

Knowledge check

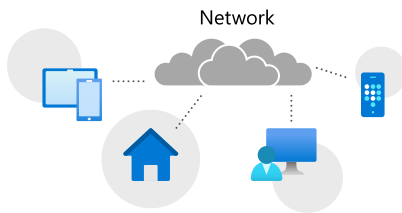
13 minutes

When you consider a move to the cloud, it's essential to know the fundamentals of how your network works. The first step in understanding the composition of a network is to understand how network devices communicate with each other. This knowledge applies to your organization's network and to more extensive networks like the web. The same principles apply to all networks.

In this unit, you learn about the essential network protocols that allow communication across internet-based networks.

Network protocols

A **network protocol is a set of conditions and rules** that specify how network devices communicate on a given network. It provides a common framework for establishing and maintaining a communications channel, and how to handle errors or faults should they occur. Network protocols allow communication between different network-enabled devices, such as laptops, tablets, smartphones, desktops, servers, and other network-enabled devices.



The network protocol is an essential building block in the design of an organization's network architecture. There are several network protocols available. Each network protocol has many properties that govern its use and implementation.

Let's define a few terms before we look at some of the commonly used network protocols.

What is a network address?

A network address is a **unique identifier** that identifies a network-enabled device. A network-enabled device might have more than one address type. For this discussion, we focus on only two address types.

The first type is a **media access control (MAC)** address that identifies the network interface on the **hardware level**. The second type is an **Internet Protocol (IP) address** that identifies the network interface on a **software level**.

We explore these two address types in more detail later.

What is a data packet?

A data packet is a unit that's used to describe the message that two devices on a network send each other. A data packet consists of **raw data, headers, and potentially a trailer**. The header contains several information items. For example, it includes the sender and destination device addresses, the size of the packet, the protocol used, and the packet number. The **trailer** in a data packet deals with **error checking**.

The concept is similar to sending someone a letter in the mail one section at a time. For example, instead of sending several pages in one envelope, each page is sent in a separate envelope. Enough information is sent in each envelope to allow the recipient to piece together the complete message after receiving all the pages.

What is a **datagram**?

no acknowledgment, independent packet of data, UDP — User Datagram Protocol

A datagram is considered the same as a data packet. Datagrams commonly refer to data packets of an unreliable service, where delivery can't be guaranteed.

What is routing?

Routing, in the context of networks, refers to the mechanism used to make sure that data packets follow the correct **delivery path** between the sending and receiving devices on different networks.

For example, think about the PC you're using and the server that's serving the page you're currently reading. Multiple networks might connect your PC and the server, and various paths might be available between these two devices.

Protocol categories

Several types of applications and hardware devices depend on specific network protocols on a typical network. For example, browsing the internet by using a web browser relies on a different protocol than sending or receiving an email. Converting the data that you see in the browser and sending this information over the network requires another protocol.

Protocols fall into three categories:

- Network communication protocols
- Network security protocols
- Network management protocols

Let's have a look at some of the protocols in these categories.

Network communication protocols

Communication protocols focus on establishing and maintaining a connection between devices. As you work with different devices and network services, you use various network communication protocols.

First, we need to define three foundational protocols of all internet-based networks. These three protocols are **Transmission Control Protocol (TCP)**, **Internet Protocol (IP)**, and **User Datagram Protocol (UDP)**. These protocols deal with the logical transmission of data over the network.

- **Transmission Control Protocol:** TCP divides data into **data packets** that can be sent securely and quickly while minimizing the chance of data loss. It provides a **stable** and **reliable** mechanism for the delivery of data packets across an **IP-based network**. Even though TCP is an effective connection-oriented protocol, it has overhead.
- **Internet Protocol:** IP is responsible for the addressing of a data packet. IP **encapsulates the data packet** to be delivered and adds an address header. The header contains information on the **sender and recipient IP addresses**. This protocol isn't concerned about the order in which the packets are sent or received. It also doesn't guarantee that a packet is delivered, only the address.
- **User Datagram Protocol:** UDP is a **connectionless** protocol that offers a **low-latency and loss-tolerant implementation**. UDP is used with processes that **don't need to verify** that the recipient device received a datagram.

The rest of the protocols that we discuss here are based on a type of application, such as an email client or a web browser. Here are the most commonly used network communication protocols:

- **Hypertext Transfer Protocol (HTTP):** The HTTP protocol uses **TCP/IP** to deliver web page content from a server to **your browser**. HTTP can also **handle the download and upload** of files from remote servers.
- **File Transfer Protocol (FTP):** FTP is used to transfer files between **different computers** on a network. Typically, you'd use FTP to upload files to a server from a remote location. While you can use FTP to download files, web-based downloads are typically handled through HTTP.
- **Post Office Protocol 3 (POP3):** POP3 is one of three email protocols and is most commonly used by an email client to allow you to **receive emails**. This protocol uses **TCP** for the management and delivery of an email.
- **Simple Mail Transfer Protocol (SMTP):** SMTP is another one of the three email protocols and is most commonly used to **send emails** from an email client via an email server. This protocol uses TCP for management and transmission of the email.
- **Interactive Mail Access Protocol (IMAP):** IMAP is the more powerful of the three email protocols. With IMAP and an email client, you can manage a single mailbox on an email server in your organization.

Network security protocols

Network security protocols are designed to maintain the security of data across your network. These protocols encrypt in-transmission messages between users, services, and applications.

Network security protocols use encryption and cryptographic principles to secure messages.

To implement a secure network, you must match the right security protocols for your needs. The following list explores the leading network security protocols:

- **Secure Socket Layer (SSL)**: SSL is a standard encryption and security protocol. It provides a secure and encrypted connection between your computer and the target server or device that you accessed over the internet.
- **Transport Layer Security (TLS)**: TLS is the successor to SSL, and provides a stronger and more robust security encryption protocol. Based on the Internet Engineering Task Force (IETF) standard, it helps stop message forgery, tampering, and eavesdropping and is typically used to protect web browser communications, email, VoIP, and instant messaging. While TLS is now used, the replacement security protocol is often still called SSL.
- **Hypertext Transfer Protocol Secure (HTTPS)**: HTTPS provides a more secure version of the standard HTTP protocol by using the TLS or SSL encryption standard. This combination of protocols ensures that all data transmitted between the server and the web browser is encrypted and secure from eavesdropping or data packet sniffing. The same principle is applied to the POP, SMTP, and IMAP protocols listed previously to create secure versions known as POPS, SMTPS, and IMAPS.
- **Secure Shell (SSH)**: SSH is a **cryptographic** network security protocol that provides a secure data connection across a network. SSH is designed to support command-line execution of instructions, which includes remote authentication to servers. FTP uses many of the SSH functions to provide a secure file transfer mechanism.
- **Kerberos**: This validation protocol provides a robust authentication for client-server-based applications through secret-key cryptography. Kerberos assumes that all endpoints in the network are insecure. It constantly enforces strong encryption for all communications and data.

Network management protocols

In your network, it's perfectly acceptable to have multiple different protocols running concurrently. Previously, we discussed communications and security protocols. Equally important to the successful day-to-day running and operating of a network are the management protocols. The focus of this type of protocol is the sustainability of the network by looking at faults and performance.

Network administrators need to monitor their networks and any devices attached to them. Each device in your network exposes some indicators about the state and health of the device. The network administrator tool requests these indicators and uses them for monitoring and reporting.

Two network management protocols are available:

- **Simple Network Management Protocol (SNMP):** SNMP is an internet protocol that allows for the collection of data from devices on your network and the management of those devices. The device has to support SNMP to gather information. Devices that support SNMP typically include switches, routers, servers, laptops, desktops, and printers.
- **Internet Control Message Protocol (ICMP):** ICMP is one of the protocols included within the Internet Protocol suite (IPS). It allows network-connected devices to send warning and error messages, along with operation information about the success or failure of a connection request, or if a service is unavailable. Unlike other network transport protocols, like UDP and TCP, ICMP isn't used to send or receive data from devices on the network.

Ports

A port is a logical construct that allows the routing of incoming messages to specific processes. There's a particular port for every type of IPS. A port is an **unsigned 16-bit** number in the range 0 to 65535, and is also known as a port number. Based on the communications protocol used, the sending TCP or UDP layer assigns the ports.

There are specific port numbers reserved for every service. The first 1,024 ports, called the well-known port numbers, are reserved for the commonly used services. The high-numbered ports, called the **ephemeral** ports, are unreserved and used by dedicated applications.


Every port links to a specific service or communications protocol. It means that the target network device, like a server, can receive multiple requests on each port and service each of them without conflict.

Well-known port numbers

Much in the same way that IP addresses are split into classes, so are ports. There are three ranges of ports: the well-known ports, the registered ports, and the dynamic/private ports.

The Internet Assigned Numbers Authority (IANA) manages the allocation of port numbers, the regional assignment of IP addresses, and Domain Name System (DNS) root zones. IANA also manages a central repository for protocol names and the registry used in internet protocols.

The following table lists some of the more common well-known port numbers.

 Expand table

Port number	Assignment
20	File Transfer Protocol for data transfer
21	File Transfer Protocol for command control
22	Secure Shell for secure authentication
23	Telnet remote authentication service for unencrypted text messages
25	Simple Mail Transfer Protocol for email routing
53	Domain Name System service
80	Hypertext Transfer Protocol for use in the web

Port number	Assignment
110	Post Office Protocol
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol for management of digital mail
161	Simple Network Management Protocol
194	Internet Relay Chat (IRC)
443	HTTP Secure HTTP over TLS/SSL

Internet Protocol suite

The Internet Protocol suite is a **collection of communication protocols**, also called a **protocol stack**. It can be referred to as the TCP/IP protocol suite, because both TCP and IP are primary protocols used in the suite.

The IPS is an abstract, layered networking reference model. The IPS describes the different layered protocols used to send and receive data on the internet and similar networks.

The IPS model is one of several similar networking models that varies between three and seven layers. The best-known model is the Open Systems Interconnection (**OSI) networking reference model**. We don't cover the OSI model here, but you can find more information at [The Open Systems Interconnection model](#) [↗](#).

Layer	Protocol					
Application	Telnet	FTP	SMTP	DNS	SNMP	SSH
Transport		TCP			UDP	
Internet	Ipssec	IPv4	IPv6	ICMP	IP	
Network	Ethernet	PPP	ATM	ARP	DSL	ISDN

- **Application layer:** The top layer of this stack is concerned with application or process communication. The application layer is responsible for determining **which communication protocols to use based** on what type of message is transmitted. For example, the layer assigns the correct email protocols such as POP, SMTP, or IMAP if the message is email content.
- **Transport layer:** This layer is responsible for **host-to-host** communication on the network. The protocols associated with this layer are TCP and UDP. TCP is responsible for flow control. UDP is responsible for providing a datagram service.
- **Internet layer:** This layer is responsible for **exchanging datagrams**. A datagram contains the data from the transport layer and adds in the origin and recipient IP addresses. The protocols associated with this layer are IP, ICMP, and the Internet Protocol Security (IPsec) suite.
- **Network access layer:** The bottom layer of this stack is responsible for defining how the data is sent across the network. The protocols associated with this layer are ARP, MAC, Ethernet, DSL, and ISDN.

Monitor networks in Azure

Maintaining and managing the health of your network is the same across all networks no matter the location of the network. For example, a local organization's network uses the same network standards and protocols as an Azure-based network.

Azure has **three network-monitoring** tools to assist you in maintaining and managing the health of your networks. You can also extend some of the monitoring features to on-premises networks:

- **Azure Network Watcher:** You can use Network Watcher to capture packet data from the Azure services you use. You can also understand the flow of data in network traffic patterns and troubleshoot network-related problems on your network.
- **Network Performance Monitor:** Network Performance Monitor monitors and reports on the health of your network, provides insights into its performance, and reports on connectivity between your applications. While Network Performance Monitor is cloud-based, it can provide a hybrid service to monitor both cloud and on-premises networks.
- **Performance Monitor:** Performance Monitor is a capability within Network Performance Monitor. Designed to monitor network connectivity across your entire estate, whether on-premises or cloud-based, it reports network issues as they occur. Performance Monitor can monitor all network routes, along with redundant paths, and report any issues. It can identify particular network segments that degrade network performance. Performance Monitor can report on the health of the network without needing to rely on SNMP.

Check your knowledge

1. Which of these standards and protocols is used predominantly for email? *

- ☐ FTP
- ☐ TCP
- ☐ SMTP

2. Which network security protocol provides a cryptographic network protocol? *

- ☐ SNMP

- ☐ HTTP
- ☐ SSH

3. What is the Internet Control Message Protocol (ICMP) used for? *

- ☐ To send alerts when an intrusion is detected.
- ☐ To send warning messages when the network is about to fail.
- ☐ To send error messages and operational information that indicate success or failure when communicating with another IP address.

4. What would you use the Simple Network Management Protocol (SNMP) for? *

- ☐ For collecting and organizing information about email servers on your IP network.
- ☐ For collecting and organizing information about user access and behavior on your IP network.
- ☐ For collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

Check your answers

Check your answers