

LESSON #1

HAZARD IDENTIFICATION, RISK ASSESSMENT AND RISK CONTROL

Occupational Safety and Health (OSH) - Is a planned system of working to prevent illness and injury where you work by recognizing and identifying hazards and risks.

Three Steps Used to Manage Health and Safety and Work

1. **Spot the Hazard (Hazard Identification)**

a. **Safety Hazard**

- a source of danger.
- Anything that could hurt you or someone else.
- Any source of potential damage, harm or adverse health effects on something or someone under certain conditions at work.

2. **Assess the Risk (Risk Assessment)**

a. **Risk Assessment**

- Assessing the risk means working out how likely it is that a hazard will harm someone and how serious the harm could be.
- Whenever you spot a hazard, assess the risk by asking yourself **two questions**.
 1. How likely is it that the hazard could harm me or someone else?
 2. How badly could I or someone else be harmed?

3. **Make the Changes (Risk Control)**

a. **Risk Control**

- It is your employer's responsibility to fix hazards.
- Sometimes you may be able to fix simple hazards yourself.
Ex. You can pick up things from the floor and put them away to eliminate a trip hazard.

WHAT TO DO?

1. Ask your supervisor for instructions and training before using equipment.
2. Ask for help moving or lifting heavy objects.
3. Tell your supervisor if you think a work practice could be implemented.

COMMON HAZARDS ENCOUNTERED IN OUR WORKPLACE

-  **Physical Hazard** – is an **agent, factor, or circumstance** that can **cause harm with or without contact**. They can be classified as a type of occupational hazard or environmental hazard

Ex.

One of the most common physical hazards involving tech support is cables running across the floor. If someone trips, falls, and hurts himself because of a cable you ran across the floor.

→ Risk Control – Use cable ties or cord covers to keep cables organized and out of the way

-  **Mechanical Hazard** – refers to **potential physical risks** associated with working in environments **where moving machinery, tools, or heavy equipment are present**

Ex.

If you're working in a data center or an industrial environment, you might be around servers, cooling systems, or other machinery with moving parts. Accidental contact with these can cause injuries.

→ Risk Control – For particularly heavy loads, use trolleys, hoists or other lifting equipment to avoid strain injuries.

-  **Chemical Hazards** – A type of **occupational hazard caused by exposure to chemicals in the workplace**. Exposure to chemicals in the workplace can cause acute or long-term detrimental health effects

Ex.

Chemicals used to clean equipment, cables, or work areas might contain harsh substances that can cause skin irritation or respiratory issues.

→ Risk Control – Personal Protective Equipment (PPE), Disposal of Hazardous Materials

-  **Electric Shock Hazard** – These hazards are **typically present in environments where electrical systems**, equipment, and installations **are used or maintained**

Ex.

Electric Shock – It occurs when a person comes into contact with a live electrical component, such as exposed wires, faulty equipment, or energized parts.

→ Risk Control – Personal Protective Equipment (PPE), De-Energize Equipment, Check for Power, Static Control

LESSON #2

NETWORK DESIGN – TOPOLOGY / DIAGRAM / SIMULATION

Networking Topology – is the [arrangement of different elements](#) (including links, nodes, and devices) in [a computer network](#), defining how each component interacts and communicates with one another.

Networking Diagram – a [schematic or map of your existing network](#) that illustrates the nodes and their connections.

NETWORK TOPOLOGY VS. NETWORK DIAGRAM

TOPOLOGY	DIAGRAM
<ul style="list-style-type: none">refers to the actual layout and structure of the network, both physical and logical	<ul style="list-style-type: none">is a visual representation of a network, showing its components (devices, connections, and paths) and how they interact.
Focus: Logical or physical arrangement of devices and connections	Focus: Visual representation of a network's components and interactions
Purpose: Describes the structure of a network	Purpose: Depicts the network's layout and connectivity
Level of Detail: Can be abstract or specific	Level of Detail: Typically more detailed and includes device names, IP addresses, and other information
Examples: Star, bus, ring, mesh	Examples: Physical layout of a network, logical representation of data flow

Physical Network Diagrams – Layer 1 is the **physical layer** of the OSI model. For network design purposes, this means **the things you can touch: the cables and the equipment**. But it technically also includes the electrical and optical signaling properties. Layer 1 defines the properties of the cables that are necessary to carry the signals. Layer 1 also worries about wireless signaling used.

Logical Network – Layer 2 is the **logical layer** of the OSI model. Logical network diagrams **represent network topologies at higher levels**. For Example, Layer 3 network diagrams depict routing paths, including static routes, and may indicate BGP peers.

***Border Gateway Protocol (BGP)** is the **protocol that makes the internet work**. It is the routing protocol used to route traffic across the internet*

IMPORTANCE OF A NETWORK DIAGRAM

- Network diagrams are essential **tools for understanding, planning, and managing network infrastructure**. They provide a visual representation of a network's components, connections, and data flow, making it easier to:

1. Understand Network Structure

- **Identify components:**
 - Network diagrams clearly **show the various devices** (routers, switches, computers, servers) **and connections** (cables, wireless links) **in a network**.
- **Visualize data flow:**
 - By understanding the layout and connectivity, you can **visualize how data travels through the network**.

2. Plan Network Changes

- **Identify potential bottlenecks:**
 - Network diagrams help **identify areas where traffic congestion may occur** or performance may be hindered.
- **Plan expansions:**
 - When adding new devices or expanding the network, diagrams **provide a clear roadmap for changes**.

- **Assess impact:**
 - Before making changes, network diagrams can help assess their potential impact on network performance and connectivity.

3. Troubleshoot Network Issues

- **Isolate problems:**
 - By analyzing the network diagram, you can quickly identify potential areas of concern and isolate the source of network problems.
- **Trace data flow:**
 - Network diagrams help trace the path of data through the network, making it easier to pinpoint issues.

4. Communicate Network Information

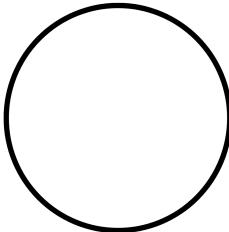
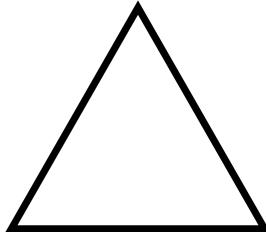
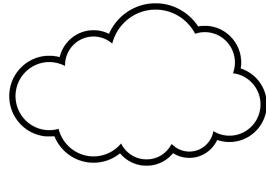
- **Share knowledge:**
 - Network diagrams are effective tools for communicating network information to colleagues, technicians, or management.
- **Document network configuration:**
 - Diagrams can serve as documentation of a network's configuration, making it easier for future reference.

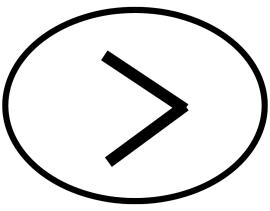
5. Ensure Compliance

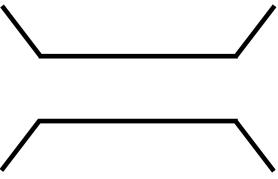
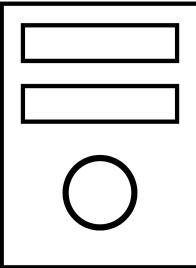
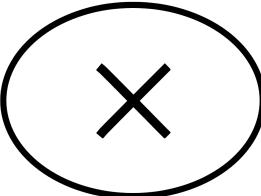
- **Meet regulations:**
 - Network diagrams can help ensure compliance with industry standards and regulations, especially in regulated environments.

UNDERSTANDING NETWORK DIAGRAM SYMBOLS

- There are some useful shorthand symbols you can use when creating network diagrams. While there aren't any universal rules, here's a list of general best practices to help you accurately communicate networking ideas with colleagues, particularly useful for drawing network topologies on a whiteboard:

SYMBOL NAME	HANDWRITTEN SHAPES	CISCO PACKET TRACER	MEANING
Layer Network 3 Devices		N/A	N/A
Layer 2 Devices		N/A	N/A
Multiplexer Devices			Triangles represent multiplexer devices, which used to be more common in network diagrams. So instead, try using triangles for IP phones .
Cloud		 Cloud-PT	Clouds are used to summarize parts of the network that aren't important for the diagram. This could mean the Internet or a WAN or even a collection of internal network segments like user VLANs.

Firewall			In software-generated or very detailed diagrams, a firewall is typically represented with a brick wall, to denote that it is a stop or checkpoint in your network data flow.
Terminal			Can be represented by a variety of end-user systems, but is typically represented by a computer.
Switch			<p>As a Layer 2 object, switches are represented by crossed arrows, denoting the flow of data and the “switching” taking place between devices.</p> <p><i>Note: while a router and a Layer 3 switch can perform similar functions, it's important to distinguish a device doing the Layer 3 routing, so it would not be represented by a switch symbol.</i></p>

Bridge		 Bridge-PT Bridge0	A representation similar to a physical road bridge is often used to represent a networking bridge.
Server		 Server-PT Server0	Traditionally represented by a computer tower, a server is noted on a diagram as a node with data flowing towards other sources on the network.
Router		 Router-PT Router0	Routers can be represented by a variety of objects, but are usually rendered as boxes into which data enters and is distributed out through multiple destinations. A layer 3 switch can also use a similar symbol if it is providing a similar function as a router.
COPPER Straight Through Cable			The most common type. Is used to connect computers to hubs or switches.

COPPER Crossover Cable			The most common type. Is used to connect computers to hubs or switches.
WIRELESS LAN			A wireless computer network that links devices within a limited area using wireless communication.

LESSON #3

ROUTERS

Router – A router receives and sends data on computer networks. Routers are sometimes confused with network hubs, modems, or network switches. However, routers can combine the functions of these components, and connect with these devices, to improve Internet access or help create business networks.

How does a router work?

- Routers guide and direct network data using **packets**
- Data packets contain **various types of data**, including files, communications, and web interactions
- **Each packet has several layers**, one of which carries identifying information
- This layer includes **sender, data type, size**, and the **destination IP**

How do routers help your business?

1. Routers are essential for **connecting employees to local networks and the Internet**.

2. They enable collaboration, communication, and access to information.
3. Routers provide security features such as firewalls and content filtering to protect against unwanted content and malicious websites.
4. Routers can also function as file-sharing servers by connecting hard drives or as print servers for network-accessible printers.

TYPES OF ROUTERS

1. Core Router

- Are generally used by service providers (i.e. AT&T, Verizon, Vodafone) or cloud providers (i.e. Google, Amazon, Microsoft).
- They provide maximum bandwidth to connect additional routers or switches.
- Most small businesses will not need core routers.
- Very large enterprises that have many employees working in various buildings or locations may use core routers as part of their network architecture.



2. Edge Router

- Also called a gateway router or just “gateway” for short
- A network's outermost point of connection with external networks, including the Internet.
- Optimized for bandwidth and designed to connect to other routers to distribute data to end users.
- Don't usually offer Wi-Fi or the ability to manage local networks fully.

- Typically have only one Ethernet port—an input to connect to the Internet and several outputs to connect additional routers.
- Edge router and modem are somewhat interchangeable terms, though the latter term is no longer commonly used by manufacturers or IT professionals when referencing edge routers.



-

3. Distribution Router

- A distribution router, or **interior router**, receives data from the edge router (or gateway) via a wired connection and sends it on to end users, typically via **Wi-Fi**, though the router usually also includes physical (Ethernet) connections for connecting users or additional routers.



-

4. Wireless Router

- Wireless routers, or **residential gateways**, combine the functions of edge routers and distribution routers.
- These are commonplace **routers for home networks and Internet access**.
- Most service providers provide full-featured wireless routers as standard equipment.

- But even if you have the option to use an ISP's wireless router in your small business, you may want to **use a business-level router to take advantage of better wireless performance**, more connectivity controls, and security.



-

5. Virtual Router

- Virtual routers are **pieces of software that allow some router functions to be virtualized in the cloud** and delivered as a service.
- These routers are **ideal for large businesses** with complex network needs. They offer flexibility, easy scalability, and a lower entry cost.
- Another benefit of virtual routers is reduced management of local network hardware.

How to choose small business routers?

1. **Connectivity** - Ensure the **router has necessary ports** for devices and expansion.
2. **Bandwidth** - **Adequate bandwidth is essential for optimal performance**, especially with multiple users. Consider additional routers or hubs if needed to prevent bottlenecks.
3. **Wireless Capability** - Opt for **Wi-Fi 6** higher speeds and compatibility with older standards.
4. **Simplified Setup and Management** - Look for **routers with intuitive mobile apps** for easy setup administration.
5. **Security** - Prioritize routers with **WPA/WPA2 encryption**, firewall software, MAC address filtering, and automatic updates for protection against malware viruses.

LESSON #4

PEER-TO-PEER

KEY REMINDERS:

- **Enable Network Discovery** - Ensure that network discovery is turned on so that devices can see and communicate with each other on the network
- **Set the Network Type** - Make sure your network is set to either Private (recommended for P2P networks) or Domain (if applicable), as this allows easier sharing and discovery between devices
- **File and Printer Sharing** - Enable file and printer sharing to allow peers to access shared files and printers. This can be done in the same advanced sharing settings menu.
- **Create Shared Folders** - Designate specific folders to share with other peers. Right-click on the folder, select Properties, go to the Sharing tab, and click on Share.
- **Adjust Firewall Settings** - Ensure that the Windows Firewall or any other firewall software allows P2P traffic. You may need to add exceptions for specific applications used in your P2P network
- **Use the Same Workgroup** - All computers should be part of the same workgroup
- **IP Address Configuration** - Use static IP addresses for easier connectivity
- **User Permissions** - Set appropriate user permissions for shared files and folders to control who can access or modify them

COMMAND PROMPT (CMD) COMMANDS FOR MANAGING AND TROUBLESHOOTING A PEER-TO-PEER (P2P) NETWORK IN WINDOWS

1. **ipconfig** - Displays the current IP configuration for all network interfaces. Useful for checking IP addresses, subnet masks, and default gateways.
2. **ping** - Tests connectivity between two network devices by sending packets. You can use it to check if a peer is reachable.
3. **net share** - Displays a list of shared resources on the local computer. This command is helpful to check what is being shared in a P2P environment.
4. **netstat** - Displays active connections and listening ports, which can help you identify which applications are using the network.

5. **net config workstation** - Displays the configuration of the workstation service, including the current workgroup
6. **net localgroup** - Displays local group memberships, which can help in managing user permissions for shared resources.
7. **netsh** - A powerful command-line scripting utility for configuring and monitoring network settings. For example, you can view or set IP addresses "netsh interface ip show config"

LESSON #5

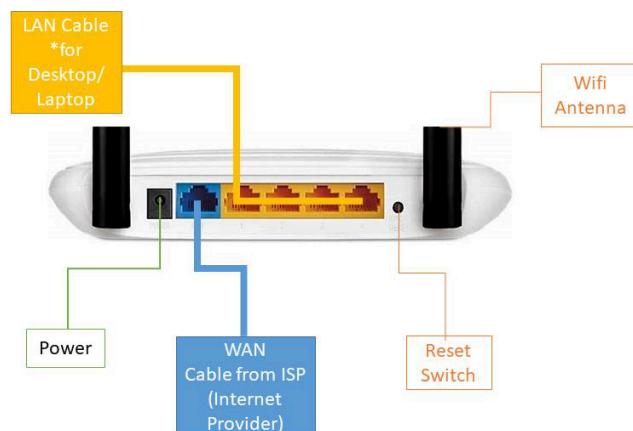
ROUTER CONFIGURATION

SOME BRANDS OF ROUTER



1. TPLINK

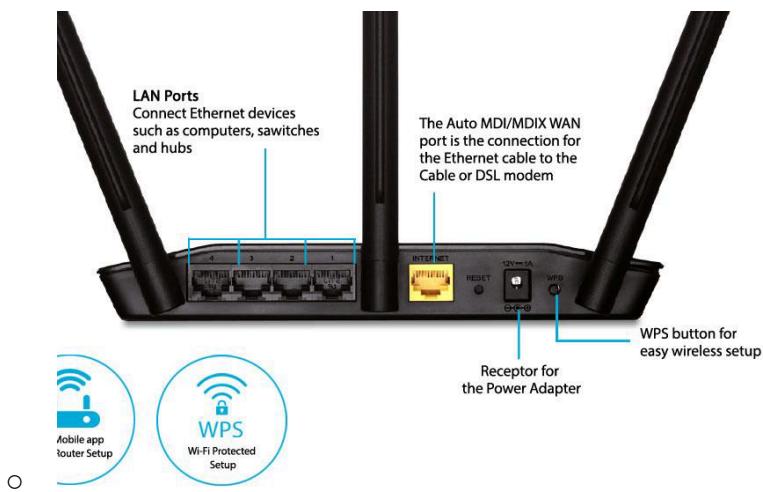
- Sometimes you may fail to access <http://tplinkwifi.net> or <http://tplinkdeco.net> to manage your TP-Link Router and would like to access the Router's IP address directly as a workaround.
- Normally your TP-Link Router's default IP address is <http://192.168.0.1> or <http://192.168.1.1>; TP-Link Deco's default IP address is <http://192.168.68.1>.
- **USERNAME:admin // PASSWORD:admin**



- *Any devices with a RJ45 Ethernet port can be connected not just Desktop or Laptop

2. D-LINK

- Q: How do I log in to my router?
A: Secure by Default: All D-Link routers purchased after 2017 are secure by default. The password can be located on the bottom of the unit by the serial number.
- *Note: The web UI is not a website on the Internet, it is built into the router. Make sure your computer or device is connected to the router*



3. LINKSYS BY CISCO

- The default password is admin, and the default username is blank (don't type anything).
- The default IP address is 192.168.1.1/0.1
- You can reset the router to restore these default login details.



TOOLS AND EQUIPMENT USED IN NETWORK INSTALLATIONS

TOOL	IMAGE	HOW IT IS USED
Crimping Tool		a device used to conjoin two pieces of metal by deforming one or both of them to hold each other
Pass Through Crimping Tool		Easily identify wiring order, the pass-through function allows the wires to pass all the way through the plug to let you verify they are in the correct order before crimping the plug
Non-Pass Through Crimping Tool		work with most standard crimp tools

Cable strippers and cutters		<p>One of the most basic and essential tools for hardware installation in structured cabling systems is a cable stripper and cutter. This tool allows you to strip off the insulation and sheath of the cable, exposing the conductors and connectors. You can also use it to cut the cable to the desired length and trim off any excess wires. Cable strippers and cutters come in different sizes and types, depending on the kind of cable you are working with, such as coaxial, twisted pair, or fiber optic.</p>
Screwdriver set		<p>Use in networking installations, such as setting up network racks, patch panels, or handling sensitive electronic equipment</p>
Network Cable Tester		<p>A network cable tester is a device that can identify whether the wires are paired correctly and whether there is a break in the insulation which allows cross-talk between two wires</p>

Network Cable
Toner and Probe
Kits



are used for finding electrical cables such as internet cables, phone lines, speaker wires, and ethernet wires in a house or building. They allow you to find cables by tracing electrical signals back to their sources.

TYPES OF PATCH PANEL

- **Copper/RJ45 Patch Panel**



- **Fiber Optic Patch Panel**



- **Coaxial Patch Panel**



- **Mix Patch Panel**



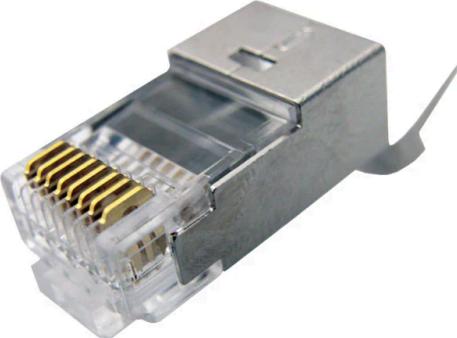
○

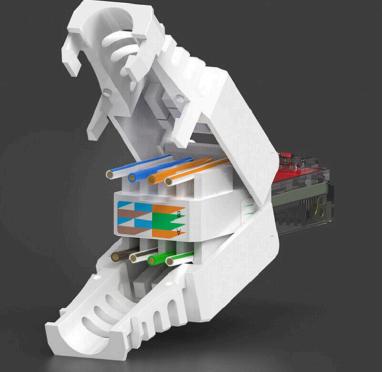
RJ45

- RJ45 stands for Registered Jack-45.
- The specifications for registered connectors refer to the wiring patterns of the jacks and not to their physical properties.
- The number 45 refers to the number in the register. If you want to be precise, you have to call it an “8P8C RJ45 Ethernet connector”.
 - 8P8C means eight positions / eight contacts.
 - It refers to a type of modular connector.
 - This is normally used at the end of Ethernet patch cables.
 - When attached to the end of an Ethernet cable, it is referred to as an RJ45 8P8C connector.

TYPES OF RJ45

TYPE	IMAGE	DEFINITION
Regular RJ45 Connectors/Standard RJ45 Connectors/Single-Piece RJ45 Connectors		Standard RJ45 connectors can also be named as non-pass-through RJ45 connectors, which are usually referred to as 8P8C modular plugs. Usually require a professional tool - RJ45 crimping tool

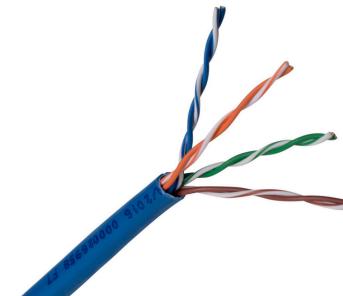
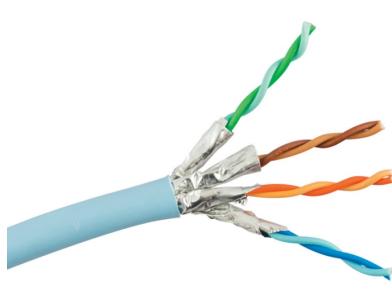
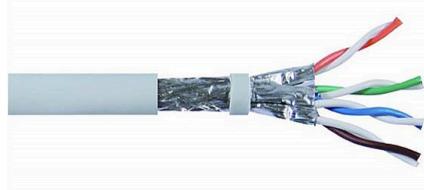
Pass-through RJ45 Connectors		<p>Pass-through RJ45 connectors allow the network cable wires to pass out of the connector body. Compared to standard RJ45 connectors, pass-through RJ45 connectors are easy to keep Ethernet cable wires aligned before terminating connectors. In addition, pass-through RJ45 connectors are easier to operate, ideal for novices or DIYers. Pass-through RJ45 connectors usually require a specific crimping tool.</p>
Shielded RJ45 Connectors		<p>Shielded RJ45 connectors usually feature a metal shield to avoid too much electromagnetic interference (EMI). The metal shielding structure is usually plated with nickel or gold. But nickel-plated shielding structure is more common on the market. Remember not to use a shielded RJ45 connector on an unshielded network cable as it may affect the connection. Shielded RJ45 connectors are often paired with shielded Ethernet cable for maximum performance.</p>

Unshielded RJ45 Connectors		<p>Unshielded RJ45 connectors have a plastic housing. If you use an unshielded cable, choose an unshielded connector and if the cable is shielded, use the shielded RJ45 connector.</p>
Toolless RJ45 Connectors		<p>A toolless RJ45 connector or field termination plug can be easily terminated without a crimping tool. Toolless connectors can be used in emergent situations and field termination. For example, they are designed for quick connection in the field and frequently moved cabling. What's more, toolless RJ45 connectors can also be reused a few times without affecting the data transmission.</p>
Two-piece RJ45 Connectors		<p>Compared to single-piece RJ45 connectors, two-piece RJ45 connectors have an additional load bar, designed to help align eight wires for easy and quick wiring. In addition, the load bar can also improve RJ45 connectors' resistance to interference.</p>

Ethernet Cable/Cat Cables

- An Ethernet cable, or "Cat" cables, short for "category", are used to connect computer network devices such as modems, routers, computers, servers and switches.
- They are also called network , LAN cables.

TYPES OF SHIELDING

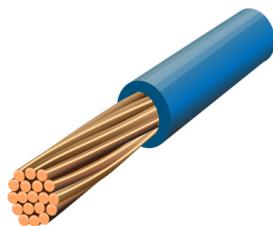
TYPE	IMAGE	DEFINITION
U/UTP		Unshielded cable, unshielded twisted pairs
F/UTP		Foil shielded cable, unshielded twisted pairs
U/UFTP		Unshielded cable, foil shielded twisted pairs
S/FTP		braided shielded cable, foil shielded twisted pairs

TP = twisted pair, U = unshielded, F = foil shielded, S = braided shielding.

TYPE OF WIRE

1. Stranded Cable

- This type of wire is more flexible and it is more applicable for Ethernet cables where the cable may be moved - often it is ideal for patch leads at desks or general connections to PCs, etc where some movement may be needed and expected.



-

2. Solid Cable

- Solid cable is not as flexible as the stranded type, but it is also more durable.
- This makes it best for use in permanent installations like cable installations under floors, embedded in walls and the like.

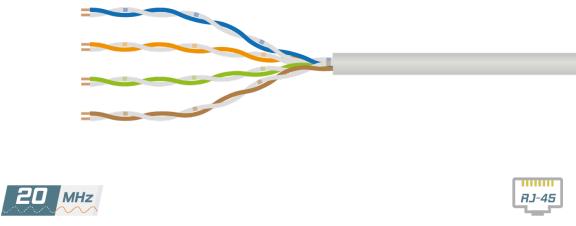
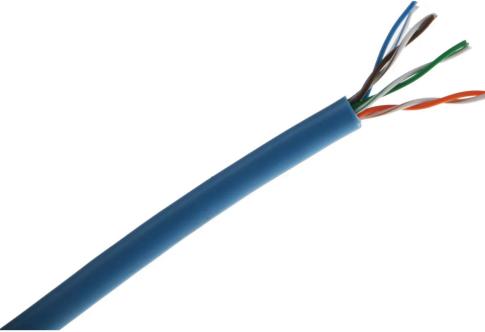


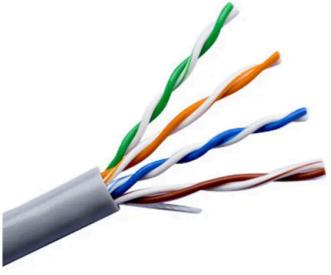
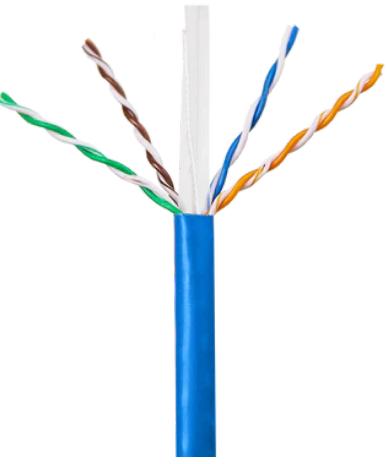
-

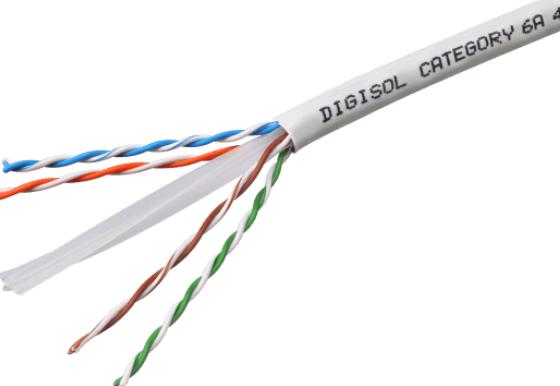
CATEGORIES FOR ETHERNET CABLES

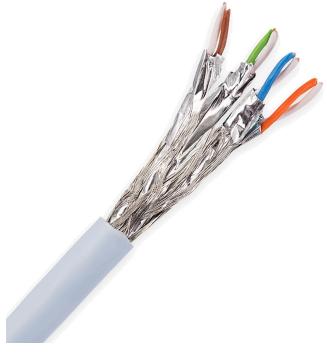
often recognised by the **TIA** (Telecommunications Industries Association). This association develops industry standards, drafts policy initiatives, and conducts market intelligence

CATEGORY	IMAGE	DEFINITION
Cat-1	<p>Category 1 Ethernet LAN Cables 1983 - 128~1000 Kbps</p>  <p>100-400 KHz</p> <p>All Rights Reserved, Samsun Teknoloji telecom.samsun.com / telecom@samsun.com</p>	<ul style="list-style-type: none"> - This is not recognised by the TIA/EIA. - It is the form of wiring that is used for standard telephone (POTS) wiring, or for ISDN.
Cat-2	<p>Category 2 Ethernet LAN Cables 1987 - 1~4 Mbps</p>  <p>1-4 MHz</p> <p>RJ-11</p> <p>All Rights Reserved, Samsun Teknoloji telecom.samsun.com / telecom@samsun.com</p>	<ul style="list-style-type: none"> - This is not recognised by the TIA/EIA. - It was the form of wiring that was used for 4Mbit/s token ring networks.
Cat-3	<p>Category 3 Ethernet LAN Cables 1991 - 10 Mbps</p>  <p>16 MHz</p> <p>RJ-12</p> <p>All Rights Reserved, Samsun Teknoloji telecom.samsun.com / telecom@samsun.com</p>	<ul style="list-style-type: none"> - This cable is defined in TIA/EIA-568-B. - It is used for data networks employing frequencies up to 16 MHz. - It was popular for use with 10 Mbps Ethernet networks (100Base-T), but has now been superseded by Cat-5 cable.

Cat-4	<p>Category 4 Ethernet LAN Cables 1993 - 16 Mbps</p> 	<ul style="list-style-type: none"> - This cable is not recognised by the TIA/EIA. - However it can be used for networks carrying frequencies up to 20 MHz. - It was often used on 16Mbps token ring networks.
Cat-5		<ul style="list-style-type: none"> - This is not recognised by the TIA/EIA. - This is the network cable that is widely used for 100Base-T and 1000Base-T networks as it provides performance to allow data at 100 Mbps and slightly more (125 MHz for 1000Base-T) Ethernet. - The Cat 5 cable superseded the Cat 3 version and for a number of years it became the standard for Ethernet cabling. - Cat 5 cable uses twisted pairs to prevent internal crosstalk, XT and also crosstalk to external wires, AXT. - Although not standardized, the Cat 5 cable normally uses 1.5 - 2 twists per centimeter. - It has been superseded by Cat-5 cable.

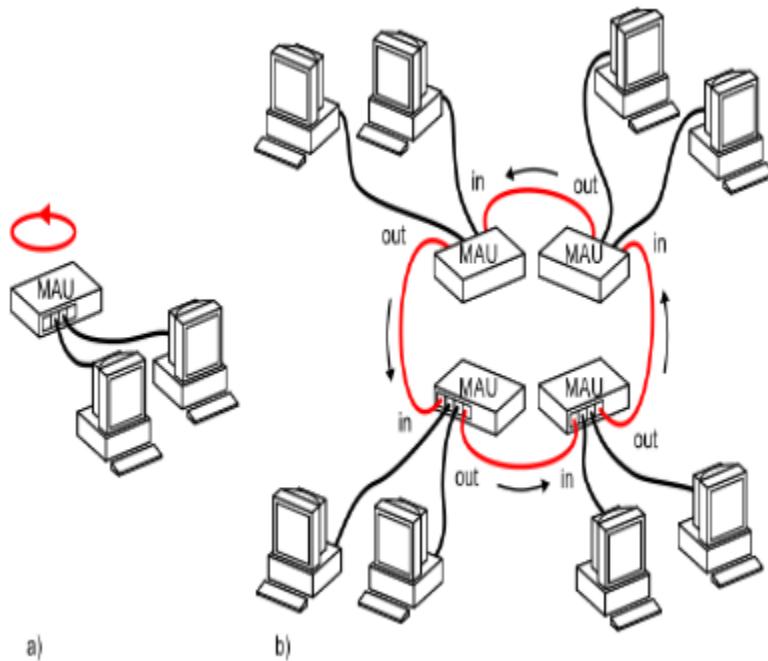
Cat-5e		<ul style="list-style-type: none"> - This form of cable is recognised by the TIA/EIA and is defined in TIA/EIA-568, being last revised in 2001. - It has a slightly higher frequency specification than Cat-5 cable as the performance extends up to 125 Mbps. - Cat-5e can be used for 100Base-T and 1000Base-t (Gigabit Ethernet). - Cat 5e standard for Cat 5 enhanced and it is a form of Cat 5 cable manufactured to higher specifications although physically the same as Cat 5. - It is tested to a higher specification to ensure it can perform at the higher data speeds. - The twisted pairs within the network cables tend to have the same level of twisting as the Cat 5 cables.
Cat-6		<ul style="list-style-type: none"> - This cable is defined in TIA/EIA-568-B provides a significant improvement in performance over Cat5 and Cat 5e. - During manufacture Cat 6 cables are more tightly wound than either Cat 5 or Cat 5e and they often have an outer foil or braided shielding.

		<ul style="list-style-type: none"> - The shielding protects the twisted pairs of wires inside the Ethernet cable, helping to prevent crosstalk and noise interference. - Cat-6 cables can technically support speeds up to 10 Gbps, but can only do so for up to 55 metres - even so this makes them relatively long Ethernet cables. - The Cat 6 Ethernet cables generally have 2+ twists per cm and some may include a nylon spline to reduce crosstalk, although this is not actually required by the standard.
Cat-6a		<ul style="list-style-type: none"> - The “a” in Cat 6a stands for “Augmented” and the standard was revised in 2008. - The Cat 6a cables are able to support twice the maximum bandwidth, and are capable of maintaining higher transmission speeds over longer network cable lengths. - Cat 6a cables utilize shielded which is sufficient to all but eliminate crosstalk. - However this makes them less flexible than Cat 6 cable.

Cat-7		<ul style="list-style-type: none"> - This is an informal number for ISO/IEC 11801 Class F cabling. - It comprises four individually shielded pairs inside an overall shield. - It is aimed at applications where transmission of frequencies up to 600 Mbps is required.
Cat-8		<ul style="list-style-type: none"> - Cat 8 cables have now been released and provide a huge step up in data rate / bandwidth. - Accordingly these Cat 8 cables are generally more expensive than older versions like Cat 6, or even Cat 7.
GG45-GigaGate45		<ul style="list-style-type: none"> - it was developed by NEXANS.GG45 connector used in cat 7 cable. - It is a connector for high-speed category 7 Cable. - Used for backbone connections between servers within a data center. provides an alternative to using fiber optic cabling. - Design to support a much higher frequency signal than cat5e and Cat6. But not widely adopted.

TOKEN RING

- a physical and data link layer computer networking technology used to build local area networks.
- It was introduced by IBM in 1984, and standardized in 1989 as IEEE 802.5.
- It uses a special three-byte frame called a token that is passed around a logical ring of workstations or servers.
- This token passing is a channel access method providing fair access for all stations, and eliminating the collisions of contention-based access methods.

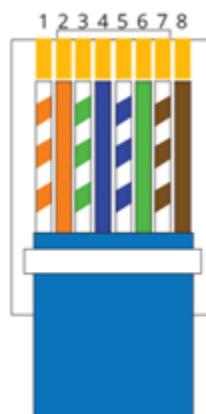
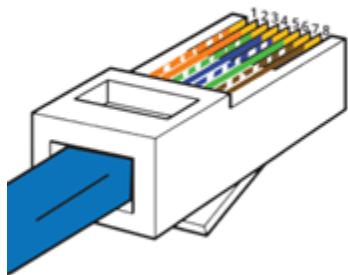


NICE TO KNOW

PATTERNS

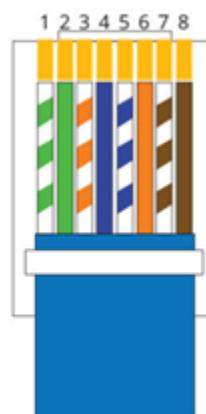
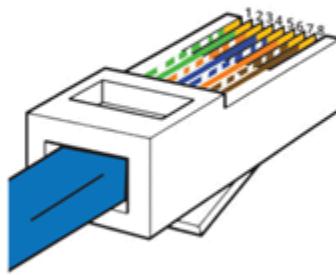
CROSSOVER

SIDE ONE



- | | |
|-----------------|----------------|
| 1. White Orange | 5. White Blue |
| 2. Orange | 6. Green |
| 3. White Green | 7. White Brown |
| 4. Blue | 8. Brown |

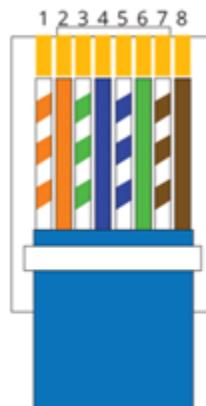
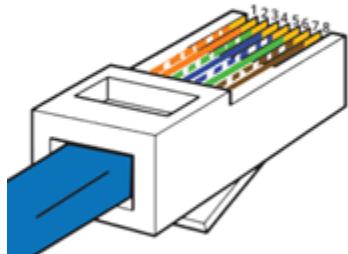
SIDE TWO



- | | |
|-----------------|----------------|
| 1. White Green | 5. White Blue |
| 2. Green | 6. Orange |
| 3. White Orange | 7. White Brown |
| 4. Blue | 8. Brown |

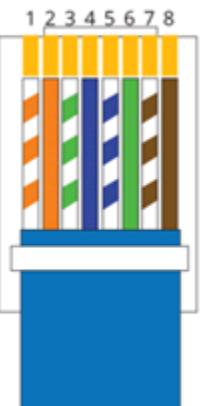
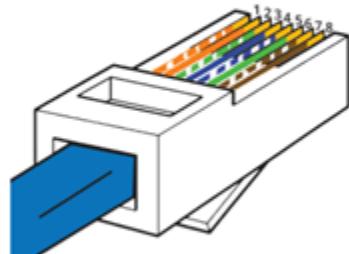
STRAIGHT-THROUGH

SIDE ONE



- | | |
|-----------------|----------------|
| 1. White Orange | 5. White Blue |
| 2. Orange | 6. Green |
| 3. White Green | 7. White Brown |
| 4. Blue | 8. Brown |

SIDE TWO



- | | |
|-----------------|----------------|
| 1. White Orange | 5. White Blue |
| 2. Orange | 6. Green |
| 3. White Green | 7. White Brown |
| 4. Blue | 8. Brown |