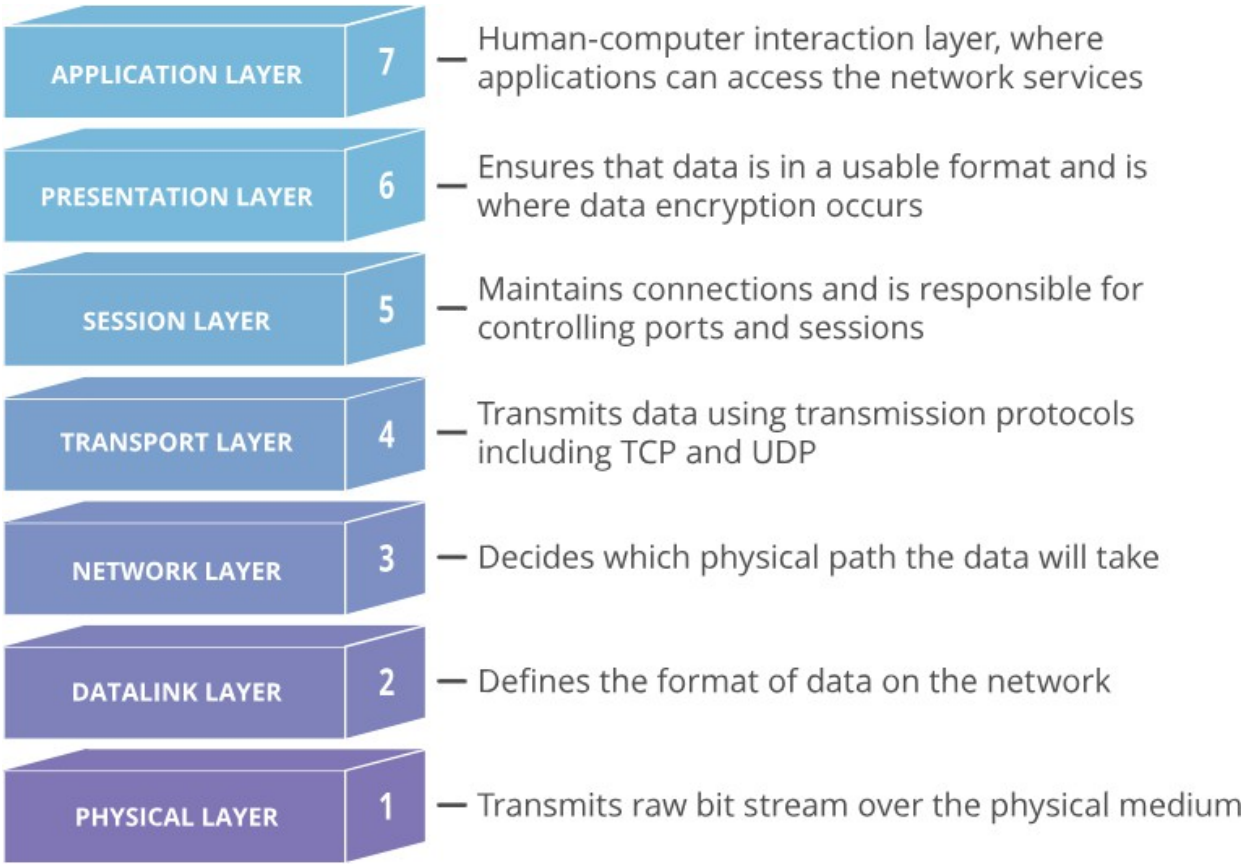
How do ports make network connections more efficient?

Vastly different types of data flow to and from a computer over the same network connection. The use of ports helps computers understand what to do with the data they receive.

Suppose Bob transfers an MP3 audio recording to Alice using the File Transfer Protocol (FTP). If Alice's computer passed the MP3 file data to Alice's email application, the email application would not know how to interpret it. But because Bob's file transfer uses the port designated for FTP (port 21), Alice's computer is able to receive and store the file.

Meanwhile, Alice's computer can simultaneously load HTTP webpages using port 80, even though both the webpage files and the MP3 sound file flow to Alice's computer over the same WiFi connection.

The OSI model is a conceptual model of how the Internet works. It divides different Internet services and processes into 7 layers. These layers are:



Ports are a transport layer (layer 4) concept. Only a transport protocol such as the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) can indicate which port a packet should go to. TCP and UDP headers have a section for indicating port numbers. Network layer protocols — for instance, the Internet Protocol (IP) — are unaware of what port is in use in a given network connection. In a standard IP header, there is no place to indicate which port the data packet should go to. IP headers only indicate the destination IP address, not the port number at that IP address.

almost always used in conjunction with a transport layer protocol. However, this does impact the functionality of testing software, which is software that "pings" IP addresses using Internet Control Message Protocol (ICMP) packets. ICMP is a network layer protocol that can ping networked devices — but without the ability to ping specific ports, network administrators cannot test specific services within those devices.

Some ping software, such as My Traceroute, offers the option to send UDP packets. UDP is a transport layer protocol that can specify a particular port, as opposed to ICMP, which cannot specify a port. By adding a UDP header to ICMP packets, network administrators can test specific ports within a networked device.

Layer 1 protocols(physical layer)

- USB Physical layer
- varieties of 802.11 Wi-Fi physical layers
- DSL
- ISDN
- T1 and other T-carrier links
- E1 and other E-carrier links
- Bluetooth physical layer
- Ethernet physical layer including 10 BASE T, 100 BASE T,100 BASE TX,100 BASE FX, 1000 BASE T and other variants

Layer 2 protocols (Data Link Layer)

- CDP
- Ethernet
- Frame Relay
- IEEE 802.11 Wi-Fi
- CHAP — Challenge Handshake Authentication Protocol
- HDLC — High-Level Data Link Control
- LLC — Logic Link Control
- LACP — Link Aggregation Control Protocol
- LLDP — Link layer discovery protocol
- LCP — Link Control Protocol (part of PPP)
- MAC — Media Access Control
- PPP — Point-to-Point Protocol
- STP — Spanning Tree Protocol
- VTP — VLAN Trunking Protocol
- VLAN — Virtual Local Area Network

Layer 3 protocols(Network Layer in OSI or Internet layer in TCP/IP)

- IPv4
- IPv6
- ATM — Asynchronous Transfer Mode
- EIGRP — Enhanced Interior Gateway Routing Protocol
- GRE — Generic Routing Encapsulation
- GLBP — Gateway Load Balancing Protocol
- HSRP — Hot Standby Router Protocol
- RIP
- RIPv2

IGRP	Interior Gateway Routing protocol
ICMP	Internet Control Message Protocol
• ICMPv6	
• IGMP	Internet Group Management Protocol
• IPSec	Internet Protocol Security
• IS-IS	Intermediate System- Intermediate System
• MPLS	Multi-Protocol Label Switching
• NAT	Network Address Translation
• OSPF	Open Shortest Path First
• VRRP	Virtual Router Redundancy Protocol

Layer 4 protocols (transport layer or Host-to-Host layer)

• AH	Authentication header over IP or Ipsec
• TCP	Transmission Control Protocol
• UDP	User Datagram Protocol
• DCCP	Datagram Congestion Control Protocol
• ESP	Encapsulating Security Payload over IP or IPSec
• FCP	Fibre Channel Protocol
• SCTP	Stream Control Transmission Protocol

Layer 5 protocols (Session Layer)

• SIP	Password Authentication Protocol
• PPTP	Point-to-Point Tunneling Protocol
• SMB	Server Message Block protocol
• NFS	Network File System (NFS) Protocol
• PAP	Printer Access Protocol
• RPC	Remote Procedure Call
• SMPP	Short Message Peer-to-Peer

Layer 6 protocols (Presentation Layer)

- TLS Transport Layer Security
- SSL Secure Socket Tunneling
- AFP Apple Filing Protocol

Layer 7 (Application Layer)

- BitTorrent A peer to peer file sharing system
- BGP Border Gateway Protocol
- DNS Domain name System
- DHCP Dynamic Host Configuration Protocol
- FTP Transfer Protocol
- HTTP Hypertext Transfer Protocol
- HTTPS Hypertext Transfer Protocol secure
- IRC Internet Relay Chat
- NTP Network Time Protocol
- POP3 Post Office Protocol version 3
- RTP Real-time Transport Protocol
- SSH Secure Shell
- SMTP SMTP Simple Mail Transfer Protocol
- SNMP Simple Network Management Protocol
- Telnet Remote terminal access protocol
- TFTP Trivial File Transfer Protocol
- URL Uniform Resource Locator

List of Common Ports and Protocols

Port Number	Service Name	Description	Protocol
Ports 20-21	FTP	File Transfer Protocol	TCP
Port 22	SSH	Secure Shell; used for secure logins, file transfers, and port forwarding	TCP
Port 23	Telnet	Telnet protocol; used for unencrypted text communications	TCP / UDP
Port 25	SMTP	Simple Mail Transfer Protocol, used for email routing between mail servers	TCP
Port 53	DNS	Domain Name System; translates 'host names' into IP addresses	TCP / UDP
Port 69	TFTP	Trivial File Transfer Protocol	UDP
Port 80	HTTP	Hypertext Transfer Protocol; used for unencrypted web traffic	TCP
Port 102	ISO-TSAP	ISO Transport Service Access Point (TSAP)	TCP / UDP
Port 110	POP3	Post Office Protocol; used to connect to a mail server to retrieve emails	TCP / UDP
Port 123	NTP	Network Time Protocol	UDP
Port 135	DCE/RPC Endpoint Mapper	Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Endpoint Mapper	TCP / UDP
Port 139	NetBIOS-ssn	NetBIOS Session Service	TCP / UDP
Port 161	SNMP-agents	Simple Network Management Protocol; agents communicate on this port	TCP / UDP
Ports 381 - 383	HP Performance Data Collector	Collects performance data from managed nodes	TCP / UDP
Port 389	LDAP	Lightweight Directory Access Protocol	TCP / UDP
Port 443	HTTPS	Hypertext Transfer Protocol Secure; used for encrypted web traffic	TCP / UDP
Port 445	Microsoft DS SMB	Microsoft Directory Services; TCP used for AD and Windows shares, UDP for SMB file-sharing	TCP / UDP
Port 464	Kerberos	Used for changing or setting passwords in Kerberos-based authentication systems, such as Active Directory	TCP / UDP
Port 465	SMTP	Simple Mail Transfer Protocol; used to securely transmit mail messages from email clients to email servers.	TCP
Port 514	syslog	Syslog Protocol; for collecting and organizing all log files sent from various devices on a network	UDP

Port 587	SMTP	Simple Mail Transfer Protocol; used for email message submission	UDP
Port 593	RPC Mapper Service	Enables secure remote connections and function execution over HTTP.	TCP / UDP
Port 636	LDAP / LDAPS	Lightweight Directory Access Protocol (over SSL); used to store data in the LDAP directory and authenticate users to access the directory	TCP / UDP
Port 691	Microsoft Exchange Routing Engine (RESvc)	Used by Microsoft Exchange servers to update routing tables for efficient message delivery.	TCP
Port 902	VMware vSphere	Used to manage your ESXi hosts and the virtual machines (VMs) that run on them	TCP / UDP
Port 993	IMAP	Internet Message Access Protocol; used to deliver and manage messages on email servers on behalf of email clients	TCP
Port 995	POP3	Post Office Protocol version 3 (over SSL); lets email users download messages from an email server using an email client	TCP / UDP
Port 1433	Microsoft SQL Server	Allows encrypted access to and management of databases and servers	TCP
Port 1521	Oracle Database	Oracle client apps communicate with Oracle database servers	TCP
Port 3306	MySQL	Used to connect with MySQL clients and utilities	TCP
Port 3389	Remote Desktop Protocol	Allows client device to remotely access and control a Windows desktop computer over this port	TCP
Port 5060	SIP	Session Initiation Protocol; used to signal and control communication sessions	TCP / UDP
Ports 6881-6999	BitTorrent	Peer-to-peer file sharing	TCP / UDP
Port 10000	Webmin	Used for remote server communication and configuration	TCP
Port 31337	Back Orifice / ncat	Used for remote control of servers by hacking tools and remote administration utilities	TCP / UDP

Network Ports and Protocols

Thank you