# **Networking**

There are two advantages to using routers in your network:

1. They don’t forward broadcasts by default.

2. They can filter the network based on layer 3 (Network layer) information such as an IP address.

Here are four ways a router functions in your network:

1. Packet switching

2. Packet filtering

3. Internetwork communication

4. Path selection

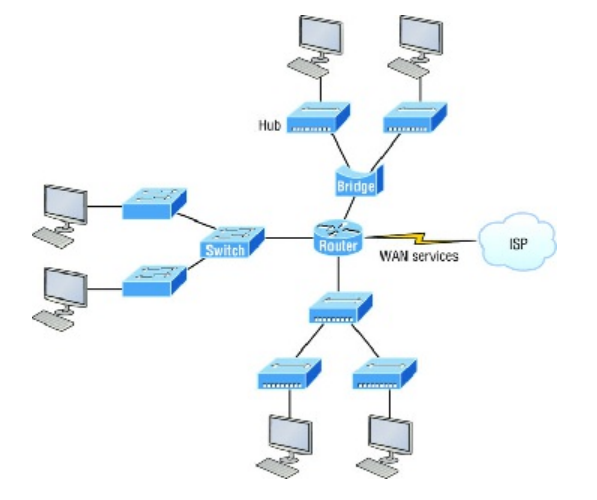
Note: Layer 2 forward or filter frames, routers (layer 3 switches) use logical

addressing and provide an important capacity called packet switching.

Routers can also provide packet filtering via access lists, and when routers connect two or more networks together and use logical addressing (IP or IPv6), you then have an internetwork.

Finally, routers use a routing table, which is essentially a map of the internetwork, to make best path selections for getting data to its proper destination and properly forward packets to remote networks.

Note: switches don’t forward packets to other networks like routers do. Instead, they only “switch” frames from one port to another within the switches.



How many collision domains and broadcast domains are really there in this internetwork? I hope you answered nine collision domains and three broadcast domains! The broadcast domains are definitely the easiest to spot because

only routers break up broadcast domains by default, and since there are three interface connections, that gives you three broadcast domains.

I’ll explain. The all- hub network at the bottom is one collision domain; the bridge network on top equals three collision domains. Add in the switch network of five collision domains—one for each switch port—and you get a total of nine.

Each port on the switch is a separate collision domain, and each VLAN would be a separate broadcast domain. So how many collision domains do you see here? I’m counting 12—remember that connections between the switches are considered a collision domain! Since the figure doesn’t show any VLAN information, we can assume the default of one broadcast domain is in place.

\*When networks first came into being, computers could typically communicate only with computers from the same manufacturer. companies ran either a complete DECnet solution or an IBM solution, never both together.

Then, OSI model come in picture. The OSI model was meant to help vendors create interoperable network devices and software in the form of protocols so that different vendor networks could work in peaceable accord with each other. Like world peace, it’ll probably never happen completely, but it’s still a great goal!

Any-way the OSI (Open Systems Interconnection) model is the primary architectural model for networks. It describes how data and network information are communicated from an application on one computer through the network media to an application on another computer. The OSI reference model breaks this approach into layers.

The OSI reference model has the following seven layers:

1. Application layer (layer 7): [data] {Network process to application}

2. Presentation layer (layer 6): [data] {Data representation and Encryption}

3. Session layer (layer 5): [data] {Interhost communication}

4. Transport layer (layer 4): [segments] {End-to-end connection}

5. Network layer (layer 3): [packets] {Path determination and IP}

6. Data Link layer (layer 2): [frames] {Mac and Physical addressing}

7. Physical layer (layer 1): [bits] {Media, Signal and Binary Transmission}

Some people like to use a mnemonic to remember the seven layers, such as

“All People Seem To Need Data Processing”.

Collision Domain

Broadcast Domain

Now, to reduce Collision we have CSMA/CD protocol. CSMA/CD is a protocol that helps devices share the bandwidth evenly without having two devices transmit at the same time on the network medium. Although it does not eliminate collisions, it helps to greatly reduce them, which reduces retransmissions, resulting in a more efficient transmission of data for all devices.

* Half- and Full-Duplex Ethernet

Ethernet Cabling:

1. Straight-through cable: Host to switch or hub, Router to switch or hub

2. Crossover cable: Switch to switch, hub to hub router to router

3. Rolled cable: Although rolled cable isn’t used to connect any Ethernet connections together, you can use a rolled Ethernet cable

to connect a host EIA-TIA 232 interface to a router console serial communication (COM) port. If you have a Cisco router or switch, you would use this cable to connect your PC, Mac, or a device like an iPad to

the Cisco hardware.

TCP/IP and the DoD Mode:

1. Process/Application layer

2. Host-to-Host layer or Transport layer

3. Internet layer

4. Network Access layer or Link layer

**TELNET: port no.- 23**

Telnet is a network protocol used to virtually access a computer and to provide a two-way, collaborative and text-based communication channel between two machines.

It follows a user command Transmission Control Protocol/Internet Protocol (TCP/IP) networking protocol for creating remote sessions.

A drawback is that there are no encryption techniques available within the Telnet protocol, so everything must be sent in clear text, including passwords!

Telnet uses an 8-bit, byte-oriented data connection over TCP.

How Telnet works:

Telnet is a type of client-server protocol that can be used to open a command line on a remote computer, typically a server. Users can utilize this tool to ping a port and find out whether it is open. Telnet works with what is called a virtual terminal connection emulator, or an abstract instance of a connection to a computer, using standard protocols to act like a physical terminal connected to a machine. FTP may also be used along with Telnet for users working to send data files.

Users connect remotely to a machine using Telnet, sometimes referred to as Telnetting into the system. They are prompted to enter their username and password combination to access the remote computer, which enables the running of command lines as if logged in to the computer in person. Despite the physical location of users, their IP address will match the computer logged in to rather than the one physically used to connect.

**Secure Shell (SSH): port no.- 22**

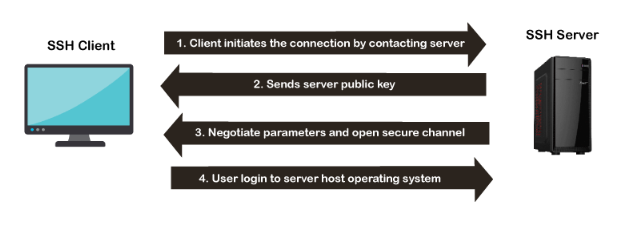
SSH stands for Secure Shell or Secure Socket Shell. It is a cryptographic network protocol that allows two computers to communicate and share the data over an insecure network such as the internet. It is used to login to a remote server to execute commands and data transfer from one machine to another machine.

The SSH protocol was developed by SSH communication security Ltd to safely communicate with the remote machine.

Secure communication provides a strong password authentication and encrypted communication with a public key over an insecure channel. It is used to replace unprotected remote login protocols such as Telnet, rlogin, rsh, etc., and insecure file transfer protocol FTP.

How does SSH Works?

The SSH protocol works in a client-server model, which means it connects a secure shell client application (End where the session is displayed) with the SSH server (End where session executes).



OpenSSH 9.3p2 (2023-07-19) OpenSSH 9.3p2 was released on 2023-07-19.

The public-key is a public key-based authentication method, which supports DSA, ECDSA, or RSA keypairs.

**File Transfer Protocol (FTP): port no.- 21**

FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.

It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.

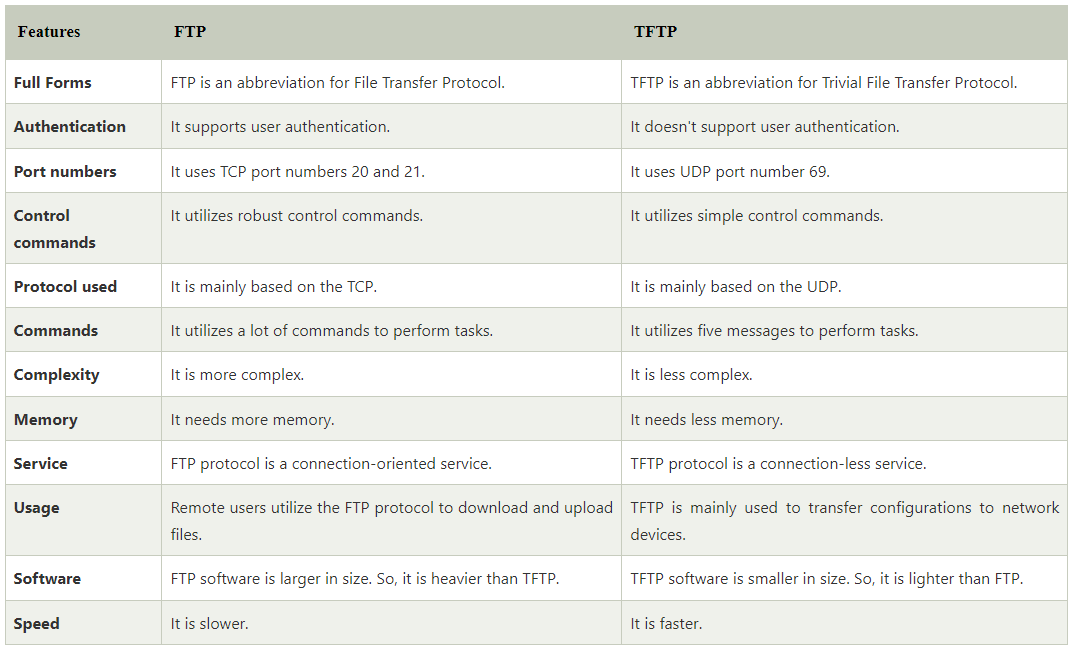
It is also used for downloading the files to computer from other servers.

Why FTP?

Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

**Trivial File Transfer Protocol (TFTP): port no.- 69**

TFTP is an abbreviation for "Trivial File Transfer Protocol". It is a sample protocol that is commonly used for file transmission. TFTP employs the User Datagram Protocol (UDP) to transport data from one end to the other. In comparison to the FTP, it is very simple in design and has limited functionalities (FTP). TFTP doesn't provide authentication or security while transferring data. As a result, boot data or configuration files are typically shared between computer systems in a local setup.



**Hypertext Transfer Protocol (HTTP-S): port no.-80, 443**

It is a protocol used to access the data on the World Wide Web (www).

The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.

This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.

HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.

HTTP is used to carry the data in the form of MIME-like format.

HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

TFTP (Trivial File Transfer Protocol) and HTTP (Hypertext Transfer Protocol) are two different protocols used for file transfer over a network. Here are some key **differences between TFTP and HTTP:**

**Purpose:** TFTP is primarily designed for simple and lightweight file transfer operations, often used for bootstrapping devices or transferring firmware and configuration files. On the other hand, HTTP is a more comprehensive protocol used for transferring hypertext, web pages, files, and other resources over the internet.

**Protocol:** TFTP operates at the transport layer of the OSI model and is based on UDP (User Datagram Protocol). It provides basic file transfer functionality with no built-in security features. HTTP operates at the application layer of the OSI model and is based on TCP (Transmission Control Protocol). It supports more advanced features like request/response, caching, authentication, and encryption.

**Port:** TFTP typically uses port 69 for communication, and it employs a simple connectionless model. HTTP commonly uses port 80 for unencrypted communication and port 443 for encrypted communication (HTTPS).

**File Transfer:** TFTP transfers files in a simple block-by-block manner, with no support for file compression or complex file structures. It lacks features like resuming interrupted transfers or supporting partial file downloads. HTTP supports more advanced file transfer operations, allowing for compression, resumable downloads, range requests, and the ability to handle more complex file structures like HTML, images, videos, etc.

**Usage and Support:** TFTP is commonly used in scenarios where simplicity and speed are more important than advanced features, such as network booting, firmware updates for networking devices, or initial OS installations. HTTP, being a more versatile protocol, is widely used for web browsing, web application APIs, downloading files from web servers, and various internet-related activities.

**Security:** TFTP lacks built-in security features and does not support encryption or authentication by default. It is often used within a trusted network environment. On the other hand, HTTP supports various security mechanisms, including HTTPS (HTTP over SSL/TLS), which provides encrypted communication, data integrity, and authentication using digital certificates.

