Practical 3 : Illustration of various networking command.

Questions:

Illustration of various networking commands:

• ping {hostname}	• netstat –nt	• netstat –a
• traceroute {hostname}	• telnet {hostname} {port}	• arp
• ipconfig	• host	• ftp
• nslookup {hostname}		

1.which command is used for checking network connectivity?
(a)Ping
(b)host
(r)netstat
(d)arp

2.which command is used for fetching the IP address or the domain name from DNS records?
(a)Ping
(b)nslookup
(r)netstat
(d)arp

3. which command is used to find domain name associated with the IP address?
(a)Ping
(b)host
(r)netstat
(d)arp

4. which command is used to display routing table, connection information, the status of ports?
(a)Ping
(b)host
(r)netstat
(d)arp

5.Which command is used to display and modify ARP cache, that contains the mapping of IP address to MAC address?
(a)Ping

(b)host
(r)netstat
(d)arp

6. Which command is used to set or display the IP address and netmask of a network interface?
(a)Ping
(b)host
(r)netstat
(d)ipconfig

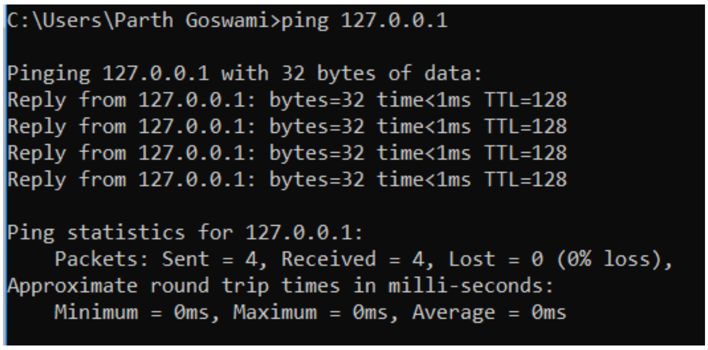
7. Which command is used to get the route of a packet?
(a)traceroute
(b)host
(r)netstat
(d)ipconfig

8. Which command is a network protocol that provides a command-line interface to communicate with a device?
(a)traceroute
(b)host
(r)telnet
(d)ipconfig

Ping Command:

The ping command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer. The ping command is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device. The receipt of corresponding echo Reply messages are displayed, along with round-trip times. ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.

syntax : ping {host name}/ip address



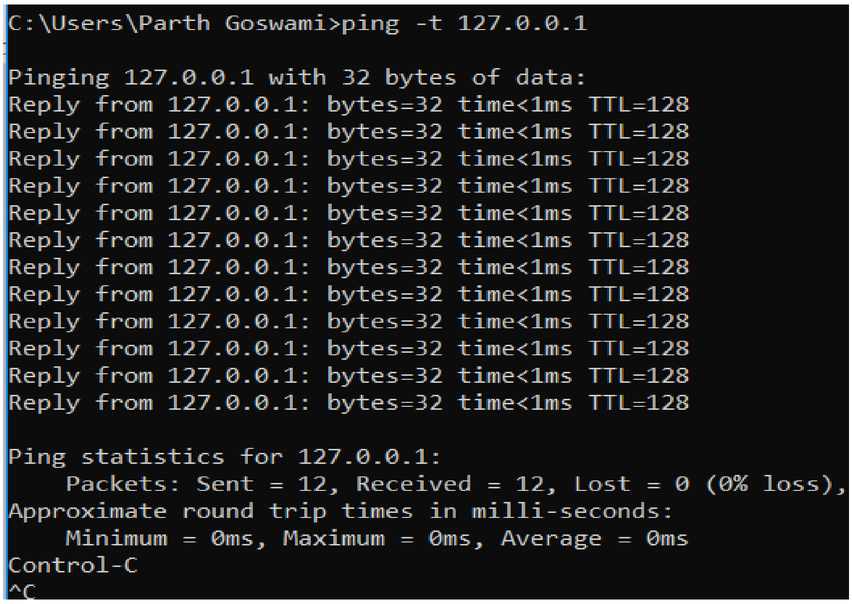
```
C:\Users\Parth Goswami>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Here there are four packets of 32 bytes has been sent and recieve in less than 1 ms.The 0% loss reported under Ping statistics for 127.0.0.1 tells me that each ICMP Echo Request message sent to 127.0.0.1 was returned.

here there are some option of ping command

options	**Description**
-t	Pings the specified host until stopped. To stop - type Control-C
-n count	Number of echo requests to send
-l size	Send buffer size
-i TTL	Set Time To Live

here is some example of ping command with options.



```
C:\Users\Parth Goswami>ping -t 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 12, Received = 12, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
```

```
C:\Users\Parth Goswami>ping -n 5 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\Parth Goswami>ping -l 16 127.0.0.1

Pinging 127.0.0.1 with 16 bytes of data:
Reply from 127.0.0.1: bytes=16 time<1ms TTL=128
Reply from 127.0.0.1: bytes=16 time<1ms TTL=128
Reply from 127.0.0.1: bytes=16 time<1ms TTL=128
Reply from 127.0.0.1: bytes=16 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Netstat -nt Command :

this command is used to display the TCP/IP network protocol statistics and information.

```
C:\Windows\system32>netstat -nt
Active Connections
  Proto  Local Address          Foreign Address        State           Offload
tate
  TCP    127.0.0.1:49404        127.0.0.1:49405        ESTABLISHED     InHost
  TCP    127.0.0.1:49405        127.0.0.1:49404        ESTABLISHED     InHost
  TCP    127.0.0.1:49409        127.0.0.1:49410        ESTABLISHED     InHost
  TCP    127.0.0.1:49410        127.0.0.1:49409        ESTABLISHED     InHost
  TCP    127.0.0.1:49416        127.0.0.1:49417        ESTABLISHED     InHost
  TCP    127.0.0.1:49417        127.0.0.1:49416        ESTABLISHED     InHost
  TCP    127.0.0.1:49658        127.0.0.1:49659        ESTABLISHED     InHost
  TCP    127.0.0.1:49659        127.0.0.1:49658        ESTABLISHED     InHost
  TCP    127.0.0.1:50917        127.0.0.1:50918        TIME_WAIT       InHost
  TCP    127.0.0.1:51129        127.0.0.1:51130        TIME_WAIT       InHost
  TCP    127.0.0.1:51200        127.0.0.1:51201        ESTABLISHED     InHost
  TCP    127.0.0.1:51201        127.0.0.1:51200        ESTABLISHED     InHost
  TCP    127.0.0.1:51206        127.0.0.1:51207        ESTABLISHED     InHost
  TCP    127.0.0.1:51207        127.0.0.1:51206        ESTABLISHED     InHost
  TCP    127.0.0.1:51220        127.0.0.1:51221        ESTABLISHED     InHost
  TCP    127.0.0.1:51221        127.0.0.1:51220        ESTABLISHED     InHost
  TCP    127.0.0.1:51223        127.0.0.1:51224        ESTABLISHED     InHost
  TCP    127.0.0.1:51224        127.0.0.1:51223        ESTABLISHED     InHost
  TCP    127.0.0.1:51226        127.0.0.1:51227        ESTABLISHED     InHost
  TCP    127.0.0.1:51227        127.0.0.1:51226        ESTABLISHED     InHost
  TCP    127.0.0.1:51229        127.0.0.1:51230        ESTABLISHED     InHost
  TCP    127.0.0.1:51230        127.0.0.1:51229        ESTABLISHED     InHost
  TCP    127.0.0.1:51232        127.0.0.1:51233        ESTABLISHED     InHost
  TCP    127.0.0.1:51233        127.0.0.1:51232        ESTABLISHED     InHost
```

-n | Displays active TCP connections, however, addresses and port

| numbers are expressed numerically and no attempt is made to determine names.

-t | Display only TCP connections & current connection of offload state.

Netstat provides statistics for the following:

1) Proto - The name of the protocol (TCP or UDP). UDP | UDP is used to sends short messages called datagrams but overall it is an unreliable connectionless protocol

(User Datagram Protocol)

2)Local Address - The IP address of the local computer and the port number being used. The name of the local computer that corresponds to the IP address and the name of the port is shown unless the -n parameter is specifie An asterisk (*) is shown for the host if the server is listening on all interfaces. If the port is not yet established, the port number is shown as an asterisk.

3)Foreign Address - The IP address and port number of the remote computer to which the socket is connected The names that corresponds to the IP address and the port are shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).

4) State - Indicates the state of a TCP connection. The possible states are as follows: CLOSE_WAIT, CLOSED, ESTABLISHED, FIN_WAIT_1, FIN_WAIT_2, LAST_ACK, LISTEN, SYN_RECEIVED, SYN_SEND, and TIME_WAIT. For more information about the states of a TCP .

TCP connection state	Abbreviation in MVS™ console	Abbreviation in TSO or UNIX shell	Description
LISTEN	Listen	Listen	Waiting for a connection request from a remote TCP application. This is the state in which you can find the listening socket of a local TCP server.
SYN-SENT	SynSent	SynSent	Waiting for an acknowledgment from the remote endpoint after having sent a connection request. Results after step 1 of the three-way TCP handshake.
SYN-RECEIVED	SynRcvd	SynRcvd	This endpoint has received a connection request and sent an acknowledgment. This endpoint is waiting for final acknowledgment that the other endpoint did receive this endpoint's acknowledgment of the original connection request. Results after step 2 of the three-way TCP handshake.
ESTABLISHED	Estblsh	Establsh	Represents a fully established connection; this is the normal state for the data transfer phase of the connection.
FIN-WAIT-1	FinWt1	FinWait1	Waiting for an acknowledgment of the connection termination request or for a simultaneous connection termination request from the remote TCP. This state is normally of short duration.
FIN-WAIT-2	FinWt2	FinWait2	Waiting for a connection termination request from the remote TCP after this endpoint has sent its connection termination request. This state is normally of short duration, but if the remote socket endpoint does not close its socket shortly after it has received information that this socket endpoint closed the connection, then it might last for some time. Excessive FIN-WAIT-2 states can indicate an error in the coding of the remote application.

CLOSE-WAIT	ClosWt	ClosWait	This endpoint has received a close request from the remote endpoint and this TCP is now waiting for a connection termination request from the local application.
CLOSING	Closing	Closing	Waiting for a connection termination request acknowledgment from the remote TCP. This state is entered when this endpoint receives a close request from the local application, sends a termination request to the remote endpoint, and receives a termination request before it receives the acknowledgment from the remote endpoint.
LAST-ACK	LastAck	LastAck	Waiting for an acknowledgment of the connection termination request previously sent to the remote TCP. This state is entered when this endpoint received a termination request before it sent its termination request.
TIME-WAIT	TimeWt	TimeWait	Waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request.
CLOSED	Closed	Closed	Represents no connection state at all.

Traceroute {hostname} :

Traceroute Command (Data Communication & Networking)

- A traceroute is a function which traces the path from one network to another. It allows us to diagnose the source of many problems.
- It is a convenient tool that you can use under different operation systems – Windows (Tracert), MacOS, Linux (traceroute) and even on mobile (Android and iOS).
- You can use traceroute, and see the full route that the packets take to their destination (domain or IP address). Apart from that, you will see the hostnames and IPs of the routers on the way and the latency, the time it takes for each device to receive and resend the data.

➢ **Time to Live (TTL)**

- Each packet that you send contains a TTL (time to live). It is not a time but a limit of hops it can do before getting the result.

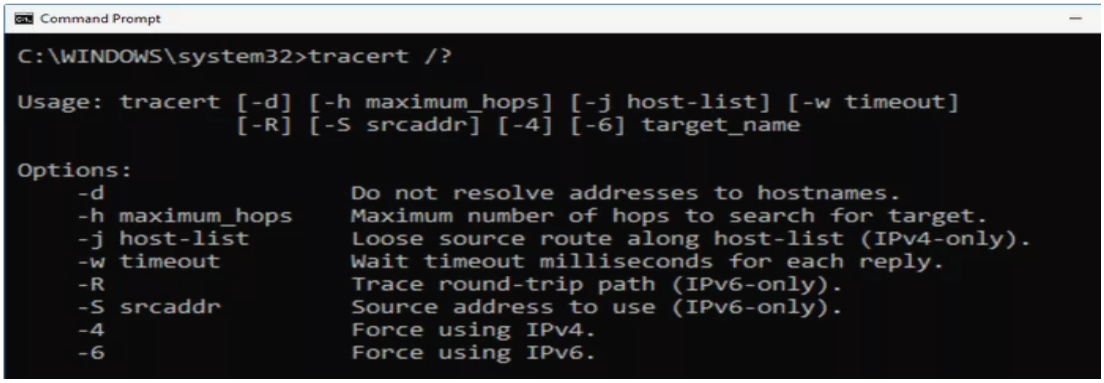
- Usual limit is 30, but it can be more like 64 for example. This limit stops your data after a certain amount of hops so it won't go forever. The IP packet will follow until it gets "time exceeded" or "port unreachable" when it gets to the host.

➢ **Syntax:**

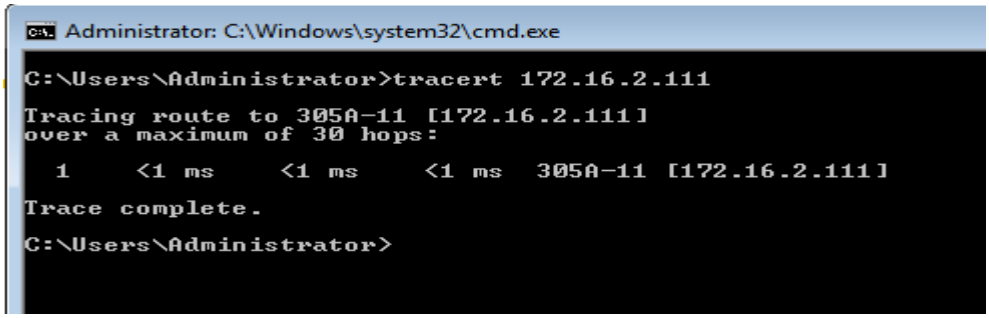
tracert [-d] [-h maximum_hops][-j host-list][-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Option	Description
-d	Do not resolve addresses to hostnames

-h maximum_hops	Maximum number of hops to search for target
-j host-list	Loose source route along host-list (IPv4-only)
-w timeout	Wait timeout milliseconds for each reply
-R	Trace round-trip path (IPv6-only)
-S src_addr	Source address to use (IPv6-only)
-4	Force using IPv4
-6	Force using IPv6



- **Practical Implementation**



```
C:\Users\Administrator>tracert www.google.com

Tracing route to www.google.com [172.217.166.68]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.16.0.1
  2   139 ms    10 ms     2 ms  172.24.195.242
  3     8 ms     *        *     218.248.235.198
  4    16 ms    12 ms    12 ms  74.125.48.138
  5     *        *        *     Request timed out.
  6    13 ms    13 ms    13 ms  216.239.57.188
  7    12 ms    16 ms    14 ms  108.170.248.218
  8    17 ms    13 ms    13 ms  108.170.248.177
  9    12 ms    12 ms    12 ms  209.85.242.111
 10    11 ms    12 ms    12 ms  bom05s15-in-f4.1e100.net [172.217.166.68]

Trace complete.
```

```
C:\Users\Administrator>tracert -d yahoo.com

Tracing route to yahoo.com [98.137.246.8]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.16.0.1
  2     1 ms    <1 ms    <1 ms  172.24.195.242
  3     *        8 ms     *     218.248.235.198
  4    13 ms    19 ms    15 ms  61.246.195.185
  5   226 ms   225 ms   225 ms  182.79.222.237
  6   212 ms   213 ms   224 ms  206.82.104.49
  7   228 ms   225 ms   224 ms  216.115.96.7
  8   234 ms   249 ms   233 ms  184.165.16.44
  9   274 ms   274 ms   280 ms  216.115.96.34
 10   284 ms   284 ms   286 ms  216.115.101.195
 11   283 ms   283 ms   288 ms  66.196.67.111
 12   280 ms   280 ms   289 ms  67.195.37.99
 13   311 ms   311 ms   312 ms  98.137.120.25
 14   282 ms   283 ms   282 ms  98.137.246.8

Trace complete.
```

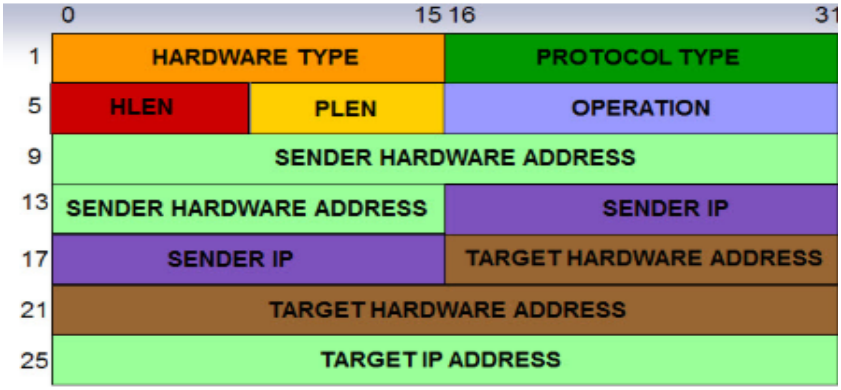
```
C:\Users\Administrator>tracert -h 3 www.google.com

Tracing route to www.google.com [172.217.166.68]
over a maximum of 3 hops:

  1    <1 ms    <1 ms    <1 ms  172.16.0.1
  2     1 ms     1 ms     1 ms  172.24.195.242
  3     *        *        *     Request timed out.

Trace complete.
```

- **Conclusion**
  - By using the newly collected data, you can see if there is any problem on the route (not responsive server or very slow one) and later focus your attention to fix it.

Arp :

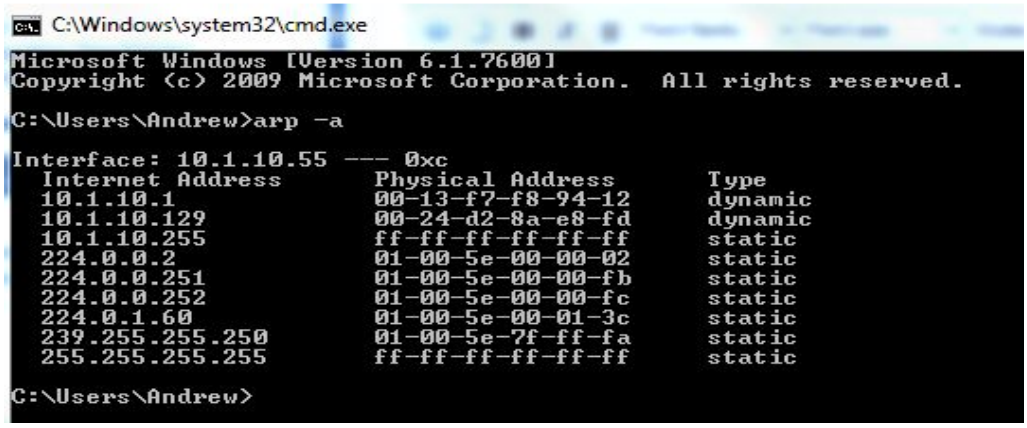
- ARP stands for Address Resolution Protocol. This protocol is used by network nodes to match IP addresses to MAC addresses. The original specification was RFC 826. That has since been updated by RFC 5227, and RFC 5494.
- One part determines a physical address when sending a packet.
- Other part answers requests from other machines.
- So ARP provides method for hosts send message to destination address on physical network. Ethernet hosts must convert a 32-bit IP address into a 48-bit Ethernet address. The host checks its ARP cache to see if address mapping from IP to physical address is known:

- The ARP protocol format looks like this:



- The **arp** command is useful for viewing the ARP cache and resolving address resolution problems.
- Syntax (Inet means Internet address)
- **arp** [**-a** [*InetAddr*] [**-N** *IfaceAddr*]] [**-g** [*InetAddr*] [**-N** *IfaceAddr*]] [**-d** *InetAddr* [*IfaceAddr*]] [**-s** *InetAddr EtherAddr* [*IfaceAddr*]] and also you can use **/?:** Displays help at the command prompt.

- **Using arp on Windows:**
  To run the arp command in Windows click START> RUN> CMD. Now enter 'arp -a' at the > prompt:



Using arp on a MAC or Linux System:

To run the arp command in MAC-OSX or Linux, first open a Terminal window. Now enter 'arp -a' at the $ or # prompt:

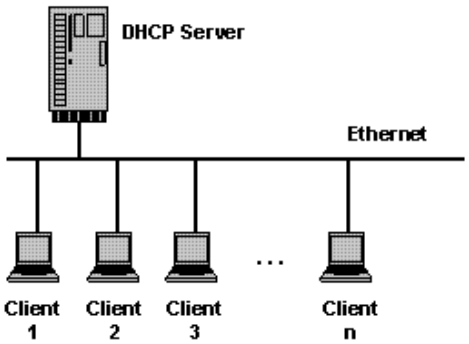
```
awalding — -bash — 80×24
Andrews-iMac:~ awalding$ arp -a
? (169.254.30.82) at 5c:f9:38:94:d7:70 on en0 [ethernet]
? (169.254.216.21) at 48:ba:4e:57:13:c6 on en0 [ethernet]
? (192.168.1.1) at 70:77:81:dd:c3:7c on en0 ifscope [ethernet]
? (192.168.1.109) at cc:20:e8:a7:4c:97 on en0 ifscope [ethernet]
? (192.168.1.111) at 9c:f4:8e:60:b4:4a on en0 ifscope [ethernet]
? (192.168.1.122) at bc:14:85:db:95:1e on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
broadcasthost (255.255.255.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
Andrews-iMac:~ awalding$
```

- There are two types of ARP entries- static and dynamic. Most of the time, the computer will use dynamic ARP entries. This means that the ARP entry (the Ethernet MAC to IP address link) has been learned (usually from the default gateway) and is kept on a device for some period of time, as long as it is being used.

Ipconfig :

Ipconfig command

- Ipconfig (sometimes written as IPCONFIG) is a command line tool used to control the network connections on Windows machines.
- Ipconfig displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings.
- Used without parameters, ipconfig displays the IP address, subnet mask, and default gateway for all adapters.



A DHCP Server assigns IP addresses to client computers.

DNS

A DNS server is a computer server that contains a database of public IP addresses and their associated hostnames, and in most cases serves to resolve, or translate, those names to IP addresses as requested. DNS servers run special software and communicate with each other using special protocols.

The Purpose of DNS Servers

It's easier to remember a domain or hostname like lifewire.com than it is to remember the site's IP address numbers 151.101.129.121.

Subnet Mask

A subnet mask is a number that defines a range of IP addresses available within a network.

ipconfig command

ipconfig /all	it gives out a detailed description of the Network Adapters connected to your machine, with additional information like the Description, DNS Servers and all.
ipconfig /release	release an IP address.
ipconfig /renew	renew an IP address.
ipconfig /**registerdns**	you can also refresh all DHCP leases and re-register DNS names using the **registerdns** parameter.
ipconfig /**flushdns**	If you need to clear the DNS resolver cache on the local computer, you can use the **flushdns** parameter.
ipconfig /**displaydns**	To view the contents of the DNS resolver cache, use the **displaydns** parameter.

```
C:\Users\Bhadresh>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAPTOP-7DI247IC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 32-D1-6B-F3-16-1F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter
   Physical Address. . . . . . . . . : 30-D1-6B-F3-16-1F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::191e:efb0:b23f:9580%9(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.43.233(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 20 July 2019 12:02:52
   Lease Expires . . . . . . . . . . : 20 July 2019 13:52:26
   Default Gateway . . . . . . . . . : 192.168.43.1
   DHCP Server . . . . . . . . . . . : 192.168.43.1
   DHCPv6 IAID . . . . . . . . . . . : 103862635
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-0C-0F-A7-38-4B-73-F0-02-16
   DNS Servers . . . . . . . . . . . : 192.168.43.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Host :

host command in Linux system is used for DNS (Domain Name System) lookup operations. In simple words, this command is used to find the IP address of a particular domain name or if you want to find out the domain name of a particular IP address the host command becomes handy. You can also find more specific details of a domain by specifying the corresponding option along with the domain name.

Syntax:

```
host [-aCdlriTWV] [-c class] [-N ndots] [-t type] [-W time]
    [-R number] [-m flag] hostname [server]
```

host command without any option: It will print the general syntax of the command along with the various options that can be used with the host command as well as gives a brief description about each option.

Example:

```
anshul@anshul-VirtualBox:~$ host
Usage: host [-aCdilrTvVw] [-c class] [-N ndots] [-t type] [-W time]
            [-R number] [-m flag] hostname [server]
        -a is equivalent to -v -t ANY
        -c specifies query class for non-IN data
        -C compares SOA records on authoritative nameservers
        -d is equivalent to -v
        -i IP6.INT reverse lookups
        -l lists all hosts in a domain, using AXFR
        -m set memory debugging flag (trace|record|usage)
        -N changes the number of dots allowed before root lookup is done
        -r disables recursive processing
        -R specifies number of retries for UDP packets
        -s a SERVFAIL response should stop query
        -t specifies the query type
        -T enables TCP/IP mode
        -v enables verbose output
        -V print version number and exit
        -w specifies to wait forever for a reply
        -W specifies how long to wait for a reply
        -4 use IPv4 query transport only
        -6 use IPv6 query transport only
anshul@anshul-VirtualBox:~$
```

Different options with the host command:

- **host domain_name:** This will print the IP address details of the specified domain.
  Example:
  host geeksforgeeks.org

```
anshul@anshul-VirtualBox:~$ host geeksforgeeks.org
geeksforgeeks.org has address 52.25.109.230
geeksforgeeks.org mail is handled by 1 aspmx.l.google.com.
geeksforgeeks.org mail is handled by 10 alt3.aspmx.l.google.com.
geeksforgeeks.org mail is handled by 10 alt4.aspmx.l.google.com.
geeksforgeeks.org mail is handled by 5 alt1.aspmx.l.google.com.
geeksforgeeks.org mail is handled by 5 alt2.aspmx.l.google.com.
anshul@anshul-VirtualBox:~$
```

- **host IP_Address:** This will display the domain details of the specified IP Address.

Example:
host 52.25.109.230

```
anshul@anshul-VirtualBox:~$ host 52.25.109.230
230.109.25.52.in-addr.arpa domain name pointer ec2-52-25-109-230.us-west-2.compute.amazonaws.com.
anshul@anshul-VirtualBox:~$
```

- **-a or -v:** It used to specify the query type or enables the verbose output.
  Example:
  host -a geeksforgeeks.org

```
anshul@anshul-VirtualBox:~$ host -v geeksforgeeks.org
Trying "geeksforgeeks.org"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14557
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;geeksforgeeks.org.             IN      A

;; ANSWER SECTION:
geeksforgeeks.org.      8       IN      A       52.25.109.230

Received 51 bytes from 127.0.0.53#53 in 1 ms
Trying "geeksforgeeks.org"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11597
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;geeksforgeeks.org.             IN      AAAA

Received 35 bytes from 127.0.0.53#53 in 583 ms
Trying "geeksforgeeks.org"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43282
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;geeksforgeeks.org.             IN      MX

;; ANSWER SECTION:
geeksforgeeks.org.      278     IN      MX      5 alt2.aspmx.l.google.com.
geeksforgeeks.org.      278     IN      MX      5 alt1.aspmx.l.google.com.
geeksforgeeks.org.      278     IN      MX      10 alt4.aspmx.l.google.com.
geeksforgeeks.org.      278     IN      MX      10 alt3.aspmx.l.google.com.
geeksforgeeks.org.      278     IN      MX      1 aspmx.l.google.com.

Received 153 bytes from 127.0.0.53#53 in 3 ms
anshul@anshul-VirtualBox:~$
```

- **-t :** It is used to specify the type of query.
  Example 1:
  host -t ns geeksforgeeks.org

```
anshul@anshul-VirtualBox:~$ host -t ns geeksforgeeks.org
geeksforgeeks.org name server ns-869.awsdns-44.net.
geeksforgeeks.org name server ns-245.awsdns-30.com.
geeksforgeeks.org name server ns-1569.awsdns-04.co.uk.
geeksforgeeks.org name server ns-1520.awsdns-62.org.
anshul@anshul-VirtualBox:~$
```

Example 2: To print SOA record
host -t SOA geeksforgeeks.org

```
anshul@anshul-VirtualBox:~$ host -t SOA geeksforgeeks.org
geeksforgeeks.org has SOA record ns-869.awsdns-44.net. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
anshul@anshul-VirtualBox:~$
```

Example 3: To print *txt* record
host -t txt geeksforgeeks.org

```
anshul@anshul-VirtualBox:~$ host -t txt geeksforgeeks.org
geeksforgeeks.org descriptive text "v=spf1 include:amazonses.com include:_spf.google.com -all"
anshul@anshul-VirtualBox:~$
```

- **-C :** In order to compare the SOA records on authoritative nameservers.
  Example:
  host -C geeksforgeeks.org

```
anshul@anshul-VirtualBox:~$ host -C geeksforgeeks.org
Nameserver 205.251.198.33:
        geeksforgeeks.org has SOA record ns-869.awsdns-44.net. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
Nameserver 205.251.197.240:
        geeksforgeeks.org has SOA record ns-869.awsdns-44.net. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
Nameserver 205.251.192.245:
        geeksforgeeks.org has SOA record ns-869.awsdns-44.net. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
Nameserver 205.251.195.101:
        geeksforgeeks.org has SOA record ns-869.awsdns-44.net. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
anshul@anshul-VirtualBox:~$
```

- **-R :** In order to specify the number of retries you can do in case one try fails. If anyone try succeeds then the command stops.
  Example:
  host -R 3 geeksforgeeks.org

```
anshul@anshul-VirtualBox:~$ host -R 3 geeksforgeeks.org
geeksforgeeks.org has address 52.25.109.230
geeksforgeeks.org mail is handled by 10 alt4.aspmx.l.google.com.
geeksforgeeks.org mail is handled by 5 alt1.aspmx.l.google.com.
geeksforgeeks.org mail is handled by 5 alt2.aspmx.l.google.com.
geeksforgeeks.org mail is handled by 1 aspmx.l.google.com.
geeksforgeeks.org mail is handled by 10 alt3.aspmx.l.google.com.
anshul@anshul-VirtualBox:~$
```

- **-l :**In order to list all hosts in a domain.For this command to work you need to be either an admin or a node server.

Example:
host -l geeksforgeeks.org

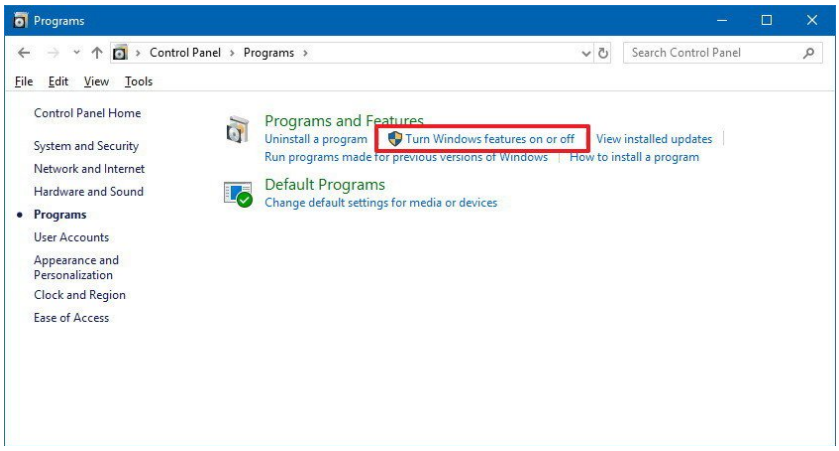
FTP SERVER :

How to install the FTP server components on Windows 10

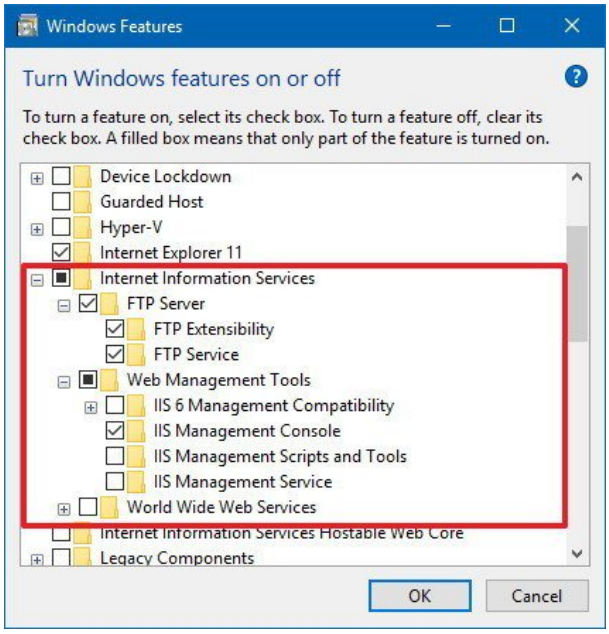
Although Windows 10 includes support to set up an FTP server, you need to add the required components manually.

To install the FTP server components, do the following:

1. Open **Control Panel**.
2. Click on **Programs**.
3. Under "Programs and Features," click the **Turn Windows features on or off** link.



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



7. Click the **OK** button.
8. Click the **Close** button.

Once you've completed the steps, the components to set up an FTP server will be installed on your device.

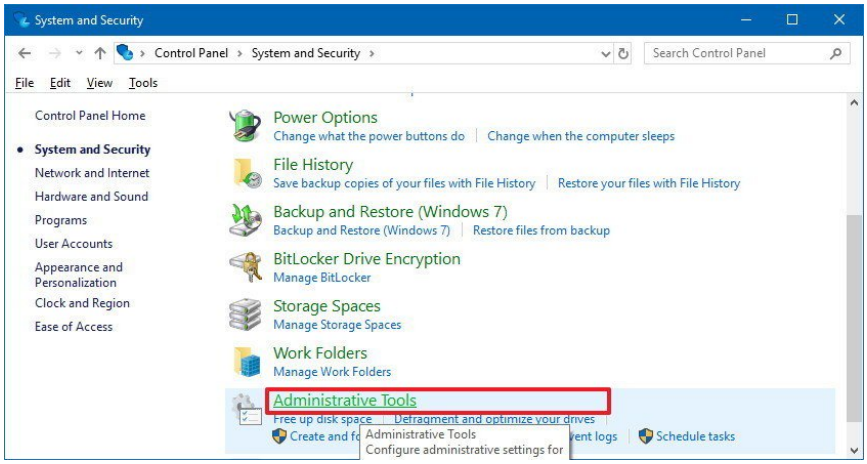
How to configure an FTP server site on Windows 10

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.

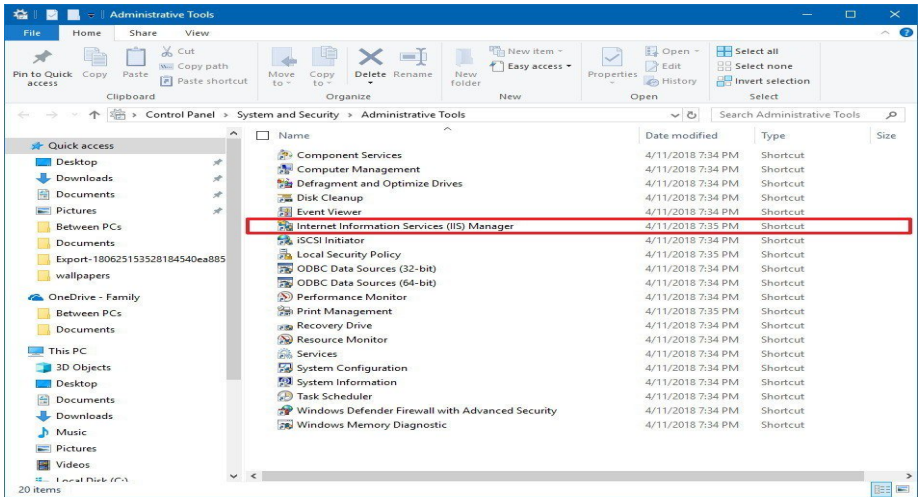
Setting up an FTP site

To set up an FTP site, do the following:

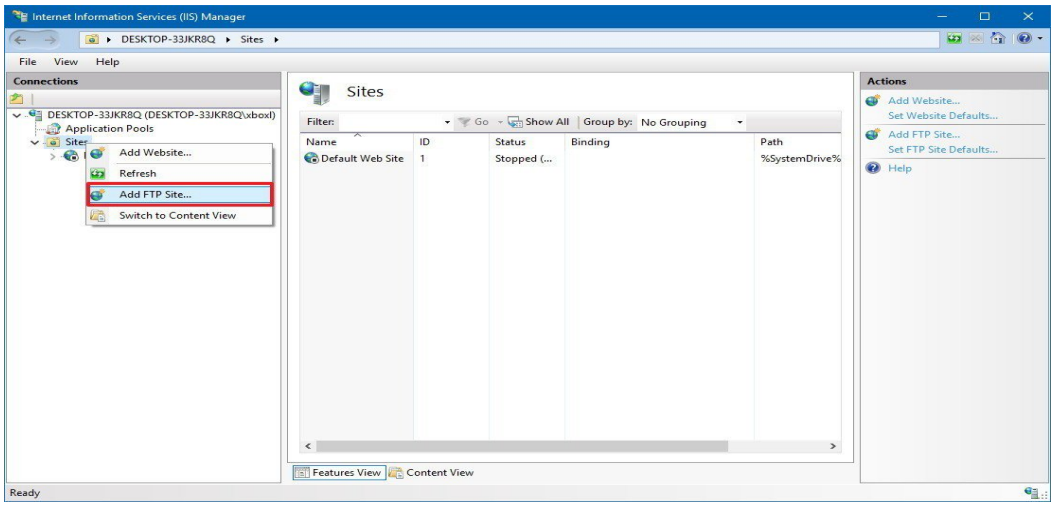
1. Open **Control Panel**.
2. Click on **System and Security**.
3. Click on **Administrative Tools**.



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



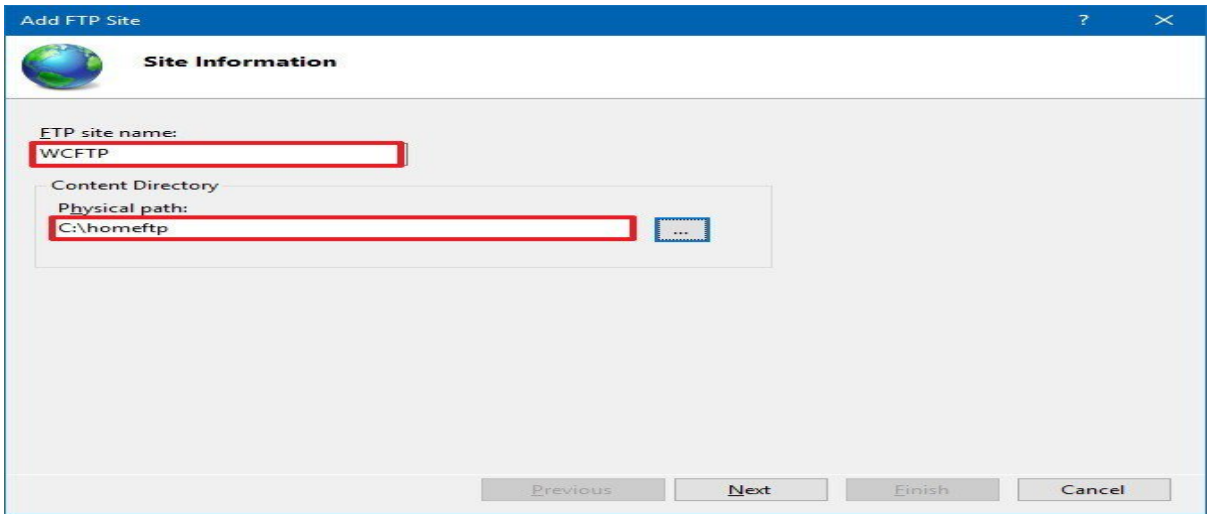
5. On the "Connections" pane, right-click **Sites**, and select the **Add FTP Site** option.



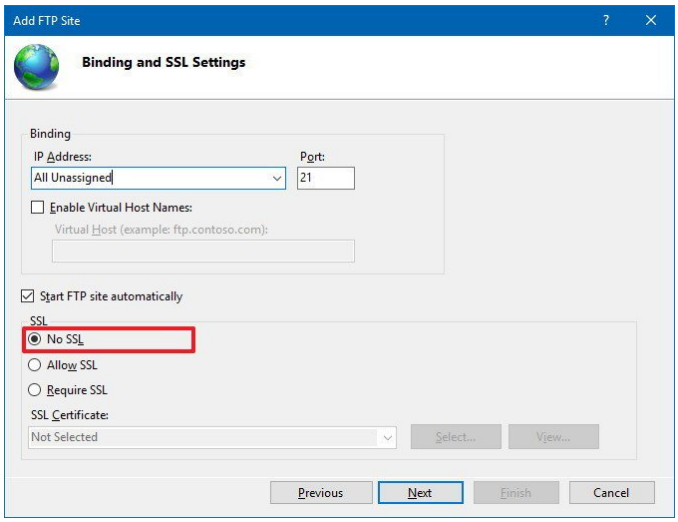
6. In the FTP site name, type a short descriptive name for the server.
7. In the "Content Directory" section, under "Physical path," click the button on the right to locate the folder you want to use to store your FTP files.

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.)

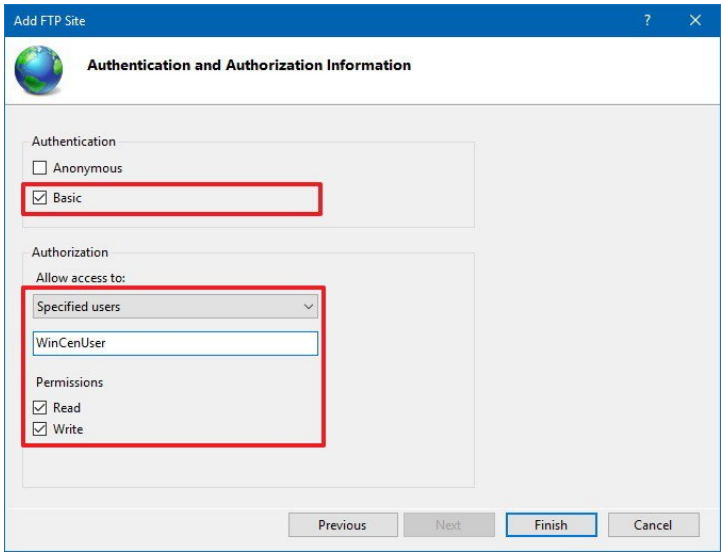


8. Click the **Next** button.
9. Use the default **Binding** settings selections.
10. Check the **Start FTP site automatically** option.
11. In the "SSL" section, check the **No SSL** option.



Important: In a business environment or on an FTP server that will host sensitive data, it's best practice to configure the site to require SSL to prevent transmitting data in clear text.

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



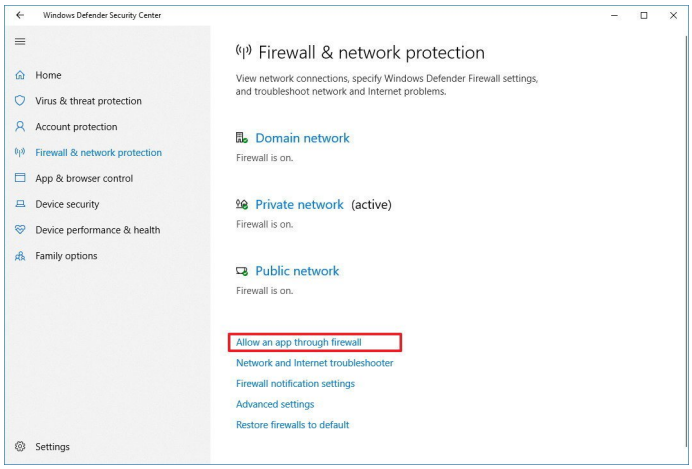
17. Click the **Finish** button.

After completing the steps, the FTP site should now be operational on your computer.

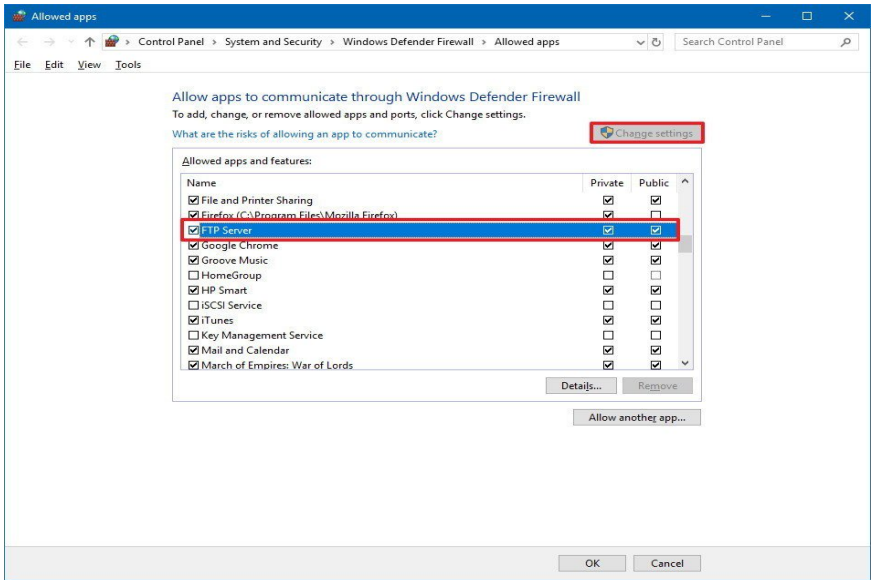
Configuring firewall rules

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:

1. Open **Windows Defender Security Center**.
2. Click on **Firewall & network protection**.
3. Click the **Allow an app through firewall** option.



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



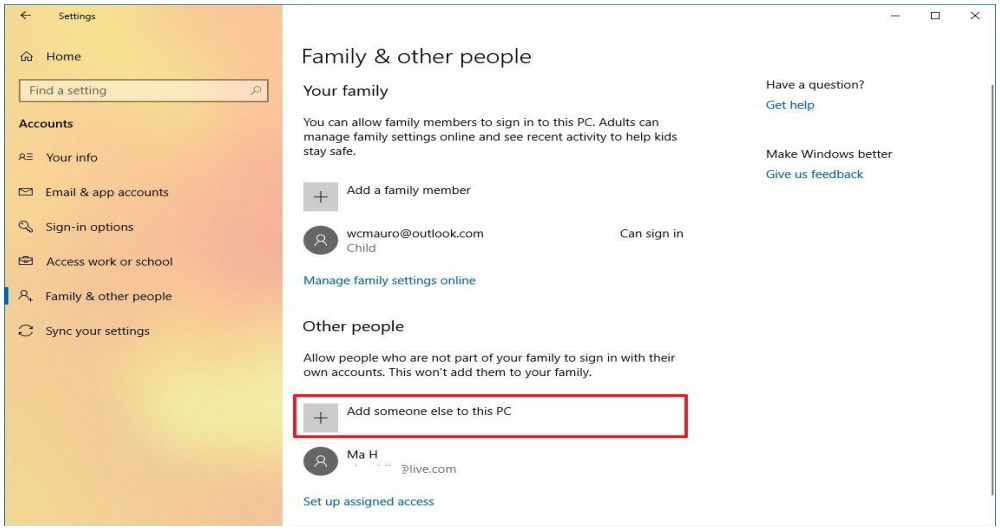
Once you've completed the steps, the FTP server should now be accessible from the local network.

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.

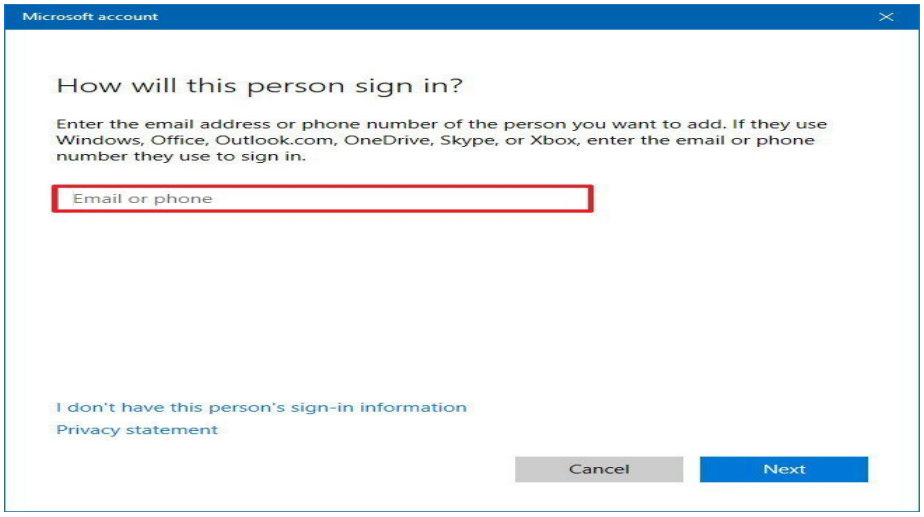
Creating new user accounts

To add multiple accounts to an FTP server, do the following:

1. Open **Settings**.
2. Click on **Accounts**.
3. Click on **Family & other people**.
4. Click the **Add someone else to this PC** button.



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



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.

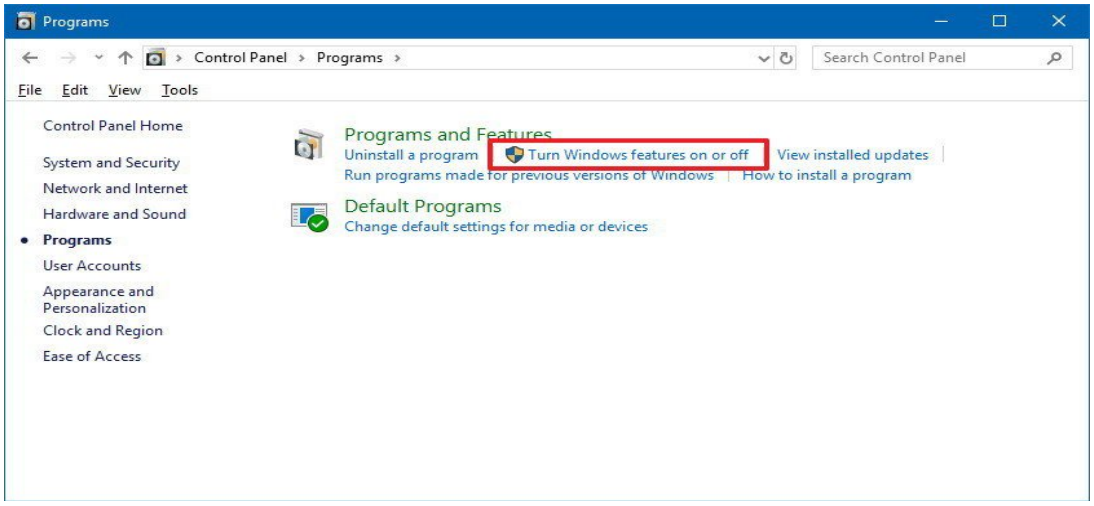
6. Click the **Next** button.

Once you've completed the steps, you may need to repeat the steps to create additional accounts.

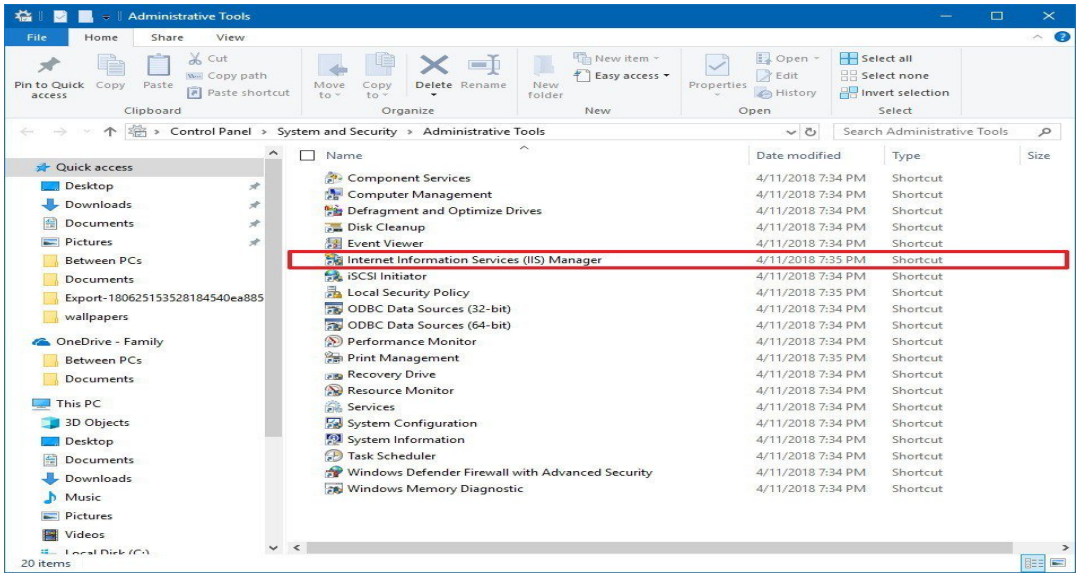
Configuring user accounts to FTP server

If you want multiple users to access the FTP server at the same time, you need to modify the server settings using these steps:

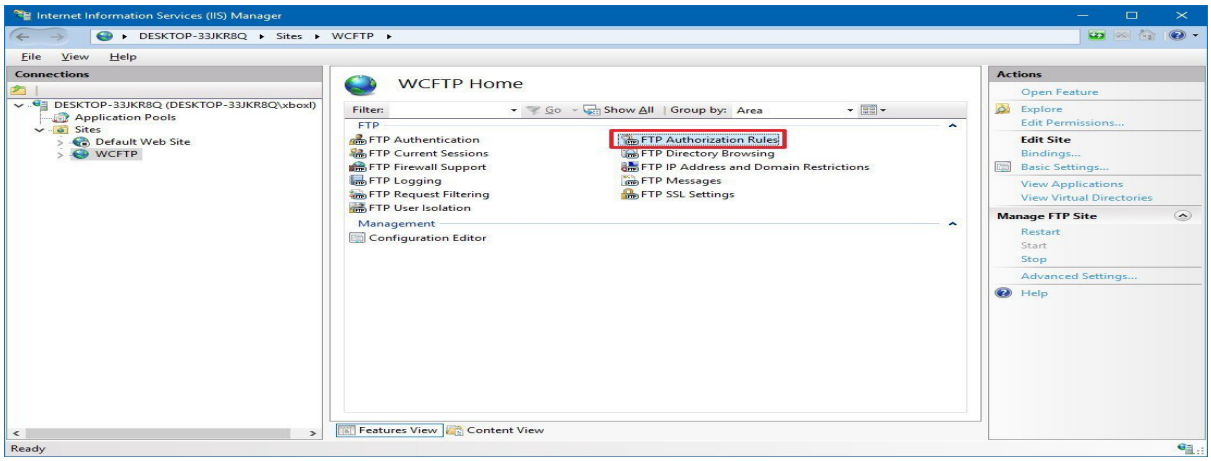
1. Open **Control Panel**.
2. Click on **System and Security**.
3. Click on **Administrative Tools**.



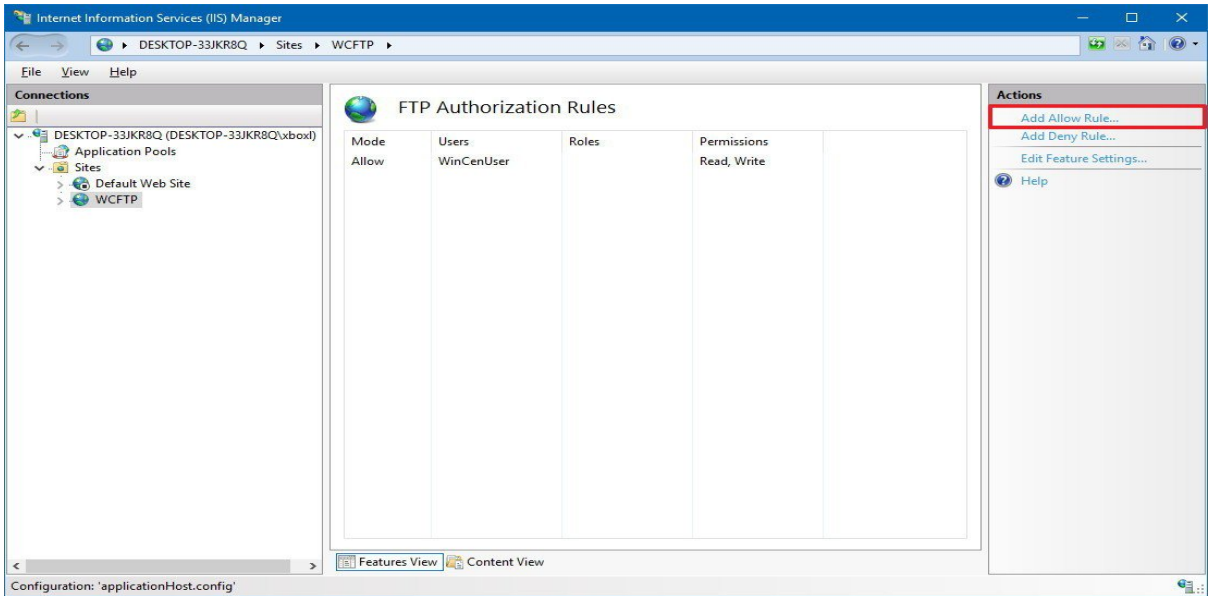
4. Double-click the **Internet Information Services (IIS) Manager** shortcut.



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



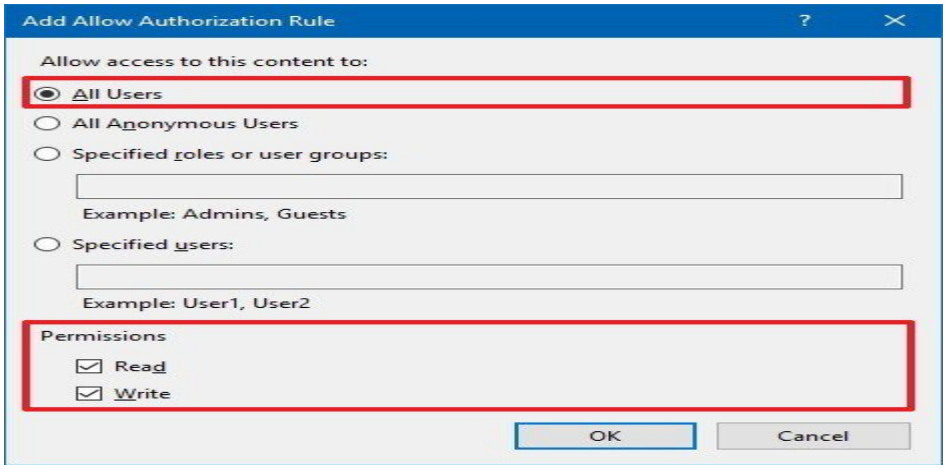
7. On the right pane, click the **Add Allow Rule** option.



8. 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.)

9. Check the **Read** and **Write** options.



10. 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.

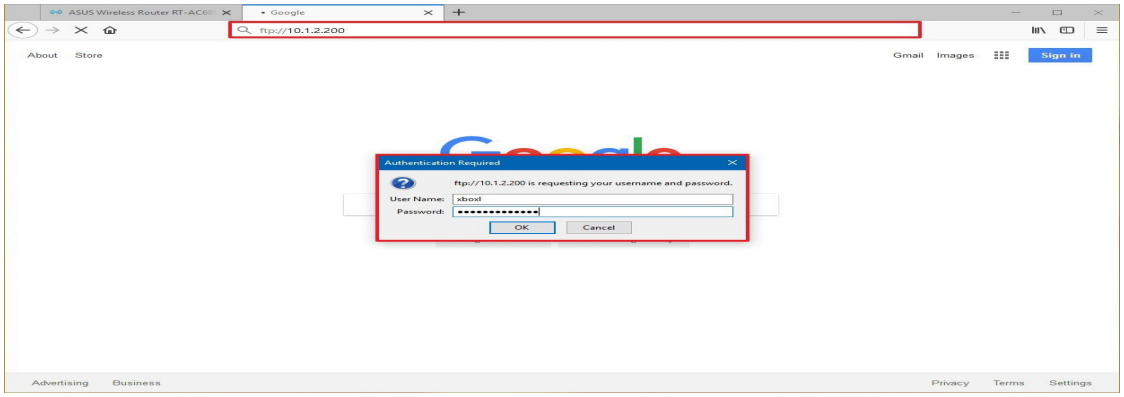
How to connect to an FTP server remotely on Windows 10

Once you've created and configured your FTP server, there are many ways to view, download, and upload files.

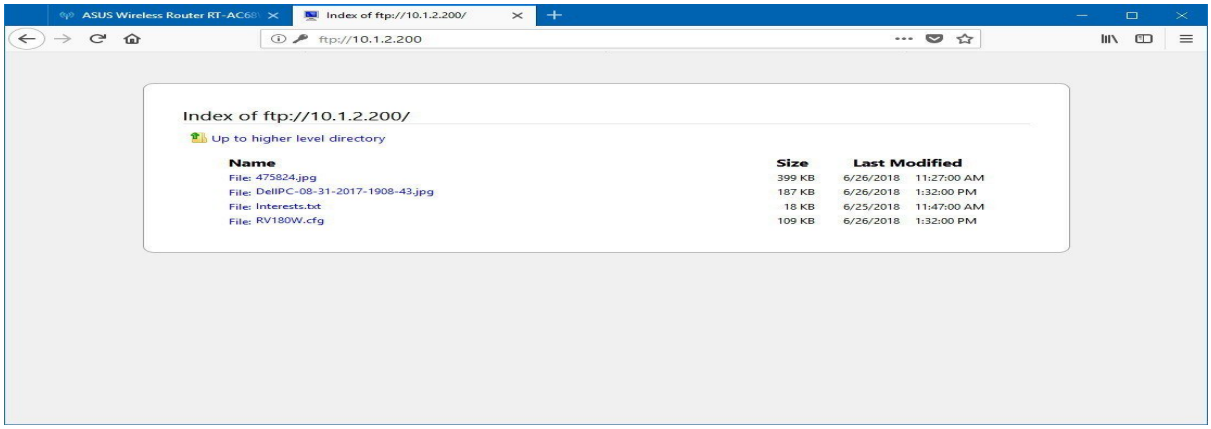
Viewing and downloading files

If you want to browse and download files, you can do this using Internet Explorer, Firefox, or Chrome:

1. Open a **web browser**.
2. In the address bar, type the server IP address using **ftp://**, and press **Enter**. For example, **ftp://192.168.1.100**.
3. Type your account credentials.
4. Click the **Log on** button.



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



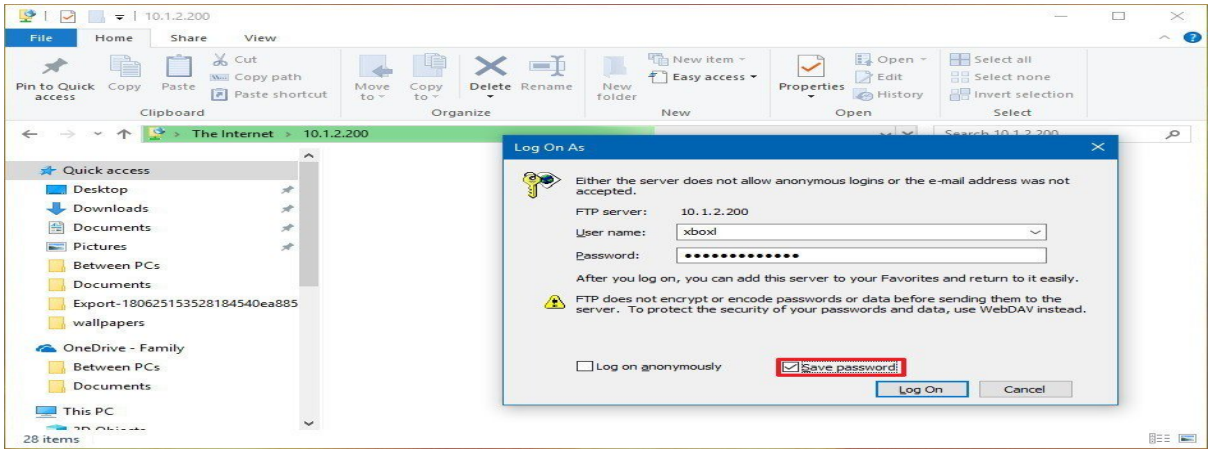
In the case that you're trying to connect from the internet, you have to specify the public (internet) IP address of the network hosting the FTP server.

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 an 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.

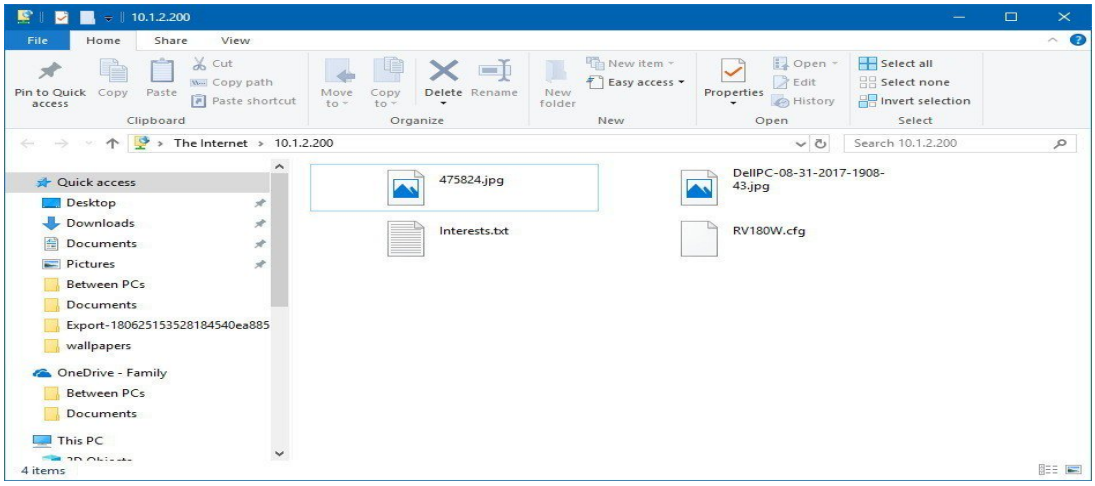
Viewing, downloading, and uploading files

The easiest way to browse, download and upload files is to use File Explorer with these steps.

1. Open **File Explorer**.
2. In the address bar, type the server address using **ftp://**, and press **Enter**. For example, **ftp://192.168.1.100**.
3. Type your account credentials.
4. Check the **Save password** option.
5. 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.



You can avoid going through the steps to reconnect to the FTP server by right-clicking **Quick Access** in the left pane, and selecting the **Pin current folder to Quick Access** option.

Of course, you're not limited to use File Explorer as there are plenty of FTP clients, such as FileZilla that you can use to transfer files.

Nslookup {hostname} :

nslookup is the name of a program that lets an Internet server administrator or any computer user enter a host name (for example, "whatis.com") and find out the corresponding IP address. It will also do reverse name lookup and find the host name for an IP address you specify.
For example, if you entered "whatis.com" (which is one of the TechTarget sites), you would receive as a response our IP address, which happens to be :
65.214.43.37
Or if you entered "65.214.43.37", it would return "sites.techtarget.com".

nslookup sends a domain name query packet to a designated (or defaulted) domain name system (DNS) server. Depending on the system you are using, the default may be the local DNS name server at your service provider, some intermediate name server, or the root server system for the entire domain name system hierarchy.

Using the Linux and possibly other versions of nslookup, you can locate other information associated with the host name or IP address, such as associated mail services. nslookup is included with some UNIX-based operating systems and in later Windows systems. In Windows XP, the command can be entered on the "Command prompt" screen. A more limited alternative to nslookup for looking up an IP address is the ping command.

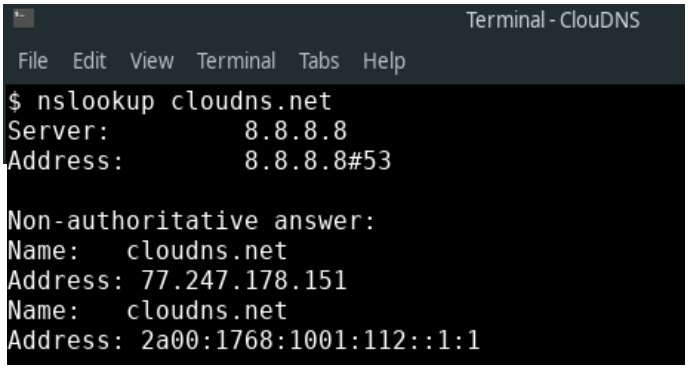
Using Nslookup :

To illustrate the use of nslookup we are going to use it to:

- Find the IP address of a host.
- Find the domain name of an IP address.
- Find mail servers for a domain.

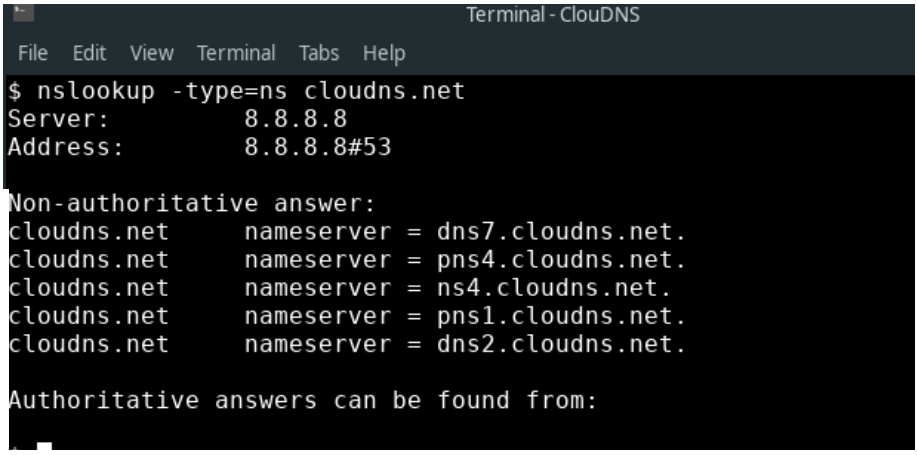
1. How to find the A record of a domain.

Command line: $ nslookup example.com



2. How to check the NS records of a domain.

Command line: $nslookup -type=ns example.com



3. How to query the SOA record of a domain.
Command line: $nslookup -type=soa example.com

```
Terminal - ClouDNS
File  Edit  View  Terminal  Tabs  Help
$ nslookup -type=soa cloudns.net
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
cloudns.net
        origin = pns1.cloudns.net
        mail addr = support.cloudns.net
        serial = 2018112002
        refresh = 7200
        retry = 3600
        expire = 1209600
        minimum = 60

Authoritative answers can be found from:
```

4. How to find the MX records responsible for the email exchange.
Command line: $ nslookup -query=mx example.com

```
$ nslookup -query=mx cloudns.net
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
cloudns.net     mail exchanger = 10 ALT4.ASPMX.L.GOOGLE.COM.
cloudns.net     mail exchanger = 5 ALT1.ASPMX.L.GOOGLE.COM.
cloudns.net     mail exchanger = 1 ASPMX.L.GOOGLE.COM.
cloudns.net     mail exchanger = 10 ALT3.ASPMX.L.GOOGLE.COM.
cloudns.net     mail exchanger = 5 ALT2.ASPMX.L.GOOGLE.COM.

Authoritative answers can be found from:
```

5. How to find all of the available DNS records of a domain.
Command line: $ nslookup -type=any example.com

```
Terminal - ClouDNS
File  Edit  View  Terminal  Tabs  Help
$ nslookup -type=any cloudns.net
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
cloudns.net
        origin = pns1.cloudns.net
        mail addr = support.cloudns.net
        serial = 2018112002
        refresh = 7200
        retry = 3600
        expire = 1209600
        minimum = 60
cloudns.net     text = "v=spf1 include:_spf.google.com include:_spf.topdns.com i
nclude:_spf.orderbox.cloudns.net ip4:109.201.133.0/24 ip6:2a00:1768:1001:9::/64
ip6:2a00:1768:1001:112::/64 ip6:2a00:1768:2001:63::/64 ip4:185.206.180.112 ip4:4
6.166.184.96/27 ip4:77.247.178.151 ip4:" "77.247.178.152 ip4:77.247.178.153 ip4:
45.32.232.230 -all"
cloudns.net     nameserver = dns2.cloudns.net.
cloudns.net     nameserver = pns4.cloudns.net.
cloudns.net     nameserver = pns1.cloudns.net.
cloudns.net     nameserver = dns7.cloudns.net.
cloudns.net     nameserver = ns4.cloudns.net.
cloudns.net     mail exchanger = 10 ALT3.ASPMX.L.GOOGLE.COM.
```

6. How to check the using of a specific DNS Server.
Command line: $ nslookup example.com ns1.nsexample.com

```
Terminal - ClouDNS
File  Edit  View  Terminal  Tabs  Help
$ nslookup cloudns.net ns1.cloudns.net
Server:         ns1.cloudns.net
Address:        85.159.233.17#53

Name:   cloudns.net
Address: 77.247.178.151
Name:   cloudns.net
Address: 2a00:1768:1001:112::1:1

$
```

7. How to check the Reverse DNS Lookup.
Command line: $ nslookup 10.20.30.40

```
Terminal - ClouDNS
File  Edit  View  Terminal  Tabs  Help
$ nslookup 185.136.96.96
96.96.136.185.in-addr.arpa      name = pns21.cloudns.net.

Authoritative answers can be found from:
```

8. How to enable debug mode.
Debug mode provides important and detailed information both for the question and for the received answer.
Command line: $ nslookup -debug example.com

```
Terminal - ClouDNS
File  Edit  View  Terminal  Tabs  Help
$ nslookup -debug cloudns.net
Server:         8.8.8.8
Address:        8.8.8.8#53

------------
    QUESTIONS:
        cloudns.net, type = A, class = IN
    ANSWERS:
    ->  cloudns.net
        internet address = 77.247.178.151
        ttl = 59
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   cloudns.net
Address: 77.247.178.151
------------
    QUESTIONS:
        cloudns.net, type = AAAA, class = IN
    ANSWERS:
    ->  cloudns.net
        has AAAA address 2a00:1768:1001:112::1:1
        ttl = 59
```

Telnet :

Teletype Network Protocol (Telnet)

What is Telnet?

- Telnet, developed in 1969, is a protocol that provides a command line interface for communication with a remote device or server, sometimes employed for remote management but also for initial device setup like network hardware. Telnet stands for Teletype Network, but it can also be used as a verb; 'to telnet' is to establish a connection using the telnet protocol.
- Because it was developed before the mainstream adaptation of the internet, telnet does not employ any form of encryption, making it outdated in terms of modern security. It has largely been overlapped by Secure Shell (SSH) protocol, at least on the public internet.

How does Telnet work?

- Telnet provides users with a bidirectional interactive text-oriented communication system utilizing a virtual terminal connection over 8 byte. User data is interspersed in-band with telnet control information over the transmission control protocol (TCP). Often, Telnet was used on a terminal to execute functions remotely.
- The user connects to the server by using the Telnet protocol, which means entering Telnet into a command prompt by following this syntax: telnet hostname port. The user then executes commands on the server by using specific Telnet commands into the Telnet prompt. To end a session and log off, the user ends a Telnet command with Telnet.

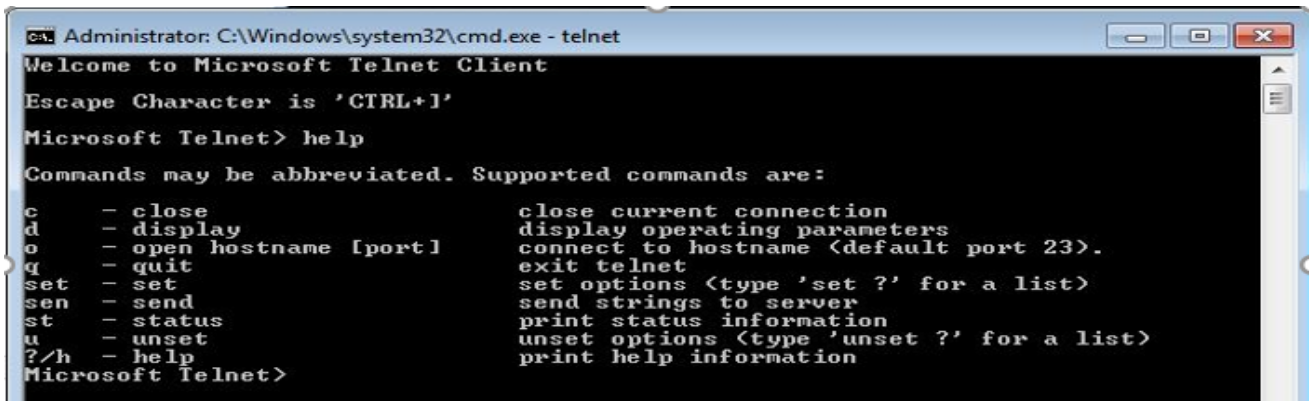
What are common uses for Telnet?

- Telnet can be used to test or troubleshoot remote web or mail servers, as well as for remote access to MUDs (multi-user dungeon games) and trusted internal networks.

Resolution

To use telnet, follow the steps below:

1. To find port number.



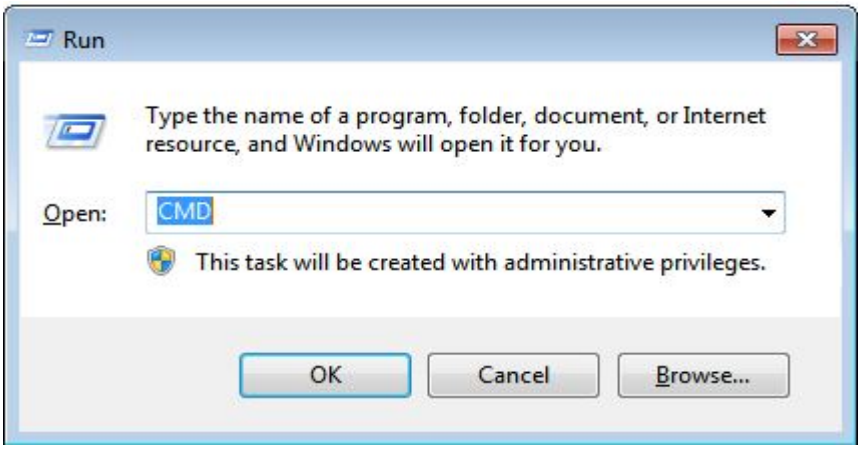
2. First, find out the ip address of the server/main computer. For this you need to access the server and use the ipconfig command in MS-DOS. See Additional Information section for more details about this command.

```
Administrator: C:\Windows\system32\cmd.exe
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet> ipconfig
Invalid Command. type ?/help for help
Microsoft Telnet> q

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::418a:1606:1a1f:8b8e%11
   IPv4 Address. . . . . . . . . . . : 172.16.2.117
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.16.0.1

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::99fe:b1f8:e41b:d47c%13
   IPv4 Address. . . . . . . . . . . : 192.168.32.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::74f0:62d3:9d6e:1b3f%14
   IPv4 Address. . . . . . . . . . . : 192.168.204.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{1283E13A-25ED-4774-9DDB-11516601097F}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

C:\Users\Administrator>
```

3. Select the Windows key and the R key.

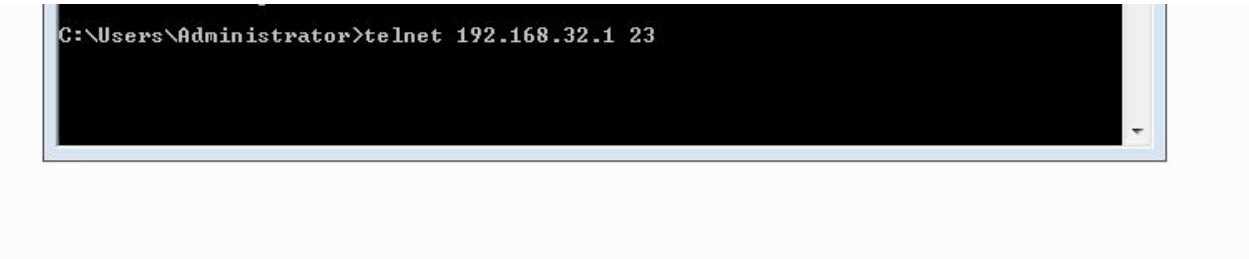
    +R

4. In the Run box type CMD.

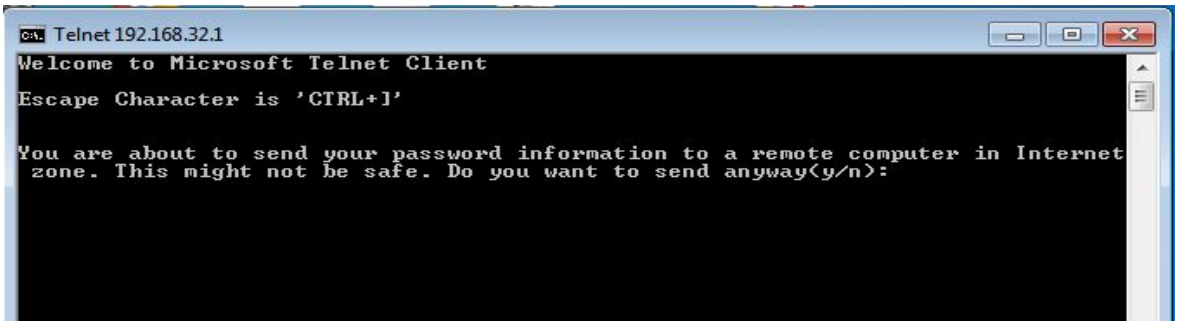


5. Select OK.

6. Type Telnet <IP Address> 23.



7. Note: Do not include the <> when entering the IP Address.

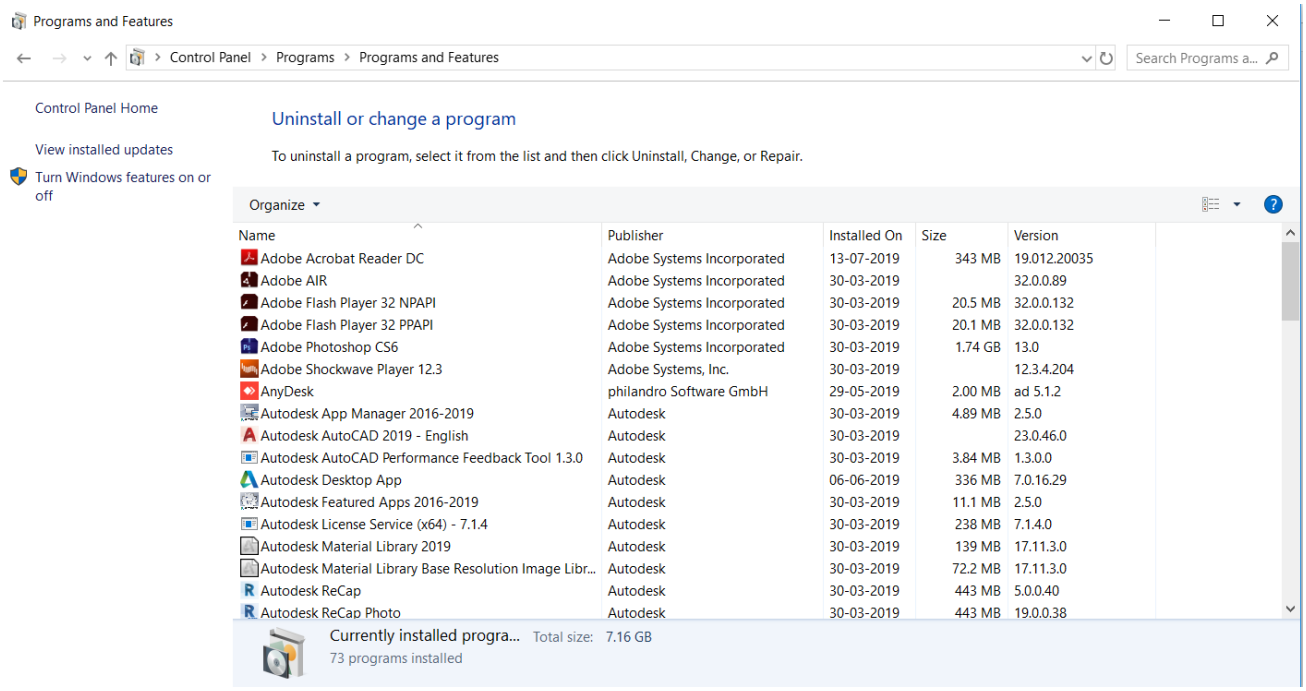


If you see a blank cursor then the connection is fine. You can close the command prompt window. If you get the message that 'telnet' is not recognized as an internal or external command, operable program or batch file. you will want to enable Telnet. See Additional Information on how to Enable telnet. If you get an error or are unable to telnet to the server please contact your Network Administrator.

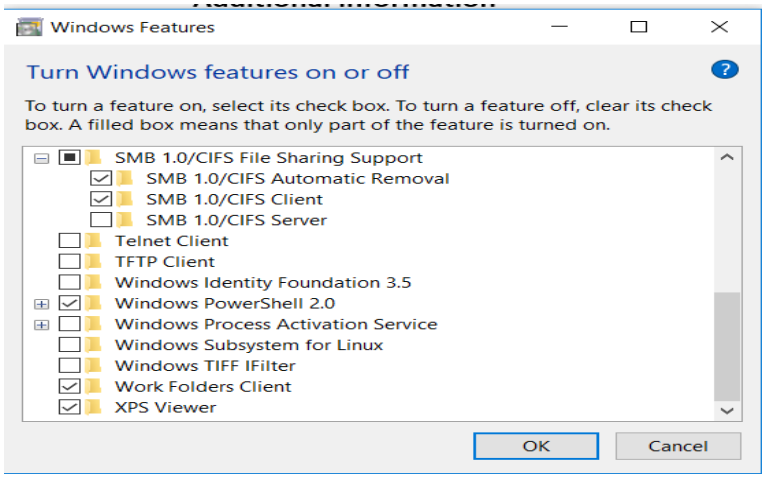
Additional information

To enable Telnet follow these steps:

1. Select Start, Control Panel, then Programs and Features (or Programs)



2. Select Turn Windows Features on or off
3. Check the box for both Telnet Client and Telnet Server



4. Select OK and Verify that you can now Telnet the port