UNIT-5 (ICT HARDWARE)

Switched-Mode Power Supply (SMPS)

A switched-mode power supply (SMPS) is an electronic circuit that converts power using switching devices that are turned on and off at high frequencies, and storage components such as inductors or capacitors to supply power when the switching device is in its non-conduction state.

Switching power supplies have high efficiency and are widely used in a variety of electronic equipment, including computers and other sensitive equipment requiring stable and efficient power supply.

A switched-mode power supply is also known as a switch-mode power supply or switching-mode power supply.

Switched-mode power supplies are classified according to the type of input and output voltages. The four major categories are:

- AC to DC
- DC to DC
- DC to AC
- AC to AC

A basic isolated AC to DC switched-mode power supply consists of:

- Input rectifier and filter
- Inverter consisting of switching devices such as MOSFETs
- Transformer
- Output rectifier and filter
- Feedback and control circuit

The input DC supply from a rectifier or battery is fed to the inverter where it is turned on and off at high frequencies of between 20 KHz and 200 KHz by the switching MOSFET or power transistors. The high-frequency voltage pulses from the inverter are fed to the transformer primary winding, and the secondary AC output is rectified and smoothed to produce the required DC voltages. A feedback circuit monitors the output voltage and instructs the control circuit to adjust the duty cycle to maintain the output at the desired level.

There are different circuit configurations known as topologies, each having unique characteristics, advantages and modes of operation, which determines how the input power is transferred to the output.

Most of the commonly used topologies such as flyback, push-pull, half bridge and full bridge, consist of a transformer to provide isolation, voltage scaling, and multiple output voltages. The non-isolated configurations do not have a transformer and the power conversion is provided by the inductive energy transfer.

Advantages of switched-mode power supplies:

- Higher efficiency of 68% to 90%
- Regulated and reliable outputs regardless of variations in input supply voltage
- Small size and lighter
- Flexible technology
- High power density

Disadvantages:

- Generates electromagnetic interference
- Complex circuit design
- Expensive compared to linear supplies

Switched-mode power supplies are used to power a wide variety of equipment such as computers, sensitive electronics, battery-operated devices and other equipment requiring high efficiency.

Network interface card (NIC)

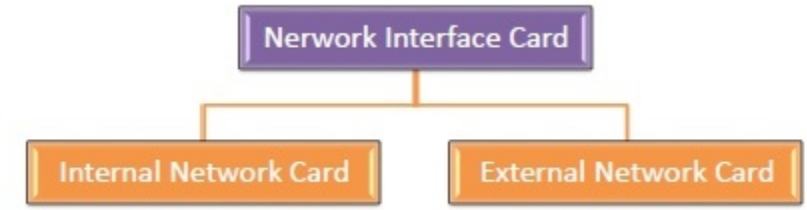
A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

Purpose

- NIC allows both wired and wireless communications.
- NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
- NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Types of NIC Cards

NIC cards are of two types −

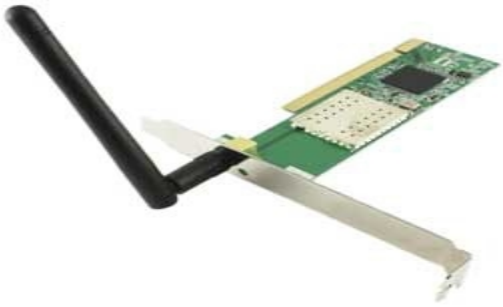


Internal Network Cards

In internal networks cards, motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access. Internal network cards are of two types. The first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).

External Network Cards

In desktops and laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.



What is Network Cabling?

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size.

Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following sections discuss the types of cables used in networks and other related topics.

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable
- Cable Installation Guides
- Wireless LANs
- Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks (See fig. 1).

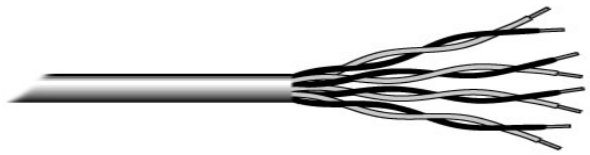


Fig.1. Unshielded twisted pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated six categories of wire (additional categories are emerging).

Categories of Unshielded Twisted Pair

Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring (Rarely used)

5	100 Mbps (2 pair)	100BaseT Ethernet
	1000 Mbps (4 pair)	Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

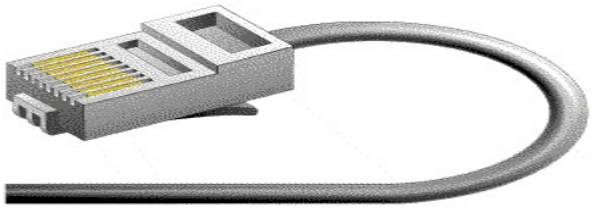


Fig. 2. RJ-45 connector

Shielded Twisted Pair (STP) Cable

Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

Shielded twisted pair cable is available in three different configurations:

1. Each pair of wires is individually shielded with foil.
2. There is a foil or braid shield inside the jacket covering all wires (as a group).
3. There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See fig. 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

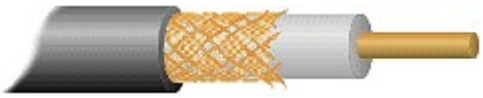


Fig. 3. Coaxial cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable has been popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See fig. 4). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.

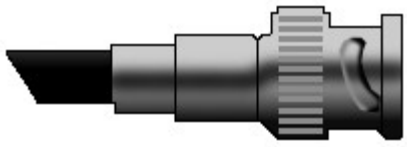


Fig. 4. BNC connector

Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See fig. 5). It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount

of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

The center core of fiber cables is made from glass or plastic fibers (see fig 5). A plastic coating then cushions the fiber center, and kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of teflon or PVC.

Fig. 5. Fiber optic cable

There are two common types of fiber cables -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.

Specification	Cable Type
10BaseT	Unshielded Twisted Pair
10Base2	Thin Coaxial
10Base5	Thick Coaxial
100BaseT	Unshielded Twisted Pair
100BaseFX	Fiber Optic
100BaseBX	Single mode Fiber
100BaseSX	Multimode Fiber

1000BaseT	Unshielded Twisted Pair
1000BaseFX	Fiber Optic
1000BaseBX	Single mode Fiber
1000BaseSX	Multimode Fiber

Installing Cable - Some Guidelines

When running cable, it is best to follow a few simple rules:

- Always use more cable than you need. Leave plenty of slack.
- Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
- Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
- If it is necessary to run cable across the floor, cover the cable with cable protectors.
- Label both ends of each cable.
- Use cable ties (not tape) to keep cables in the same location together.

Wireless LANs

More and more networks are operating without cables, in the wireless mode. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations, servers, or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.

Wireless networks are great for allowing laptop computers, portable devices, or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast. Line-of-sight communication means that there must be an unblocked direct

line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network. Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

Wireless standards and speeds

The Wi-Fi Alliance is a global, non-profit organization that helps to ensure standards and interoperability for wireless networks, and wireless networks are often referred to as WiFi (Wireless Fidelity). The original Wi-Fi standard (IEEE 802.11) was adopted in 1997. Since then many variations have emerged (and will continue to emerge). Wi-Fi networks use the Ethernet protocol.

Standard	Max Speed	Typical Range
802.11a	54 Mbps	150 feet
802.11b	11 Mbps	300 feet
802.11g	54 Mbps	300 feet
802.11n	100 Mbps	300+ feet

Wireless Security

Wireless networks are much more susceptible to unauthorized use than cabled networks. Wireless network devices use radio waves to communicate with each other. The greatest vulnerability to the network is that rogue machines can "eves-drop" on the radio wave communications. Unencrypted information transmitted can be monitored by a third-party, which, with the right tools (free to download), could quickly gain access to your entire network, steal valuable passwords to local servers and online services, alter or destroy data, and/or access personal and confidential information stored in your network servers. To minimize the possibility of this, all modern access points and devices have configuration options to encrypt transmissions. These encryption methodologies are still evolving, as are the tools used by malicious hackers, so always use the strongest encryption available in your access point and connecting devices.

A NOTE ON ENCRYPTION: As of this writing WEP (Wired Equivalent Privacy) encryption can be easily hacked with readily-available free tools which circulate the internet. WPA and WPA2 (WiFi Protected Access versions 1 and 2) are much better at protecting information, but using weak passwords or passphrases when enabling these encryptions may allow them to be

easily hacked. If your network is running WEP, you must be very careful about your use of sensitive passwords or other data.

Three basic techniques are used to protect networks from unauthorized wireless use. Use any and all of these techniques when setting up your wireless access points:

Encryption.

> Enable the strongest encryption supported by the devices you will be connecting to the network. Use strong passwords (strong passwords are generally defined as passwords containing symbols, numbers, and mixed case letters, at least 14 characters long).

Isolation.

> Use a wireless router that places all wireless connections on a subnet independent of the primary private network. This protects your private network data from pass-through internet traffic.

Hidden SSID.

> Every access point has a Service Set IDentifier (SSID) that by default is broadcast to client devices so that the access point can be found. By disabling this feature, standard client connection software won't be able to "see" the access point. However, the eves-dropping programs discussed previously can easily find these access points, so this alone does little more than keep the access point name out of sight for casual wireless users.

Advantages of wireless networks:

- Mobility - With a laptop computer or mobile device, access can be available throughout a school, at the mall, on an airplane, etc. More and more businesses are also offering free WiFi access ("Hot spots").
- Fast setup - If your computer has a wireless adapter, locating a wireless network can be as simple as clicking "Connect to a Network" -- in some cases, you will connect automatically to networks within range.
- Cost - Setting up a wireless network can be much more cost effective than buying and installing cables.
- Expandability - Adding new computers to a wireless network is as easy as turning the computer on (as long as you do not exceed the maximum number of devices).

Disadvantages of wireless networks:

- Security - Be careful. Be vigilant. Protect your sensitive data with backups, isolated private networks, strong encryption and passwords, and monitor network access traffic to and from your wireless network.
- Interference - Because wireless networks use radio signals and similar techniques for transmission, they are susceptible to interference from lights and electronic devices.

- Inconsistent connections - How many times have you hears "Wait a minute, I just lost my connection?" Because of the interference caused by electrical devices and/or items blocking the path of transmission, wireless connections are not nearly as stable as those through a dedicated cable.
- Speed - The transmission speed of wireless networks is improving; however, faster options (such as gigabit Ethernet) are available via cables. If you are only using wireless for internet access, the actual internet connection for your home or school is generally slower than the wireless network devices, so that connection is the bottleneck. If you are also moving large amounts of data around a private network, a cabled connection will enable that work to proceed much faster.

I/O box

The IO Box module is a device that enables tomography data to be used for closed loop process control.

The ITS Input-Output Module (or IO Box) is a multiple input / multiple output (MIMO) device that allows the p2+ tomography instrument to import and export 4-20mA signals. It is a free standing unit that connects via USB 2.0 port to the PC running the ITS tomography program.

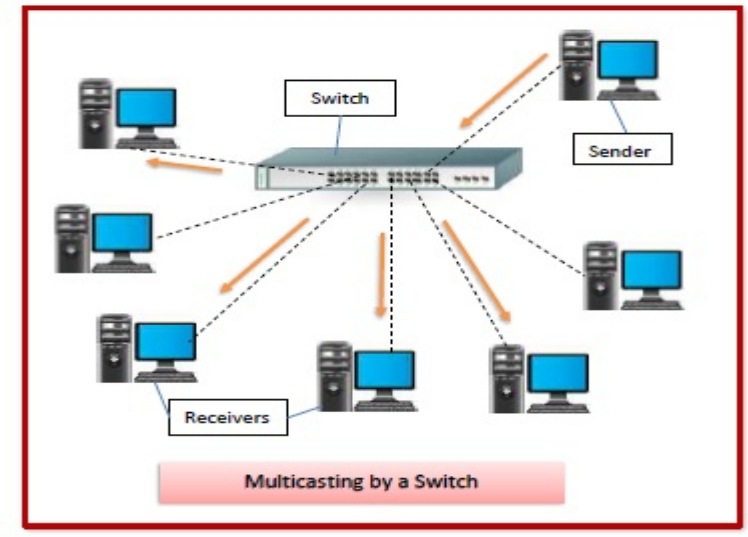
Input data allows tomography calculations to be integrated with flow, temperature, absolute conductivity or other measurements. These can be displayed or exported with a common timestamp. ITS software has an inbuilt algorithm that allows engineers to take data – such as temperature and then use this to separate out conductivity changes due to process environment vs. concentration.

Users can select from a range of variables measured by the p2+ tomography software. Most commonly this can be average measurements relating to conductivity or concentration; spatial information such as statistics relating to an interface or processed tomography information on flow conditions or mixing indices.

Switches

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).It supports unicast, multicast as well as broadcast communications.

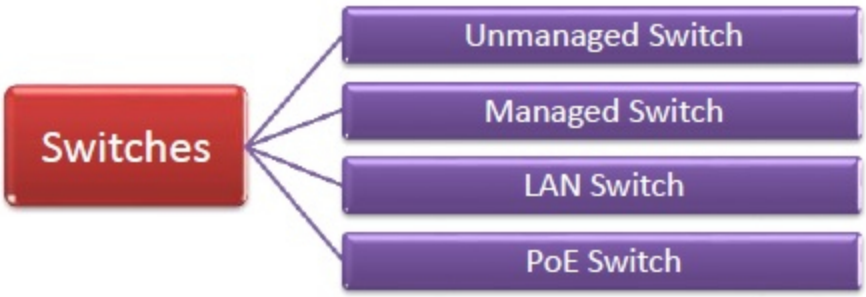


Features of Switches

- A switch operates in the layer 2, i.e. data link layer of the OSI model.
- It is an intelligent network device that can be conceived as a multiport network bridge.
- It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
- It uses packet switching technique to receive and forward data packets from the source to the destination device.
- It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
- Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.
- Switches are active devices, equipped with network software and network management capabilities.
- Switches can perform some error checking before forwarding data to the destined port.
- The number of ports is higher – 24/48.

Types of Switches

There are variety of switches that can be broadly categorised into 4 types −



- **Unmanaged Switch** − These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices needs to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.
- **Managed Switch** − These are costly switches that are used in organisations with large and complex networks, since they can be customized to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.
- **LAN Switch** − Local Area Network (LAN) switches connects devices in the internal LAN of an organization. They are also referred as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.
- **PoE Switch** − Power over Ethernet (PoE) switches are used in PoE Gogabit Ethernets. PoE technology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections

RJ45 is a type of connector commonly used for Ethernet networking. It looks similar to a telephone jack, but is slightly wider. Since Ethernet cables have an RJ45 connector on each end, Ethernet cables are sometimes also called RJ45 cables.

The "RJ" in RJ45 stands for "registered jack," since it is a standardized networking interface. The "45" simply refers to the number of the interface standard. Each RJ45 connector has eight pins, which means an RJ45 cable contains eight separate wires. If you look closely at the end of an Ethernet cable, you can actually see the eight wires, which are each a different color. Four of them are solid colors, while the other four are striped.

RJ45 cables can be wired in two different ways. One version is called T-568A and the other is T-568B. These wiring standards are listed below:

T-568A **T-568B**

White/Green (Receive +)	White/Orange (Transmit +)
Green (Receive -)	Orange (Transmit -)
White/Orange (Transmit +)	White/Green (Receive +)
Blue	Blue
White/Blue	White/Blue
Orange (Transmit -)	Green (Receive -)
White/Brown	White/Brown
Brown	Brown

The T-568B wiring scheme is by far the most common, though many devices support the T-568A wiring scheme as well. Some networking applications require a crossover Ethernet cable, which has a T-568A connector on one end and a T-568B connector on the other. This type of cable is typically used for direct computer-to-computer connections when there is no router, hub, or switch available.

What is a Patch Panel and What Is Its Purpose?

Share:

These days, it seems that just about everything is wireless. But to take advantage of the blazingly fast Internet now available in most homes and businesses, a wired network often will allow you to achieve speeds much closer to the promised maximum.

What Is A Patch Panel?

If you want to set up a wired network that includes multiple wall ports in various rooms, a patch panel in a central location can provide a simple, neat and easy-to-manage solution. So what is a patch panel you ask? A patch panel is essentially an array of ports on one panel. Each port connects, via a patch cable, to another port located elsewhere in your building.

How Do Patch Panels Work?

Patch panels bundle multiple network ports together to connect incoming and outgoing lines — including those for local area networks, electronics, electrical systems and communications. When patch panels are part of a LAN, they can connect computers to other computers and to outside lines. Those lines, in turn, allow LANs to connect to wide area networks or to the Internet. To arrange circuits using a patch panel, you simply plug and unplug the appropriate patch cords. Troubleshooting problems are simplified with patch panels since they provide a single location for all input jacks. They're frequently used in industries that require extensive sound equipment because they work well for connecting a variety of devices.

Managing the Tangle

The primary advantage of using patch panels, also known as patch bays, is improved organization and easier management of your wired network. For most newer patch panel designs, the main focus is on cable management. By using a front-access patch panel, for instance, you can get to all your cables and terminations easily. Front-access panels work especially well in tight spaces. For businesses, patch panels are often around found in areas that house telecommunications equipment and they play a central role in network functionality. By centralizing cables in one place, patch panels make it easy for network administrators to move, add or change complex network architectures. In a business environment, patch panels are the smart way to quickly transfer communications lines from office to another.

Copper or Fiber?

Patch panels can be part of networks with either fiber or copper cabling. While fiber is much faster than copper, networking professionals disagree on whether the materials show significant performance differences in patch panels. The primary role of the panels is to direct signal traffic rather than move signal at a required speed. There's no question, however, that fiber panels cost more. All patch panels are subject to the same standards that provide signal and speed performance ratings for other network components.

It's All About the Ports

Ports are a component of patch panels because they provide physical entry and exit points for data. Most patch panels have either 24 or 48 ports. However, panels can include 96 ports, and some specialty versions reach 336 or more. The number of ports on a panel is not subject to

physical limit other than the room to place them. However, panels include modules with eight ports because it's easier to perform replacements and maintenance on smaller groupings. When a malfunction occurs, smaller groups of ports mean fewer wires to connect to a new module.

Using Patch Panels

If you can wire an Ethernet jack, you can wire a patch panel. You'll simply need to repeat the sequence multiple times for your various ports. A patch panel with eight ports should suffice for most home networks, but it's easy to expand when you need more capacity. Panels with eight to 24 ports are readily available, and you can make use of multiple panels together to create a larger one. If you're putting together a home or business network, can you get the job done without patch panels? Certainly, since patch panels serve more as a convenience than necessity. But by incorporating a patch panel — or several — you can expect better cable management and easier fixes when a network component inevitably breaks down.

Patch Cord

Typically, a patch cord is a copper cable that has an RJ45, TERA or GG45 connector on both ends A patch cable, patch cord or patch lead is an electrical or optical cable used to connect ("patch in") one electronic or optical device to another for signal routing. Devices of different types (e.g., a switch connected to a computer, or a switch to a router) are connected with patch cords. A patch cord may also be used to connect a switch port or a server to the structured cabling system.

Network Rack: What it is and How it Compares to a 2 Post Rack

What is a Network Rack?

Known by many names, a **network rack** is a metal frame chassis that holds, stacks, organizes, secures and protects various computer network and server hardware devices. The term "network" refers to the rack actually housing this type of hardware.

How to Set-Up a Network Rack

Some network racks hold servers and other computer systems, although some are designed with specific device types in mind. The rack works by securing technology with brackets, bolts, and other rack hardware to keep this equipment in place. You can also mount this equipment using certain types of rails and shelves, such as switch rails and switch shelves.

Network Rack Equipment

These racks can house a lot of different types of equipment. Network equipment is really just an umbrella term that encapsulates various kinds of technology. Some of these devices include the following:

- **Switches –** Multi-port, high-speed devices that receive data and redirect them to the correct destination on a local area network (LAN). Information can only go across a single network using a switch.
- **Routers –** Similar to switches, routers receive and forward information, but they can carry data over multiple networks. This is why, for example, different devices or networks can access the Internet using one single router.
- **Modems –** This device actually connects the source of your internet to your router. This is typically done using an Ethernet cord.

Network Rack vs. 2 Post Relay Rack

A 2 post, open frame relay rack can serve as a lower-cost, easy-to-use entry into network rack mounting equipment. Thus, a 2 post rack can be a network rack if you use it for mounting this type of equipment. A 2 post rack works by having two thinner, centralized parallel posts extending from a larger, balanced base either 19 or 23 inches apart.

Installing Network Equipment in a 2 Post Rack

The 2 post rack is easy to set up and start with because of the light and easy to move frame compared to more robust racks. You secure network equipment into the rack by installing a brace on network hardware and bolting the brace to the posts.

Once installed, the two post rack allows for you to stack several different network devices on top of each other, taking advantage of vertical space to reduce how much floor space you use to store your gear. The racks are also very sturdy and can be secured into the floor, making it very difficult to knock over any installed equipment. Additionally, the open nature of the rack minimizes airflow obstruction and makes it easier to manage your cables.

If you're using 2 post relay racks to mount your network hardware, center-mount your devices on the rack for the safest, most secure hold. Center mounting refers to attaching the center of the hardware bracket to the parallel posts on both sides. Using the center mounting position on a 2 post server rack centralizes the weight distribution which reduces pressure on the rack itself and improves balance. Flush mounting only works well with lighter, low-profile technology.

IP address definition

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

What is an IP?

An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.

IP addresses are not random. They are mathematically produced and allocated by the Internet Assigned Numbers Authority (IANA), a division of the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a non-profit organization that was established in the United States in 1998 to help maintain the security of the internet and allow it to be usable by all. Each time anyone registers a domain on the internet, they go through a domain name registrar, who pays a small fee to ICANN to register the domain.

How do IP addresses work

If you want to understand why a particular device is not connecting in the way you would expect or you want to troubleshoot why your network may not be working, it helps understand how IP addresses work.

Internet Protocol works the same way as any other language, by communicating using set guidelines to pass information. All devices find, send, and exchange information with other connected devices using this protocol. By speaking the same language, any computer in any location can talk to one another.

The use of IP addresses typically happens behind the scenes. The process works like this:

1. Your device indirectly connects to the internet by connecting at first to a network connected to the internet, which then grants your device access to the internet.
2. When you are ~~at~~ home, that network will probably be your Internet Service Provider (ISP). At work, it will be your company network.
3. Your IP address is assigned to your device by your ISP.
4. Your internet activity goes through the ISP, and they route it back to you, using your IP address. Since they are giving you access to the internet, it is their role to assign an IP address to your device.
5. However, your IP address can change. For example, turning your modem or router on or off can change it. Or you can contact your ISP, and they can change it for you.

6. When you are out and about – for example, traveling – and you take your device with you, your home IP address does not come with you. This is because you will be using another network (Wi-Fi at a hotel, airport, or coffee shop, etc.) to access the internet and will be using a different (and temporary) IP address, assigned to you by the ISP of the hotel, airport or coffee shop.

As the process implies, there are different types of IP addresses, which we explore below.

Types of IP addresses

There are different categories of IP addresses, and within each category, different types.

Consumer IP addresses

Every individual or business with an internet service plan ~~will~~ have two types of IP addresses: their private IP addresses and their public IP address. The terms public and private relate to the network location — that is, a private IP address is used inside a network, while a public one is used outside a network.

Private IP addresses

Every device that connects to your internet network has a private IP address. This includes computers, smartphones, and tablets but also any Bluetooth-enabled devices like speakers, printers, or smart TVs. With the growing internet of things, the number of private IP addresses you have at home is probably growing. Your router needs a way to identify these items separately, and many items need a way to recognize each other. Therefore, your router generates private IP addresses that are unique identifiers for each device that differentiate them on the network.

Public IP addresses

A public IP address is the primary address associated with your whole network. While each connected device has its own IP address, they are also included within the main IP address for your network. As described above, your public IP address is provided to your router by your ISP. Typically, ISPs have a large pool of IP addresses that they distribute to their customers. Your public IP address is the address that all the devices outside your internet network will use to recognize your network.

Public IP addresses

Public IP addresses come in two forms – dynamic and static.

Dynamic IP addresses

Dynamic IP addresses change automatically and regularly. ISPs buy a large pool of IP addresses and assign them automatically to their customers. Periodically, they re-assign them and put the older IP addresses back into the pool to be used for other customers. The rationale for this approach is to generate cost savings for the ISP. Automating the regular movement of IP

addresses means they don't have to carry out specific actions to re-establish a customer's IP address if they move home, for example. There are security benefits, too, because a changing IP address makes it harder for criminals to hack into your network interface.

Static IP addresses

In contrast to dynamic IP addresses, static addresses remain consistent. Once the network assigns an IP address, it remains the same. Most individuals and businesses do not need a static IP address, but for businesses that plan to host their own server, it is crucial to have one. This is because a static IP address ensures that websites and email addresses tied to it will have a consistent IP address — vital if you want other devices to be able to find them consistently on the web.

This leads to the next point – which is the two types of website IP addresses.

There are two types of website IP addresses

For website owners who don't host their own server, and instead rely on a web hosting package – which is the case for most websites – there are two types of website IP addresses. These are shared and dedicated.

Shared IP addresses

Websites that rely on shared hosting plans from web hosting providers will typically be one of many websites hosted on the same server. This tends to be the case for individual websites or SME websites, where traffic volumes are manageable, and the sites themselves are limited in terms of the number of pages, etc. Websites hosted in this way will have shared IP addresses.

Dedicated IP addresses

Some web hosting plans have the option to purchase a dedicated IP address (or addresses). This can make obtaining an SSL certificate easier and allows you to run your own File Transfer Protocol (FTP) server. This makes it easier to share and transfer files with multiple people within an organization and allow anonymous FTP sharing options. A dedicated IP address also allows you to access your website using the IP address alone rather than the domain name — useful if you want to build and test it before registering your domain.

How to look up IP addresses

The simplest way to check your router's public IP address is to search "What is my IP address?" on Google. Google will show you the answer at the top of the page.

Other websites will show you the same information: they can see your public IP address because, by visiting the site, your router has made a request and therefore revealed the information. The site IPLocation goes further by showing the name of your ISP and your city.

Generally, you will only receive an approximation of location using this technique — where the provider is, but not the actual device location. If you are doing this, remember to log out of your

VPN too. Obtaining the actual physical location address for the public IP address usually requires a search warrant to be submitted to the ISP.

Finding your private IP address varies by platform:

In Windows:

- Use the command prompt.
- Search for “cmd” (without the quotes) using Windows search
- In the resulting pop-up box, type “ipconfig” (no quote marks) to find the information.

On a Mac:

- Go to System Preferences
- Select network – and the information should be visible.

On an iPhone:

- Go to Settings
- Select Wi-Fi and click the “i" in a circle () next to the network you are on – the IP address should be visible under the DHCP tab.

If you need to check the IP addresses of other devices on your network, go into the router. How you access the router depends on the brand and the software it uses. Generally, you should be able to type the router's gateway IP address into a web browser on the same network to access it. From there, you will need to navigate to something like "attached devices," which should display a list of all the devices currently or recently attached to the network — including their IP addresses.

IP address security threats

Cybercriminals can use various techniques to obtain your IP address. Two of the most common are social engineering and online stalking.

Attackers can use social engineering to deceive you into revealing your IP address. For example, they can find you through Skype or a similar instant messaging application, which uses IP addresses to communicate. If you chat with strangers using these apps, it is important to note that they can see your IP address. Attackers can use a Skype Resolver tool, where they can find your IP address from your username.

Online stalking

Criminals can track down your IP address by merely stalking your online activity. Any number of online activities can reveal your IP address, from playing video games to commenting on websites and forums.

Once they have your IP address, attackers can go to an IP address tracking website, such as whatismyipaddress.com, type it in, and then get an idea of your location. They can then cross-reference other open-source data if they want to validate whether the IP address is associated

with you specifically. They can then use LinkedIn, Facebook, or other social networks that show where you live, and then see if that matches the area given.

If a Facebook stalker uses a phishing attack against people with your name to install spying malware, the IP address associated with your system would likely confirm your identity to the stalker.

If cybercriminals know your IP address, they can launch attacks against you or even impersonate you. It is important to be aware of the risks and how to mitigate them. Risks include:

Downloading illegal content using your IP address

Hackers are known to use hacked IP addresses to download illegal content and anything else they do not want to be traced back to them. For example, using the identity of your IP address, criminals could download pirated movies, music, and video – which would breach your ISP's terms of use – and much more seriously, content related to terrorism or child pornography. This could mean that you – through no fault of your own – could attract the attention of law enforcement.

Tracking down your location

If they know your IP address, hackers can use geolocation technology to identify your region, city, and state. They only need to do a little more digging on social media to identify your home and potentially burgle it when they know you are away.

Directly attacking your network

Criminals can directly target your network and launch a variety of assaults. One of the most popular is a DDoS attack (distributed denial-of-service). This type of cyberattack occurs when hackers use previously infected machines to generate a high volume of requests to flood the targeted system or server. This creates too much traffic for the server to handle, resulting in a disruption of services. Essentially, it shuts down your internet. While this attack is typically launched against businesses and video game services, it can occur against an individual, though this is much less common. Online gamers are at particularly high risk for this, as their screen is visible while streaming (on which an IP address can be discovered).

Hacking into your device

The internet uses ports as well as your IP address to connect. There are thousands of ports for every IP address, and a hacker who knows your IP can try those ports to attempt to force a connection. For example, they could take over your phone and steal your information. If a criminal does obtain access to your device, they could install malware on it.

How to protect and hide your IP address

Hiding your IP address is a way to protect your personal information and online identity. The two primary ways to hide your IP address are:

1. Using a proxy server
2. Using a virtual private network (VPN)

A proxy server is an intermediary server through which your traffic is routed:

- The internet servers you visit see only the IP address of that proxy server and not your IP address.
- When those servers send information back to you, it goes to the proxy server, which then routes it to you.

A drawback of proxy servers is that some of the services can spy on you — so you need to trust it. Depending on which one you use, they can also insert ads into your browser.

VPN offers a better solution:

- When you connect your computer – or smartphone or tablet – to a VPN, the device acts as if it is on the same local network as the VPN.
- All your network traffic is sent over a secure connection to the VPN.
- Because your computer behaves as if it is on the network, you can securely access local network resources even when you are in another country.
- You can also use the internet as if you were present at the VPN's location, which has benefits if you are using public Wi-Fi or want to access geo-blocked websites.

Kaspersky Secure Connection is a VPN that protects you on public Wi-Fi, keeps your communications private, and ensures that you are not exposed to phishing, malware, viruses, and other cyber threats.

When should you use VPN

Using a VPN hides your IP address and redirects your traffic through a separate server, making it much safer for you online. Situations where you might use a VPN include:

When using public Wi-Fi

When using a public Wi-Fi network, even one that is password-protected, a VPN is advisable. If a hacker is on the same Wi-Fi network, it is easy for them to snoop on your data. The basic security that the average public Wi-Fi network employs does not provide robust protection from other users on the same network.

Using a VPN will add an extra layer of security to your data, ensuring you bypass the public Wi-Fi's ISP and encrypting all your communication.

When you are traveling

If you are traveling to a foreign country – for example, China, where sites like Facebook are blocked – a VPN can help you access services that may not be available in that country.

The VPN will often allow you to use streaming services that you paid for and have access to in your home country, but they are not available in another because of international rights issues. Using a VPN can enable you to use the service as if you were at home. Travelers may also be able to find cheaper airfare when using a VPN, as prices can vary from region to region.

When you are working remotely

This is especially relevant in the post-COVID world, where many people are working remotely. Often employers require the use of a VPN to access company services remotely for security reasons. A VPN that connects to your office's server can give you access to internal company networks and resources when you are not in the office. It can do the same for your home network while you are out and about.

When you just want some privacy

Even in the comfort of your own home, using the internet for everyday purposes, using a VPN can be a good idea. Whenever you access a website, the server you connect to logs your IP address and attaches it to all the other data the site can learn about you: your browsing habits, what you click on, how long you spend looking at a particular page. They can sell this data to advertising companies who use it to tailor ads straight to you. This is why ads on the internet sometimes feel oddly personal: it's because they are. Your IP address can also be used to track your location, even when your location services are turned off. Using a VPN prevents you from leaving footprints on the web.

Don't forget your mobile devices, either. They have IP addresses too, and you probably use them in a wider variety of locations than your home computer, including public Wi-Fi hotspots. It is advisable to use a VPN on your mobile when connecting to a network you may not fully trust.

Other ways to protect your privacy

Change privacy settings on instant messaging applications

Apps installed on your device are a major source of IP address hacking. Instant messaging and other calling apps can be used as a tool by cybercriminals. Using IM apps only allows direct connections from contacts and doesn't accept calls or messages from people you don't know. Changing your privacy settings makes it harder to find your IP address because people who don't know you cannot connect with you.

Create unique passwords

Your device password is the only barrier that can restrict people from accessing your device. Some people prefer to stick to their devices' default passwords, which makes them vulnerable to attack. Like all your accounts, your device needs to have a unique and strong password that is not easy to decode. A strong password contains a mix of upper- and lower-case letters, numerals, and characters. This will help to safeguard your device against IP address hacking.

Stay alert to phishing emails and malicious content

A high proportion of malware and device tracking software is installed via phishing emails. When you connect with any site, this provides the site with access to your IP address and device location, making it vulnerable to hacking. Be vigilant when opening emails from unknown senders and avoid clicking on links that could send you to unauthorized sites. Pay close attention to the emails' content, even if they appear to come from well-known sites and legitimate businesses.

Use a good antivirus solution and keep it up to date

Install comprehensive antivirus software and keep it up to date. For example, Kaspersky's Anti-Virus protection guards you from viruses on your PC and Android devices, secures and stores your passwords and private documents, and encrypts the data you send and receive online with VPN.

Protecting your IP address is a crucial aspect of protecting your online identity. Securing it through these steps is a way to stay safe against the wide variety of cybercriminals' attacks