## F Book Title: CompTIA N10-008 Network+ Course

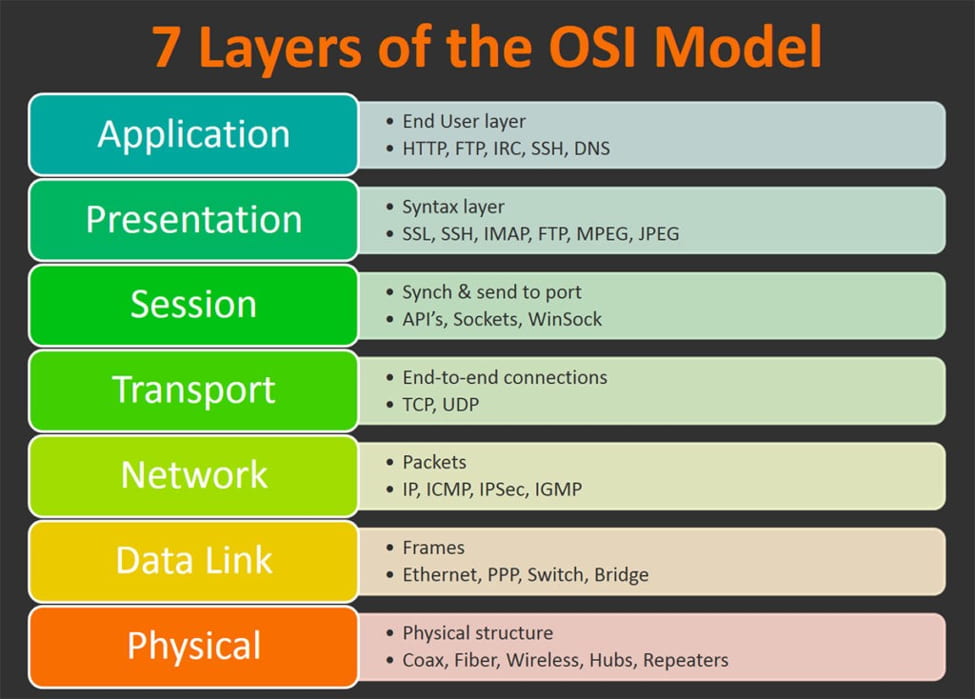
Author: Bakhshial

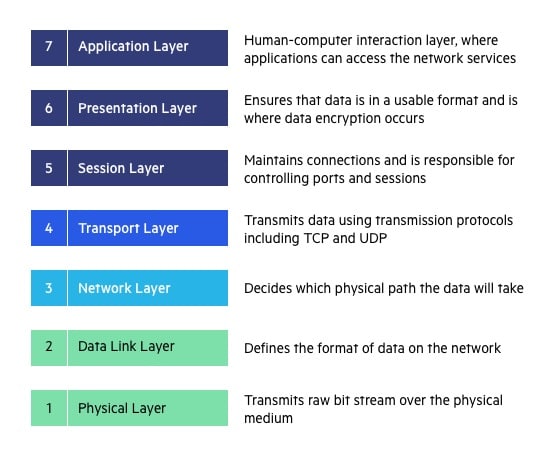
## This note content is taken from Professor Messer’s CompTIA N10-008 Network+ Course Free videos

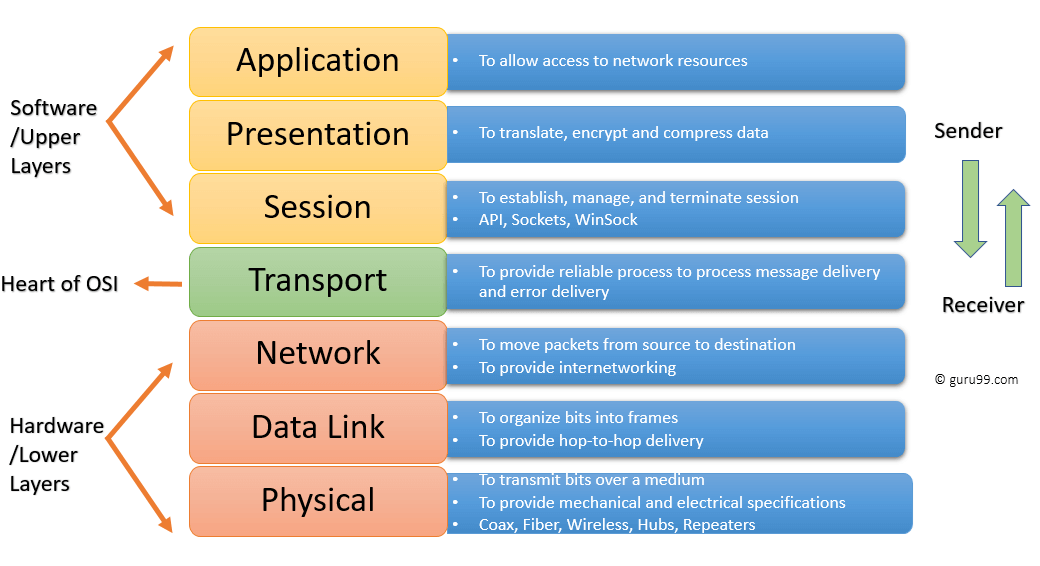
## Section 1: Networking Concepts

# 1.1 OSI Model:

## What is OSI Model?

* The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network.
* It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s
* The modern Internet is not based on OSI, but on the simpler TCP/IP model.
* it helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems.
* The Open Systems Interconnect (OSI) model is a conceptual framework that describes networking or telecommunications systems as seven layers, each with its own function. 





# Seven Layer:

## Application layer:

## The application layer is used by end-user software such as web browsers and email clients.

## It provides protocols that allow software to send and receive information and present meaningful data to users.

## It should be made clear that client software applications are not part of the application layer; rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user.

## A few examples of application layer protocols are the [Hypertext Transfer Protocol](https://www.imperva.com/learn/performance/http2/) (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

## Presentation Layer:

## The presentation layer prepares data for the application layer.

## It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end.

## The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

* layer 6 makes the data presentable for applications to consume. The presentation layer is responsible for translation, [encryption](https://www.cloudflare.com/learning/ssl/what-is-encryption/), and compression of data.
* Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand.
* If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender’s end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.
* Finally the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

## Session Layer:

## The session layer creates communication channels, called sessions, between devices.

## It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends.

## The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

* This is the layer responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.
* The session layer also synchronizes data transfer with checkpoints. For example, if a 100 megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.

## Transport layer:

## The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end.

## It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer.

## The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

* Layer 4 is responsible for end-to-end communication between the two devices. This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.
* The transport layer is also responsible for flow control and error control. Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection does not overwhelm a receiver with a slow connection. The transport layer performs error control on the receiving end by ensuring that the data received is complete, and requesting a retransmission if it isn’t.

## Network layer:

## The network layer has two main functions.

## One is breaking up segments into network packets, and reassembling the packets on the receiving end.

## The other is routing packets by discovering the best path across a physical network.

## The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

* The [network layer](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/) is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer breaks up segments from the transport layer into smaller units, called [packets](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/), on the sender’s device, and reassembling these packets on the receiving device. The network layer also finds the best physical path for the data to reach its destination; this is known as [routing](https://www.cloudflare.com/learning/network-layer/what-is-routing/).
* Network layer protocols include IP, the [Internet Control Message Protocol (ICMP)](https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/), the [Internet Group Message Protocol (IGMP)](https://www.cloudflare.com/learning/network-layer/what-is-igmp/), and the [IPsec](https://www.cloudflare.com/learning/network-layer/what-is-ipsec/) suite.

## Data Link layer:

## The data link layer establishes and terminates a connection between two physically-connected nodes on a network.

## It breaks up packets into frames and sends them from source to destination.

## The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the same network. The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. Like the network layer, the data link layer is also responsible for flow control and error control in intra-network communication (The transport layer only does flow control and error control for inter-network communications).

## This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

## Physical layer:

## The physical layer is responsible for the physical cable or wireless connection between network nodes.

## It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

## Refernce:

## <https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/>

## <https://www.imperva.com/learn/application-security/osi-model/>

# Data Communication

## PDU, or a protocol data unit:

## Getting data moved from one part of the network to the other relies on something called a PDU, or a protocol data unit. Also called transmission units, because we’re taking a little bit of data and transferring it across the network as a single unit.

## For example, if we’re running Ethernet, we know that Ethernet is going to send everything within an Ethernet frame from one device or MAC address on the network to another MAC address that’s on the network.

## A similar thing happens at the next layer up with layer 3, or the IP layer, where everything within the IP layer is being sent across the network from one IP address to the other. Inside of that IP packet is UDP data, TCP data, or some other type of data, but IP doesn’t care what’s on the inside. It simply knows that it’s moving data across the network from one IP address to another.

## TCP header or UDP header, there’s probably going to be a TCP segment, or what we call a UDP datagram within that particular part of the packet.

## Encapsulation and DE capsulation: Data Encapsulation and Decapsulation | NetworkByte

## What is Data Encapsulation and de-encapsulation in networking?

## TCP flag:

## For example, on layer 4, we have TCP data. And within the TCP header, such as we have here, there’s information called a TCP flag. This helps us understand how we can process this data as it’s going through the network. This control information is setting bits that are within the header of this packet, and each one of those bits has a particular definition. This means that the device that’s receiving this data can interpret those bits and understand how to process the data properly.

## We call these bits control flags, and we can identify whether a flag has been turned on or turned off, and then decide how these particular flags can affect the data flow.

## For example, we can look at the flags in this particular protocol decode and we can see that one flag has been set to 1. That means the data that’s contained within this TCP part of the packet is acknowledgment data that has been set.

## tcp-analysis-section-4-1

## **Types of Flags:**

## ****Synchronization (SYN):**** It is used in first step of [connection establishment](https://www.geeksforgeeks.org/computer-network-tcp-connection-establishment/) phase or 3-way handshake process between the two hosts. Only the first packet from sender as well as receiver should have this flag set. This is used for synchronizing sequence number i.e. to tell the other end which sequence number they should accept.

## ****Acknowledgement (ACK)** –** It is used to acknowledge packets which are successful received by the host. The flag is set if the acknowledgement number field contains a valid acknowledgement number.  In given below diagram, the receiver sends an ACK = 1 as well as SYN = 1 in the second step of connection establishment to tell sender that it received its initial packet.

 **Finish (FIN) –** It is used to request for [connection termination](https://www.geeksforgeeks.org/computer-network-tcp-connection-termination/) i.e. when there is no more data from the sender, it requests for connection termination. This is the last packet sent by sender. It frees the reserved resources and gracefully terminate the connection. 

 **Reset (RST) –** It is used to terminate the connection if the RST sender feels something is wrong with the TCP connection or that the conversation should not exist. It can get send from receiver side when packet is send to particular host that was not expecting it.

 **Urgent (URG) –** It is used to indicate that the data contained in the packet should be prioritized and handled urgently by the receiver. This flag is used in combination with the Urgent Pointer field to identify the location of the urgent data in the packet.

##  ****Push (PSH)** –** It is used to request immediate data delivery to the receiving host, without waiting for additional data to be buffered on the sender’s side. This flag is commonly used in applications such as real-time audio or video streaming.

## Maximum transmission unit, or an MTU.

## We determine the maximum size that you’re able to send using something called a maximum transmission unit, or an MTU.

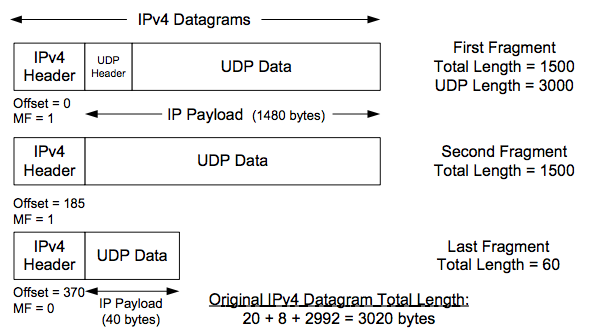
* When a host sends data over a network, the size of a packet depends on what the local network can support. The maximum size for the IP datagram (packet) is restricted by the local network’s data link. In networking lingo, we refer to this maximum size as the IP Maximum Transmission Unit (MTU).
* The MTU is the largest size packet in bytes that can be transmitted across a network’s data link. The MTU can vary across different networks, typically around 1500 bytes for networks provided over Ethernet. That said, the MTU can vary depending on the type of Ethernet being used.
* Packets transmitted from a network that supports one MTU may not be compatible with another network. If, for example, packets need to be sent over the internet or through an encrypted VPN tunnel, the MTU size may be too large resulting in fragmentation and sluggish data transfer.
* In other instances, packets may need to be sent over a network with a different [Maximum Segment Size (MSS)](https://www.cloudflare.com/en-gb/learning/network-layer/what-is-mss/). The MSS is the largest TCP segment size that can be transmitted over a network. When either of these limiting factors is met, IP fragmentation will occur.
* This designates the size of the data that we’re able to send through the network without having to fragment any of that information further. The reason we don’t want to fragment is that it commonly slows down the overall flow of traffic, and if you can optimize your network communication so that you’re not fragmenting, you’ll have a much higher throughput of traffic. This also eliminates any overhead of having to chop the data into smaller pieces, send those individual pieces across the network, and then rebuild those pieces when they get to the other side.
* That’s why it’s important to know the MTU value that would be used all the way through the network from the beginning of the communication all the way to the very end. But understanding what the MTU might be could sometimes be a very complicated process. There may be many different hops that are used to be able to communicate from point A to point B, and each one of those hops may be using a different MTU. There is an automated process that your system will use to attempt to determine what the MTU is when communicating to that other device, but unfortunately, if ICMP is filtered in that communication, there’s no way to automate that process, which means you’ll have to manually set the MTU on your side.

## Ethernet Frame:

* Let’s take a look at what this fragmentation really means. We’ve seen before, where we’ve taken some TCP, data we put a TCP header in front of it, an IP header in front of that, and finally, a DLC header on the outside to send it across our Ethernet network. The data that’s on the inside from the IP header all the way through to the data that’s being transmitted is our IP packet, and the maximum size of an IP packet on an Ethernet network is 1,500 bytes.
* If there’s no fragmentation that’s occurring anywhere on the network, you’ll be able to send all 1,500 bytes through the network without having any of that data fragmented along the way. Let’s take an example, where we can only send a very small amount of data through the network. In this example, 16 bytes of data is the maximum transmission unit that’s supported on this particular network.
* That means we might have 44 bytes of data that needs to be fragmented, and as we’re sending it through the network, we’re going to fragment the first section of it, or the first 16 bytes. We’ll then send another frame of data that has another 16 bytes, and the last frame is going to send the remaining amount of data, up to 16 bytes. So if we do need to send data across the network that’s 44 bytes in length, but the MTU of this network is only 16 bytes, we’re going to end up taking a single frame and splitting it up into three separate frames.

## Ethernet in Networking | Ethernet Frame Format | Gate Vidyalay

## What is IP Fragmentation?

* IP fragmentation is the process of breaking down packets into smaller chunks, known as fragments, so that they can be transmitted over a network with a smaller maximum transmission unit (MTU) or maximum segment size (MSS) than that of the original packet. When a packet is fragmented, the fragments are transmitted across the network and reassembled at their destination to reconstruct the original packet.
* The process of IP fragmentation usually takes place in a router or switch but may also occur on a network interface card (if the card has been configured to perform fragmentation). During the fragmentation process, the original packet is broken into multiple fragments that each contain a copy of the header for the original IP datagram – with minor modifications made to some header fields. These modifications identify the fragment as part of the original packet and permit reassembly when the fragments reach their destination.
* Although IP fragmentation is a neat solution to common networking problems, it can result in unwanted side effects and issues. Below, we will take a closer look at how IP fragmentation works and what kind of problems it causes. 

## What problems can IP fragmentation cause?

* IP fragmentation causes significant overheads that routers are not usually designed to cope with. During IP fragmentation, the router (or network switch) must create fragments and then re-assemble those fragments. This causes sluggishness over the network by sapping up the router’s resources.
* Another issue with IP fragmentation is that if any fragment is dropped during transmission, the whole process has to start again. The original packet, which is discarded during fragmentation, must be retransmitted, fragmented, and reassembled. This makes the fragmentation process inefficient and resource-heavy. For this reason, network administrators avoid IP fragmentation whenever possible.
* IP fragmentation can also cause disordered packet delivery, which results in the need to reorder packets. This is most common when only some packets are fragmented, or if [link aggregation](https://en.wikipedia.org/wiki/Link_aggregation) or other path-splitting technologies are in use. (IP fragmentation can cause problems when used in conjunction with path-splitting technologies because the fragmentation process can result in packets being transmitted over different paths; causing them to arrive at their destination out of order.)

# 1.2 – Network Topologies and Types:

## What is a network topology?

* A network topology is the physical and logical arrangement of nodes and connections in a network. Nodes usually include devices such as switches, routers and software with switch and router features. Network topologies are often represented as a graph.
* Network topologies describe the arrangement of networks and the relative location of traffic flows. Administrators can use network topology diagrams to determine the best placements for each [node](https://www.techtarget.com/searchnetworking/definition/node) and the optimal path for traffic flow. With a well-defined and planned-out network topology, an organization can more easily locate faults and fix issues, improving its data transfer efficiency.

## Network Topologies:

* **Bus network.** In the [bus network](https://www.techtarget.com/searchnetworking/definition/bus-network) topology, every node is connected in series along a single cable. This arrangement is found today primarily in cable broadband distribution networks.
* **Star network.** In the [star network](https://www.techtarget.com/searchnetworking/definition/star-network) topology, a central device connects to all other nodes through a central hub. Switched local area networks based on Ethernet switches and most wired home and office networks have a physical star topology.
* **Ring network.** In the [ring network](https://www.techtarget.com/whatis/definition/ring-network) topology, the nodes are connected in a closed-loop [configuration](https://www.techtarget.com/whatis/definition/configuration). Some rings pass data in one direction only, while others are capable of transmission in both directions. These bidirectional ring networks are more resilient than bus networks since traffic can reach a node by moving in either direction. Metro networks based on Synchronous Optical Network technology are the primary example of ring networks.
* **Mesh network.** The [mesh network](https://internetofthingsagenda.techtarget.com/definition/mesh-network-topology-mesh-network) topology links nodes with connections so that multiple paths between at least some points of the network are available. A network is considered to be fully meshed if all nodes are directly connected to all other nodes and partially meshed if only some nodes have multiple connections to others. Meshing multiple paths increases resiliency but also increases cost. However, more space is needed for dedicated links.
* **Tree network.** The tree network topology consists of one root node, and all other nodes are connected in a hierarchy. The topology itself is connected in a star configuration. Many larger Ethernet switch networks, including data center networks, are configured as trees.
* **Hybrid network.** The hybrid network topology is any combination of two or more topologies. Hybrid topologies typically provide exceptional flexibility, as they can accommodate a number of setups. For example, different departments in the same organization may opt for personalized network topologies that are more adaptable to their network needs.

## The Various Types of Network Topologies - swiss network solutions - swissns GmbH

## Type of Network:

## 

## An introduction to 8 types of network devices | TechTarget7 types of networks and their use cases | TechTarget

# WAN Termination

## Demarcation point, or simply the dmarc:

* if you’re using services from a wide area network provider or an internet service provider, there needs to be a physical location that designates the connection point between the provider’s network and your internal network. We refer to this location as the demarcation point, or simply the dmarc.
* This dmarc might be a location that’s connected to your home. For example, you could have a telephone network interface or a similar box that’s provided by your internet service provider and that box is the demarcation point.

## And when somebody needs to install a new wide area network connection, they’re usually sent to the room that we consider to be the dmarc. The location of this dmarc is important, especially when problems are occurring, so you can understand whether the problem is on the provider side of the dmarc or whether it’s on your side of the dmarc.

## A demarcation point is the physical point at which a telecommunications company’s public network ends and the customer’s private network begins. The demarcation point is often the point at which the cable physically enters the building, but this varies from one country to another.

* The demarcation point defines where the telephone company’s responsibility for maintenance ends and the consumer’s responsibility begins. The demarcation point contains a surge suppressor to protect the wiring and connected equipment in a cutomer’s home from external or internal damage. It also permits consumers to disconnect from the telephone company’s wiring for troubleshooting.
* The demarcation point is also referred to as a network terminating interface or demarc.

## Smart jack:

* This is technically a Network Interface Unit, or NIU. You’ll see these on the wall. They’ll usually have blinking lights and status lights. And they’re usually in a locked container with limited access because this is equipment owned by the network provider.
* This is, obviously, much more intelligent than just having a single RJ45 connector. This is a powered system that is monitoring and is able to provide diagnostics remotely, so the provider can connect to the smartjack, run their own tests, and determine if the problems that are occurring are something that’s in the provider side of the network, or if it’s something that might be on your side of the network.

## Smartjack is a smart and intelligent device placed right between telephone company's demarcation and customer premises. We usually call this kind of device NID but smart jack is different since it has a smart function to test a connectivity check.

# Virtual Network:

* virtual servers, we’ve realized that we **don’t need 100 separate physical servers**.
* Instead, we could create 100 virtual servers that may be **located within one single physical device.**
* A virtual network is a network where all devices, servers, virtual machines, and data centers that are connected are done so through [software and wireless technology](https://www.bmc.com/blogs/software-defined-networking/). This allows the reach of the network to be expanded as far as it needs to for peak efficiency, in addition to numerous other benefits.
* A local area network, or LAN, is a kind of wired network that can usually only reach within the domain of a single building. A wide area network, or WAN, is another kind of wired network, but the computers and devices connected to the network can stretch over a half-mile in some cases.
* Conversely, a virtual network doesn’t follow the conventional rules of networking because it isn’t wired at all.

## Network function virtualization, or NFV,

## Network functions virtualization (NFV) is the replacement of network appliance hardware with virtual machines. The virtual machines use a[hypervisor](https://www.vmware.com/topics/glossary/content/hypervisor.html) to run networking software and processes such as routing and load balancing.

## If we’re replacing physical servers with virtual servers, then we’re taking all of our physical network and we’re replacing it with a virtual network.

## Network visualization definition is self-descriptive as it recreates your network layout on a single screen, displaying information about network devices, network metrics, and data flows in the form of graphs and charts, offering at-a-glance understanding and decision-making for IT operations teams.

## Hypervisor:

* A hypervisor, also known as a virtual machine monitor or VMM, is **software that creates and runs virtual machines (VMs)**. A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing.
* This means that all of our switching, all of our routing, our VLANs, our firewalls, and anything else on the network infrastructure are now contained within this virtual system.
* This not only provides us with the same functionality we had when we had physical switches and physical routers, but in many cases, provides us with additional capabilities. For example, when you need a new switch or a new router, you don’t have to go out, purchase a new router, put it into a rack, power it up and then physically connect those devices. Instead, you simply click a few buttons inside of the hypervisor, and you can drag and drop a brand new router or a brand new switch into your network infrastructure.
* This means that you could have many different kinds of deployment options for your virtual machines, your containers, you can add fault tolerance and different monitoring services, all from this network function virtualization. As with most virtual systems, everything starts and ends with the hypervisor. This is our Virtual Machine Manager, or VMM. This Virtual Machine Manager is responsible for managing all of the operating systems, all of the virtual systems, and all of our virtual network connections that we’re deploying on this virtual system. The hypervisor is responsible for managing access to the CPU, to memory, and to the network for all of those virtual systems, but it can all be managed from this one Central Management Console. Sometimes you’ll hear this referred to as a single pane of glass, because instead of visiting all of those individual virtual systems, you simply go to one management screen and you can control everything.

## vSwitch, or a virtual switch:

* We’re simply taking the physical switch that we used to have, and we’ve moved it into the virtual world.
* We can still do all of the things that we used to do on our physical switch. We know how to set all of the forwarding options. We can configure link aggregation between different virtual switches and different servers. We can do port mirroring and NetFlow to provide additional management capabilities, even though this is contained within a virtual environment. And deploying one of these virtual switches from the hypervisor is simple. You simply drag and drop, or click a button, and you can deploy one of these virtual switches. This can also be automated through the hypervisor’s API so that this can be deployed and removed automatically using orchestration.

## Virtual network interface card, or a vNIC:

## Inside of your virtual machines will be a virtual network interface card, or a vNIC. All of these virtual servers need a vNIC so that they can then communicate out to the rest of the network. This is usually also configured through the hypervisor, and you can add additional functionality or features depending on what you need on that server. You may need multiple network interface cards to provide load balancing, or perhaps you want to add some type of VLAN capabilities or additional monitoring. All of that can be done through the hypervisor.

# Provide Link

## Satellite networking

* This satellite connectivity communicates into space to a satellite and back down to Earth again to provide your internet connections.
* This is a relatively high cost because of all of the equipment that’s required to get this working, but you can get relatively good bandwidths. For example, it’s very common to see 50 megabit download speeds and 3 megabit upload speeds.
* We’re seeing some changes with this technology. As Starlink is being rolled out, we’re seeing those speeds beginning to increase. And you may see that satellite networking becomes much more common in the future. If you have a remote site or a site that has no other option for connectivity to the internet, satellite networking may be the perfect solution. Because of the type of communication, where we’re communicating up to a satellite and back down again, we tend to have a lot of latency with this connection.
* Historically, we’ve seen latency up to 250 milliseconds as traffic is going up to the satellite and another 250 milliseconds as the traffic is sent back down again. The newer technologies from Starlink are promising to lower those latencies down to 20 to 40 milliseconds.
* These are also using high frequencies, usually 2 gigahertz frequencies, which means that they are subject to being absorbed by anything that may be in the way, specifically, rainshowers. And this is where satellite networking has problems– is during a rainstorm, you could lose connectivity to that satellite.

## Copper:

* These are relatively inexpensive to both connect inside of a building and between locations. But because it’s copper, it has a limited amount of bandwidth that we’re able to send over this connection.
* When you need higher speeds, you usually don’t use copper, and instead use something like fiber optics. But these are very common to see on wide area networks, especially wide area networks coming into our home. You often see cable modem or DSL connectivity, and those are usually provided over a copper coax connection or a copper twisted pair connection.
* There’s usually a combination between copper and fiber that we might use where we would have copper on what we call the local loop– or the connection into our local facility– and within the provider’s network, we usually would see fiber optics.

### Digital Subscriber Line

* One of these copper connection types is DSL, or Digital Subscriber Line. Often, this is actually ADSL, for Asymmetric Digital Subscriber Line because the speeds coming into our homes are different than the bandwidths and speeds available going the other direction. Therefore, it’s asymmetric.
* DSL uses the telephone lines that we already have inside of our homes and businesses to provide this connectivity. With DSL, there’s usually a limitation distance. For example, there’s usually about a 10,000 foot limitation between your location and the CO, or Central Office.
* In many DSL connections, you’ll see downstream speeds at about 200 megabits per second and upstream speeds at about 20 megabits per second. But these can differ depending on the type of DSL technology being used in your area and how far away you might be from that central office.

### Cable modem or cable broadband:

* One of the other popular copper connections for internet connectivity is a cable modem or cable broadband. We call this broadband because the signals inside of that coax connection are being transmitted across many different frequencies, or a broad number of bandwidths. There are many different traffic types, usually, inside of these coax. There may be digital television, internet connectivity, and voice.
* You may notice that the specifications for your cable modem have a specific standard called DOCSIS. This is Data Over Cable Service Interface Specification, and this is the type of connectivity that is used by this cable modem. Depending on the DOCSIS version that’s being used in your cable network, you may see speeds that range anywhere from 50 megabits per second through 1,000 megabits per second, or 1 gigabit per second.

## Fiber optic connectivity:

* This is fiber optic connectivity, and it provides some of the highest speed networks that we use. This higher speed, though, comes at a cost.
* Fiber networks are generally more expensive to implement than copper-based networks and certainly, more difficult to repair. You have to have specialized equipment and personnel to be able to repair breaks on a fiber optic network. But this does allow you to send a lot of data over a very long distance, making it perfect for those wide area networks.

## It’s very common to see internet providers and wide area network providers use fiber in the core of their network because it does provide so much speed and so much bandwidth over a long distance. This is where you would see things like SONET rings and Wavelength Division Multiplexing, or WDM. But you might also find that fiber is finding its way to your home. Many organizations are putting fiber into the ground and to your house, providing bandwidths and capabilities that we simply don’t have on copper networks.

# Copper Cabling:

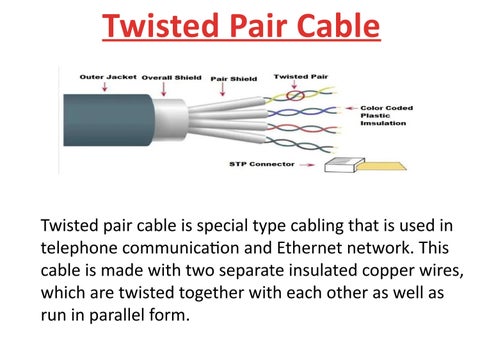
* Copper cabling is the foundation of our Ethernet networks. If you have a network at home, you’re usually connecting with copper Ethernet cable. Whenever we’re building out new networks, we need to make sure that we’re using the correct type of cable for the type of network that we’re installing. And of course, anything that we’re plugging into our network, whether it is a copper wired network or a wireless access point will ultimately come back to that wired connection.

## Twisted Pair Cabling:

## These are a type of guided media. It was invented by Alexander Graham Bell. Twisted pair cables have two conductors that are generally made up of copper and each conductor has insulation. These two conductors are twisted together, thus giving the name twisted pair cables.

## One of the conductors is used to carry the signal and the other is used as a ground reference only. The receiver uses the difference of signals between these two conductors. The noise or crosstalk in the two parallel conductors is high but this is greatly reduced in twisted pair cables due to the twisting characteristic. In the first twist, one conductor is near to noise source and the other is far from the source but in the next twist the reverse happens and the resultant noise is very less and hence the balance in signal quality is maintained and the receiver receives very less or no noise. The quality of signal in twisted pair cables greatly depends upon the number of twists per unit length of the cable.

* Experts point out that twisted pair cabling is often used to help avoid certain kinds of signal interference. **Two different types of twisted pair cable, unshielded twisted pair (UTP) and shielded twisted pair (STP)** are used in different kinds of installations. **UTP is common in Ethernet installations, while STP is used in various kinds of networks to prevent crosstalk and electromagnetic interference. STP cable can also help to provide grounding.**
* In general, twisted-pair cabling may be preferred over a common alternative, coaxial cable, for different reasons. Coaxial cable involves a single, thicker wire. Many of those who use this type of cable claim that twisted pair has a more accommodating bend radius, is easier to terminate, and provides more versatility in selecting network topologies. Different kinds of twisted-pair cable are rated by industry standards including ISO/EIC and EIA/TIA.



* **Unshielded Twisted Pair Cables (UTP) :**  
  These are a pair of two insulated copper wires twisted together without any other insulation or shielding and hence are called unshielded twisted pair cables. They reduce the external interference due to the presence of insulation. Unshielded twisted pair cables are arranged in pairs so that we can add a new connection whenever required. The DSL or telephone lines in our houses have one extra pair in them. When UTP are arranged in pairs, each pair is coded with a different color as defined by the 25-pair color code developed by AT&T Corporation. The Electronic Industries Association divides UTP into 7 categories based on some standards. Categories are based upon cable quality where 1 is the highest quality and 7 is the lowest quality. Each cable in a category is put to a different use as needed.
* **Advantages –**

1. These cables are cost-effective and easy to install owing to their compact size.
2. They are generally used for short-distance transmission of both voice and data.
3. It is less costly as compared to other types of cables.

**Disadvantages –**

1. The connection established using UTP is not secure.
2. They are efficient only for a distance up to 100 meters and have to be installed in pieces of up to 100 meters.
3. These cables have limited bandwidth.

* **Shielded Twisted Pair Cables (STP) :**  
  These types of cables have extra insulation or protective covering over the conductors in the form of a copper braid covering. This covering provides strength to the overall structure of the cable. It also reduces noise and signal interference in the cable. The shielding ensures that the induced signal can be returned to the source via ground and only circulate around the shield without affecting the main propagating signal. The STP cables are also color-coded like the UTP cables as different color pairs are required for analog and digital transmission. These cables are costly and difficult to install.
* **Advantages –**

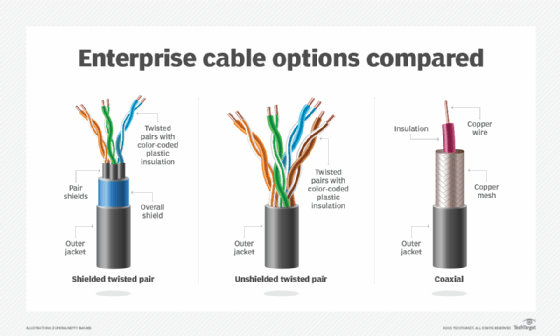
1. They are generally used for long-distance communication and transmission and are installed underground.
2. The protective shield prevents external electromagnetic noise penetration into the cable.
3. They have a higher bandwidth as compared to UTP.

* **Disadvantages –**

1. These cables are very expensive.
2. They require a lot of maintenance which increases the cost more.
3. These can be installed underground only.
4. The length of the segment is similar to UTP for these cables.

**Applications of Twisted pair cables :**

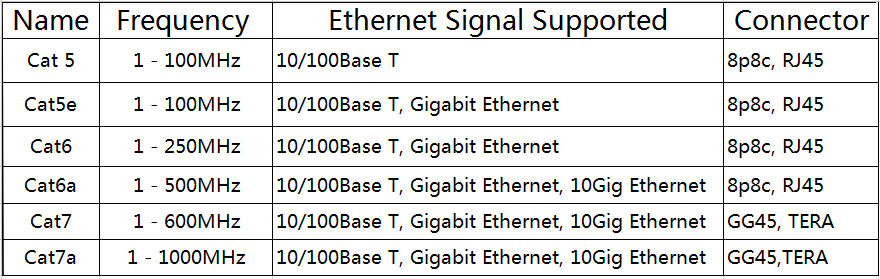
* Twisted Pair cables are used in telephone lines to provide data and voice channels.
* The DSL lines make use of these cables.
* Local Area Networks (LAN) also make use of twisted pair cables.
* They can be used for both analog and digital transmission.
* RJ-45 is a very common application of twisted pair cables.



<https://www.geeksforgeeks.org/twisted-pair-cable/>

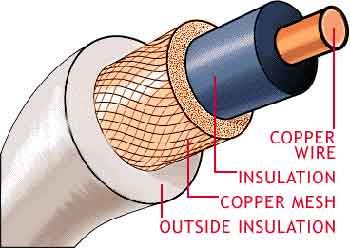
## Copper cable categories:

## 3.1 Explain basic cable types, features, and their purposes. Flashcards | Quizlet



## What is coaxial cable?

* Coaxial cable is a type of copper cable specially built with a metal shield and other components engineered to block signal interference.
* A coaxial -- or coax -- cable is primarily used by cable TV companies to connect their satellite antenna facilities to customer homes and businesses. Telephone companies also sometimes use coax cable to connect central offices to telephone poles near customers. Some homes and offices use coaxial cable, but [twisted pair cabling](https://www.techtarget.com/searchdatacenter/definition/Categories-of-twisted-pair-cabling-systems) has largely supplanted coax's widespread use as an [Ethernet](https://www.techtarget.com/searchnetworking/definition/Ethernet) connectivity medium in enterprises and data centers.
* Coaxial cable received its name because it includes one physical channel that carries the signal surrounded by another concentric physical channel, both running along the same axis. The innermost channel is typically a copper wire, which is then surrounded by a layer of insulation between it and the outer channel. The outer channel serves as a ground, typically as copper mesh. Another layer of insulation surrounds both the inner and outer channels. Many of these cables or pairs of coaxial tubes can be placed in a single outer sheathing and, with repeaters, can carry information for a great distance.
* Coaxial cable was invented in 1880 by English engineer and mathematician Oliver Heaviside, who patented the invention and design that same year. AT&T established its first cross-continental coaxial transmission system in 1940. Depending on the carrier technology used and other factors, twisted pair copper wire and [optical fiber](https://www.techtarget.com/searchnetworking/definition/fiber-optics-optical-fiber) are alternatives to coaxial cable.



## Twinaxial cabling

## Twinaxial cabling, or "Twinax", is a type of cable similar to coaxial cable, but with two inner conductors in a twisted pair instead of one. Due to cost efficiency it is becoming common in modern very-short-range high-speed differential signaling applications. Twinaxial cabling Coaxial cable Electrical cable Electrical conductor Triaxial cable, Coaxial Cable, cable, united Kingdom, braid png | PNGWing

## Structured Cabling Standards:

* There are a set of standards that dictate exactly how you should install and use these twisted pair and copper cable connections. These are the international ISO/IEC 11801 cabling standards.
* Inside of North America, you would commonly see the Telecommunications Industry Association standards, or the TIA standards, specifically the ANSI/TIA-568 standard, which is the commercial building telecommunications cabling standard. If you want more information on the TIA, you can find it on their website at tiaonline.org.
* The TIA-568 standard is extensive. But for the purposes of what we’ll talk about in this video, we’re going to talk about the standards associated with pin and pair assignments of eight-conductor 100-ohm balanced twisted pair cabling. This is the cable we often use when we’re using Ethernet networks. Specifically, we’re going to talk about two types of standards, the T568A and the T568B.
* These 568A and 568B standards dictate what type of colors of cables we will use when punching down these Ethernet connections. The T568A standard has a different set of colors than the T568B standard. But by using either the A or the B standard, we can be assured that we’re matching an A or B standard that’s used anywhere else almost universally.
* The standard itself mentions times when you may want to use T568A colors and T568B colors.

