Most Commonly Used

Well Known Protocol Port Numbers

Common TCP/IP Protocols and Ports

Protocol	TCP/ UDP	Port Number	Description
File Transfer Protocol (FTP) (RFC 959)	TCP	20/21	FTP is one of the most commonly used file transfer protocols on the Internet and within private networks. An FTP server can easily be set up with little networking knowledge and provides the ability to easily relocate files from one system to another. FTP control is handled on TCP port 21 and its data transfer can use TCP port 20 as well as dynamic ports depending on the specific configuration.
Secure Shell (SSH) (RFC 4250-4256)	TCP	22	SSH is the primary method used to manage network devices securely at the command level. It is typically used as a secure alternative to Telnet which does not support secure connections.
Telnet (RFC 854)	TCP	23	Telnet is the primary method used to manage network devices at the command level. Unlike SSH which provides a secure connection, Telnet does not, it simply provides a basic unsecured connection. Many lower level network devices support Telnet and not SSH as it required some additional processing. Caution should be used when connecting to a device using Telnet over a public network as the login credentials will be transmitted in the clear.
Simple Mail Transfer Protocol (SMTP) (RFC 5321)	TCP	25	SMTP is used for two primary functions, it is used to transfer mail (email) from source to destination between mail servers and it is used by end users to send email to a mail system.
Domain Name System (DNS) (RFC 1034-1035)	TCP/ UDP	53	The DNS is used widely on the public internet and on private networks to translate domain names into IP addresses, typically for network routing. DNS is hieratical with main root servers that contain databases that list the managers of high level Top Level Domains (TLD) (such as .com). These different TLD managers then contain information for the second level domains that are typically used by individual users (for example, cisco.com). A DNS server can also be set up within a private network to private naming services between the hosts of the internal network without being part of the global system.
Dynamic Host Configuration Protocol (DHCP)	UDP	67/68	DHCP is used on networks that do not use static IP address assignment (almost all of them). A DHCP server can be set up by an administrator or engineer with a poll of addresses that are available for assignment. When a client device is turned on it can request an IP address from the

(RFC 2131)			local DHCP server, if there is an available address in the pool it can be assigned to the device. This assignment is not permanent and expires at a configurable interval; if an address renewal is not requested and the lease expires the address will be put back into the poll for assignment.
Trivial File Transfer Protocol (TFTP) (RFC 1350)	UDP	69	TFTP offers a method of file transfer without the session establishment requirements that FTP uses. Because TFTP uses UDP instead of TCP it has no way of ensuring the file has been properly transferred, the end device must be able to check the file to ensure proper transfer. TFTP is typically used by devices to upgrade software and firmware; this includes Cisco and other network vendors' equipment.
Hypertext Transfer Protocol (HTTP) (RFC 2616)	TCP	80	HTTP is one of the most commonly used protocols on most networks. HTTP is the main protocol that is used by web browsers and is thus used by any client that uses files located on these servers.
Post Office Protocol (POP) version 3 (RFC 1939)	TCP	110	POP version 3 is one of the two main protocols used to retrieve mail from a server. POP was designed to be very simple by allowing a client to retrieve the complete contents of a server mailbox and then deleting the contents from the server.
Network Time Protocol (NTP) (RFC 5905)	UDP	123	One of the most overlooked protocols is NTP. NTP is used to synchronize the devices on the Internet. Even most modern operating systems support NTP as a basis for keeping an accurate clock. The use of NTP is vital on networking systems as it provides an ability to easily interrelate troubles from one device to another as the clocks are precisely accurate.
NetBIOS (RFC 1001-1002)	TCP/UDP	137/138/139	NetBIOS itself is not a protocol but is typically used in combination with IP with the NetBIOS over TCP/IP (NBT) protocol. NBT has long been the central protocol used to interconnect Microsoft Windows machines.
Internet Message Access Protocol (IMAP) (RFC 3501)	TCP	143	IMAP version3 is the second of the main protocols used to retrieve mail from a server. While POP has wider support, IMAP supports a wider array of remote mailbox operations which can be helpful to users.
Simple Network Management Protocol (SNMP) (RFC 1901-1908, 3411-3418)	TCP/UDP	161/162	SNMP is used by network administrators as a method of network management. SNMP has a number of different abilities including the ability to monitor, configure and control network devices. SNMP traps can also be configured on network devices to notify a central server when specific actions are occurring. Typically, these are configured to be used when an alerting condition is happening. In this situation, the device will send a trap to network management stating that an event

			has occurred and that the device should be looked at further for a source to the event.
Border Gateway Protocol (BGP) (RFC 4271)	TCP	179	BGP version 4 is widely used on the public internet and by Internet Service Providers (ISP) to maintain very large routing tables and traffic processing. BGP is one of the few protocols that have been designed to deal with the astronomically large routing tables that must exist on the public Internet.
Lightweight Directory Access Protocol (LDAP) (RFC 4510)	TCP/ UDP	389	LDAP provides a mechanism of accessing and maintaining distributed directory information. LDAP is based on the ITU-T X.500 standard but has been simplified and altered to work over TCP/IP networks.
Hypertext Transfer Protocol over SSL/TLS (HTTPS) (RFC 2818)	TCP	443	HTTPS is used in conjunction with HTTP to provide the same services but doing it using a secure connection which is provided by either SSL or TLS.
Lightweight Directory Access Protocol over TLS/SSL (LDAPS) (RFC 4513)	TCP/ UDP	636	Just like HTTPS, LDAPS provides the same function as LDAP but over a secure connection which is provided by either SSL or TLS.
FTP over TLS/SSL (RFC 4217)	TCP	989/990	Again, just like the previous two entries, FTP over TLS/SSL uses the FTP protocol which is then secured using either SSL or TLS.

Summary

While it may seem obvious that there are large number of ports that are missing from this list, the purpose here was to just cover the most commonly seen and used protocols. The complete list of assigned ports and their assigned services can be seen at http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml.