Reserved and Commonly Allocated Ports

Port number ranges

You now know that the range of port numbers used globally is from 0 to 65,535, which is a vast number range. The Internet Assigned Numbers Authority (IANA) manages these port numbers since they change over time as technology and protocols evolve. Any changes made to these port numbers require IANA's permission.

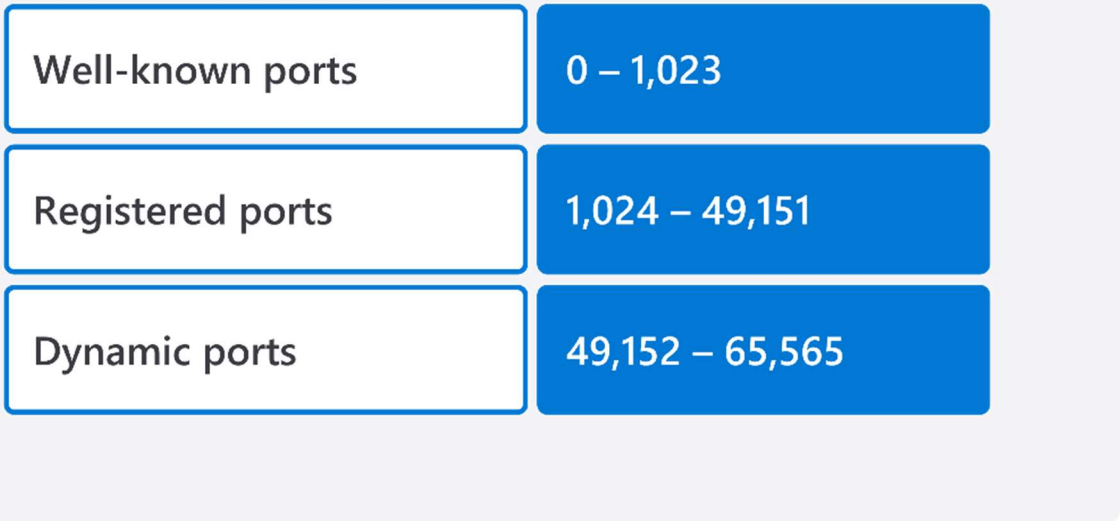
The port numbers are further divided into three ranges, each serving a slightly different purpose in the network. The classification is important in identifying different sessions across a network between devices.

The three port number ranges are:

- **Well-known ports** (0 - 1,023) are reserved for specific protocols and services used by system processes and applications.

- **Registered ports** (1,024 - 49,151) are assigned by IANA for specific services or protocols and can also be used by user applications.

- **Dynamic or private ports** (49,152 - 65,535) are used by client applications to connect to servers and are assigned temporarily for the duration of a session.



Now that you're more familiar with the different range classifications, let's explore each in a little more detail.

Well-known port numbers (0 - 1,023)

Well-known port numbers are reserved for some of the most commonly used and popular protocols in computer networks. These ports can either transfer verified data via TCP or unverified data via UDP. They are assigned at the transport layer of the OSI model or TCP/IP suite and identified at the application layer.

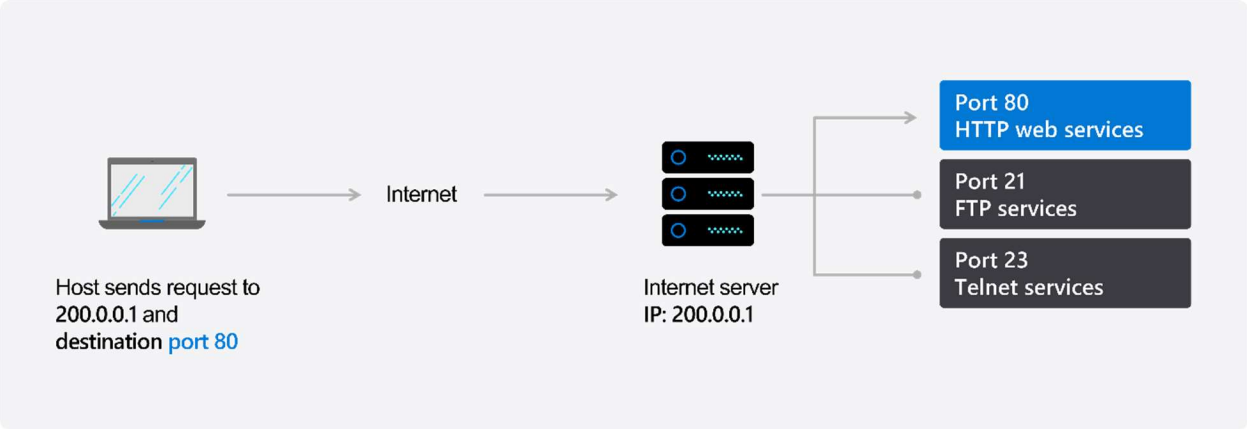
Review the table below for some of the most common well-known ports:

Port Number	TCP\UDP	Protocol	Usage
20,21	TCP	File Transfer Protocol (FTP)	Data transfer
22	TCP\UDP	Secure Shell (SSH)	Secure remote device access
23	TCP	Telnet	Remote device access
25	TCP	Simple Mail Transfer Protocol (SMTP)	Email
53	TCP\UDP	Domain Name Server (DNS)	Name to IP address resolution
67,68	UDP	Dynamic Host Configuration Protocol (DHCP)	Dynamic IP address assignment
69	UDP	Trivial File Transfer Protocol (TFTP)	Booting devices via the network
80	TCP	HyperText Transfer Protocol (HTTP)	Web page data transfer
110	TCP	Post Office Protocol (POP3)	One way mail delivery
123	UDP	Network Time Protocol (NTP)	Keeps time for the network
143	TCP\UDP	Internet Message Access Protocol (IMAP4)	Managing mailboxes
161, 162	TCP\UDP	Simple Network Management Protocol (SNMP)	Network device management
389	TCP and UDP	Lightweight Directory Access Protocol (LDAP)	Authentication services
443	TCP\UDP	HTTP with Secure Sockets Layer (SSL) (HTTPS)	Secure web page retrieval
500	UDP	Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)	Authentication
636	TCP\UDP	Lightweight Directory Access Protocol over TLS/SSL (LDAPS	Secure authentication services
989/990	TCP	FTP over TLS/SSL	Secure data transfer

For a complete list of all protocols, please review the following resource from IANA:

- Service names and port numbers
-

When using protocol port numbers, the destination port is usually specified as the initial step in requesting the correct service from the device that provides the service. If a server can support multiple protocols, the destination port must specify which protocol it wants to use.
The following diagram illustrates how ports are used to identify services:



To improve the security of data being transmitted over networks, many protocols now have alternative versions. These alternative versions often involve encryption using a security protocol to enhance security. One such example is HTTPS, which uses the Transport Layer Security (TLS) protocol to encrypt data as it moves across the network. TLS is also used in other protocols to improve their security, with the letter 'S' added to the end of the original protocol name to signify the use of TLS.

Registered ports (1,024 - 49,151)

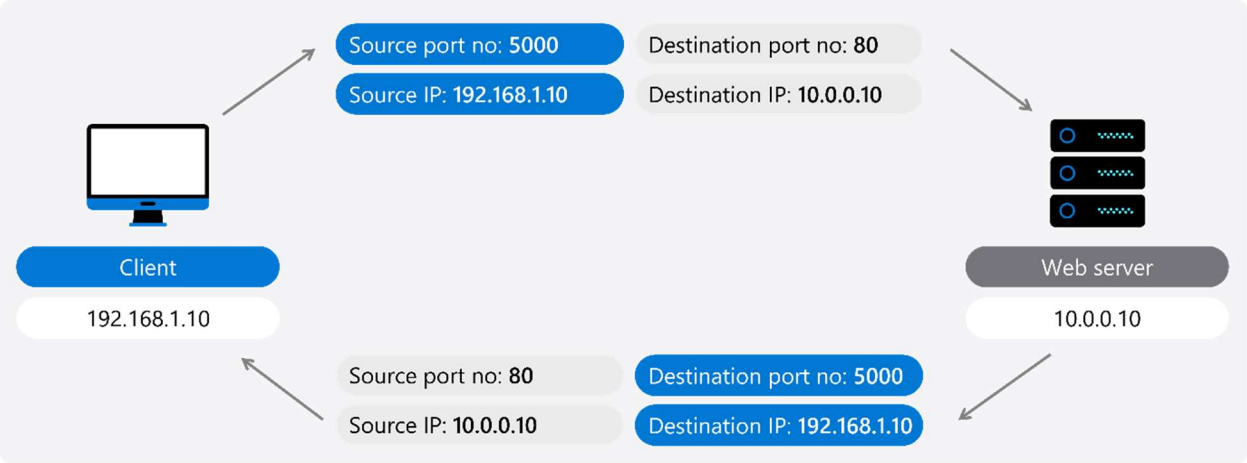
Registered ports are assigned by IANA to companies for specific services that they want to use. These ports are often used in the gaming sector to identify the ports that need to be opened in home networks to allow games to function.

Examples include port 3074 for the XBOX live network or ports 3,479/80 for the PlayStation network. These ports have changed as games become less relevant and new ones emerge on the market. As technology changes, new ports are assigned and old ones are retired. Some registered ports have been around for a while, such as SIP and H323 which are video conferencing protocols that use port numbers 1,719, 1,720, 5,060, and 5,061. For SIP, port 5,060 is used for unencrypted data, while port 5,061 is used for encrypted data.

Dynamic or private ports (49,152 - 65,535)

Dynamic or private ports are essential for communication between protocols using TCP or UDP. When a computer has multiple web pages open simultaneously, dynamic ports are used to identify different sessions. Each open web page will be associated with a different port number, which serves as the source port number for communication between devices. This is crucial because it allows your computer to determine which data belongs to which web page, and it is also the number used for devices to communicate responses.

The following example demonstrates how a client PC and web server use IP addresses to communicate with each other. In this scenario, the client PC sends a web service request (HTTP request) to the web server using port number 80. The client PC also specifies a source port number (port 5000) for the web server to send its response. This source port number helps the client PC identify which application and session the data is for.



Conclusion

In summary, devices use different port numbers to manage network traffic. Well-known ports are for common applications, registered ports for constantly changing protocols and newer technologies, and dynamic ports for identifying individual sessions. Engineers manage network traffic by configuring and monitoring data flow through specific port numbers, assigning them to specific applications or services, setting up firewall rules, and analyzing network traffic to improve performance.

By managing network traffic effectively, engineers ensure data is transmitted securely and efficiently, and applications and services are accessible to users.