

National Institute of Technology, Raipur
Department of Computer Science & Engineering

Computer Network Lab



Course - B.Tech. (CBCS Scheme)

Semester- IV

Faculty Incharge:

Dr. Jairam Naik

Ms. Rakhi Seth

Research Scholar

Ms. Kavita Jaiswal

Mr. Rahul Shrivastava

S.No.	List of Experiments
1	Introduction to Local Area Network with its cables, connectors and topologies.
2	Installation of Switch. Hub their cascading and network mapping.
3	Installation of UTP, Co-axial cable, Cross cable, parallel cable NIC and LAN card.
4	Case Study of Ethernet (10 base 5,10 base 2,10 base T)
5	Installation and working of Net meeting and Remote Desktop.
6	Installation and working with Telnet (Terminal Network).
7	Installation and working with FTP (File Transfer Protocol).
8	Installation and Computers via serial or Parallel ports and enable the computers to share disk and printer port.
9	Installation of NS-2/3 Network Simulator: Basics of Network Simulation
10	Simulating a Local Area Network and LAN topologies.
11	Implementation of various MAC protocol.
12	Measuring Network Performance: Network Performance Evaluation, Performance Evaluation Metrics.
13	Performance Evaluation of routing Protocol.
14	Parameter Affecting the Performance of Network, Performance Evaluation Technique, Network Performance Evaluation using NS-2/3

Introduction

- An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as **Network devices** and include things such as routers, switches, hubs, and bridges.
- A computer network can be categorized by their size. A **computer network** is mainly of **four types**:
 1. LAN(Local Area Network)
 2. PAN(Personal Area Network)
 3. MAN(Metropolitan Area Network)
 4. WAN(Wide Area Network)

LAN(Local Area Network)

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.



PAN

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

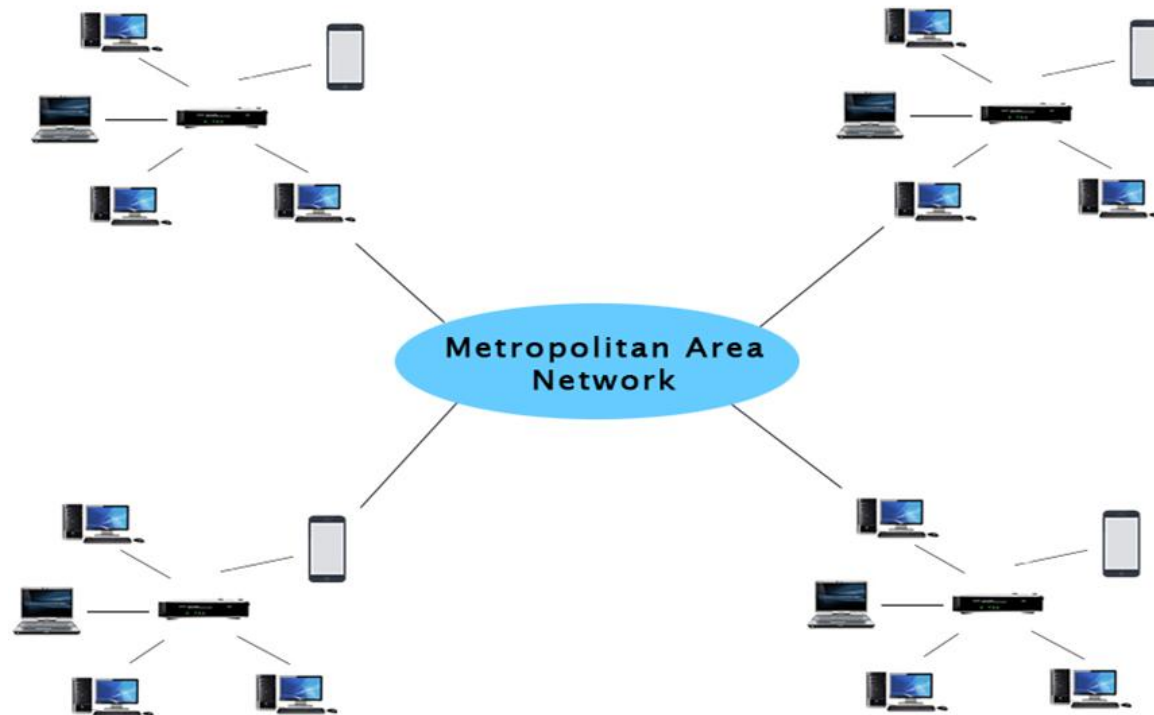


There are two types of PAN are present:

- Wired Personal Area Network
- Wireless Personal Area Network
- **Wireless Personal Area Network:** Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.
- **Wired Personal Area Network:** Wired Personal Area Network is created by using the USB.

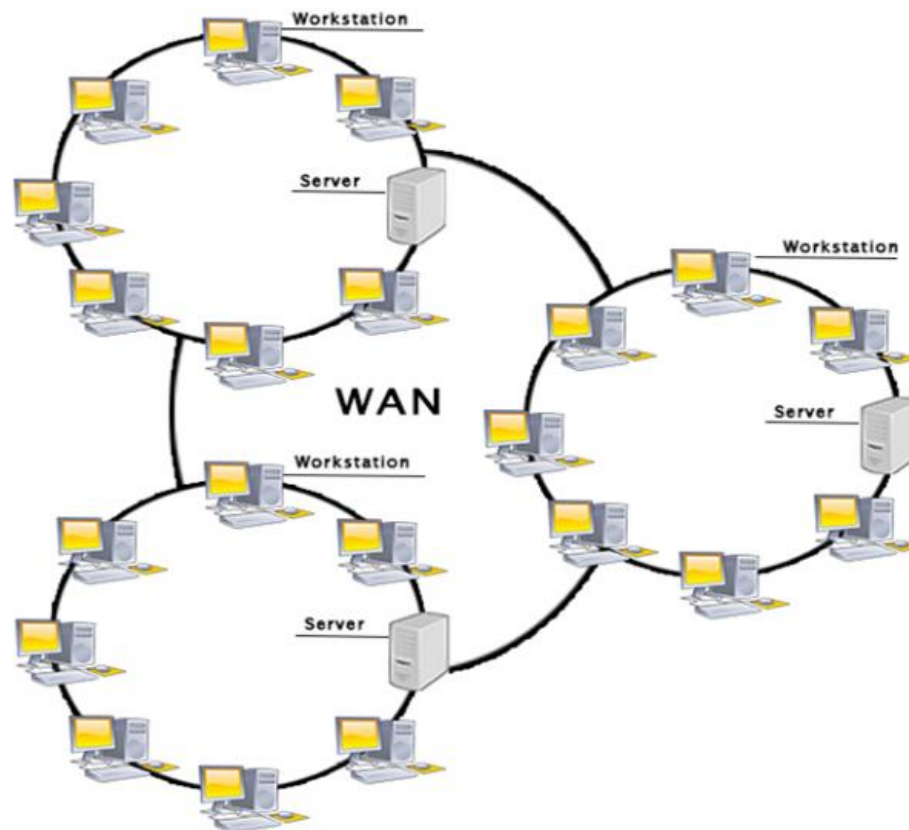
MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).



WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



In this Lab, you will also Learn:

What is NS2

NS2 stands for Network Simulator Version 2. It is an open-source event-driven simulator designed specifically for research in computer communication networks.

Features of NS2

1. It is a discrete event simulator for networking research.
2. It provides substantial support to simulate bunch of protocols like TCP, FTP, UDP, https and DSR.
3. It simulates wired and wireless network.
4. It is primarily Unix based.
5. Uses TCL as its scripting language.
6. Otcl: Object oriented support
7. Tclcl: C++ and otcl linkage
8. Discrete event scheduler

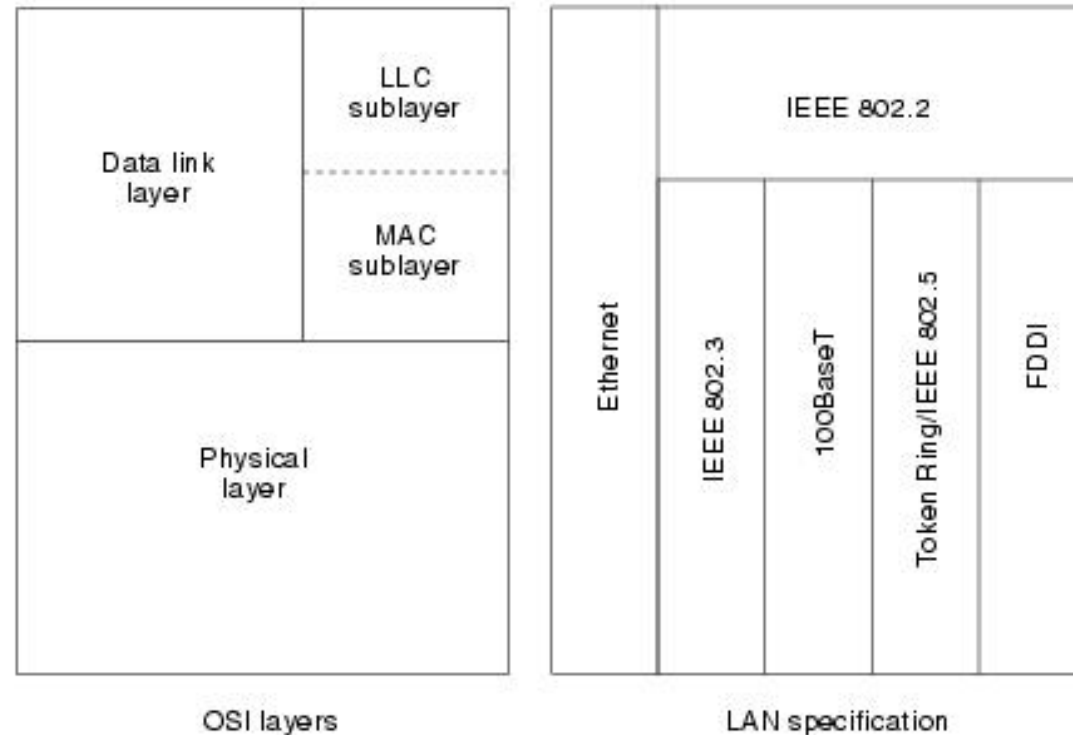
You will also Learn the Installation process of NS2

Experiment 1

Aim: Introduction to Local Area Network with its cables, connectors and topologies.

LAN Protocols and the OSI Reference Model

LAN protocols function at the lowest two layers of the OSI reference model. Following figure illustrates how several popular LAN protocols map to the OSI reference model.



MAC Addresses

Media Access Control (MAC) addresses identify network devices in LANs. MAC addresses are unique for each LAN interface on a device. MAC addresses are 48 bits in length and are expressed as 12 hexadecimal digits. The first six hexadecimal digits, which are administered by the IEEE, identify the manufacturer or vendor and comprise the organizational unique identifier (OUI). The last six hexadecimal digits comprise the interface serial number, or another value administered by the specific vendor. MAC addresses are sometimes referred to as burned-in addresses (BIAs) because they are burned into read-only memory (ROM) and are copied into random-access memory (RAM) when the interface card initializes. MAC addresses are supported at the data link layer of the OSI model. According to the IEEE's specifications, Layer 2 comprises two components: the MAC sublayer and the logical link control (LLC) sublayer. The MAC sublayer interfaces with the physical layer (OSI model Layer 1), and the LLC sublayer interfaces with the network layer (OSI model Layer 3).

Network Layer Addresses

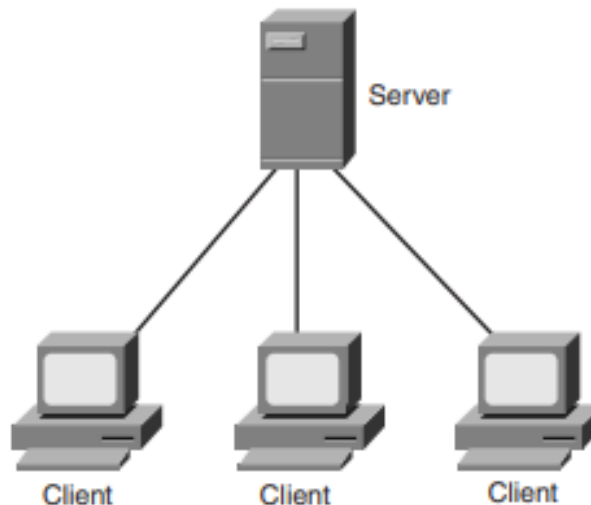
Network layer addresses identify a device at the OSI network layer (Layer 3). Network addresses exist within a hierarchical address space and sometimes are called virtual or logical addresses. Network layer addresses have two parts: the network of which the device is a part and the device, or host, number of that device on that network. Devices on the same logical network must have addresses with the same network part; however, they will have unique device parts, such as network and host addresses in an IP or IPX network. For example, an IP address is often expressed as a dotted decimal notation, such as x.x.x.x. Each x in the address indicates either a network or host number, demonstrated as n.n.h.h. The subnet mask determines where the network boundary ends and the host boundary begins.

LAN transmissions fit into one of three categories:

- Unicast
- Multicast
- Broadcast

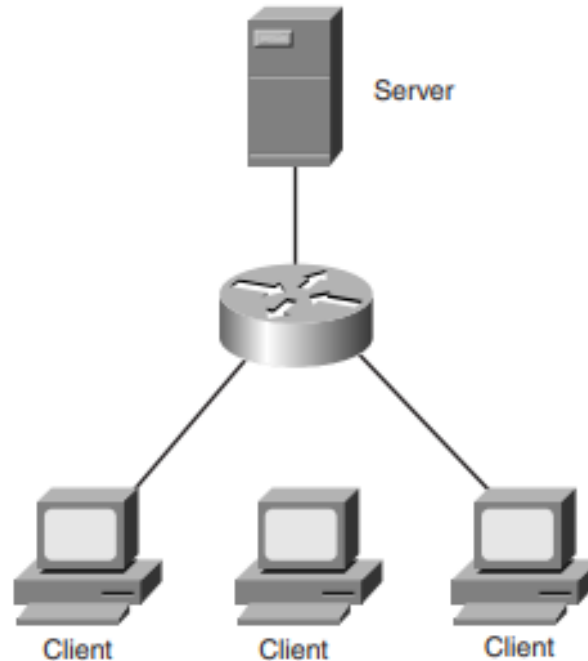
Unicast

With unicast transmissions, a single packet is sent from the source to a destination on a network. The source-node addresses the packet by using the network address of the destination node. The packet is then forwarded to the destination network and the network passes the packet to its final destination.



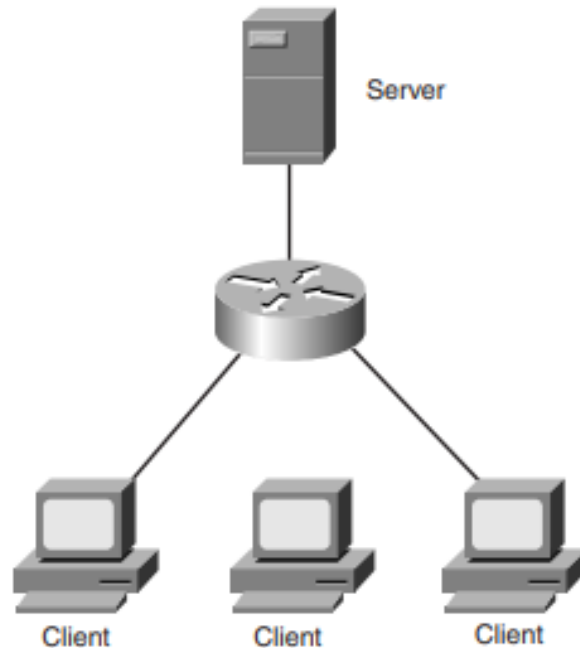
Multicast

- With a multicast transmission, a single data packet is copied and forwarded to a specific subset of nodes on the network. The source node addresses the packet by using a multicast address. For example, the TCP/IP suite uses 224.0.0.0 to 239.255.255.255. The packet is then sent to the network, which makes copies of the packet and sends a copy to each segment with a node that is part of the multicast address.



Broadcast

Broadcasts are found in LAN environments. Broadcasts do not traverse a WAN unless the Layer 3 edge-routing device is configured with a helper address (or the like) to direct these broadcasts to a specified network address. This Layer 3 routing device acts as an interface between the local-area network (LAN) and the wide-area network (WAN).

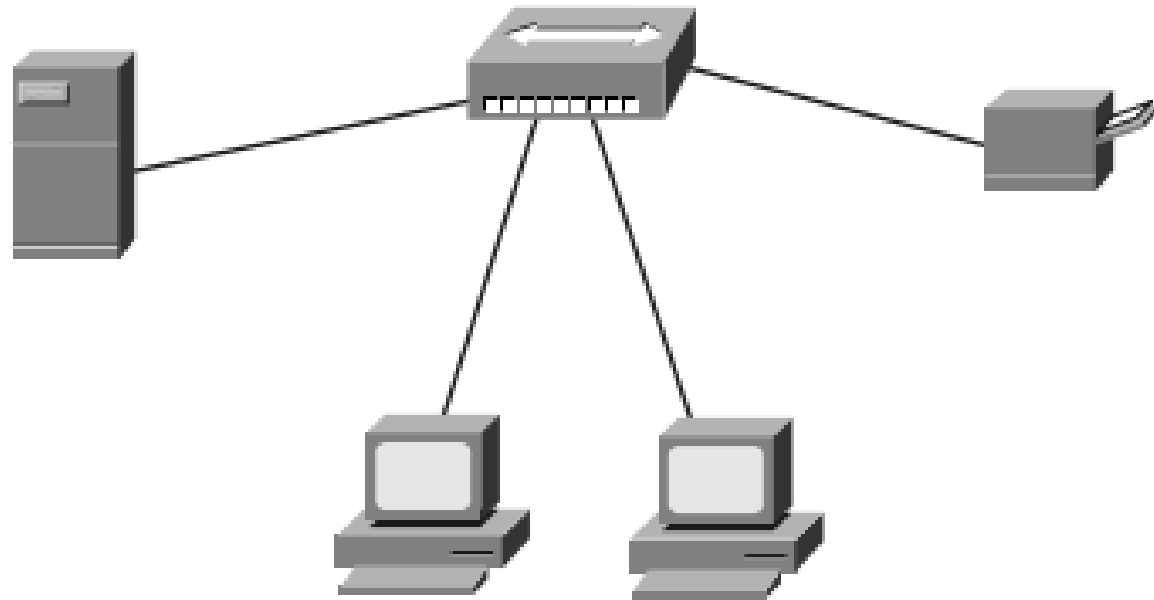


Four LAN topologies exist:

- Star (Hub-and-Spoke)
- Ring
- Bus
- Tree

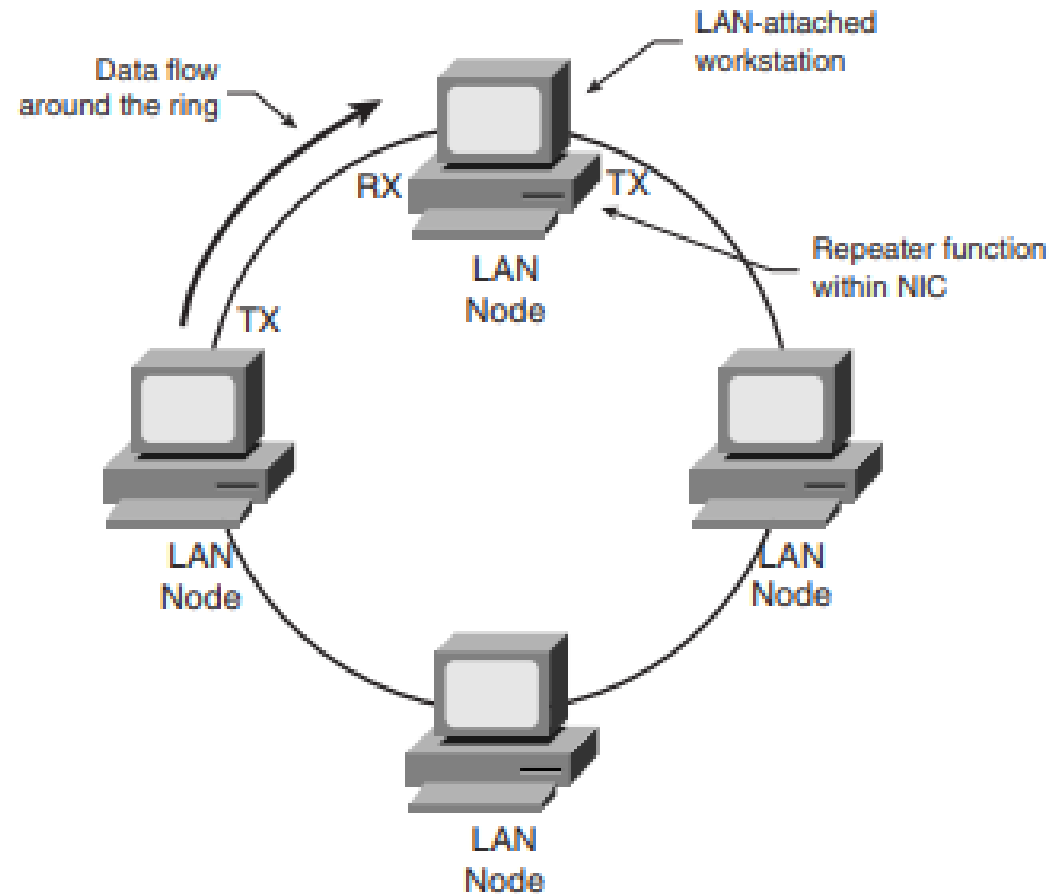
Star (Hub-and-Spoke) Topology

All stations are attached by cable to a central point, usually a wiring hub or other device operating in a similar function. Several different cable types can be used for this point-to-point link, such as shielded twisted-pair (STP), unshielded twisted-pair (UTP), and fiber-optic cabling. Wireless media can also be used for communications links.



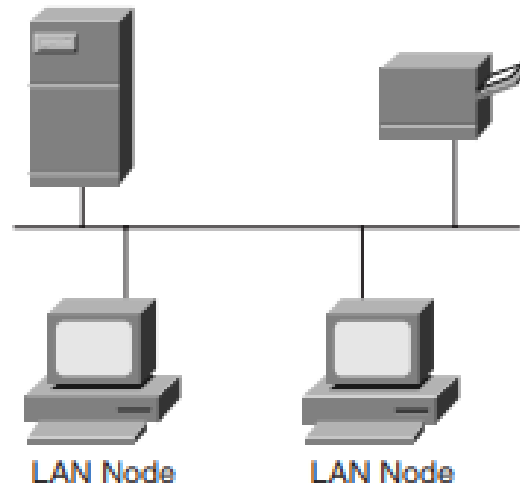
Ring Topology

All stations in a ring topology are considered repeaters and are enclosed in a loop. Unlike the star (hub-and-spoke) topology, a ring topology has no end points. The repeater in this case is a function of the LAN-attached station's network interface card (NIC).



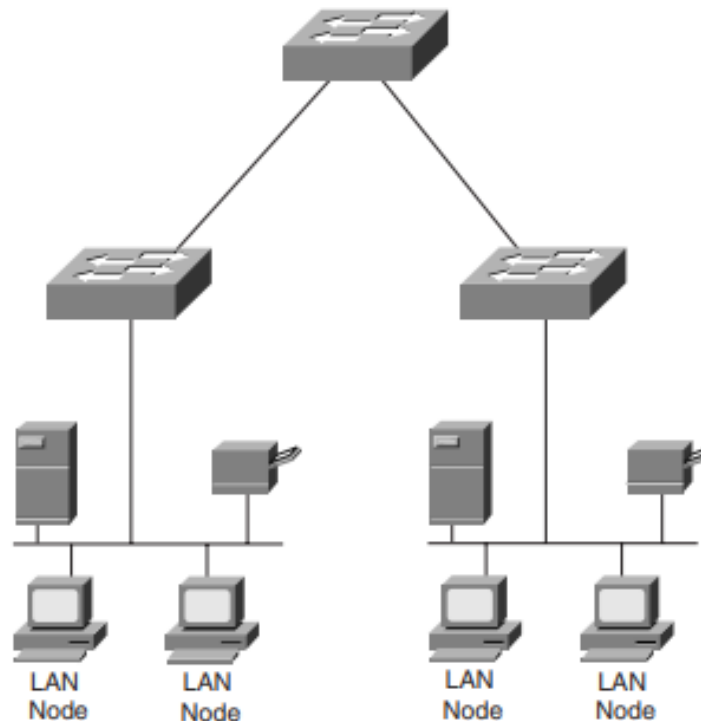
- Bus Topology

- Sometimes referred to as linear-bus topology, Bus is a simple design that utilizes a single length of cable, also known as the medium, with directly attached LAN stations. All stations share this cable segment. Every station on this segment sees transmissions from every other station on the cable segment; this is known as a broadcast medium. The LAN attachment stations are definite endpoints to the cable segment and are known as bus network termination points. This single cable segment lends itself to being a single point of failure. If the cable is broken, no LAN station will have connectivity or the ability to transmit and receive Ethernet (IEEE 802.3) best represents this topology. Ethernet has the ability to utilize many different cable schemes.



Tree Topology

- The tree topology is a logical extension of the bus topology and could be described as multiple interconnected bus networks. The physical (cable) plant is known as a branching tree with all stations attached to it. The tree begins at the root, the pinnacle point, and expands to the network endpoints. This topology allows a network to expand dynamically with only one active data path between any two network endpoints. A tree topology network is one that does not employ loops in its topology. An example of a tree topology network is a bridged or switched network running the spanning tree algorithm, usually found with Ethernet (IEEE 802.3) networks. The spanning tree algorithm disables loops in what would otherwise be a looped topology. Spanning tree expands through the network and ensures that only one active path exists between any two LAN-attached stations



Connector, Cables

- Type of network cable connector (such as RJ-45, RJ-11, USB, MT-RJ, Coaxial BNC, LC Local Connector, MT-RJ, USB BNC and AUI) is used to connect what type of network cable.
- USB (Universal Serial Bus)
- Universal Serial Bus, or USB, is a computer standard designed to eliminate the guesswork in connecting peripherals to a PC. It is expected to replace serial and parallel ports. A single USB port can be used to connect up to 127 peripheral devices, such as mice, modems, keyboards, digital camera's, printers, scanners, MP3 players and many more. USB also supports Plug-and-Play installation and hot plugging.
- USB 1.1 standard supports data transfer rates of 12 Mbps.
- USB 2.0 (Also referred to as Hi-Speed USB) specification defines a new High-speed transfer rate of 480 Mb/sec.
- USB 2.0 is fully compatible with USB 1.1 and uses the same cables and connectors. USB has with two connector types. The first is Type A (on the right), This connector connects to the PC's USB port. The Type B (on the left) connector and is for connecting to the relevant peripheral. Where as the type A connector is truly standard, the Type B connector could be changed in size etc. with individual peripherals meaning they require there own unique cables.

- RJ-11 (Registered Jack)
- Standard telephone cable connectors, **RJ-11** has 4 wires (and RJ-12 has 6 wires). **RJ-11** is the acronym for Registered Jack-11, a four- or six-wire connector primarily used to connect telephone equipment.



RJ-11 Pin	Signal Name
1	VCC (5 volts regulated)
2	Power Ground
3	OneWire Data
4	OneWire Ground

RJ-45 (Registered Jack)

The acronym for **Registered Jack-45** is RJ-45. The **RJ-45** connector is an eight-wire connector that is commonly used to connect computers to a local area network (LAN), particularly Ethernet LANs. Although they are slightly larger than the more commonly used **RJ-11** connectors, RJ-45s can be used to connect some types of telephone equipment.



F-Type

The **F connector** is a type of RF connector commonly used for cable and universally for satellite television. They are also used for the cable TV connection in DOCSIS cable modems, usually with RG-6 tri-shield cable. The F connector is inexpensive, yet has good performance up to 1 GHz. One reason for its low cost is that it uses the center wire of the coaxial cable as the pin of the male connector. The male connector body is typically crimped onto the exposed outer braid. Female connectors have a 3/8-32 thread. Most male connectors have a matching threaded connecting ring, though push-on versions are also available.

- ST (Straight Tip) and SC (Subscriber Connector or Standard Connector)
- Fiber network segments always require two fiber cables: one for transmitting data, and one for receiving. Each end of a fiber cable is fitted with a plug that can be inserted into a network adapter, hub, or switch. In the North America, most cables use a square SC connector (Subscriber Connector or Standard Connector) that slides and locks into place when inserted into a node or connected to another fiber cable, Europeans use a round ST connector (Straight Tip) instead.



- Fiber LC (Local Connector)
- These connectors are used for single-mode and multimode fiber-optic cables. FC connectors offer extremely precise positioning of the fiber-optic cable with respect to the transmitter's optical source emitter and the receiver's optical detector. FC connectors feature a position locatable notch and a threaded receptacle.



MT-RJ (Mechanical Transfer Registered Jack)

MT-RJ connectors are used with single-mode and multimode fiber-optic cables. The **MT-RJ** connectors are constructed with a plastic housing and provide for accurate alignment via their metal guide pins and plastic ferrules.

Used for Gigabit ethernet. To connect to modules with **MT-RJ** interfaces, use multimode fiber-optic cables.

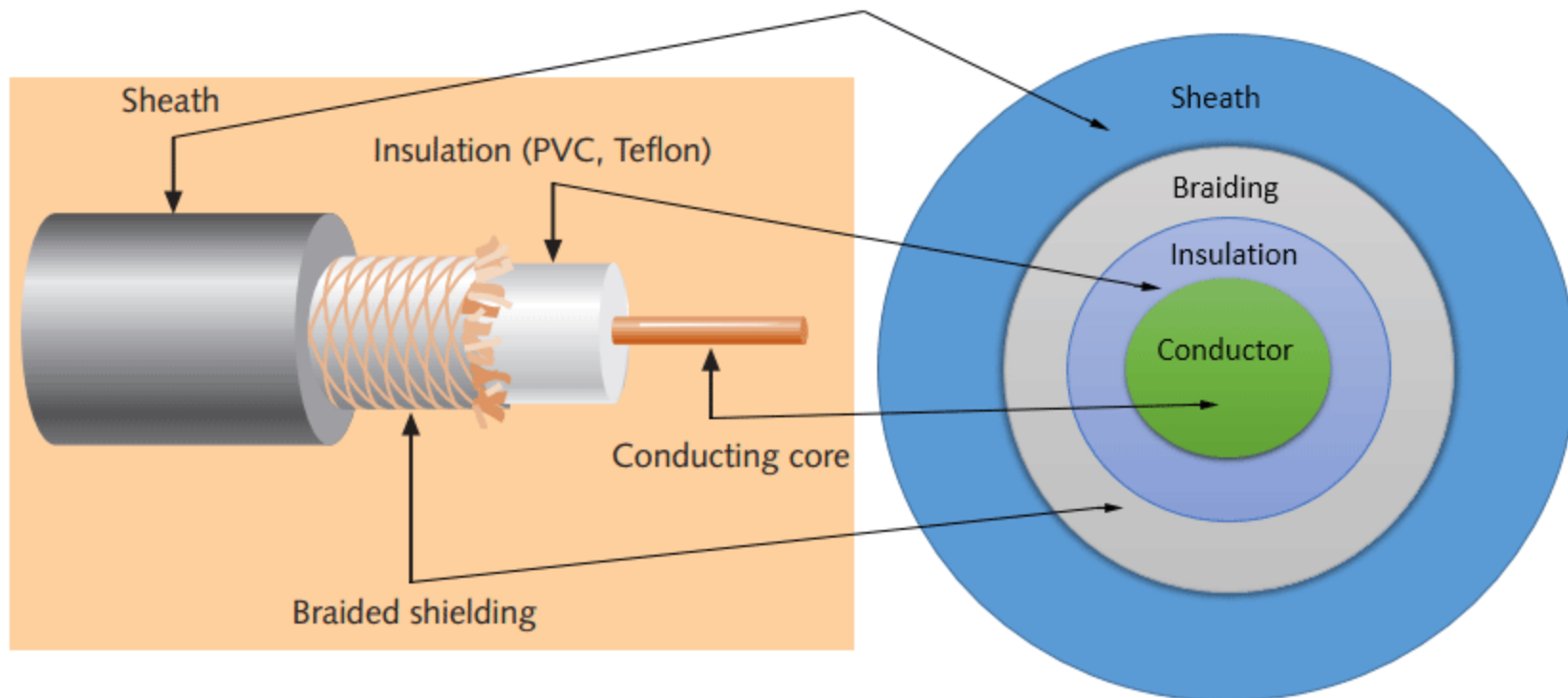


Cables

To connect two or more computers or networking devices in a network, network cables are used. There are three types of network cables; coaxial, twisted-pair, and fiber-optic.

Coaxial cable

- This cable contains a conductor, insulator, braiding, and sheath. The sheath covers the braiding, braiding covers the insulation, and the insulation covers the conductor.
- The following image shows these components.



Sheath

- This is the outer layer of the coaxial cable. It protects the cable from physical damage.

Braided shield

- This shield protects signals from external interference and noise. This shield is built from the same metal that is used to build the core.

Insulation

- Insulation protects the core. It also keeps the core separate from the braided-shield. Since both the core and the braided-shield use the same metal, without this layer, they will touch each other and create a short-circuit in the wire.

Conductor

- The conductor carries electromagnetic signals. Based on conductor a coaxial cable can be categorized into two types; single-core coaxial cable and multi-core coaxial cable.
- A **single-core** coaxial cable uses a single central metal (usually copper) conductor, while a **multi-core** coaxial cable uses multiple thin strands of metal wires. The following image shows both types of cable.



Single core coaxial cable

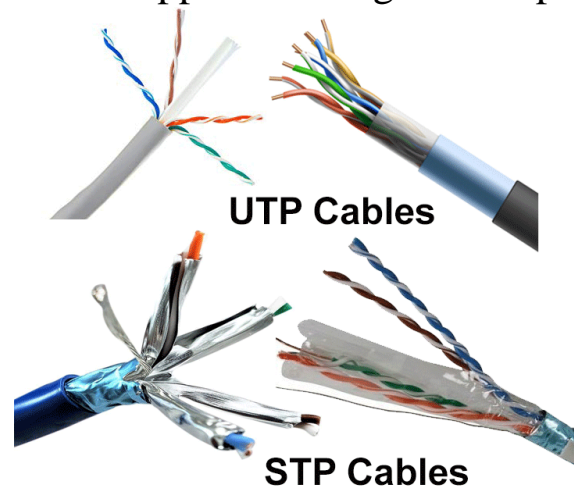


Multi-core coaxial cable

Type	Ohms	AWG	Conductor	Description
RG-6	75	18	Solid copper	Used in cable network to provide cable Internet service and cable TV over long distances.
RG-8	50	10	Solid copper	Used in the earliest computer networks. This cable was used as the backbone-cable in the bus topology. In Ethernet standards, this cable is documented as the 10base5 Thicknet cable.
RG-58	50	24	Several thin strands of copper	This cable is thinner, easier to handle and install than the RG-8 cable. This cable was used to connect a system with the backbone-cable. In Ethernet standards, this cable is documented as the 10base2 Thinnet cable.
RG-59	75	20 - 22	Solid copper	Used in cable networks to provide short-distance service.

Twisted-pair cables

- The twisted-pair cable was primarily developed for computer networks. This cable is also known as **Ethernet cable**. Almost all modern LAN computer networks use this cable.
- This cable consists of color-coded pairs of insulated copper wires. Every two wires are twisted around each other to form pair. Usually, there are four pairs. Each pair has one solid color and one stripped color wire. Solid colors are blue, brown, green and orange. In stripped color, the solid color is mixed with the white color.
- Based on how pairs are stripped in the plastic sheath, there are two types of twisted-pair cable; UTP and STP.
- In the **UTP** (*Unshielded twisted-pair*) **cable**, all pairs are wrapped in a single plastic sheath.
- In the **STP** (*Shielded twisted-pair*) **cable**, each pair is wrapped with an additional metal shield, then all pairs are wrapped in a single outer plastic sheath.

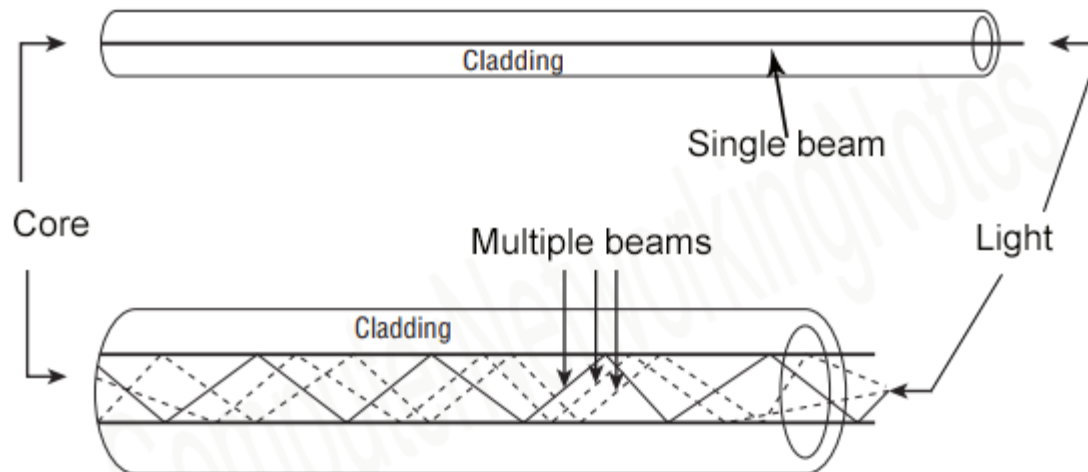


Category / name of the cable	Maximum supported speed	Bandwidth/support signals rate	Ethernet standard	Description
Cat 1	1Mbps	1MHz	Not used for data	This cable contains only two pairs (4 wires). This cable was used in the telephone network for voice transmission.
Cat 2	4Mbps	10MHz	Token Ring	This cable and all further cables have a minimum of 8 wires (4 pairs). This cable was used in the token-ring network.
Cat 3	10Mbps	16MHz	10BASE-T Ethernet	This is the first Ethernet cable that was used in LAN networks.
Cat 4	20Mbps	20MHz	Token Ring	This cable was used in advanced Token-ring networks.
Cat 5	100Mbps	100MHz	100BASE-T Ethernet	This cable was used in advanced (fast) LAN networks.
Cat 5e	1000Mbps	100MHz	1000BASE-T Ethernet	This cable/category is the minimum requirement for all modern LAN networks.
Cat 6	10Gbps	250MHz	10GBASE-T Ethernet	This cable uses a plastic core to prevent cross-talk between twisted-pair. It also uses a fire-resistant plastic sheath.
Cat 6a	10Gbps	500MHz	10GBASE-T Ethernet	This cable reduces attenuation and cross-talk. This cable also potentially removes the length limit. This is the recommended cable for all modern Ethernet LAN networks.
Cat 7	10Gbps	600MHz	Not drafted yet	This cable sets a base for further development. This cable uses multiple twisted-pairs and shields each pair by its own plastic sheath.

Fiber optic cable

- This cable consists of core, cladding, buffer, and jacket. The core is made from the thin strands of glass or plastic that can carry data over the long distance. The core is wrapped in the cladding; the cladding is wrapped in the buffer, and the buffer is wrapped in the jacket.
- Core carries the data signals in the form of the light.
- Cladding reflects light back to the core.
- Buffer protects the light from leaking.
- The jacket protects the cable from physical damage.
- Fiber optic cable is completely immune to EMI and RFI. This cable can transmit data over a long distance at the highest speed. It can transmit data up to 40 kilometers at the speed of 100Gbps.
- Fiber optic uses light to send data. It reflects light from one endpoint to another. Based on how many beams of light are transmitted at a given time, there are two types of fiber optical cable; SMF and MMF.

SMF (Single mode fiber) optical cable



MMF (multi-mode fiber) optical cable

Network Devices The four primary devices used in LANs are as follows:

Hubs

Bridges

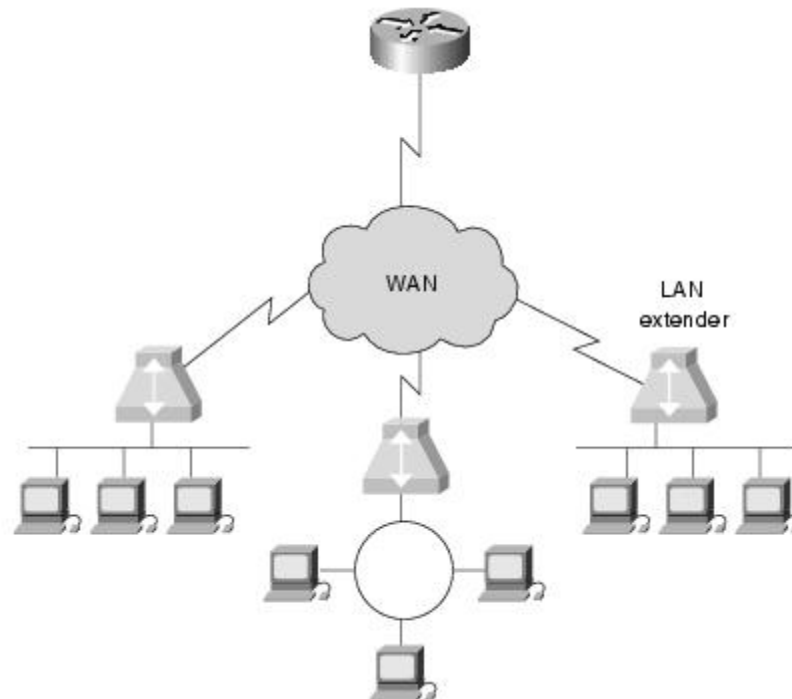
Switches

Routers

Repeaters

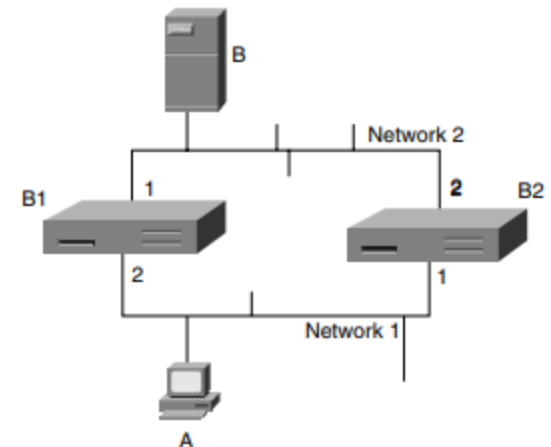
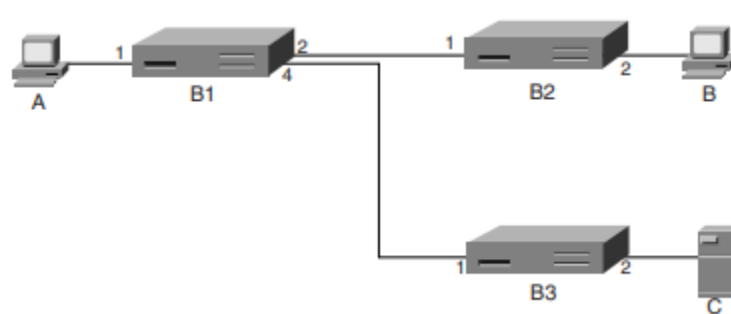
Hubs

Hubs operate at the physical layer (Layer 1) of the OSI model. A hub is used to connect devices so that they are on one shared LAN



Bridges

- Bridges have a physical layer (Layer 1), but are said to operate at the data link layer (Layer 2) of the OSI model. Bridges forward data frames based on the destination MAC address.
- Bridges also forward frames based on frame header information. Bridges create multiple collision domains and are generally deployed to provide more useable bandwidth. Bridges don't stop broadcast traffic; they forward broadcast traffic out every port of each bridge device. Each port on a bridge has a separate bandwidth (collision) domain, but all ports are on the same broadcast domain.



Experiment 4

Aim: Case Study of Ethernet (10 base 5,10 base 2,10 base T)

Ethernet is a family of frame-based computer networking technologies for local area networks (LANs). The name comes from the physical concept of the ether. It defines a number of wiring and signaling standards for the physical layer, through means of network access at the Media Access Control (MAC)/Data Link Layer, and a common addressing format.

Ethernet is standardized as IEEE 802.3. The combination of the twisted pair versions of Ethernet for connecting end systems to the network, along with the fiber optic versions for site backbones, is the most widespread wired LAN technology. It has been in use from around 1980 to the present, largely replacing competing LAN standards such as token ring, FDDI, and ARCNET. In recent years, Wi-Fi, the wireless LAN standardized by IEEE 802.11, is prevalent in home and small office networks and augmenting Ethernet in larger installations.

10BASE2

10BASE2 (also known as *cheapernet*, *thin ethernet*, *thinnet* or *thinwire*) is a variant of Ethernet that uses thin coaxial cable (RG-58 or similar, as opposed to the thicker RG-8 cable used in 10BASE5 networks), terminated with BNC connectors. For many years this was the dominant 10 Mbit/s Ethernet standard, but due to the immense demand for high speed networking, the low cost of Category 5 Ethernet cable, and the popularity of 802.11 wireless networks, both 10BASE2 and 10BASE5 have become almost obsolete.





Network design

In a 10BASE2 network, each segment of cable is connected to the transceiver(which is usually built into the network adaptor) using a BNC T-connector, with one segment connected to each arm of the T. At the physical end of the network a 50 Ohm terminator is required. This is most commonly connected directly to the T-connector on a workstation though it does not technically have to be.

When wiring a 10BASE2 network, special care has to be taken to ensure that cables are properly connected to all T-connectors, and appropriate terminators are installed. One, and only one, terminator must be connected to ground via a ground wire. Bad contacts or shorts are especially difficult to diagnose, though a time-domain reflectometer will find most problems quickly. A failure at any point of the network cabling tends to prevent all communications. For this reason, 10BASE2 networks could be difficult to maintain and were often replaced by 10BASE-T networks, which (provided category 3 cable or better was used) also provided a good upgrade path to 100BASE-TX. An alternative reliable connection has been established by the introduction of EAD-sockets

Comparisons to 10BASE-T

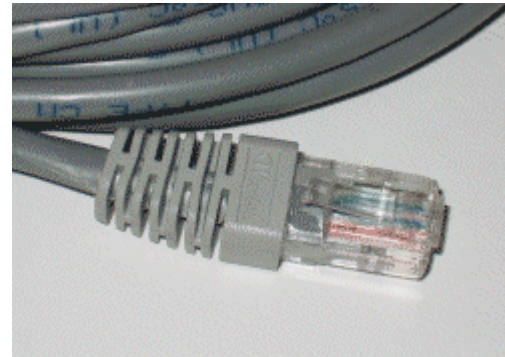
- 10BASE2 networks cannot generally be extended without breaking service temporarily for existing users and the presence of many joints in the cable also makes them very vulnerable to accidental or malicious disruption. There were proprietary wallport/cable systems that claimed to avoid these problems (e.g. *SaferTap*) but these never became widespread, possibly due to a lack of standardization.
- 10BASE2 systems do have a number of advantages over 10BASE-T. They do not need the 10BASE-T hub, so the hardware cost is very cheap, and wiring can be particularly easy since only a single wire run is needed, which can be sourced from the nearest computer. These characteristics mean that 10BASE2 is ideal for a small network of two or three machines, perhaps in a home where easily concealed wiring may be an advantage. For a larger complex office network the difficulties of tracing poor connections make it impractical. Unfortunately for 10BASE2, by the time multiple home computer networks became common, the format had already been practically superseded. As a matter of fact, it is becoming very difficult to find 10BASE2-compatible network cards as distinct pieces of equipment, and integrated LAN controllers on motherboards don't have the connector, although the underlying logic may still be present.
- **10BASE5**
- **10BASE5** (also known as **thicknet**) is the original "full spec" variant of Ethernet cable, using special cable similar to RG-8/U coaxial cable. This is a stiff, 0.375 inch (approx. 9.5 mm) diameter cable with an impedance of 50 ohms, a solid center conductor, a foam insulating filler, a shielding braid, and an outer jacket. The outer sheath is often yellow-to-orange/brown foam fluorinated ethylene propylene (for fire resistance) so it frequently is just called "yellow cable", "orange hose", or sometimes humorously "frozen yellow garden hose". 10BASE5 is obsolete, though due to its widespread deployment in the early days, some systems may still be in use.

- **Network design**
- 10BASE5 cable is designed to allow transceivers to be added while existing connections are live. This is achieved using a *vampire tap* - a device which (with sufficient practice) clamps onto the cable, forcing a spike to pierce through the outer shielding to contact the inner conductor while other spikes bite into the outer conductor. This is often built into the transceiver and a more flexible multi-wire cable carries the connection between the transceiver and the node. Transceivers can also be connected by using N connectors at the end of a cable segment.
- The maximum practical number of nodes that can be connected to a 10BASE5 segment is limited to 100 and transceivers may be installed only at 2.5 metre intervals. This distance was chosen to *not* correspond to the wavelength of the signal; this ensures that the reflections from multiple taps are not in phase. These suitable points are marked on the cable with black bands. The cable must be one linear run; T-connections are not allowed. A 50 ohm resistive terminator is required at each end of the cable.
- The transceivers connect to nodes using an interface called Attachment Unit Interface (AUI). This interface uses a 15 pin, two row D-style connector but with clips instead of the more normal screws for cable restraint.



Ethernet over twisted pair(10 BASE T)

- There are several standards for **Ethernet over twisted pair** or copper-based computer networking physical connectivity methods. The currently most widely used of these are **10BASE-T**, **100BASE-TX**, and **1000BASE-T**(Gigabit Ethernet), running at 10 Mbit/s, 100 Mbit/s, and 1000 Mbit/s (1 Gbit/s) respectively. These three standards all use the same connectors. Higher speed implementations nearly always support the lower speeds as well, so that in most cases different generations of equipment can be freely mixed. They use 8 position modular connectors, usually (but incorrectly) called RJ45 in the context of Ethernet over twisted pair. The cables usually used are four-pair Category 5 or above twisted pair cable. Each of the three standards support both full duplex and half-duplex communication. According to the standards, they all operate over distances of 'up to 100 meters'.



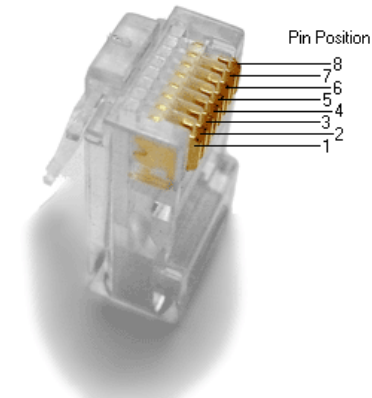
- The common names of the standards are derived from several aspects of the physical media. The **number** refers to the theoretical maximum transmission speed in Megabits per second (Mbit/s). The **BASE** is short for baseband, meaning that there is no frequency division multiplexing (FDM) or other frequency shifting modulation in use; each signal has full control of wire, on a single frequency. The **T** designates twisted pair cable, where the pairs of wires are twisted together for purposes of reducing crosstalk (FEXT and NEXT) when the pulsing direct current goes across the wires and creates electromagnetic induction effects. Where there are several standards for the same transmission speed, they are distinguished by a letter or digit following the T, such as TX. Some higher-speed standards use twin-axial cable, designated by CX.

Cabling

- Twisted-pair Ethernet standards are such that the majority of cables can be wired 'straight-through' (pin 1 to pin 1, pin 2 to pin 2 and so on), but others may need to be wired in the 'crossover' form (receive to transmit and transmit to receive).
- 10BASE-T and 100BASE-TX only require two pairs to operate, pins 1 and 2 (transmit or TX), and pins 3 and 6 (receive or RX). Since 10BASE-T and 100BASE-TX need only two pairs and Category 5 cable has four pairs, it is possible, but not standard, to run two network connections (or a network connection and two phone lines) over a cat 5 cable by using the normally unused pairs in these 10 and 100 Mbit/s configurations. This is not possible with 1000BASE-T since it requires all four pairs to operate, pins 1 and 2, 3 and 6 — as well as 4 and 5, 7 and 8.
- It is conventional to wire cables for 10 or 100 Mbit/s Ethernet to either the T568A or T568B standards. Since these standards only differ in that they swap the positions of the two pairs used for transmitting and receiving (TX/RX), a cable with TIA-568A wiring at one end and TIA-568B wiring at the other will be a crossover cable. The terms used in the explanations of the 568 standards, tip and ring, refer to older communication technologies, and equate to the positive and negative parts of the connections.

- A 10BASE-T node (such as a PC) that transmits on pins 1/2 and receives on pins 3/6 to a network device is most often on a "straight-through" cable in the "MDI" wiring pattern where RX goes to RX and TX goes to TX. A straight-through cable is usually used to connect a node to its network device. In order for two network devices or two nodes to communicate with each other (such as a switch to another switch or computer to computer) a crossover cable is often required at speeds of 10 or 100. If available, connections can be made with a straight-through cable by means of an "MDI-X" port, also known as an "internal crossover" or "embedded crossover" connection. Hub and switch ports with such internal crossovers are usually labelled as such, with "uplink" or "X". For example, 3Com usually labels their ports 1X, 2X, and so on.
- To connect two PCs directly together without a switch, an Ethernet crossover cable is often used. Although many modern Ethernet host adapters can automatically detect another PC connected with a straight-through cable and then automatically introduce the required crossover, if needed; if one or neither of the PC does not, then a crossover cable is required. If both devices being connected support 1000BASE-T according to the standards, they will connect regardless of the cable being used or how it is wired.
- To connect two hubs or switches directly together, a crossover cable can be used, but some hubs and switches have an "uplink" port used to connect network devices together, or have a way to manually select MDI or MDI-X on a single port so that a straight-through cable can connect that port to another switch or hub. Most newer switches have automatic crossover ("auto MDI-X" or "auto-uplink") on all ports, eliminating the uplink port and the MDI/MDI-X switch, and allowing all connections to be made with straight-through cables.
- 100BASE-TX follows the same wiring patterns as 10BASE-T but is more sensitive to wire quality and length, due to the higher bit rates.
- 1000BASE-T uses all four pairs bi-directionally and the standard includes auto MDI-X, however implementation is optional. With the way that 1000BASE-T implements signaling, how the cable is wired is immaterial in actual usage. The standard on copper twisted pair is IEEE 802.3ab for Cat 5e UTP, or 4D-PAM5; 4 Directions using PAM (pulse amplitude modulation) with 5 voltages, -2, -1, 0, +1, and +2

- Unlike earlier Ethernet standards using broadband and coaxial cable, such as 10BASE5 (thicknet) and 10BASE2 (thinnet), 10BASE-T does not specify the exact type of wiring to be used but instead specifies certain "characteristics" which a cable must meet. This was done in anticipation of using 10BASE-T in existing twisted pair wiring systems that may not conform to any specified wiring standard. Some of the specified characteristics are attenuation, characteristic impedance, timing jitter, propagation delay, and several types of noise. Cable testers are widely available to check these parameters to determine if a cable can be used with 10BASE-T. These characteristics are expected to be met by 100 meters of 24 gauge unshielded twisted-pair cable, and 100 meters is the stated maximum length for baseband signal runs. However, with high quality cabling, cable runs of 150 meters or longer are often obtained and are considered viable by most technicians familiar with the 10baseT specification, though -- as with all CSMA/CD network environments — the absolute limit on run length is determined by the size of the collision domain and cable quality. In reality, what meets the standards may not work, and those that don't meet the standards might work.
- 100BASE-TX and 1000BASE-T both require a minimum of Category 5 cable (5e or 6 with 1000) and also specify a maximum cable length of 100 meters. Furthermore while 10BASE-T is more tolerant of poor wiring such as split pairs, poor terminations and even use of short sections of flat cable, 100BASE-T is not as much so, and 1000BASE-T is less tolerant still. Since testing of cable is often limited to checking if it works with Ethernet, running faster speeds over existing cable is often problematic. This problem is made worse by the fact that Ethernet's auto negotiation takes account only of the capabilities of the end equipment not of the cable in between.



TIA/EIA-568-A T568A Wiring

Pin	Pair	Wire	Color
1	3	tip	white/green
2	3	ring	green
3	2	tip	white/orange
4	1	ring	blue
5	1	tip	white/blue
6	2	ring	orange
7	4	tip	white/brown
8	4	ring	brown

TIA/EIA-568-A T568A Wiring

Pin	Pair	Wire	Color
1	3	tip	white/green
2	3	ring	green
3	2	tip	white/orange
4	1	ring	blue
5	1	tip	white/blue
6	2	ring	orange
7	4	tip	white/brown
8	4	ring	brown

Experiment No: 7

Aim: Installation and working with FTP.

- Setting up a File Transfer Protocol (FTP) server on Windows 10 is perhaps one of the most convenient solutions to upload and download files from virtually anywhere to your computer without the limitations typically found with cloud storage services.
- Using an FTP server, you're basically creating a private cloud that you have absolute control. You don't have monthly transfers caps and speeds can be fast (depending on your internet subscription).
- Also, there not file type or size restrictions, which means that you can transfer a 1KB text file as well as 1TB backup file, and you can create as many accounts as you want to let family and friends store and share files with each other.
- There are plenty third-party solutions to set up a file server of this kind, but even though it may sound complicated, the FTP feature bundled on Windows 10 isn't difficult to set up.
- In this Windows 10 guide, we'll walk you through the steps to set up and manage an FTP server on your computer to transfer files within your home network or remotely over the internet.
- **How to install the FTP server components on Windows 10**
- Although Windows 10 includes support to set up an FTP server, you need to add the required components manually.
- To install the FTP server components, do the following:
- Open **Control Panel**.
- Click on **Programs**.
- Under "Programs and Features," click the **Turn Windows features on or off** link.

Programs

← → ▾ ↑  > Control Panel > Programs >



Search Control Panel



File Edit View Tools

Control Panel Home

System and Security

Network and Internet

Hardware and Sound

• Programs

User Accounts

Appearance and
Personalization

Clock and Region

Ease of Access



Programs and Features

Uninstall a program



Turn Windows features on or off

View installed updates

Run programs made for previous versions of Windows

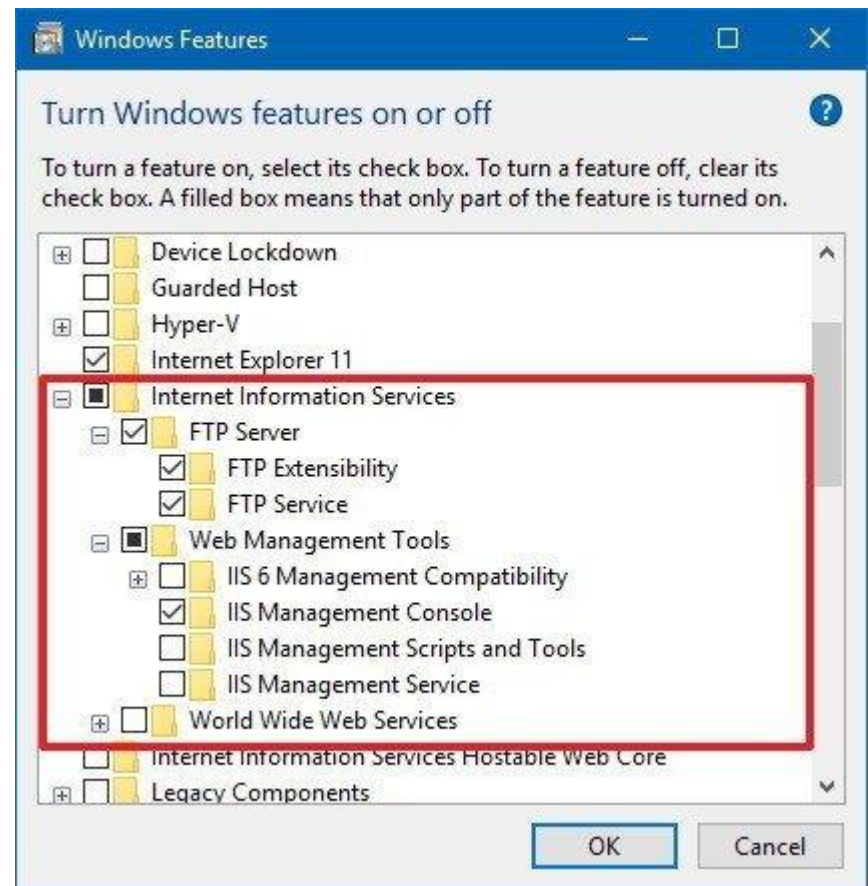
How to install a program



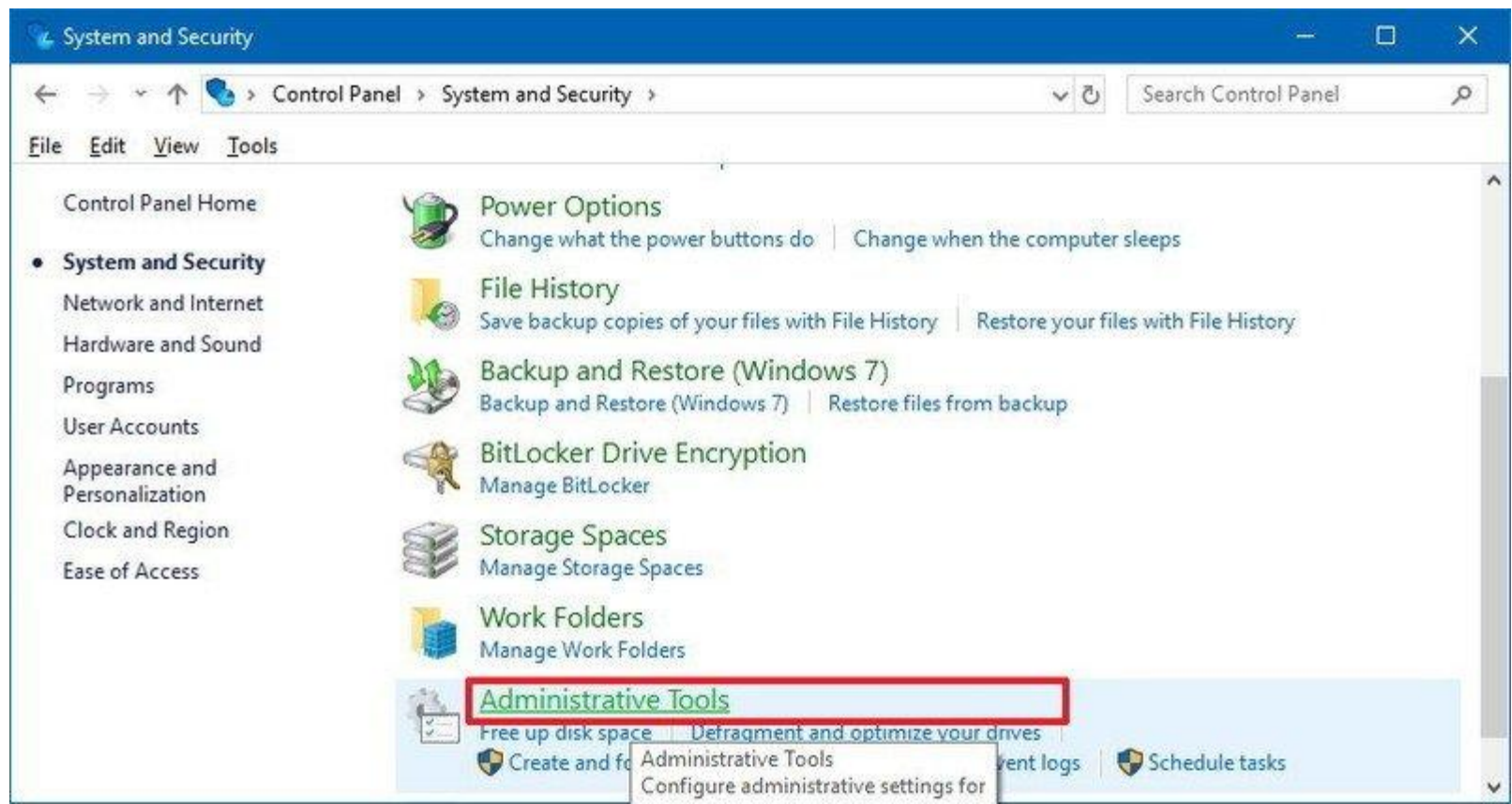
Default Programs

Change default settings for media or devices

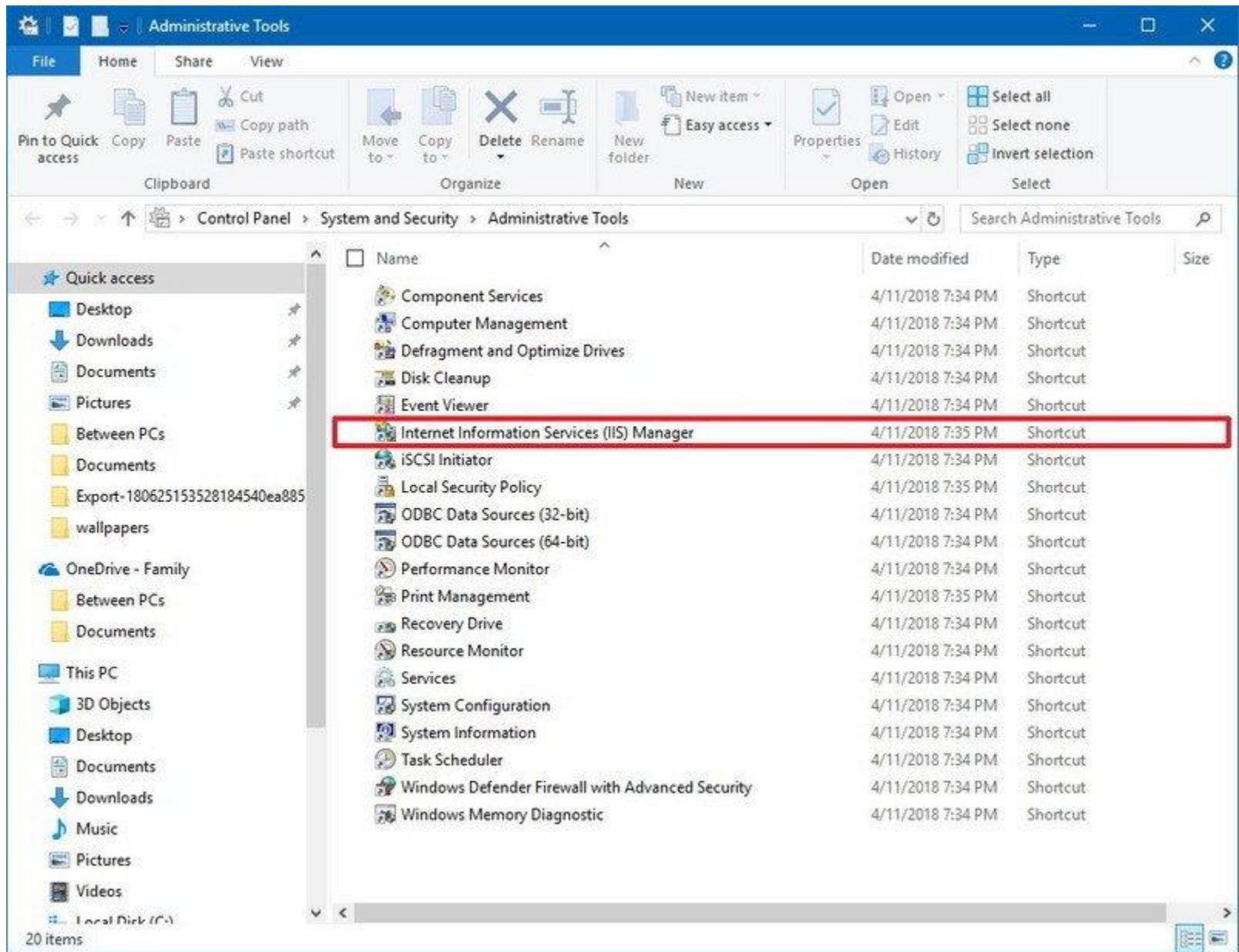
- Expand the "Internet Information Services" feature, and expand the **FTP server** option.
- Check the **FTP Extensibility** and **FTP Service** options.
- Check the **Web Management Tools** option with the default selections, but making sure that the **IIS Management Console** option is checked.
- Click the **OK** button.
- Click the **Close** button.



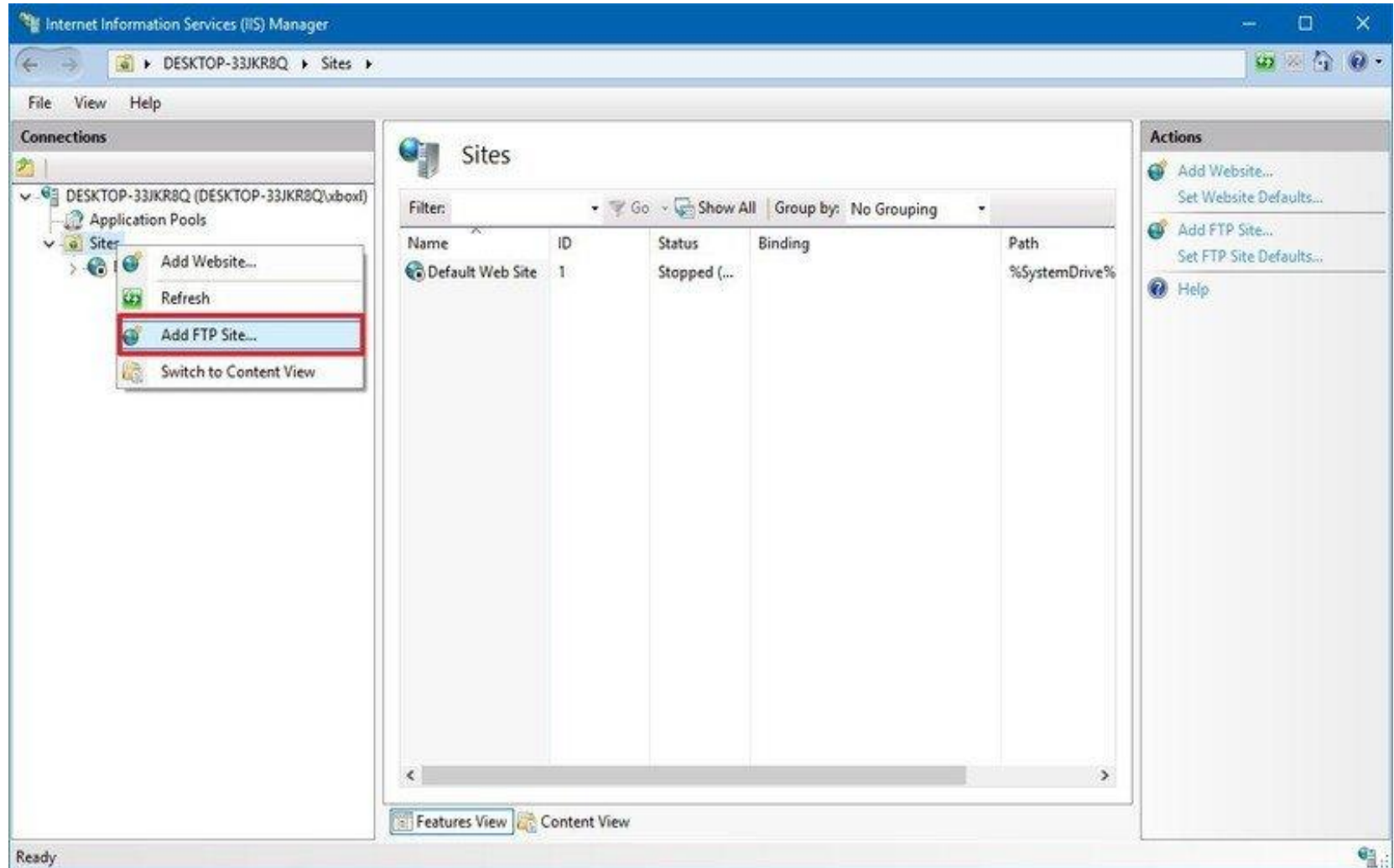
- **How to configure an FTP server site on Windows 10**
- After installing the required components, you can proceed to configure an FTP server on the computer, which involves creating a new FTP site, setting up firewall rules, and allowing external connections.
- **Setting up an FTP site**
- To set up an FTP site, do the following:
- Open **Control Panel**.
- Click on **System and Security**.
- Click on **Administrative Tools**.



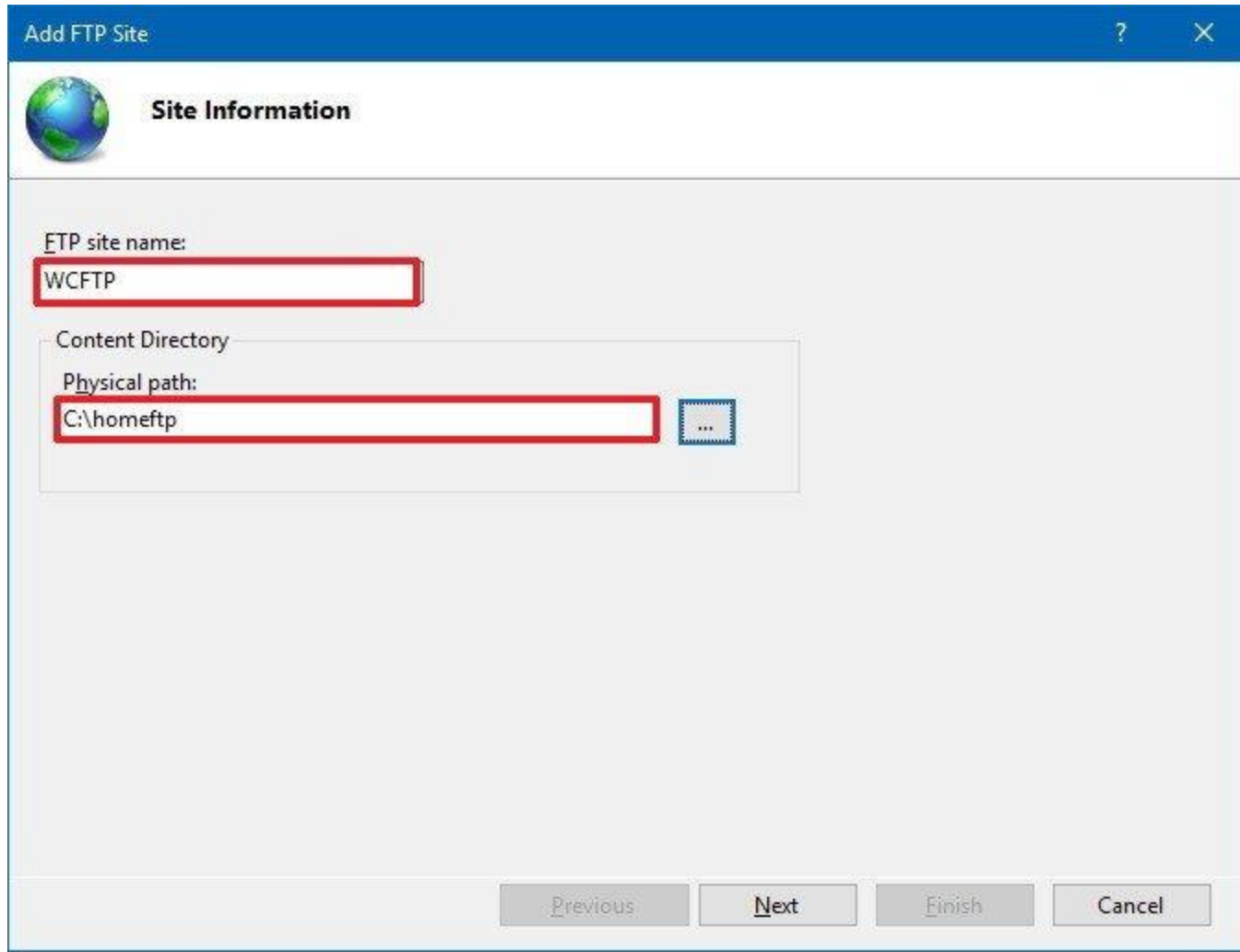
- Double-click the **Internet Information Services (IIS) Manager** shortcut.



- On the "Connections" pane, right-click **Sites**, and select the **Add FTP Site** option.




- In the FTP site name, type a short descriptive name for the server.
- In the "Content Directory" section, under "Physical path," click the button on the right to locate the folder you want to use to store your FTP files.
- **Quick Tip:** It's recommended to create a folder in the root of the main system drive, or on an entirely different hard drive. Otherwise, if you set the home folder in one of your default folders when adding multiple accounts, users won't have permission to access the folder. (You can adjust folder permissions, but it's not recommended.)




The screenshot shows the 'Add FTP Site' wizard in Windows, specifically the 'Site Information' step. The window has a blue title bar with the text 'Add FTP Site' and standard window controls. Below the title bar is a header section with a globe icon and the text 'Site Information'. The main area contains two input fields: 'FTP site name:' with the value 'WCFTP' and 'Content Directory' section containing 'Physical path:' with the value 'C:\homeftp'. A red rectangle highlights the 'FTP site name' field, and another red rectangle highlights the 'Physical path' field. To the right of the 'Physical path' field is a small button with three dots. At the bottom of the window are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

Add FTP Site

 **Site Information**

FTP site name:
WCFTP

Content Directory

Physical path:
C:\homeftp 

Previous Next Finish Cancel

- Click the **Next** button.
- Use the default **Binding** settings selections.
- Check the **Start FTP site automatically** option.
- In the "SSL" section, check the **No SSL** option.

The screenshot shows the 'Add FTP Site' dialog box with the 'Binding and SSL Settings' tab selected. The 'Binding' section has 'All Unassigned' selected for the IP Address and '21' for the Port. The 'Start FTP site automatically' checkbox is checked. In the 'SSL' section, the 'No SSL' radio button is selected and highlighted with a red rectangle. The 'SSL Certificate' dropdown is set to 'Not Selected'. At the bottom, the 'Next' button is highlighted with a blue border.

Add FTP Site

Binding and SSL Settings

Binding

IP Address: All Unassigned Port: 21

☐ Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

☒ Start FTP site automatically

SSL

☒ No SSL

☐ Allow SSL

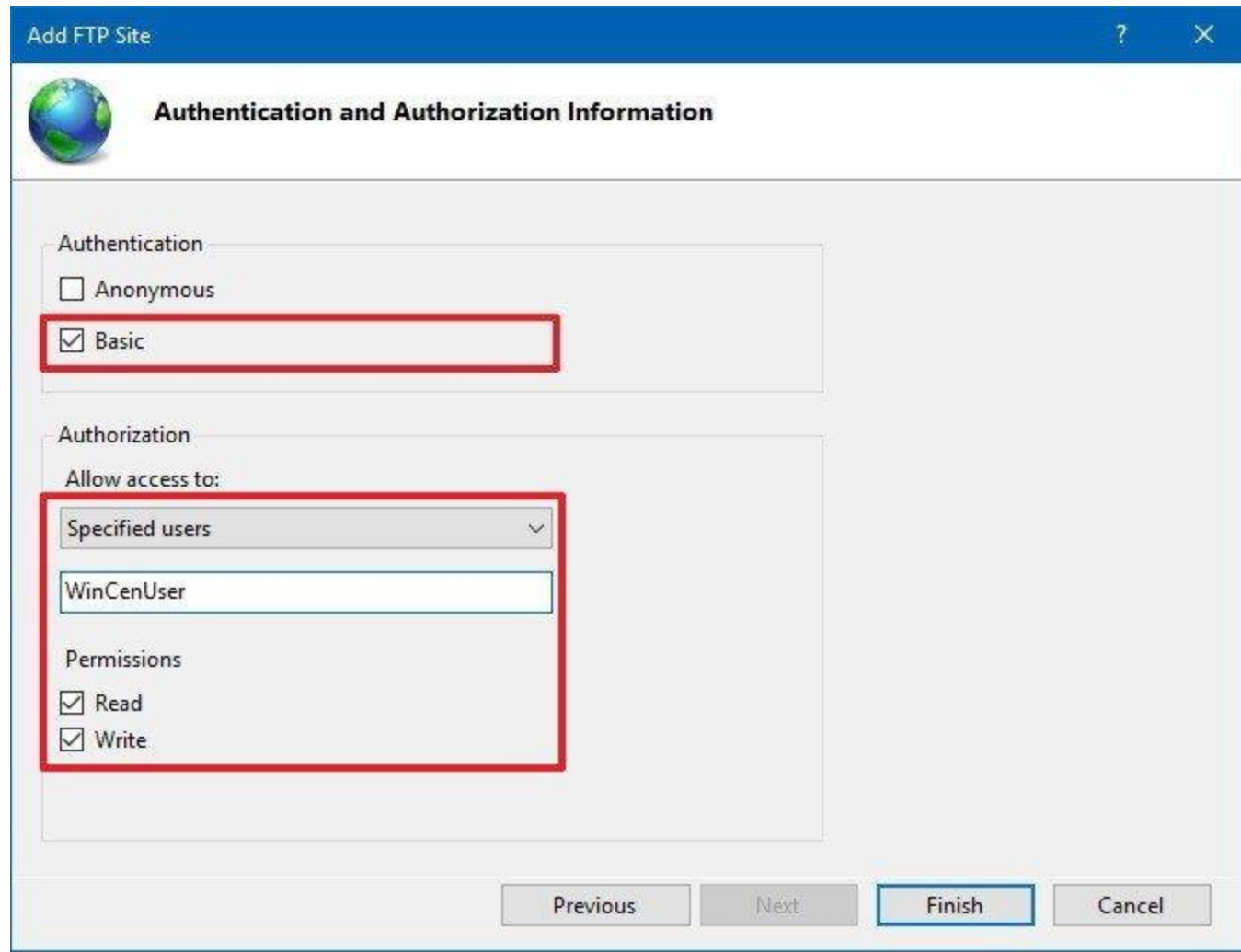
☐ Require SSL

SSL Certificate: Not Selected

Select... View...

Previous **Next** Finish Cancel

- Click the **Next** button.
- In the "Authentication" section, check the **Basic** option.
- In the "Authorization" section, use the drop-down menu, and select **Specified users** option.
- Type the email address of your Windows 10 account or local account name to allow yourself access to the FTP server.
- Check the **Read** and **Write** options.



The screenshot shows the 'Add FTP Site' dialog box with the 'Authentication and Authorization Information' tab selected. The 'Authentication' section has the 'Basic' option checked. The 'Authorization' section has the 'Allow access to:' dropdown set to 'Specified users', with 'WinCenUser' entered in the text box below. The 'Permissions' section has both 'Read' and 'Write' options checked. The 'Finish' button is highlighted with a blue border.

Add FTP Site

Authentication and Authorization Information

Authentication

☐ Anonymous

☒ Basic

Authorization

Allow access to:

Specified users

WinCenUser

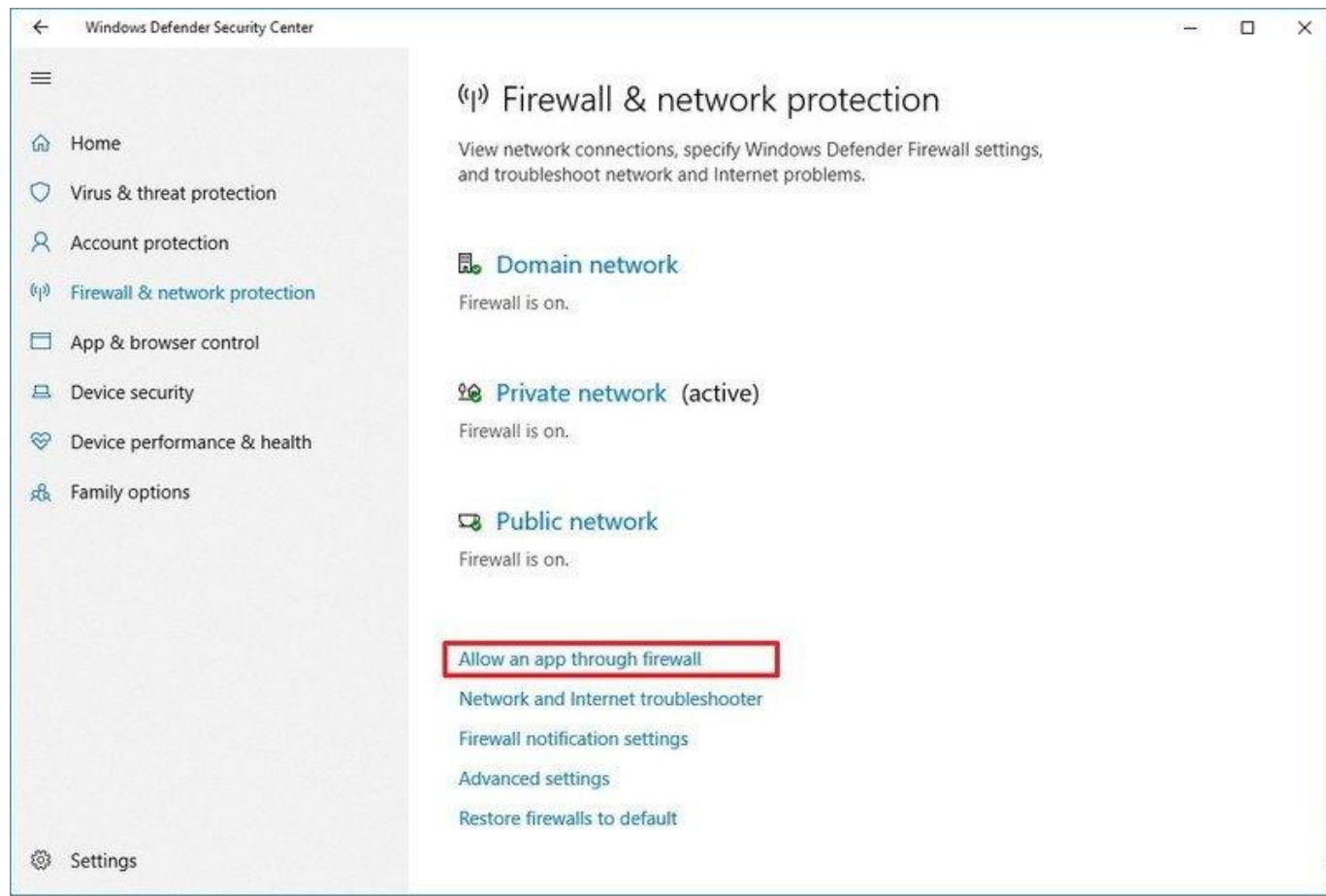
Permissions

☒ Read

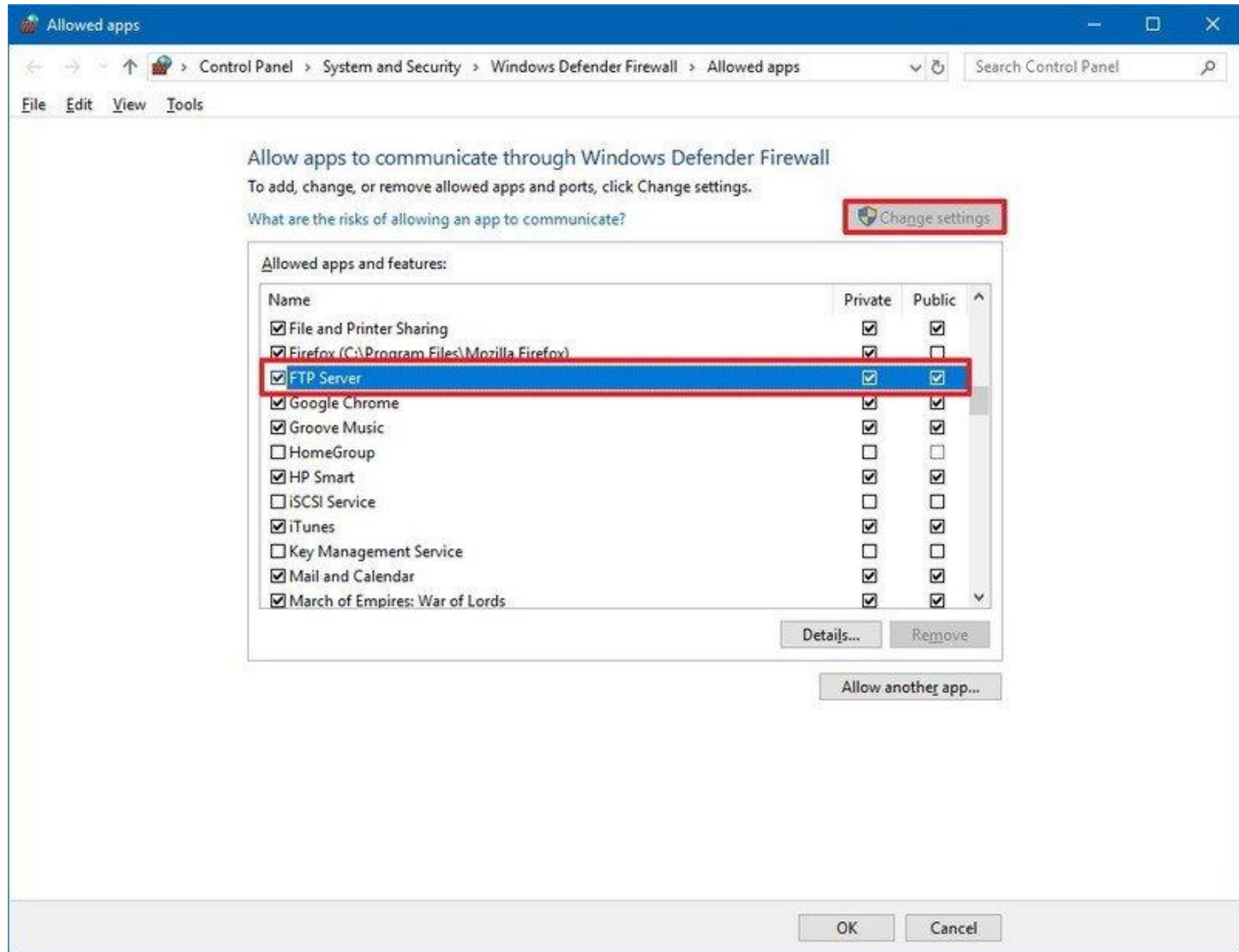
☒ Write

Previous Next **Finish** Cancel

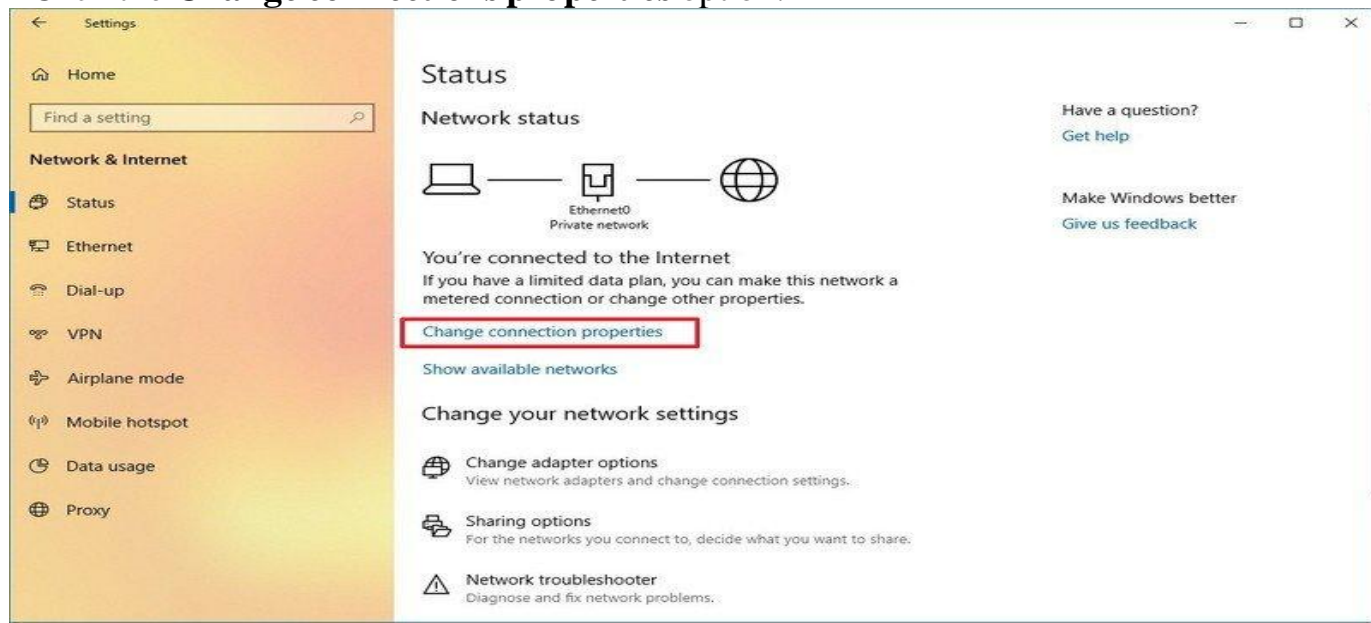
- Click the **Finish** button.
- After completing the steps, the FTP site should now be operational on your computer.
- **Configuring firewall rules**
- If you're running the built-in firewall on Windows 10, connections to the FTP server will be blocked by default until you manually allow the service through, using these steps:
- Open **Windows Defender Security Center**.
- Click on **Firewall & network protection**.
- Click the **Allow an app through firewall** option.



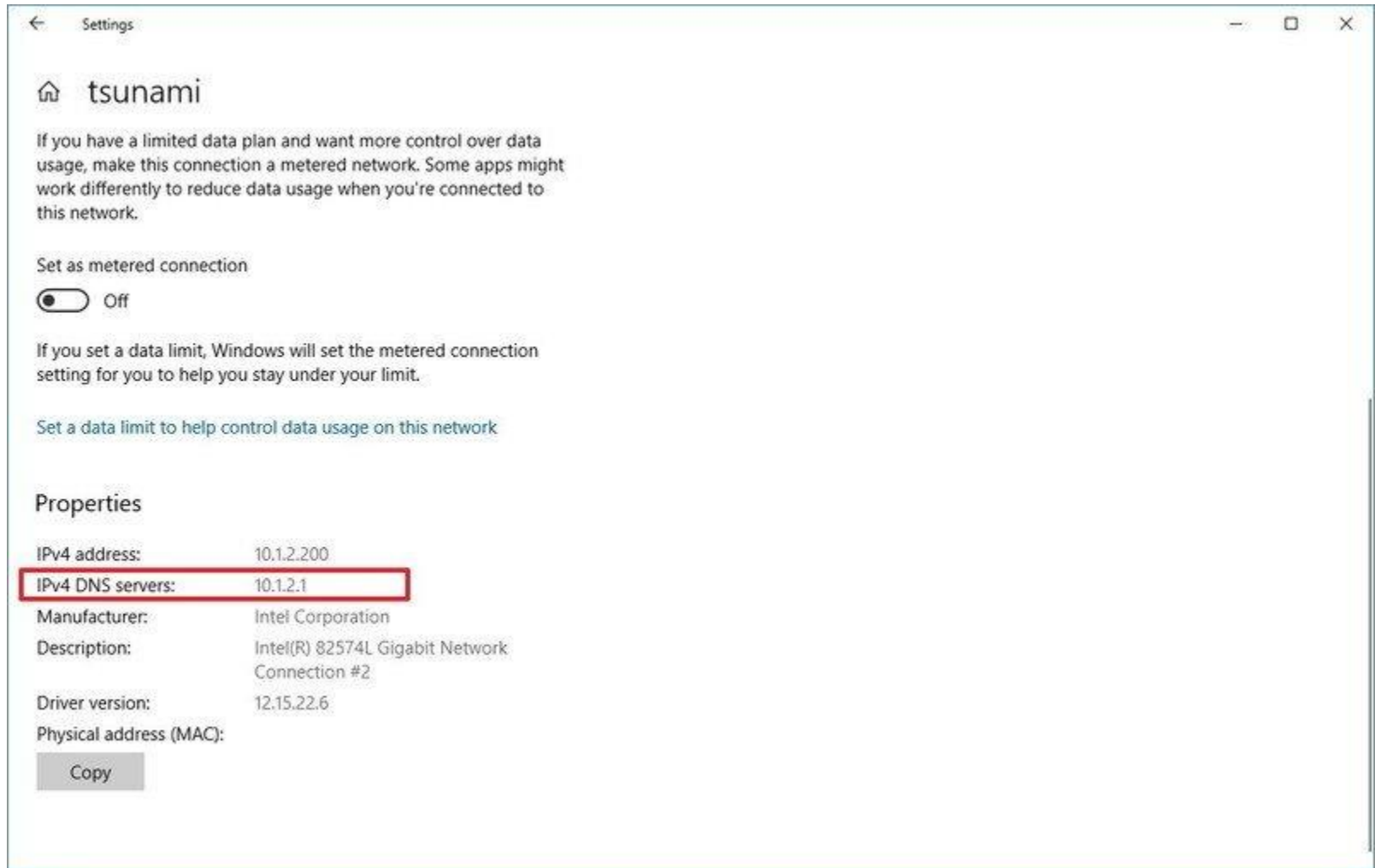
- Click the **Change settings** button.
- Check the **FTP Server** option, as well as the options to allow **Private** and **Public** access.



- Once you've completed the steps, the FTP server should now be accessible from the local network.
- In the case that you're running third-party security software, make sure to check your vendor support website for more specific details on adding firewall rules.
- **Allowing external connections**
- To make your FTP server reachable from the internet, you also need to open the Transmission Control Protocol/Internet Protocol (TCP/IP) port number 21 on your router.
- The instructions to forward a port will be different depending on the router, and even depending on the firmware version. In the steps below, we'll outline the general steps, but you may need to consult your manufacturer support website for specific details.
- To forward port 21 to allow FTP connections outside of the local network, do the following:
- **Open Settings.**
- **Click on Network & Internet.**
- **Click on Status.**
- **Click the Change connections properties option.**



- Make a note of the **IPv4 DNS server** address, which is the address of your router. Usually, it's private address in the 192.168.x.x range. For instance, 192.168.1.1 or 192.168.2.1.



- Open your default web browser.
- On the address bar enter the router's IP address (for example, 192.168.1.1) and press **Enter**.
- Sign-in with your router credentials.
- Open the **Port Forwarding** page. (Usually, these settings can be found under the WAN, NAT, or Advanced settings pages.)
- Add a new rule to forward incoming connections to the FTP server from the internet by including this information:
 - **Service name:** Type a descriptive name for the port forwarding rule.
 - **Port range:** 21.
 - **Local IP:** This is the FTP server IP address that the router will forward incoming connections. (This is your IPv4 address. **See step No. 5.**)
 - **Local port:** 21.
 - **Protocol:** TCP.
- Click the add button.
- Click the **Apply** button to save the changes.
- After completing the steps, any incoming connection on port 21 will be forwarded to the FTP server to establish a networking session.

ASUS Wireless Router RT-AC68W

router.asus.com/Advanced_VirtualServer_Content.asp

Traffic Analyzer

USB Application

AiCloud 2.0

Advanced Settings

Wireless

LAN

WAN

IPv6

VPN

Firewall

Administration

System Log

Network Tools

the LAN IP address, and leave the Local Port empty.

- When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with RT-AC68W's web user interface.
- When you set 20-21 as your FTP server's port range for your WAN setup, then your FTP server would be in conflict with RT-AC68W's native FTP server.

[Virtual Server / Port Forwarding FAQ](#)

Basic Config

Enable Port Forwarding

☐ Yes ☒ No

Famous Server List

Please select

Famous Game List

Please select

FTP Server Port

2021

Port Forwarding List (Max Limit : 32)

Service Name	Source Target	Port Range	Local IP	Local Port	Protocol	Add / Delete
					TCP	+
FTP		21	10.1.2.245	21	TCP	-

Apply

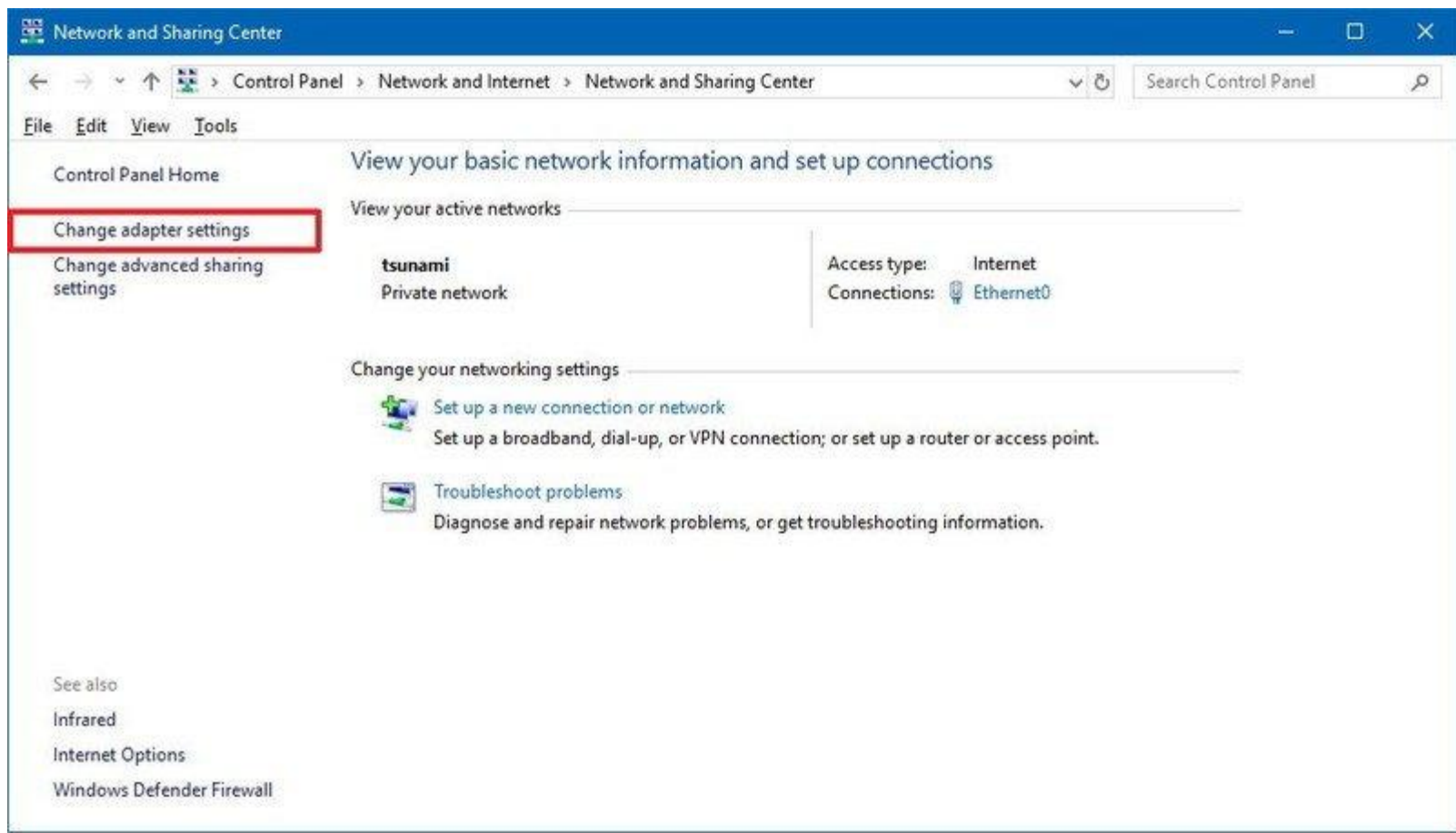
Help & Support

Manual | Utility | Feedback | Product Registration

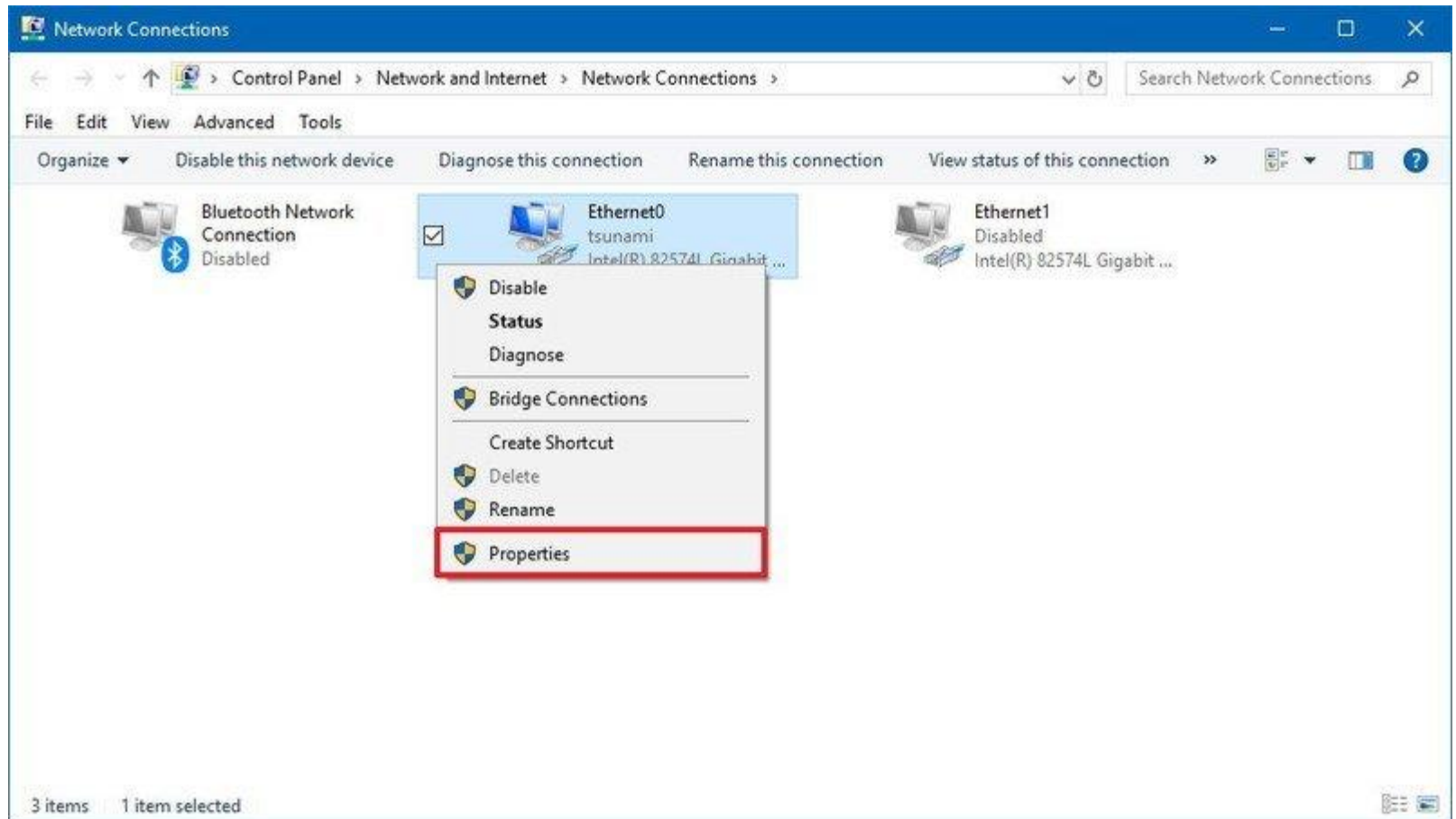
FAQ

2018 ASUSTeK Computer Inc. All rights reserved.

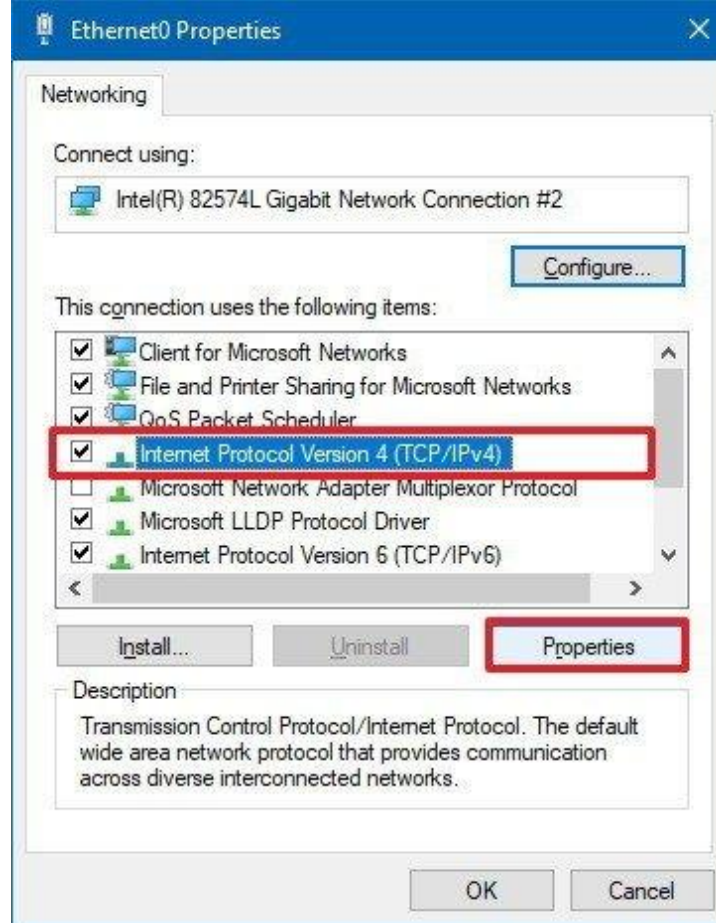
- **Setting up a static IP address**
- If you're planning to transfer files over the internet in the regular basis, then it's recommended to configure a static IP address to prevent having to reconfigure your router in the future if your device's IP changes.
- Open **Control Panel**.
- Click on **Network and Internet**.
- Click on **Network and Sharing Center**.
- In the left pane, click the **Change adapter settings** option.



- Right-click the network adapter, and select the **Properties** option.



- Select the **Internet Protocol Version 4 (TCP/IPv4)** option.
- Click the **Properties** button.



- Select the **Use the following IP address** option.
- Specify the IP settings:
 - **IP address:** Specify a static network address for the computer. You should use an address outside of the DHCP server scope configured in your router to prevent conflicts. For instance, **192.168.1.200**.
 - **Subnet mask:** In a home network, the address usually is **255.255.255.0**.
 - **Default gateway:** This is usually the IP address of the router. For example, **192.168.1.1**.
 - **Preferred DNS server:** Typically, this is also the IP address of your router.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 10 . 1 . 2 . 200

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 1 . 2 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 10 . 1 . 2 . 1

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

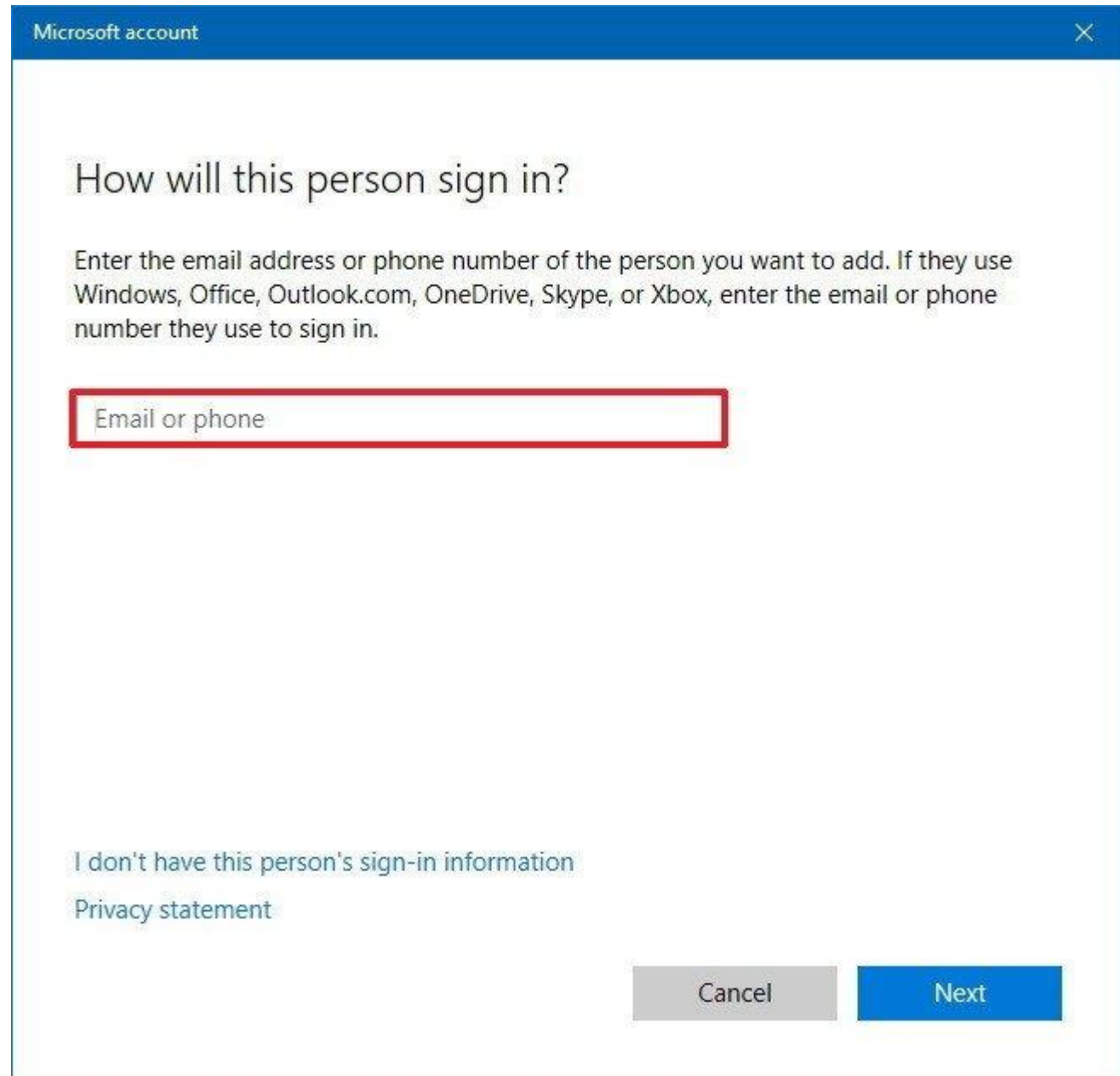
OK Cancel

- Click the **OK** button.
- Click the **Close** button.
- Once you've completed the steps, the IP configuration will no longer change, and it'll prevent potential connection problems in the future.

- **How to set up multiple FTP accounts on Windows 10**
- If you want to allow multiple people to download and upload files to the FTP server simultaneously, you need to set up multiple accounts with specific permissions.
- This process is done by creating new standard Windows 10 accounts and configuring the correct settings.
- **Creating new user accounts**
- To add multiple accounts to an FTP server, do the following:
- Open **Settings**.
- Click on **Accounts**.
- Click on **Family & other people**.
- Click the **Add someone else to this PC** button.



- Type the Microsoft account address for the user you want to allow access to the FTP server.



Microsoft account

How will this person sign in?

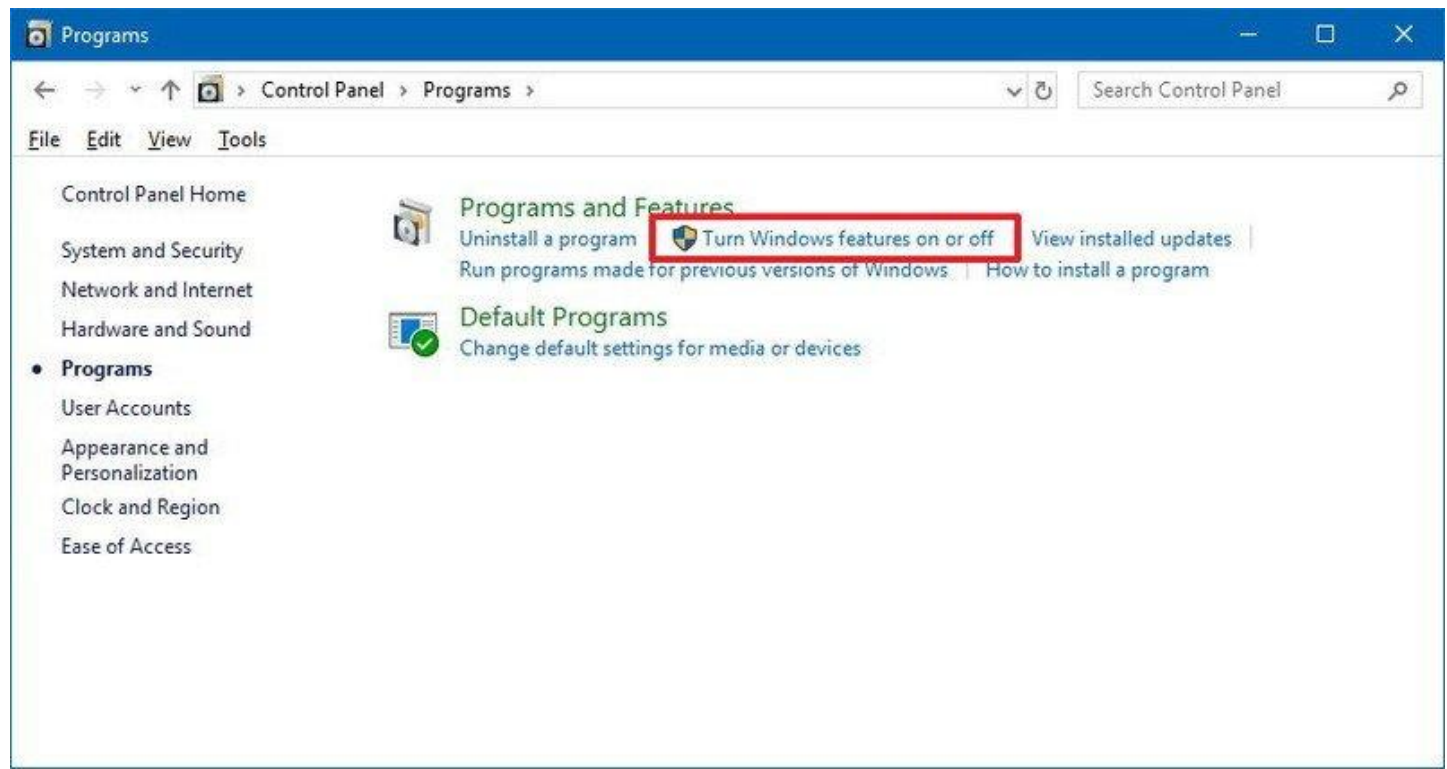
Enter the email address or phone number of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email or phone number they use to sign in.

Email or phone

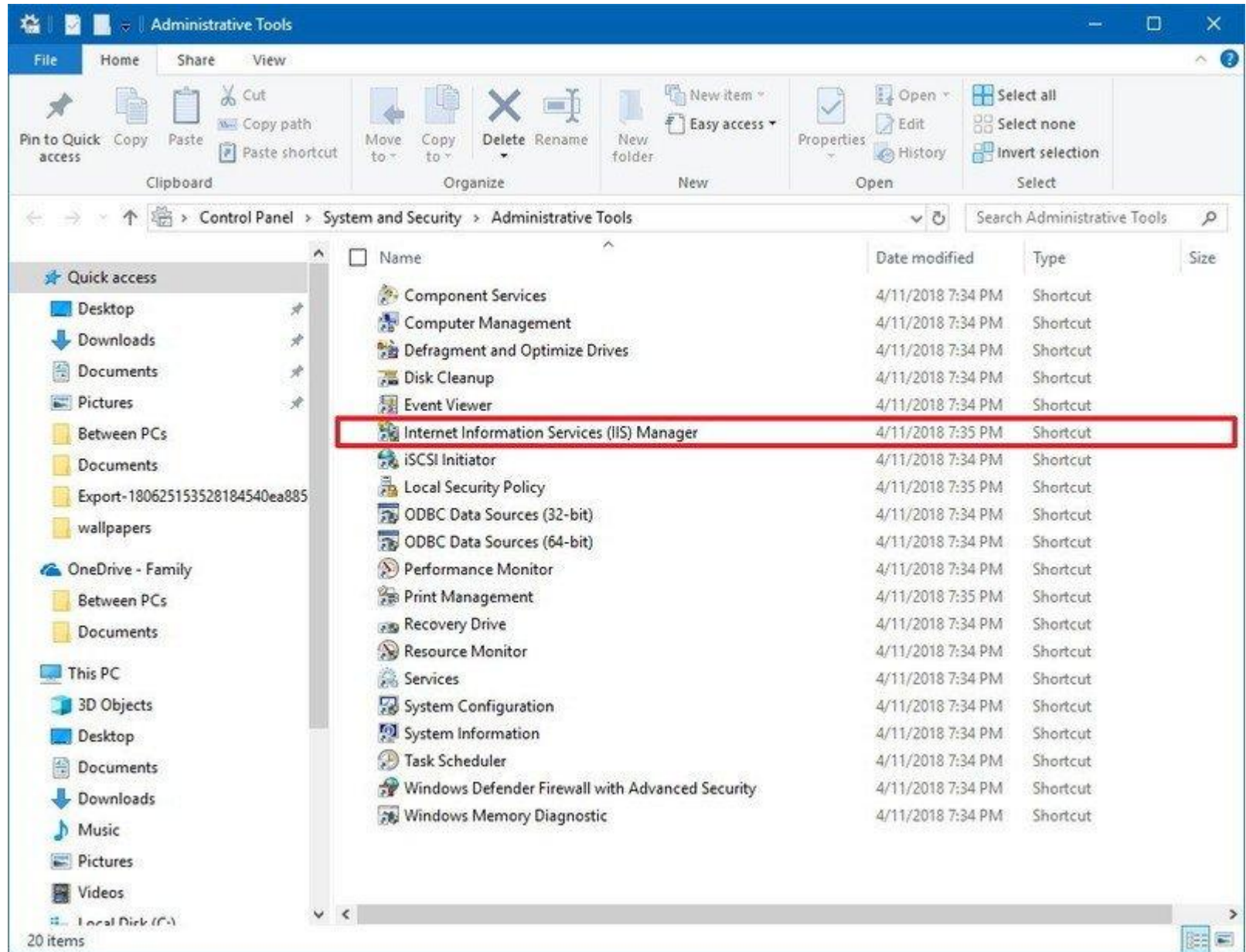
[I don't have this person's sign-in information](#)
[Privacy statement](#)

Cancel Next

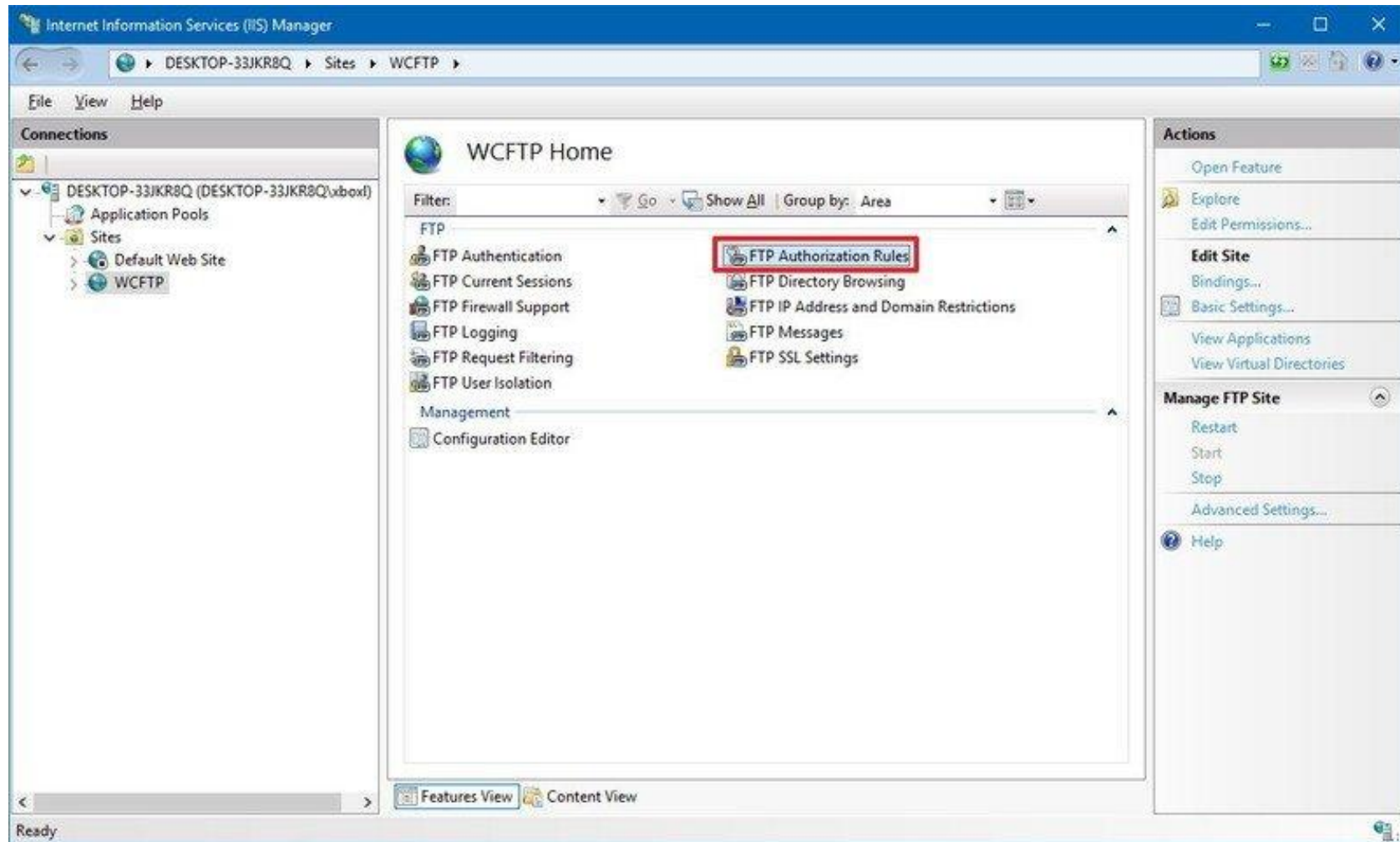
- **Quick Tip:** If you want users to access the server using [local accounts](#), then click the **I don't have this person sign-in information** option, click the **Add a user without a Microsoft account** option, and follow the on-screen direction to create the account.
- Click the **Next** button.
- Once you've completed the steps, you may need to repeat the steps to create additional accounts.
- **Configuring user accounts to FTP server**
- If you want multiple users to access the FTP server at the same time, you need to modify the server settings using these steps:
- Open **Control Panel**.
- Click on **System and Security**.
- Click on **Administrative Tools**.



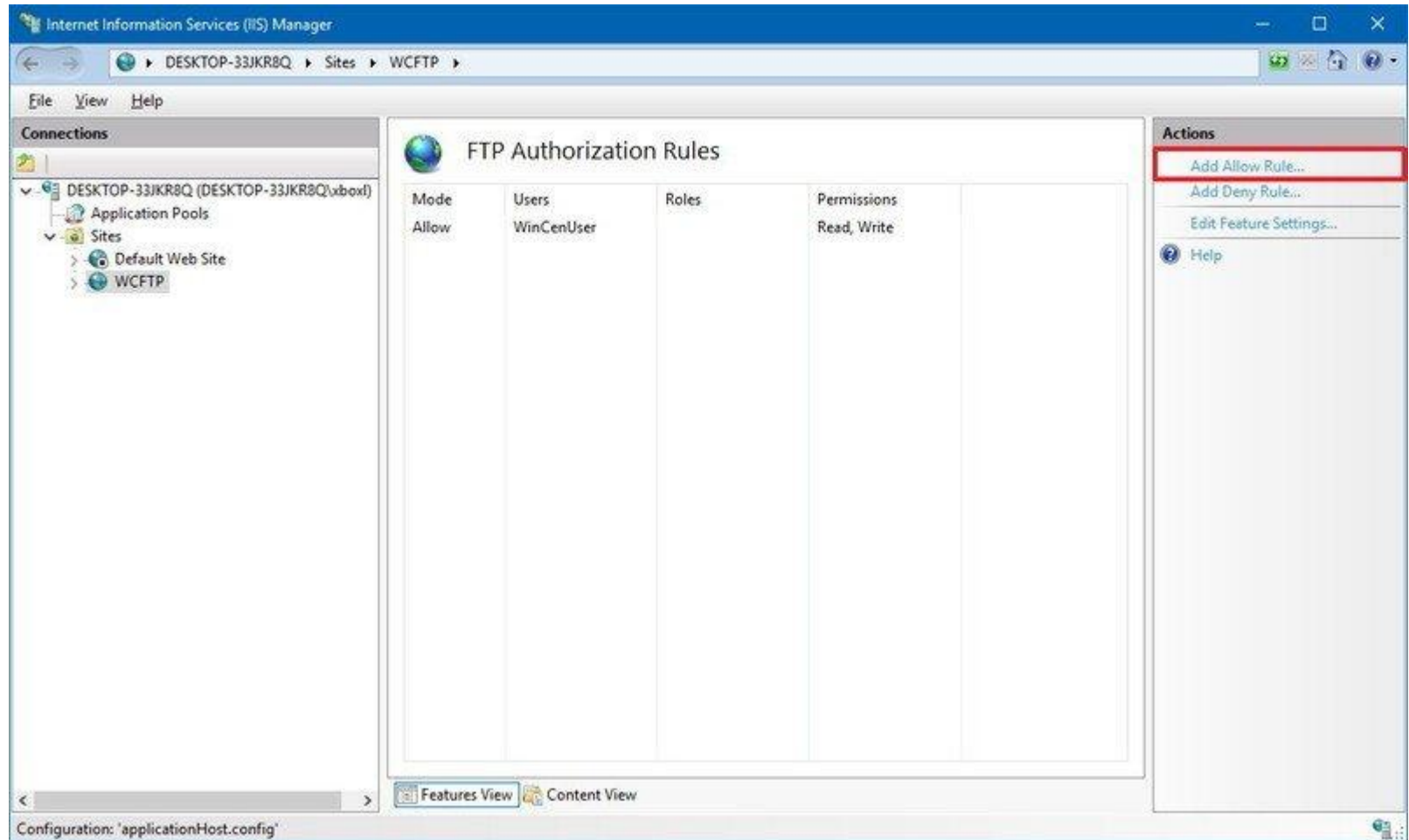
- Double-click the **Internet Information Services (IIS) Manager** shortcut.



- On the left pane, expand "Sites," and select the site you created earlier.
- Double-click the **FTP Authorization Rules** option.



- On the right pane, click the **Add Allow Rule** option.



- Select one of these two options:
 - **All Users:** Allows every user configured on your Windows 10 device to access the FTP server.
 - **Specified users:** You can use this option to specify all the users you want to access the FTP server. (You must separate each user using a comma.)
- Check the **Read** and **Write** options.
- Click the **OK** button.
- After completing the steps, all the users you specified should now be able to access the FTP server to download and upload files remotely.

Add Allow Authorization Rule

Allow access to this content to:

☒ **All Users**

☐ All Anonymous Users

☐ Specified roles or user groups:

Example: Admins, Guests

☐ Specified users:

Example: User1, User2

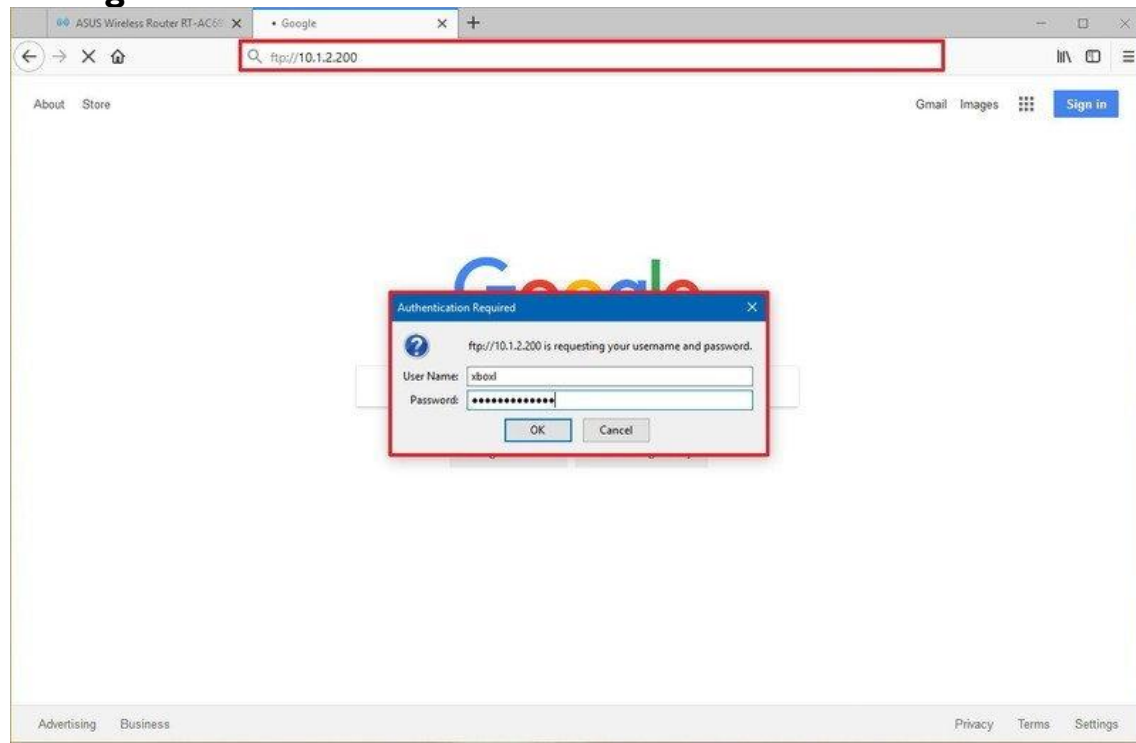
Permissions

☒ Read

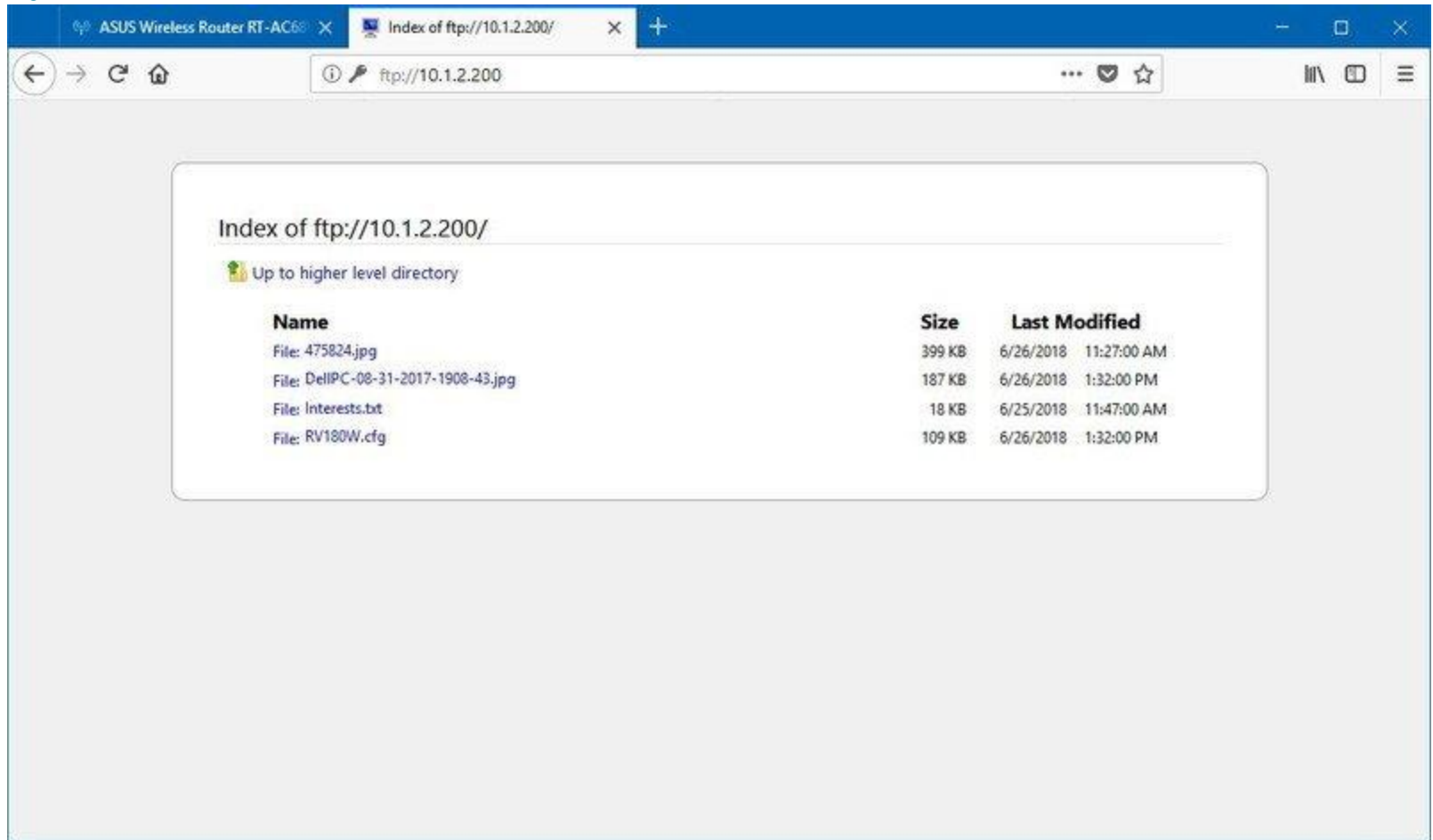
☒ Write

OK **Cancel**

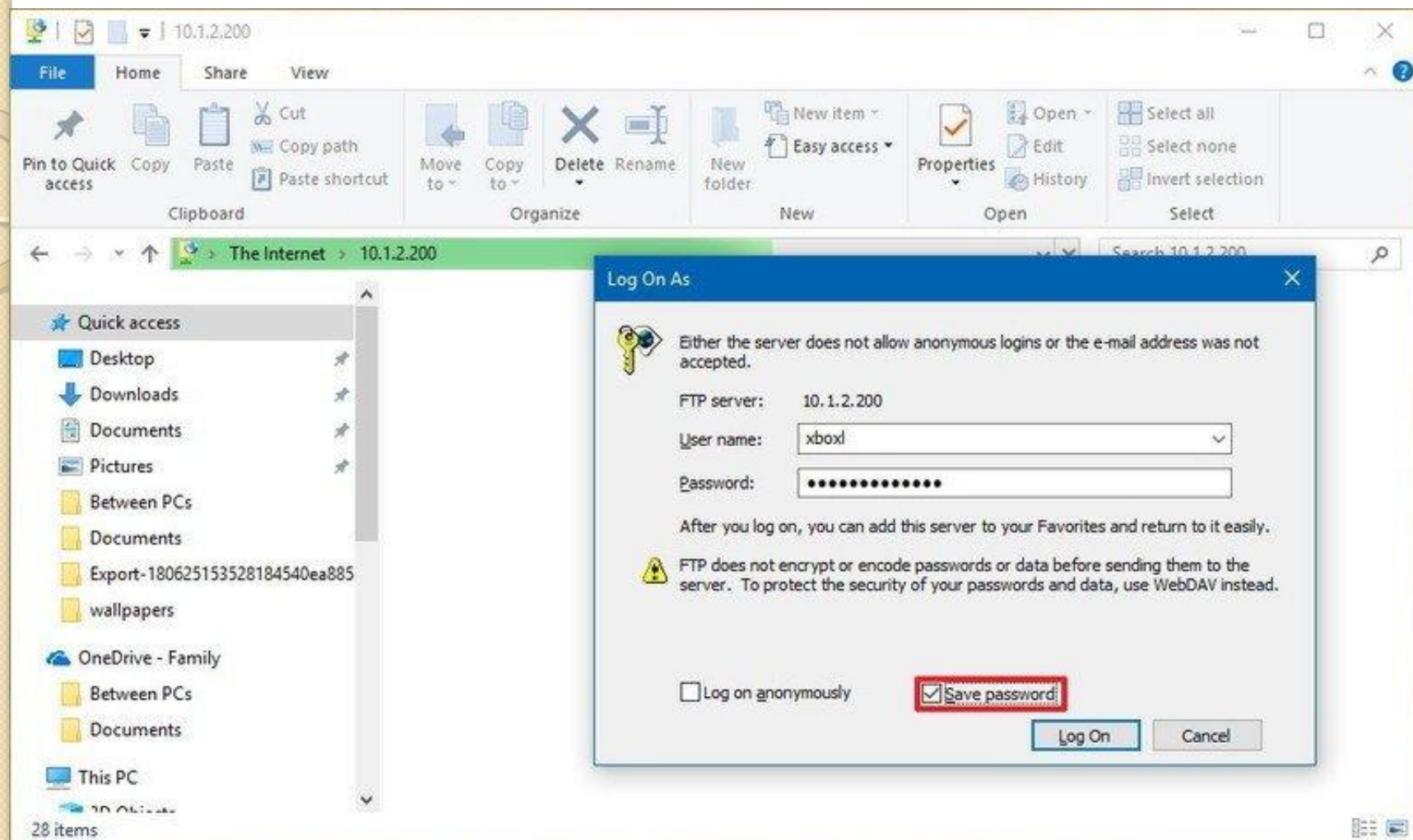
- **How to connect to an FTP server remotely on Windows 10**
- Once you've created and configured your FTP server, there are many ways to view, download, and upload files.
- **Viewing and downloading files**
- If you want to browse and download files, you can do this using Internet Explorer, Firefox, or Chrome:
- Open a **web browser**.
- In the address bar, type the server IP address using **ftp://**, and press **Enter**. For example, **ftp://192.168.1.100**.
- Type your account credentials.
- Click the **Log on** button.



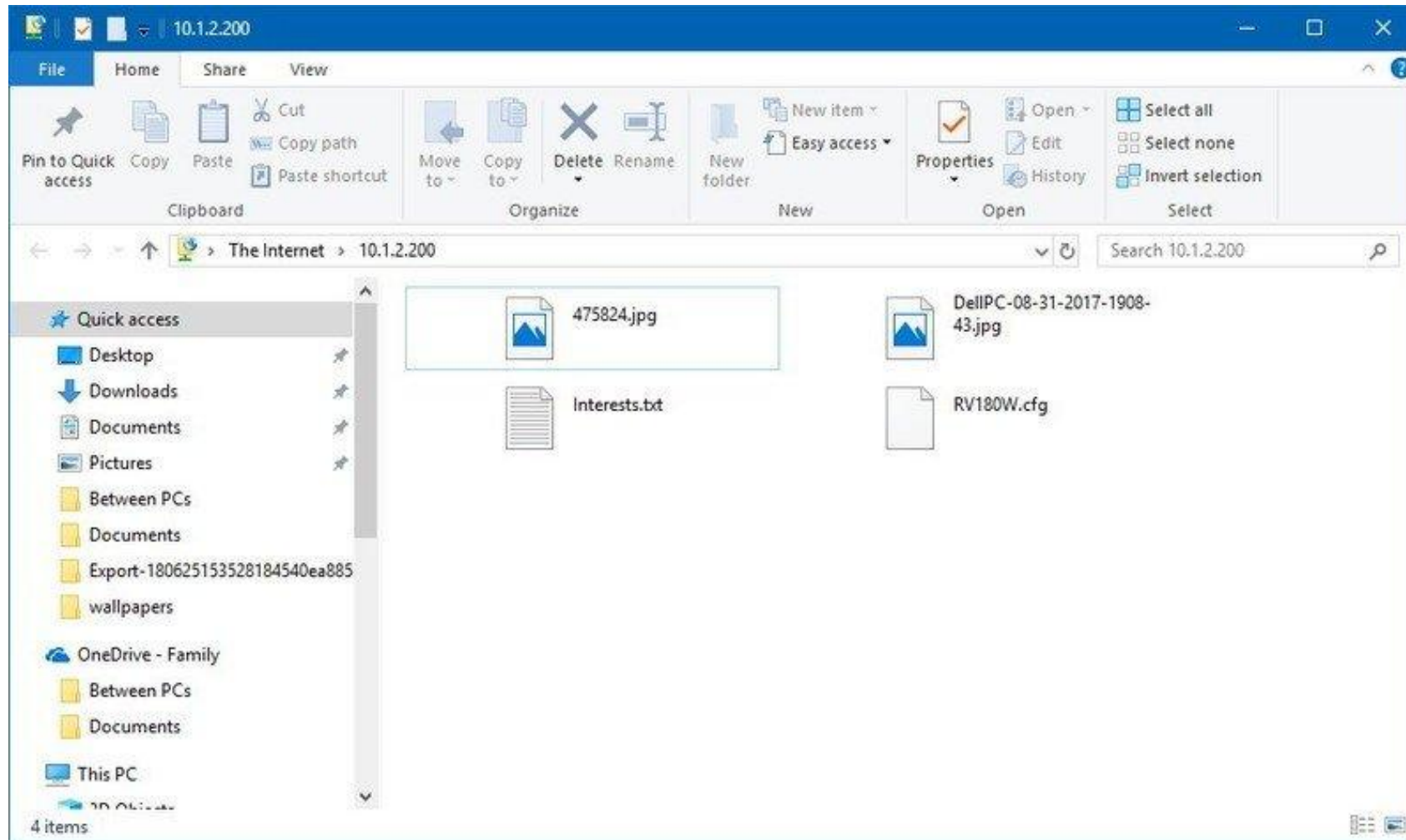
- After completing the steps, you should be able to navigate and download files and folders from the server.



- In the case that you're trying to connect from the internet, you have to specify the public (internet) IP address of the network hosting the FTP server.
- The easiest way to find out is to search for "What's my IP" in Google or Bing within the network before trying to connect from a remote connection. Also, unless you have a static IP address from your internet provider, or you're not using DDNS service, you may need to check your public IP regularly in order to connect, in case it changes.
- **Viewing, downloading, and uploading files**
- The easiest way to browse, download and upload files is to use File Explorer with these steps.
- Open **File Explorer**.
- In the address bar, type the server address using **ftp://**, and press **Enter**. For example, **ftp://192.168.1.100**.
- Type your account credentials.
- Check the **Save password** option.
- Click the **Log on** button.

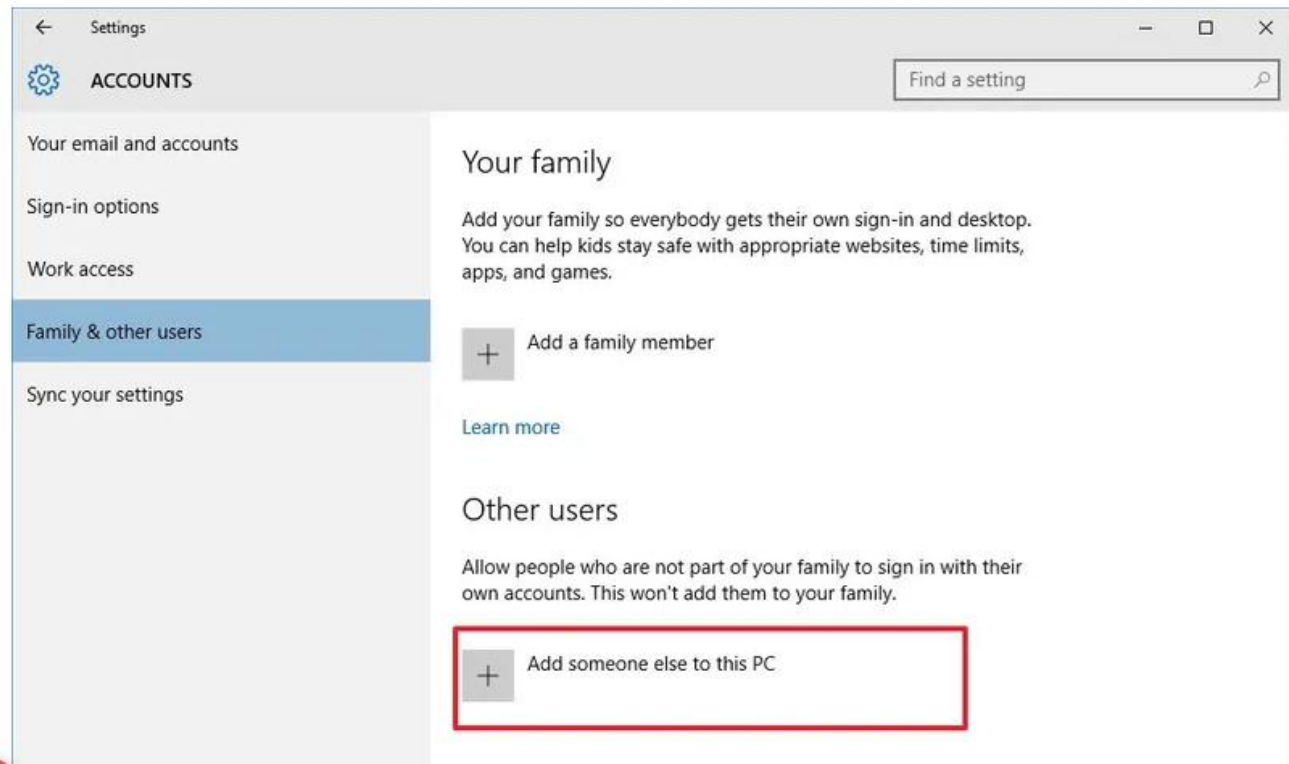


- After completing the steps, you'll be able to browse folders and files, as well as download and upload files as if they're locally stored on your device.



Configuring multiple users

- As with setup and configuration, there are multiple procedures involved to allow other users to access your FTP server.
- **Create multiple FTP accounts**
- To allow other users to access your FTP server, you have to create separate Windows 10 account for each user. To do that:
- Open settings app. You can do that with Windows key + I.
- Click accounts.
- Navigate to the left-side pane, where you'll see an option called "family & other users". Click the link.
- On the right-hand side, look for the option "add someone else to this PC."



- In the next screen, you'll be prompted to enter that person's email ID or phone number. Look for a link called "I don't have this person's sign in information" at the bottom left. Click the link.

How will this person sign in?

Enter the email address or phone number of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email or phone number they use to sign in.

[I don't have this person's sign-in information](#)

[Privacy statement](#)

Next

Cancel

- In the next screen, you'll be asked to enter the personal details of the new user. If you know the other person's Microsoft account details, you can enter. Otherwise, look for a link called "add a user without a Microsoft account" on the bottom left again.
- In the next screen, enter the details of the user. Choose a strong password for your own security as this server can be accessed from the Internet.
- These steps allow you to create a new user. Next, you'll have to add this user account to the FTP folder.
- **Add a new user to the FTP folder**
- You have to explicitly add a new user account to the FTP folder, in order for that user to access it. The steps for the same are:
- Navigate to the FTP folder, right-click on it and select "properties."
- Click the "security" tab and navigate to "edit" button.
- Look for "Add" button in the next screen and click on it.
- This will open the "select users or groups" dialog box. In this screen, enter the name of the user you want to add in the text area. Click on "check names" button to make sure that you have entered the right name. Click OK.
- This will take you back to the "add button" screen. But this time, you'll find the new user in group or user names list located just above the add button.
- Select the newly added user account and set the permissions for this user. Once done, click "apply" and OK.

Configure the user to access the FTP folder

- Once you've added the user, you have to configure to ensure that the user can access the folder. To do that:
- Go to control panel and open administrative tools.
- Double-click Internet information services (IIS) manager.
- Expand the left-hand pane and navigate to sites. Click on sites and you'll see your FTP server. Select this server.
- On the right-hand pane, you'll see many options. Look for authorization rules. Right-click on it and select "add allow rules" from the context menu.
- In the next screen, choose "selected users" option and enter the Windows 10 account you created earlier. Set the permission you'd like this user to have. Click OK
- Now the user you created is all set to access your FTP folder.
- In short, having an FTP server gives you a lot of flexibility and convenience, and it is easy to set it up too, as Windows has a built-in tool for this purpose. You can even add other users to your FTP folder easily, so all of you can send and receive files through FTP.