What’s a Network?

A **network** is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data. It does not matter whether the network contains two or thousands of machines; the concept is essentially the same. The computers on a network may be linked through cables, telephone lines, radio waves, or satellites.

Ağ, veri paylaşımına izin vermek için birbirine bağlı bilgisayarlar, sunucular, ana bilgisayarlar, ağ aygıtları, çevre birimleri veya diğer aygıtların bir koleksiyonudur. Ağın iki veya binlerce makine içermesi önemli değildir; kavram esasen aynı. Bir ağdaki bilgisayarlar kablolar, telefon hatları, radyo dalgaları veya uydular aracılığıyla bağlanabilir.



A network will provide services to its users. Historically, these services have included access to shared files, folders, and printers plus email and database applications. Modern networks provide more diverse services, including web applications, Voice over IP, and multimedia conferencing.

Bir ağ, kullanıcılarına hizmet sağlayacaktır. Geçmişte bu hizmetler, paylaşılan dosyalara, klasörlere ve yazıcılara erişimin yanı sıra e-posta ve veritabanı uygulamalarını da içeriyordu. Modern ağlar, web uygulamaları, IP üzerinden Ses ve multimedya konferansı dahil olmak üzere daha çeşitli hizmetler sağlar.

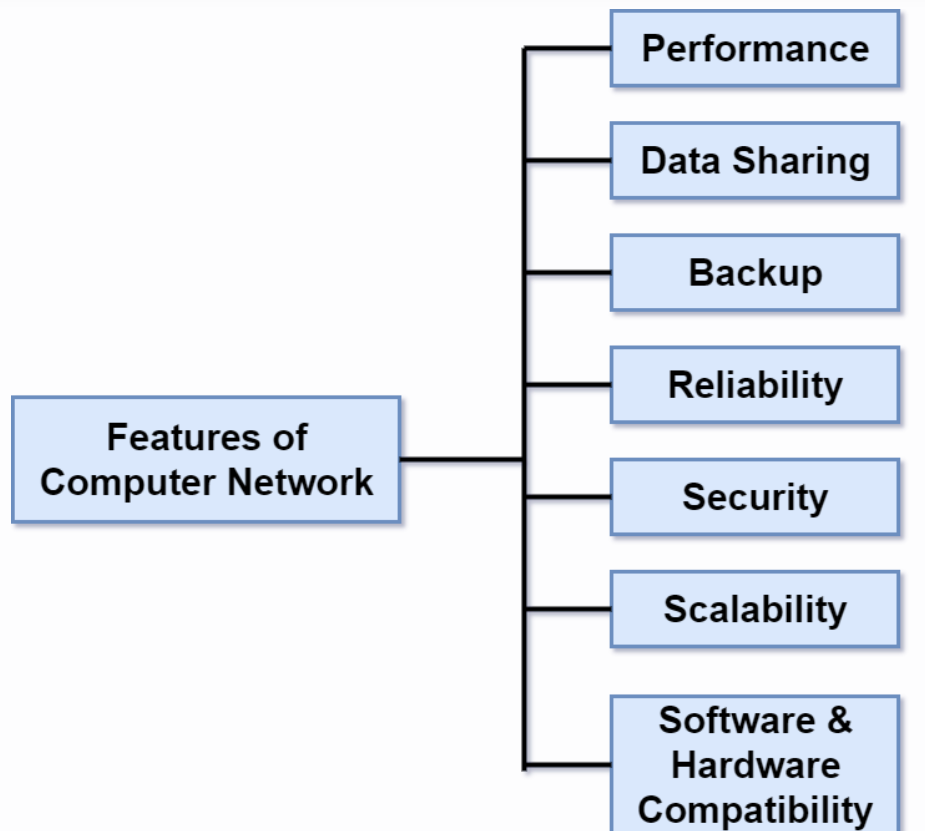
Networks of different sizes are classified in different ways. A network in a single location is often described as a **Local Area Network (LAN)**. This definition encompasses many different types and sizes of networks though. It can include both residential networks with a couple of computers and enterprise networks with hundreds of servers and thousands of workstations.

Farklı boyutlardaki ağlar farklı şekillerde sınıflandırılır. Tek bir konumdaki bir ağ, genellikle Yerel Alan Ağı (LAN) olarak tanımlanır. Bu tanım, yine de birçok farklı tür ve boyuttaki ağları kapsar. Hem birkaç bilgisayar içeren konut ağlarını hem de yüzlerce sunucu ve binlerce iş istasyonuna sahip kurumsal ağları içerebilir.

Networks in different geographic locations but with shared links are called **Wide Area Networks (WAN).**

Farklı coğrafi konumlardaki ancak paylaşılan bağlantılara sahip ağlara Geniş Alan Ağları (WAN) denir.

A computer network has the following features:



* **Performance:** Performance of a computer network is measured in terms of response time. The response time of transmitted and received data from one device to another should be minimal.
* Performans: Bir bilgisayar ağının performansı, yanıt süresi açısından ölçülür. Bir cihazdan diğerine iletilen ve alınan verilerin yanıt süresi minimum olmalıdır.
* **Data Sharing:** One of the reasons why we use a computer network is to share the data between different systems.
* Veri Paylaşımı: Bir bilgisayar ağı kullanmamızın nedenlerinden biri, verileri farklı sistemler arasında paylaşmaktır.
* **Backup:** A computer network must have a central server to keep the backup of all the shared data over a network in order to recover the data faster in case of failures.
* Yedekleme: Bir bilgisayar ağının, arıza durumunda verileri daha hızlı kurtarmak için tüm paylaşılan verilerin bir ağ üzerinden yedeklenmesini sağlamak için merkezi bir sunucuya sahip olması gerekir.
* **Reliability:** There should not be any failure in the network or if it occurs the recovery from failure should be fast.
* Güvenilirlik: Ağda herhangi bir arıza olmamalı veya meydana gelirse arızadan kurtarma hızlı olmalıdır.
* **Security:** A computer network should be secure so that the data exchanged over a network should be safe from unauthorized access. Also, the transmitted data should be received without any loss.
* Güvenlik: Bir ağ üzerinden alınıp verilen verilerin yetkisiz erişime karşı güvende olması için bir bilgisayar ağı güvenli olmalıdır. Ayrıca iletilen verilerin herhangi bir kayıp olmadan alınması gerekmektedir.
* **Scalability:** A computer network should be scalable means adding new devices to the already existing computer network should always be possible. For example, a company runs 100 computers on a network for their 100 employees, let's say they hire another 100 employees and want to add new 100 computers to the already existing LAN then, in that case, the network should allow this.
* Ölçeklenebilirlik: Bir bilgisayar ağı ölçeklenebilir olmalıdır, yani zaten mevcut olan bilgisayar ağına yeni cihazlar eklemek her zaman mümkün olmalıdır. Örneğin, bir şirket 100 çalışanı için bir ağ üzerinde 100 bilgisayar çalıştırıyor, diyelim ki 100 çalışanı daha işe alıyorlar ve zaten var olan LAN'a yeni 100 bilgisayar eklemek istiyorlar, o zaman ağ buna izin vermelidir.
* **Software and hardware compatibility:** A computer network must not limit all the computers to use the same software and hardware, instead, it should allow us to use different software and hardware configurations in the network without introducing any compatibility issues.
* Yazılım ve donanım uyumluluğu: Bir bilgisayar ağı, tüm bilgisayarları aynı yazılım ve donanımı kullanacak şekilde sınırlamamalı, bunun yerine, herhangi bir uyumluluk sorunu yaratmadan ağda farklı yazılım ve donanım yapılandırmalarını kullanmamıza izin vermelidir.

Q: What is a Computer Network?  
A: A computer network is a connection network between two or more nodes using [Physical Media](https://lms.clarusway.com/mod/lesson/view.php?id=1839) Links viz., cable or wireless to exchange data over pre-configured services and Protocols. A computer network is a collective result of – Electrical Engineering, Computer Science, Telecommunication, Computer Engineering and Information Technology involving their theoretical as well as practical aspects into action. The most widely used Computer Network of Today is the Internet which supports the World Wide Web (WWW). Bir bilgisayar ağı, önceden yapılandırılmış hizmetler ve Protokoller üzerinden veri alışverişi yapmak için Fiziksel Ortam Bağlantıları yani kablolu veya kablosuz kullanan iki veya daha fazla düğüm arasındaki bir bağlantı ağıdır. Bir bilgisayar ağı, teorik ve pratik yönlerini eyleme geçiren Elektrik Mühendisliği, Bilgisayar Bilimi, Telekomünikasyon, Bilgisayar Mühendisliği ve Bilgi Teknolojisinin ortak bir sonucudur. Günümüzün en yaygın kullanılan Bilgisayar Ağı, World Wide Web'i (WWW) destekleyen İnternet'tir.

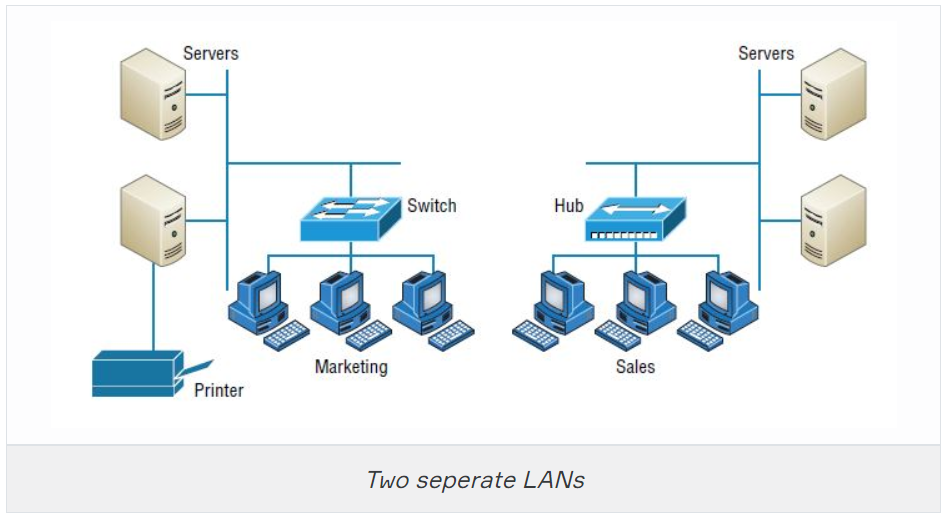
### Local Area Network (LAN)

Just as the name implies, a **local area network (LAN)** is usually restricted to spanning a particular geographic location such as an office building, a single department within a corporate office, or even a home office. Thanks to the technological advances that we’re almost free from the restrictions imposed by both the size and the distance coverage of LANs.

Adından da anlaşılacağı gibi, bir **local area network (LAN)** genellikle bir ofis binası, bir şirket ofisi içindeki tek bir departman veya hatta bir ev ofisi gibi belirli bir coğrafi konumu kapsamakla sınırlıdır. LAN'ların hem boyutu hem de mesafe kapsamının getirdiği kısıtlamalardan neredeyse kurtulduğumuz teknolojik gelişmeler sayesinde.

In a typical business environment, it’s a good idea to split your LAN according to the department divisions; for instance, you could create a LAN for Accounting, another one for Sales, and maybe another for Marketing. The figure shows two separate LANs.

Tipik bir iş ortamında, LAN'ınızı departman bölümlerine göre bölmek iyi bir fikirdir; örneğin, Muhasebe için bir LAN, Satış için bir tane ve Pazarlama için bir tane daha oluşturabilirsiniz. Şekilde iki ayrı LAN gösterilmektedir.



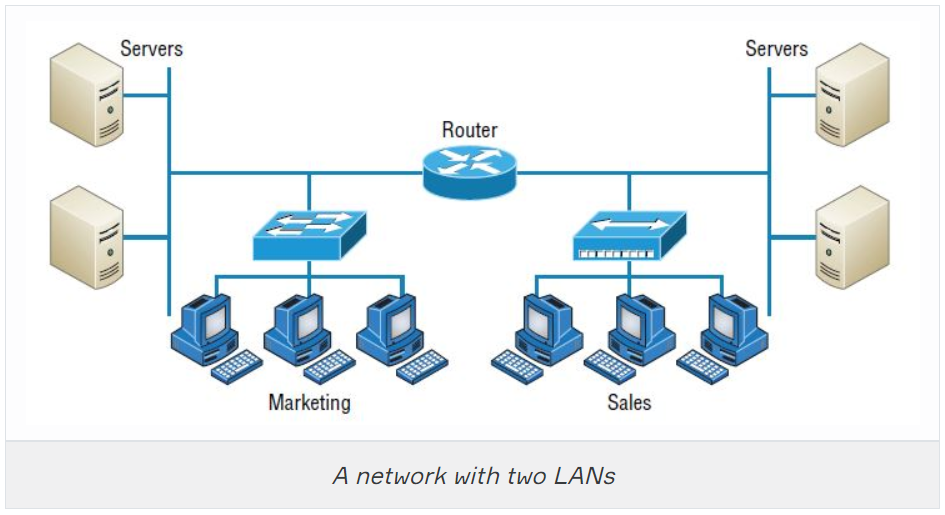
In the figure, there’s a Marketing LAN and a Sales LAN. Any device connected to the Marketing LAN can access to the resources inside the Marketing LAN—in this case, the servers and printer. There are two problems with this:

Şekilde, bir Pazarlama Ağı ve bir Satış Ağı var. Pazarlama LAN'ına bağlı herhangi bir cihaz Pazarlama LAN içindeki kaynaklara erişebilir - bu durumda sunucular ve yazıcı. Bununla birlikte iki tane sorun var:

* You must be physically connected to the LAN to get the resources from it. Kaynakları buradan almak için LAN'a fiziksel olarak bağlı olmanız gerekir.
* You can’t connect from one LAN to another and furthermore can't share data and services between these LANs. Bir LAN'dan diğerine bağlanamazsınız ve ayrıca bu LAN'lar arasında veri ve hizmetleri paylaşamazsınız.

This is a typical network issue that’s easily resolved by using a device called **router** to connect the two LANs, as shown below.

Bu, aşağıda gösterildiği gibi iki LAN'ı bağlamak için yönlendirici adı verilen bir cihaz kullanılarak kolayca çözülen tipik bir ağ sorunudur.



There it is! The problem is solved! Even though you can use **routers** for more than just connecting LANs, the **router** shown above is a great solution because the host computers from the Sales LAN can get to the resources (server data and printers) of the Marketing LAN, and vice versa.

İşte burada! Problem çözüldü! Yönlendiricileri yalnızca LAN'ları bağlamaktan daha fazlası için kullanabilmenize rağmen, yukarıda gösterilen yönlendirici harika bir çözümdür çünkü **Sales LAN**'ından ana bilgisayarlar **Marketing LAN**'ının kaynaklarına (sunucu verileri ve yazıcılar) ulaşabilir ve bunun tersi de geçerlidir.

Now, you might be thinking that we really don’t need the **router**—that we could just physically connect the two workgroups with a type of cable that would allow the Marketing and Sales workgroups to hook up somehow. Well, we could do that, but if we did, we would have only one big, cumbersome LAN instead of separate LAN for Marketing and Sales, and this kind of arrangement (one large LAN) just isn’t practical for today’s networks. That's why, with smaller, individual-yet-connected groups, the users on each LAN can enjoy much faster response times when accessing resources. Besides, the management of administrative tasks become much easier. Larger LANs usually run more slowly because the hosts within the LAN try to use the same resources simultaneously. So the **router** in the above figure, which separates the workgroups while still allowing access between them, is really a great solution!

Şimdi, yönlendiriciye gerçekten ihtiyacımız olmadığını - Pazarlama ve Satış çalışma gruplarının bir şekilde bağlantı kurmasına olanak tanıyan bir tür kabloyla iki çalışma grubunu fiziksel olarak bağlayabileceğimizi düşünüyor olabilirsiniz. Bunu yapabilirdik, ancak yapsaydık, Marketing ve Sales için ayrı LAN yerine yalnızca bir büyük, hantal LAN'ımız olurdu ve bu tür bir düzenleme (tek büyük LAN) günümüz ağları için pratik değildir. Bu nedenle, daha küçük, bireysel henüz bağlantılı gruplarla, her LAN'daki kullanıcılar kaynaklara erişirken çok daha hızlı yanıt sürelerinin keyfini çıkarabilir. Ayrıca, idari görevlerin yönetimi çok daha kolay hale geliyor. Daha büyük LAN'lar genellikle daha yavaş çalışır çünkü LAN içindeki ana bilgisayarlar aynı kaynakları aynı anda kullanmaya çalışır. Dolayısıyla, çalışma gruplarını ayırırken aralarında erişime izin veren yukarıdaki şekildeki yönlendirici(**router**) gerçekten harika bir çözüm!

The devices hub, switch, and **router** will be explained in detail in the following sections.

Q: Explain what is LAN?  
A: A LAN or Local Area Network is the network between devices that are located within a small physical location. It can be either wireless or wired. One LAN differs from another based on the following factors:  
**Topology:** The arrangement of nodes within the network - Ağ içindeki düğümlerin düzenlenmesi  
**Protocol:** Refer to the rules for the transfer of data - Veri aktarımı kurallarına bakın  
**Media:** These devices can be connected using optic fibers, twisted-pair wires, etc - Bu cihazlar optik fiberler, çift bükümlü teller, vb. kullanılarak bağlanabilir.

### Common Network Components

**Node, Stations, and Hosts:** A **node** is any device that can communicate on the network via one or more network interfaces. The term **node** can be used to describe endpoint devices, such as computers, laptops, servers, IP phones, smartphones, or printers, and connecting or forwarding devices, such as switches and routers. A **node** on a wireless network is often called as a station. - Bir **node**, bir veya daha fazla ağ arabirimi aracılığıyla ağ üzerinde iletişim kurabilen herhangi bir cihazdır. Node terimi, bilgisayarlar, dizüstü bilgisayarlar, sunucular, IP telefonları, akıllı telefonlar veya yazıcılar gibi uç nokta cihazlarını ve **stations** ve **hosts** gibi bağlantı veya iletme cihazlarını tanımlamak için kullanılabilir. Kablosuz ağdaki bir **node** genellikle **station** olarak adlandırılır.

The term **host** is often used in TCP/IP networking to mean an end system device, such as a computer, with a unique address on the network.

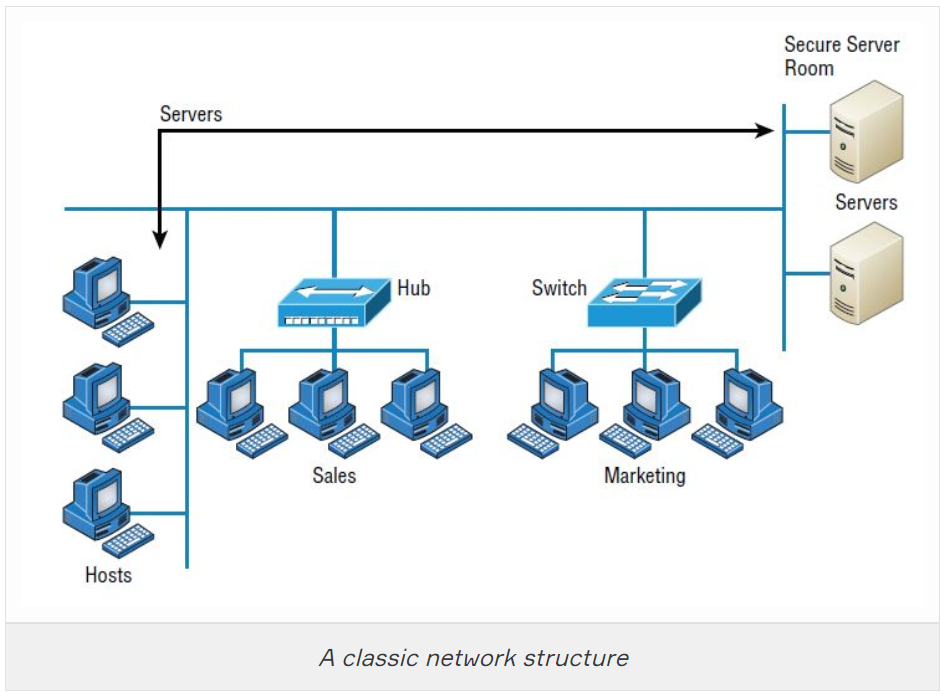
**Workstations:** Workstation is a client **machine** used to deploy an **application** or **server**. They are usually powerful **computers** that have more than one central processing unit (CPU) and whose resources are available to other users on the network when needed. Workstations are often equipped with systems for end-users to use daily. Don’t confuse workstations with client machines. Client machines can be workstations but not always. Technically speaking, they are different. A client machine is any device on the network like a printer or other hosts from a server or powerful workstation. - Workstation, bir uygulamayı veya sunucuyu dağıtmak için kullanılan bir istemci makinesidir. Genellikle birden fazla merkezi işlem birimine (CPU) sahip olan ve kaynakları gerektiğinde ağdaki diğer kullanıcılar tarafından kullanılabilen güçlü bilgisayarlardır. Workstation genellikle son kullanıcıların günlük olarak kullanması için sistemlerle donatılmıştır. İş istasyonlarını istemci makinelerle karıştırmayın. İstemci makineleri iş istasyonları olabilir, ancak her zaman değil. Teknik olarak konuşursak, farklılar. Bir istemci makine, bir sunucu veya güçlü bir iş istasyonundan yazıcı veya diğer ana bilgisayarlar gibi ağdaki herhangi bir cihazdır.

**Servers:** Servers are also powerful **computers**. They get their name because they truly are “at the service” of the network and run specialized software known as the network operating system to maintain and control the network. In a good design, they optimize the network’s performance. Servers are highly specialized and handle important labor-intensive jobs. A single server can’t do many jobs, that's why, in order to get better performance, a single task is often assigned to a dedicated server. Here’s a list of common dedicated servers: - Sunucular aynı zamanda güçlü bilgisayarlardır. Adlarını, gerçekten ağın "hizmetinde" oldukları ve ağı korumak ve kontrol etmek için ağ işletim sistemi olarak bilinen özel yazılımları çalıştırdıkları için alırlar. İyi bir tasarımda, ağın performansını optimize ederler. Sunucular son derece uzmanlaşmıştır ve emek yoğun işlerin üstesinden gelir. Tek bir sunucu birçok işi yapamaz, bu nedenle daha iyi performans elde etmek için genellikle tek bir görev özel bir sunucuya atanır. Yaygın olarak kullanılan özel sunucuların listesi aşağıda verilmiştir:

* **File Server** - Stores and dispenses files
* **Mail Server** - The network’s post office; handles email functions
* **Print Server** - Manages printers on the network
* **Web Server** - Manages web-based activities by running Hypertext Transfer Protocol (HTTP) for storing web content and accessing web pages
* **Fax Server** - The “memo maker” that sends and receives paperless faxes over the network
* **Application Server** - Manages network applications
* **Telephony Server** - Handles the call center and call routing and can be thought of as a sophisticated network answering machine
* **Proxy Server** - Handles tasks in the place of other machines on the network, particularly an internet connection.

Whether servers are designated for simple or complex network tasks, they can maintain the network’s data integrity by backing up the network’s software and providing redundant hardware (for fault tolerance). And in the meanwhile, they all serve a number of client machines. - Sunucular ister basit ister karmaşık ağ görevleri için tasarlanmış olsun, ağın yazılımını yedekleyerek ve yedek donanım (hata toleransı için) sağlayarak ağın veri bütünlüğünü koruyabilirler. Ve bu arada, hepsi bir dizi istemci makineye hizmet ediyor.

In the below figure, you can see a network topology consists of workstations (client machines) and servers. Also notice that the hosts can access the servers across the network, which is pretty much the general idea of having a network in the first place! - Aşağıdaki şekilde, iş istasyonları (istemci makineler) ve sunuculardan oluşan bir ağ topolojisini görebilirsiniz. Ayrıca, ana bilgisayarların ağ üzerindeki sunuculara erişebildiğine dikkat edin; bu, ilk etapta bir ağa sahip olmanın hemen hemen genel fikri!



**Transmission Media:** A link between network nodes is created using some form of transmission media like cables, or radio waves. - Ağ devreleri arasında bir bağlantı, kablolar veya radyo dalgaları gibi bir tür iletim ortamı kullanılarak oluşturulur.

**Local Network Devices, Segments, and Backbones:** Relatively few networks are established to connect the hosts directly. Instead of direct links among them, each host is connected to a central node, such as a **switch** or **wireless access point**. The central node provides a forwarding function, that is, receives the data from one node and re-transmits it to the others. - Ana bilgisayarları doğrudan bağlamak için nispeten az sayıda ağ kurulmuştur. Aralarındaki doğrudan bağlantılar yerine, her ana bilgisayar, anahtar veya kablosuz erişim noktası gibi merkezi bir düğüme bağlanır. Merkezi devre bir yönlendirme işlevi sağlar, yani verileri bir devreden alır ve diğerlerine yeniden iletir.

A central device such as a **switch** implies that the connected nodes are part of the same physical network and use the same type of transmission media. The term **switching** is used for this forwarding function taking place within the same physical network. The addresses of interfaces within the same network are described as **local addresses**. - Switch gibi merkezi bir cihaz, bağlı devrelerin aynı fiziksel ağın parçası olduğunu ve aynı tür iletim ortamını kullandığını belirtir. Switching terimi, aynı fiziksel ağ içinde gerçekleşen bu yönlendirme işlevi için kullanılır. Aynı ağ içindeki arayüzlerin adresleri yerel adresler olarak tanımlanır.

The term **segment** can be used to refer to a specific physical region of a network, though the scope of a segment depends on the exact technology in use. One typical usage now is to describe the link between a computer and a switch. Another usage is to refer to a region of the network where all the nodes use the same type of transmission media and have the same bandwidth. - Segment terimi, bir ağın belirli bir fiziksel bölgesine atıfta bulunmak için kullanılabilir, ancak bir segmentin kapsamı, kullanılan tam teknolojiye bağlıdır. Şimdi tipik bir kullanım, bir bilgisayar ve bir anahtar arasındaki bağlantıyı açıklamaktır. Diğer bir kullanım, tüm devrelerin aynı tür iletim ortamını kullandığı ve aynı bant genişliğine sahip olduğu bir ağ bölgesine atıfta bulunmaktır.

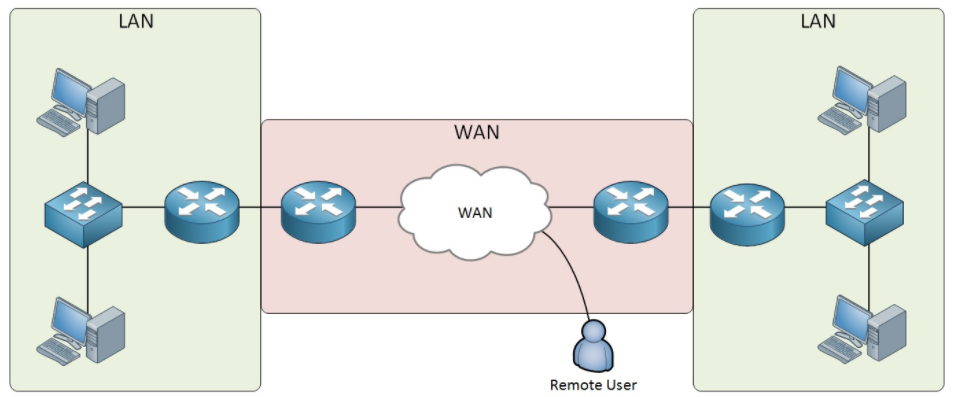
A network is typically divided into segments either to cope with the physical restrictions of the network media used or to improve performance or to improve security (or all three). A **backbone** describes a fast link among other segments of a network. The backbone carries all the communications occurring between nodes in separate segments. - Bir ağ tipik olarak, kullanılan ağ ortamının fiziksel kısıtlamalarıyla başa çıkmak veya performansı iyileştirmek veya güvenliği (veya üçü birden) artırmak için bölümlere ayrılır. Omurga(**backbone**), bir ağın diğer bölümleri arasındaki hızlı bağlantıyı tanımlar. **Backbone**, devreler arasında meydana gelen tüm iletişimleri ayrı segmentlerde taşır.

Q: What do you mean by a Node?  
A: The intersection point in a network is called as a Node. Nodes can send or receive data/ information within a network. For example, if two computers are connected to form a network, there are 2 nodes in that network. Similarly, in case of adding more computers, there will be more nodes and so on. It is not necessary for a node to be a computer, it can be any communication device such as a printer, servers, modems, etc.. - Bir ağdaki kesişim noktası Node olarak adlandırılır. Nodes bir ağ içinde veri / bilgi gönderebilir veya alabilir. Örneğin, bir ağ oluşturmak için iki bilgisayar bağlıysa, o ağda 2 node vardır. Benzer şekilde, daha fazla bilgisayar eklenmesi durumunda, daha fazla node olacaktır vb. Bir node un bilgisayar olması gerekli değildir, yazıcı, sunucu, modem vb. Herhangi bir iletişim cihazı olabilir.

### Wide Area Network (WAN)

Our own networks are called **LANs** (Local Area Network). We own and operate these networks. It’s called a **“local”** area network since all devices that make up the LAN are close to each other. Perhaps in one building or a few buildings close to each other (called a **campus**).

When we need access to other remote networks, or give others access to our LAN, we need a **WAN (Wide Area Network)**. As the name implies, WANs cover large geographical areas. This could be a network between two cities or as large as the **Internet**.



On the **LAN**, the dominant protocol that we use is **Ethernet**. For **WAN**, there are dozens of technologies and protocols we can choose from.

Below is the list of some differences between WAN and LANs:

* WANs usually need a router.
* WANs span larger geographic areas and/or can link disparate locations.
* WANs are usually slower.
* We can choose when and how long we connect to a WAN. A LAN is all or nothing—our workstation is connected to it either permanently or not at all.
* WANs can utilize either private or public data transport media such as phone lines.

We get the word Internet from the term internetwork. An internetwork is a type of LAN and/or WAN that connects a bunch of networks or intranets. In an internetwork, hosts still use hardware addresses to communicate with other hosts on the same LAN. However, they use logical addresses (IP addresses) to communicate with hosts on a different LAN (the other side of the router). And routers are the devices that make this possible. Each connection into a router is a different logical network. - İnternet kelimesini ağlar arası çalışma teriminden alıyoruz. Bir ağ çalışması, bir grup ağı veya intraneti birbirine bağlayan bir LAN ve / veya WAN türüdür. Bir ağ ağında, ana bilgisayarlar aynı LAN üzerindeki diğer ana bilgisayarlarla iletişim kurmak için donanım adreslerini kullanmaya devam eder. Ancak, farklı bir LAN'daki (yönlendiricinin diğer tarafı) ana bilgisayarlarla iletişim kurmak için mantıksal adresler (IP adresleri) kullanırlar. Yönlendiriciler, bunu mümkün kılan cihazlardır. Bir yönlendiriciye yapılan her bağlantı farklı bir mantıksal ağdır.

Q: What is WAN?  
A: WAN stands for Wide Area Network. It is an interconnection of computers and devices that are geographically dispersed. It connects networks that are located in different regions and countries. - WAN, Geniş Alan Ağı anlamına gelir. Coğrafi olarak dağınık olan bilgisayarların ve cihazların bir ara bağlantısıdır. Farklı bölge ve ülkelerde bulunan ağları birbirine bağlar.

### Physical Network Topologies

Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer network. Essentially, it is the topological structure of a network and may be depicted ***physically***or***logically*** which are the two basic categories of network topologies. - Ağ topolojisi, bir bilgisayar ağının çeşitli öğelerinin (bağlantılar, düğümler vb.) düzenlenmesidir. Esasen, bir ağın topolojik yapısıdır ve ağ topolojilerinin iki temel kategorisi olan fiziksel veya mantıksal olarak tasvir edilebilir.

The shape of the cabling layout used to link devices is called the **physical topology** of the network. This refers to the layout of cabling, the locations of nodes, the interconnections between the nodes and the cabling. The physical topology of a network is determined by the capabilities of the network access devices and media, the level of control or fault tolerance desired, and the cost associated with cabling or telecommunications circuits. - Aygıtları birbirine bağlamak için kullanılan kablolama düzeninin şekline ağın fiziksel topolojisi denir. Bu, kablolama düzeni, node larin yerleri, node lar arasındaki ara bağlantılar ve kablolama ile ilgilidir. Bir ağın fiziksel topolojisi, ağ erişim cihazlarının ve ortamının yetenekleri, istenen kontrol seviyesi veya hata toleransı ve kablolama veya telekomünikasyon devreleriyle ilişkili maliyet ile belirlenir.

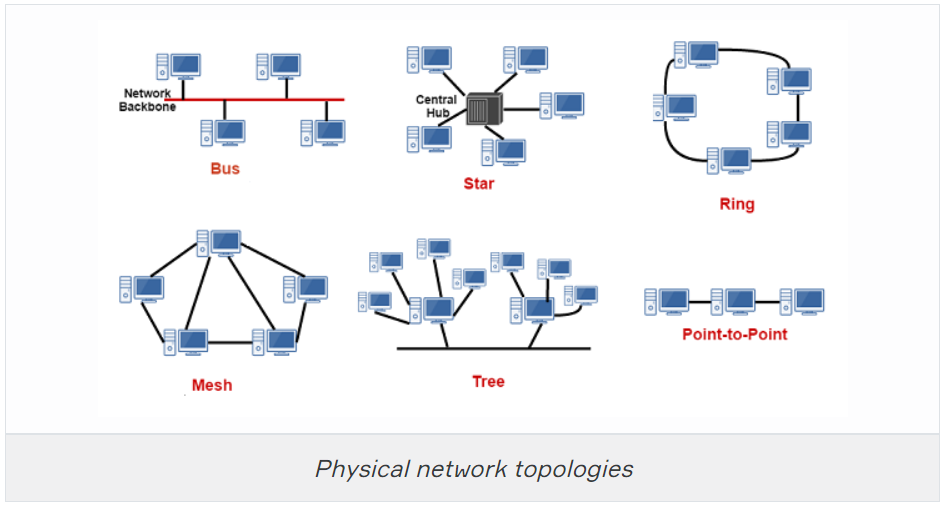
The **logical topology**, in contrast, is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices. A network’s logical topology is not necessarily the same as its physical topology. - Mantıksal topoloji, tersine, sinyallerin ağ ortamına etki etme şekli veya verilerin ağ üzerinden bir aygıttan diğerine, aygıtların fiziksel ara bağlantısına bakılmaksızın geçme biçimidir. Bir ağın mantıksal topolojisi, fiziksel topolojisiyle aynı olmak zorunda değildir.

The logical classification of network topologies generally follows the same classifications as those in the physical classifications of network topologies but describes the path that the data takes between nodes being used as opposed to the actual physical connections between nodes. The logical topologies are generally determined by network protocols as opposed to being determined by the physical layout of cables, wires, and network devices or by the flow of the electrical signals. In many cases, the paths that the electrical signals travel among the nodes may closely match the logical flow of data. That is why, the terms logical topology and signal topology can be interchangeably used.

Ağ topolojilerinin mantıksal sınıflandırması genellikle ağ topolojilerinin fiziksel sınıflandırmalarındaki sınıflandırmalarla aynı sınıflandırmaları takip eder, ancak verilerin node lar arasındaki gerçek fiziksel bağlantıların aksine kullanılan node lar arasında aldığı yolu açıklar. Mantıksal topolojiler, kabloların, tellerin ve ağ cihazlarının fiziksel yerleşimi veya elektrik sinyallerinin akışı tarafından belirlenmenin aksine genellikle ağ protokolleri tarafından belirlenir. Çoğu durumda, elektrik sinyallerinin node lar arasında gittiği yollar mantıksal veri akışı ile yakından eşleşebilir. Bu nedenle mantıksal topoloji ve sinyal topolojisi terimleri birbirinin yerine kullanılabilir.

Here’s a list of the topologies mostly used nowadays:

* Bus
* Star
* Ring
* Mesh
* Tree
* Point-to-point
* Point-to-multipoint
* Hybrid

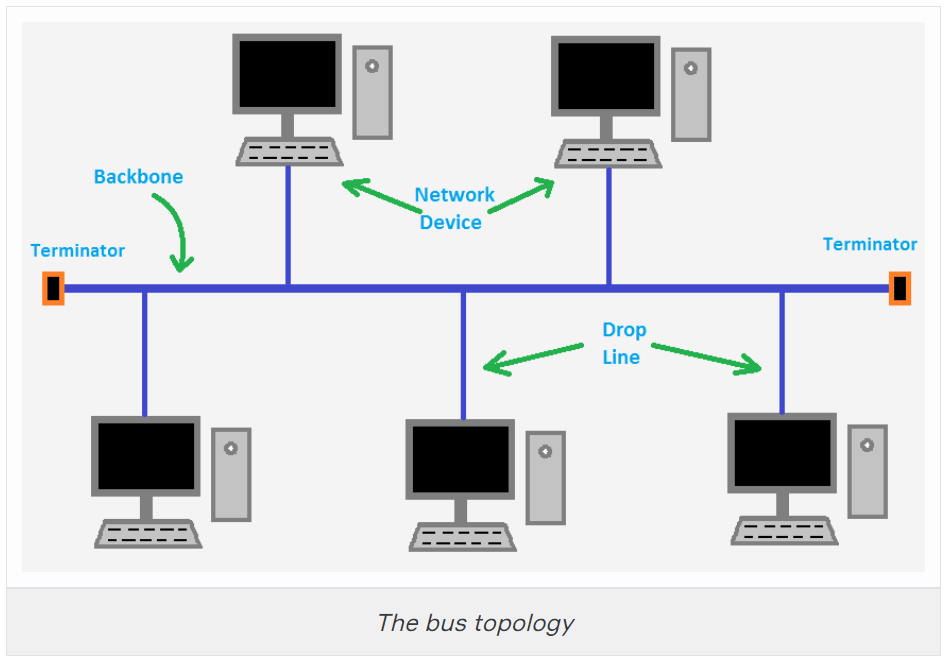


Q: What do you mean by network topology?  
A: Network topology specifies the layout of a computer network. It shows how devices and cables are connected to each other. Some types of topologies are: Bus, Star, Ring, Mesh, etc.

### Bus Topology

A bus topology consists of a single cable ( the bus ) with a terminator at each end. All nodes (file server, workstations, and peripherals) are connected to this cable. The signal travels down the bus in both directions from the source and is received by all nodes connected to the cable. The bus is terminated at both ends of the cable to absorb the signal when it has passed all connected devices.

Bir veri yolu topolojisi, her iki ucunda bir sonlandırıcı bulunan tek bir kablodan (veri yolu) oluşur. Tüm node lar (dosya sunucusu, iş istasyonları ve çevre birimleri) bu kabloya bağlıdır. Sinyal, kaynaktan her iki yönde de veri yolundan aşağıya iner ve kabloya bağlı tüm düğümler tarafından alınır. Veriyolu, bağlı tüm cihazları geçtiğinde sinyali emmek için kablonun her iki ucunda sonlandırılır.



This type of physical bus topology is no longer in widespread use. Bus networks are comparatively difficult to reconfigure (adding or removing nodes can disrupt the whole network), impose limitations on the maximum number of nodes on a segment of cable, and are difficult to troubleshoot (a cable fault could be anywhere on the segment of cable). Perhaps most importantly, a fault anywhere in the cable means that all nodes will be unable to communicate. - Bu tür fiziksel veri yolu topolojisi artık yaygın olarak kullanılmamaktadır. Veriyolu ağlarının yeniden yapılandırılması nispeten zordur (düğüm eklemek veya kaldırmak tüm ağı bozabilir), bir kablo segmentindeki maksimum düğüm sayısına sınırlamalar getirir ve giderilmesi zordur (bir kablo hatası, kablo segmentinin herhangi bir yerinde olabilir). Belki de en önemlisi, kablonun herhangi bir yerinde bir arıza olması, tüm düğümlerin iletişim kuramayacağı anlamına gelir.

The logical bus topology, however, remains the basis of most local networks. - Mantıksal veri yolu topolojisi, ancak, çoğu yerel ağın temeli olmaya devam etmektedir.

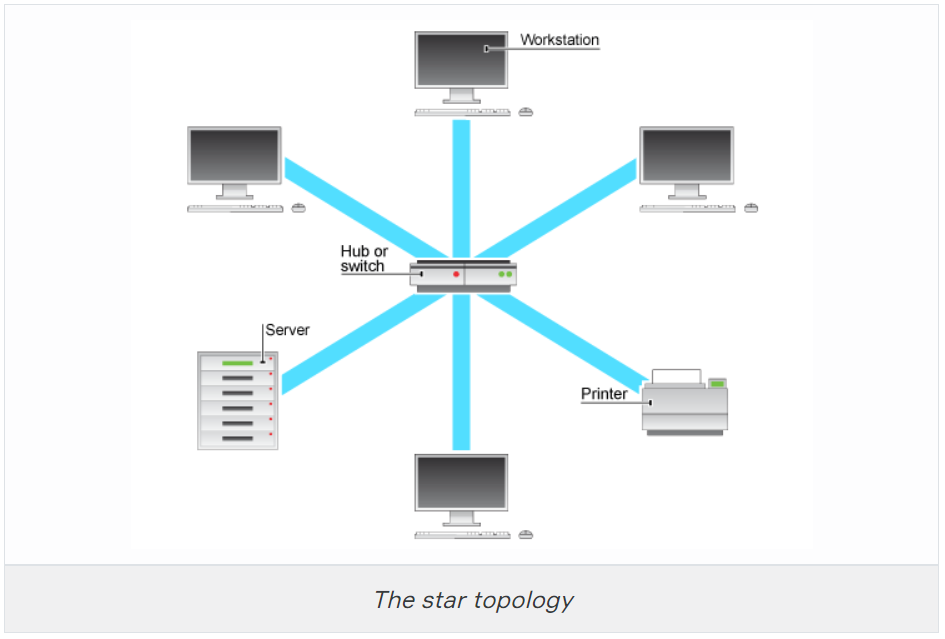
**Advantages of bus topology:**  
1. Easy installation, each cable needs to be connected with backbone cable. - Kolay kurulum, her kablonun omurga kablosuyla bağlanması gerekir.  
2. Fewer cables required than mesh and star topology - Ağ ve yıldız topolojisinden daha az kablo gerekir

**Disadvantages of bus topology:**  
1. Difficultly in fault detection. - Arıza tespitinde güçlük.  
2. Not scalable as there is a limit of how many nodes you can connect with backbone cable. - Omurga kablosuyla kaç düğüm bağlayabileceğiniz konusunda bir sınır olduğundan ölçeklendirilemez.

### Star Topology

In star topology, every node (computer workstation or any other peripheral) is connected to a central node called hub or switch. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device. All traffic that traverses the network passes through the central hub. - Yıldız topolojisinde, her node (bilgisayar iş istasyonu veya diğer herhangi bir çevre birimi), hub veya anahtar adı verilen merkezi bir düğüme bağlıdır. Ağın bir yıldız ağı olarak sınıflandırılması için mutlaka bir yıldıza benzemesi gerekmez, ancak ağdaki tüm düğümlerin tek bir merkezi cihaza bağlı olması gerekir. Ağdan geçen tüm trafik, merkezi hub'dan geçer.

The star topology is the most widely used physical topology. It is easy to reconfigure and easy to troubleshoot because all data goes through a central point, which can be used to monitor and manage the network. Faults are automatically isolated to the media, node (network card), or the hub, switch, or router at the center of the star. - Yıldız topolojisi en yaygın kullanılan fiziksel topolojidir. Tüm veriler, ağı izlemek ve yönetmek için kullanılabilen merkezi bir noktadan geçtiği için yeniden yapılandırılması ve giderilmesi kolaydır. Hatalar, yıldızın ortasındaki ortama, düğüme (ağ kartı) veya hub'a, anahtara veya yönlendiriciye otomatik olarak yalıtılır.



**Advantages of Star topology:**  
1. Less expensive because each device only needs one I/O port and needs to be connected with a hub with one link.  
2. Easier to install.  
3. Less amount of cables required because each device needs to be connected with the hub only.  
4. Robust, if one link fails, other links will work just fine.  
5. Easy fault detection because the link can be easily identified.

**Disadvantages of Star topology:**  
1. If the hub goes down every node goes down, none of the devices can work without the hub.  
2. Hub requires more resources and regular maintenance because it is the central system of star topology.

Q: Describe star topology  
A: Star topology consists of a central hub that connects the nodes. This is one of the easiest way to setup and maintain.

Q: What is the disadvantage of a star topology?  
A: One major disadvantage of star topology is that once the central hub or switch damaged, the entire network becomes unusable.

Ring Topology

A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the right acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring. If a device wants to send data to another device then it sends the data in one direction, if the received data is intended for other devices then it forwards this data until the intended device receives it. - Verilerin halka etrafında bir yönde hareket ettiği ve sağdaki her cihazın, sinyali hareket ederken güçlü tutmak için bir tekrarlayıcı görevi gördüğü dairesel bir şekilde kurulmuş bir ağ topolojisi. Her cihaz, gelen sinyal için bir alıcı ve verileri halkadaki bir sonraki cihaza göndermek için bir verici içerir. Bir cihaz başka bir cihaza veri göndermek isterse, verileri bir yönde gönderir, alınan veriler başka cihazlar için tasarlanmışsa, bu verileri amaçlanan cihaz alana kadar iletir.

|  |
| --- |
| *The ring topology* |

The physical ring topology is no longer used on LANs but it does remain as a feature of many WANs. Two ring systems (dual counter-rotating rings) can be used to provide fault tolerance. These dual rings allow the system to continue to operate if there is a failure in one ring. - Fiziksel halka topolojisi artık LAN'larda kullanılmamaktadır, ancak birçok WAN'ın bir özelliği olarak kalmaktadır. Hata toleransı sağlamak için iki halka sistemi (çift ters dönen halkalar) kullanılabilir. Bu ikili halkalar, tek bir halkada bir arıza olması durumunda sistemin çalışmaya devam etmesini sağlar.

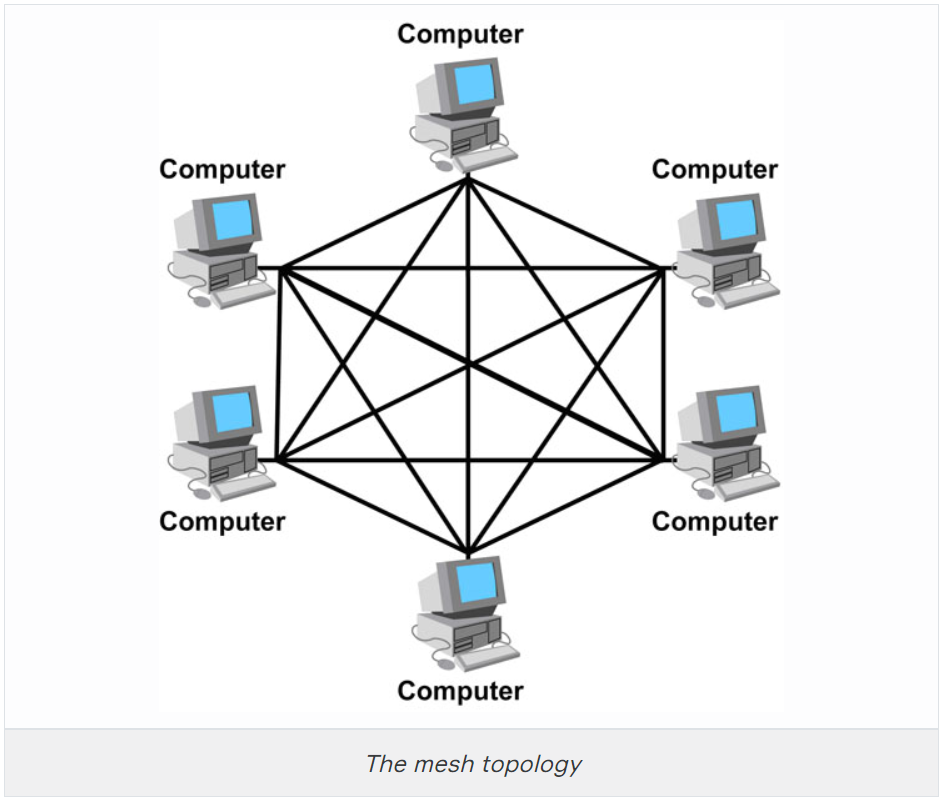
**Advantages of Ring Topology:**  
1. Easy to install.  
2. Management is easier, because to add or remove a device from the topology only requires to change just two links.

**Disadvantages of Ring Topology:**  
1. A link failure can fail the entire network as the signal will not travel ahead due to failure.  
2. Data traffic issues, since all the data is circulated in a ring.

Q: What are some drawbacks of implementing a ring topology? - Bir halka topolojisi uygulamanın bazı dezavantajları nelerdir?  
A: In case one workstation on the network suffers a malfunction, it can bring down the entire network. Another drawback is that when there are adjustments and reconfigurations needed to be performed on a particular part of the network, the entire network has to be temporarily brought down as well. - Ağdaki bir iş istasyonunun arızalanması durumunda, tüm ağı çökertebilir. Diğer bir dezavantaj, ağın belirli bir bölümünde gerçekleştirilmesi gereken ayarlamalar ve yeniden yapılandırmalar olduğunda, tüm ağın da geçici olarak kapatılmasının gerekmesidir.

### Mesh Topology

**Mesh network topologies** are commonly used in **WANs**, especially public networks like the Internet. In theory, a mesh network requires that each device has a point-to-point link with every other device on the network (**fully connected**). This approach is normally impractical, however. The number of links required by a full mesh is expressed as n(n-1)/2, where "n" is the number of nodes. For example, a network of just 4 nodes would require 6 links, while a network of 40 nodes would need 780 links!



Consequently, often a "**hybrid**" approach is used with only the most important devices interconnected in the mesh, perhaps with extra links for fault tolerance and redundancy. In this case, the topology is referred to as a **partial mesh.**



**Advantages of Mesh topology:**

1. No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.
2. Mesh topology is reliable and robust as a failure of one link doesn’t affect the other links and the communication between other devices on the network.
3. Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.
4. Fault detection is easy.

**Disadvantages of Mesh topology:**

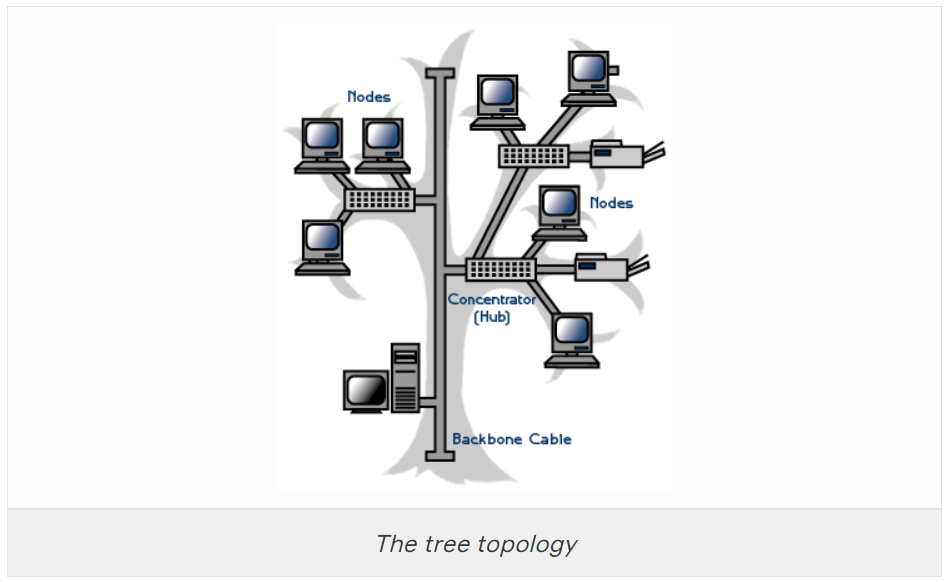
1. The amount of wires required to connected each system is tedious.
2. Since each device needs to be connected with other devices, a number of I/O ports required must be huge.
3. Scalability issues because a device cannot be connected with a large number of devices with a dedicated point to point link.

Q: What is mesh topology?  
A: Mesh topology is a setup wherein each device is connected directly to every other device on the network. Consequently, it requires that each device has at least two network connections.

Q: What is one advantage of mesh topology?  
A: In the event that one link fails, there will always be another available. Mesh topology is actually one of the most fault-tolerant network topology.

### Tree Topology

A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable. Tree topologies allow for the expansion of an existing network.



**Advantages of tree topology:**  
1. It is scalable. Secondary nodes allow more devices to be connected to a central node.  
2. Point to point connection of devices.  
3. Having different levels of network makes it more manageable hence easier fault identification and isolation.

**Disadvantages of tree topology:**  
1. Maintenance of the network may be an issue when the network spans a great area.  
2. Since it is a variation of bus topology, if the backbone fails, the entire network is down.

Point-to-Point Topology

It's the simplest topology where there is a permanent link between two endpoints. These endpoints may be hubs, routers, switches, computers, etc. which give you one communication path. Switched point-to-point topologies are the basic model of conventional telephony. The value of a permanent point-to-point network is unimpeded communications between the two endpoints.

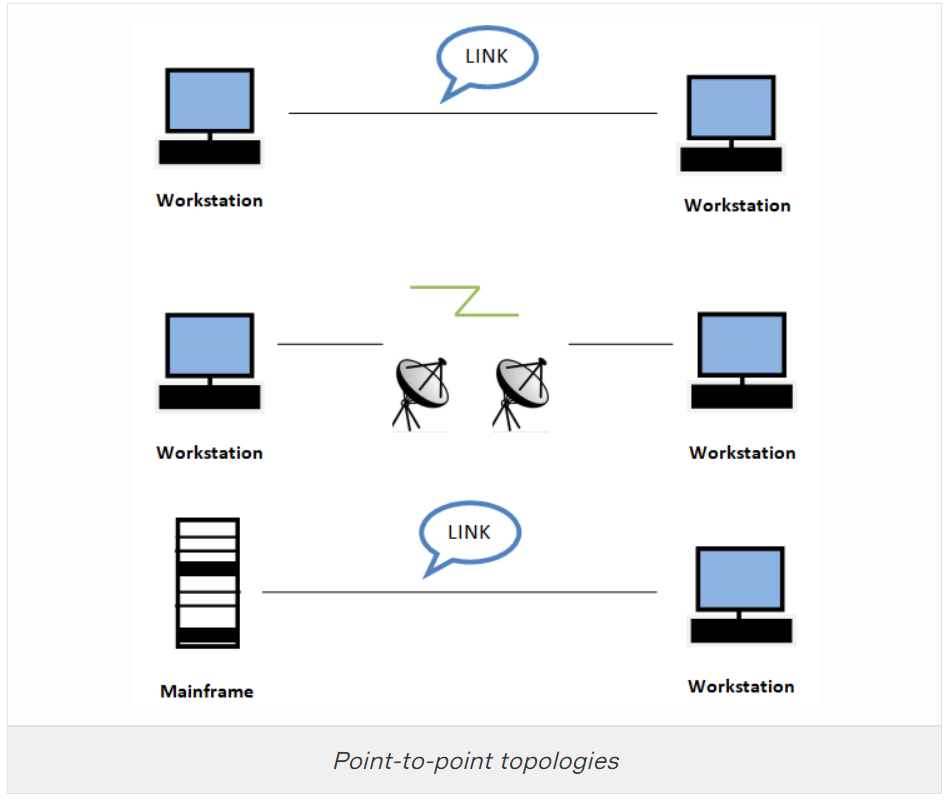
* **Permanent (dedicated)**

Easiest to understand, of the variations of point-to-point topology, is a point-to-point communications channel that appears, to the user, to be permanently associated with the two endpoints. A children’s tin can telephone is one example of a physical dedicated channel.

Within many switched telecommunications systems, it is possible to establish a permanent circuit. One example might be a telephone in the lobby of a public building, which is programmed to ring only the number of a telephone dispatcher. “Nailing down” a switched connection saves the cost of running a physical circuit between the two points. The resources in such a connection can be released when no longer needed.

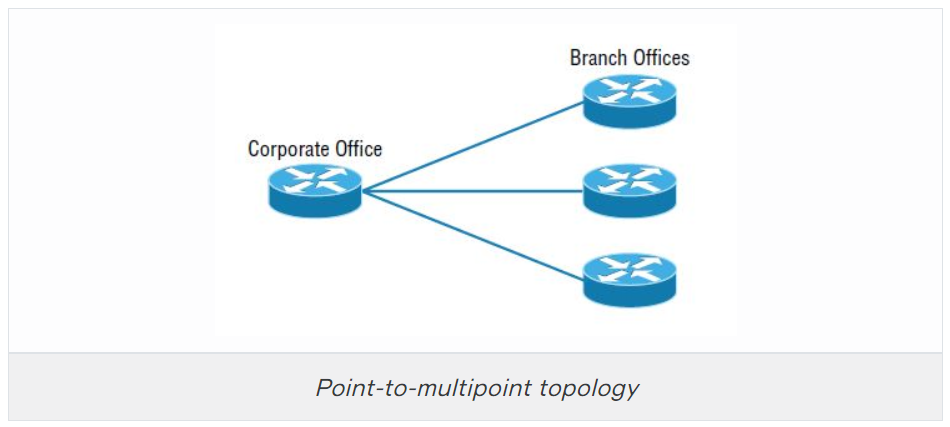
* **Switched**

Using circuit-switching or packet-switching technologies, a point-to-point circuit can be set up dynamically and dropped when no longer needed. This is the basic model of conventional telephony.

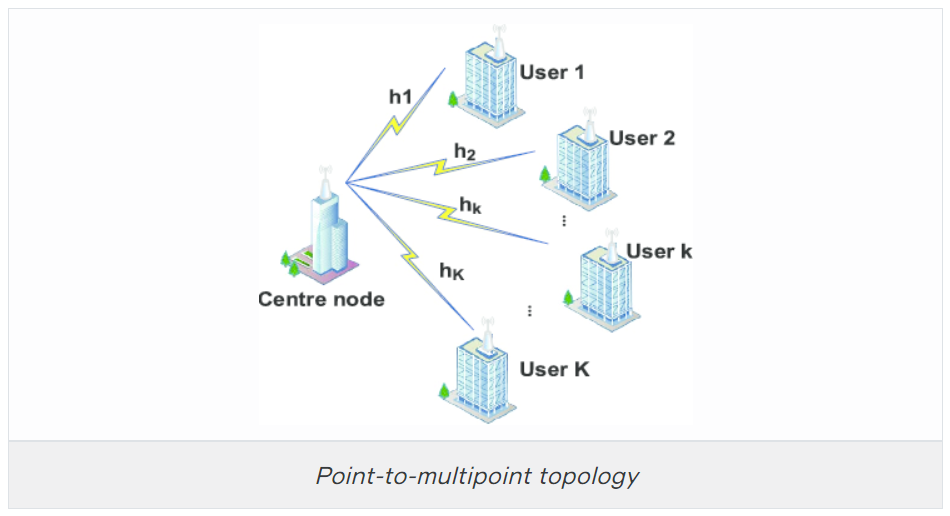


### Point-to-Multipoint Topology

A **point-to-multipoint** topology consists of a succession of connections between an interface on one router and multiple destination routers—one point of connection to multiple points of connection. Each of the routers and every one of their interfaces involved in the point-to-multipoint connection is part of the same network.

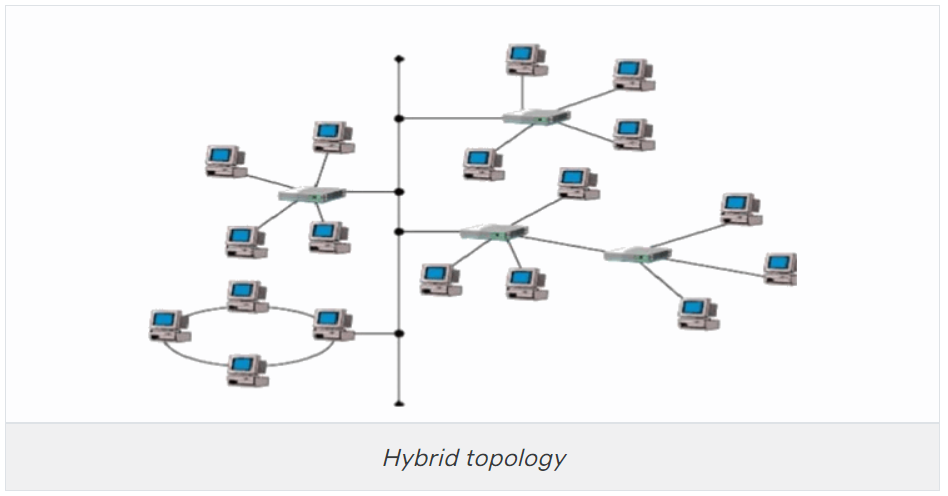


The below figure shows another prime example of a point-to-multipoint network: a college or corporate campus.



### Hybrid Topology

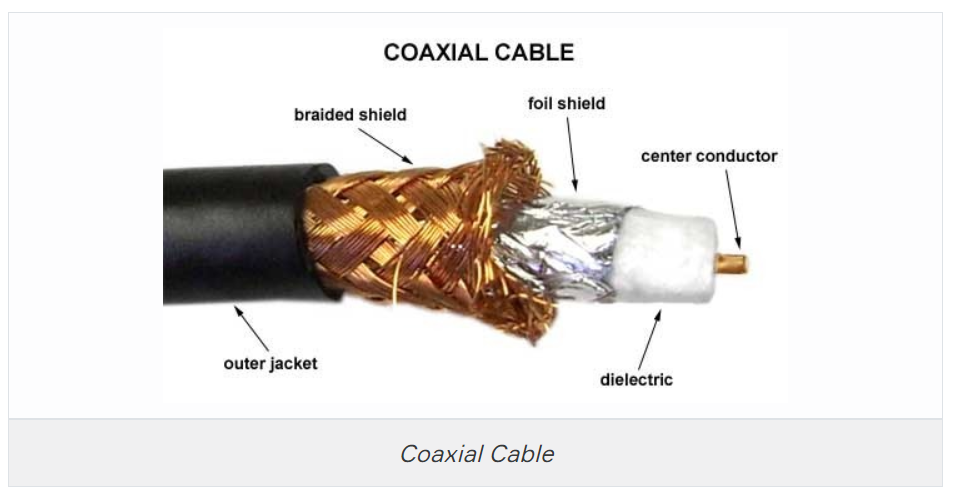
**Hybrid topology** means just that—a combination of two or more types of physical or logical network topologies working together within the same network.



## **Physical Media**

### Coaxial Cable

**Coaxial cable** is a type of copper cable specially built with a metal shield and other components engineered to block signal interference. Thus, coaxial cable shields data transmissions from electromagnetic interference (EMI). It is primarily used by cable TV companies to connect their satellite antenna facilities to customer homes and businesses and also to connect a cable modem to an Internet service provider (ISP). This connection enables a computer to access the Internet. It is also sometimes used by telephone companies to connect central offices to telephone poles near customers.



The cable is named as coaxial because the central copper wire and the braided metal shield share a common axis or centerline. The metal wire is generally covered sequentially from center to outside by insulation (dielectric), foil shield, braided metal shield, and jacket layers. The outer channel serves as a ground. 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.

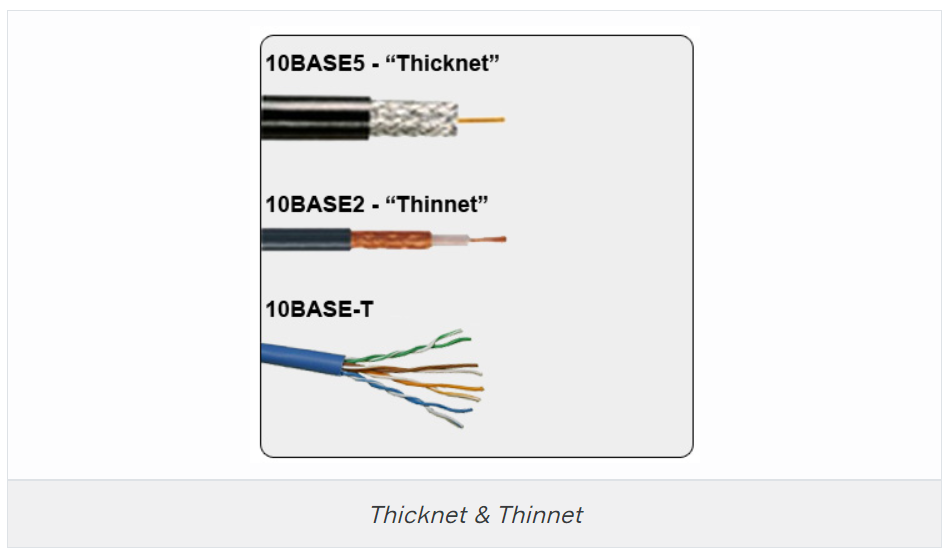
**Advantages of coaxial cable**

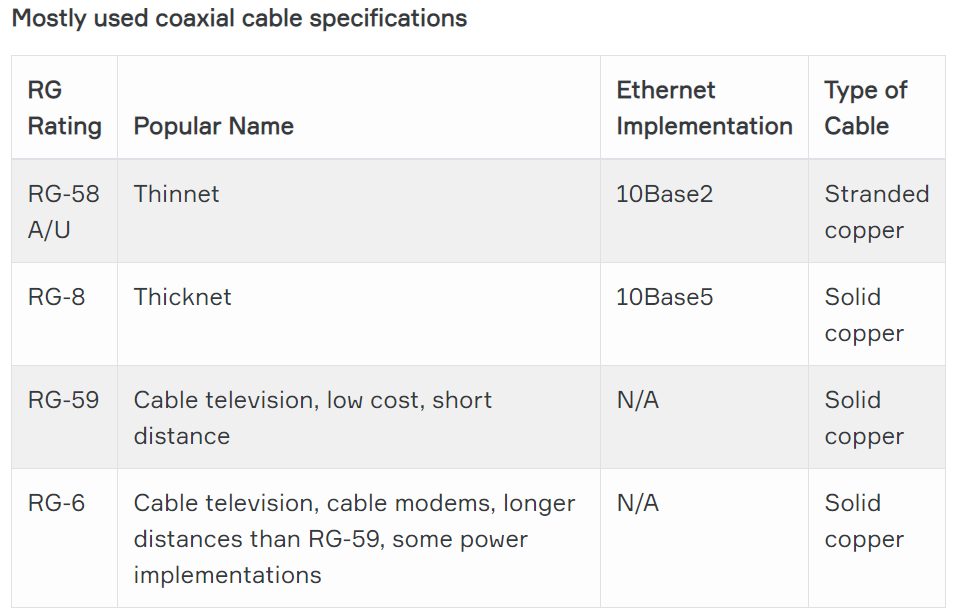
* Inexpensive
* Easy to wire and install
* Easy to expand
* Good resistance to EMI (Electromagnetic Interference)
* Up to 10Mbps capacity
* Durable

Another **benefit** of coaxial cable that it can be installed next to metal objects without losing power, unlike other types of transmission lines.

The main **disadvantage** of using the coaxial cable is that single cable failure can take down an entire network.

**Thin Ethernet** (also referred to as *Thinnet* or *10Base2*) and **Thick Ethernet** (also referred to as *Thicknet* or *10Base5* are coaxial cable types. They have the same properties except for the thickness of the cables is different. (Thinnet is only about 5 mm, or 2/10″, diameter coaxial cable).

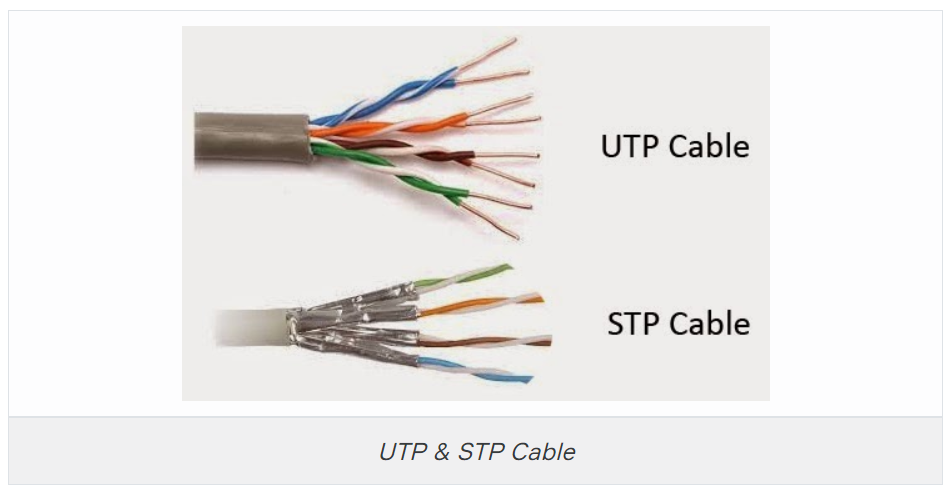




Twisted-Pair Cable

A **twisted-pair** cable is a type of cable made by putting two separate insulated wires together in a twisted pattern and running them parallel to each other. This type of cable is widely used in different kinds of data and voice infrastructures.

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*.



In general, twisted-pair cabling may be preferred over a common alternative, coaxial cable, for different reasons. Coaxial cable involves a single, thicker wire. 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 cables are rated by industry standards including ISO/EIC and EIA/TIA.

Ethernet cable types are described using a code that follows this format:

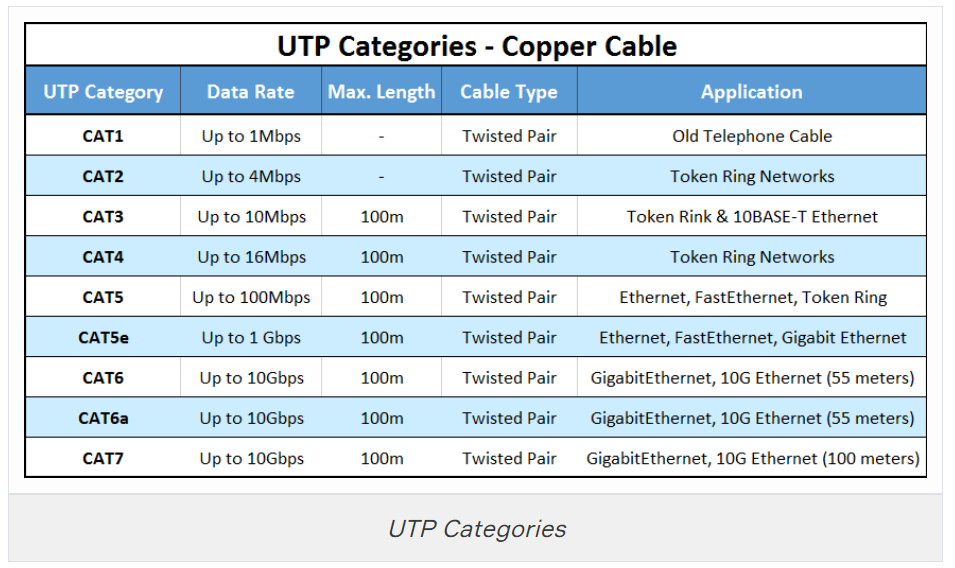
**N <Signaling> X**.

The **N** refers to the *signaling rate in megabits per second*. **<Signaling>** stands for the *signaling type*—either baseband or broadband *(will be discussed in the following lessons)*—and the **X** is a *unique identifier* for a specific Ethernet cabling scheme.

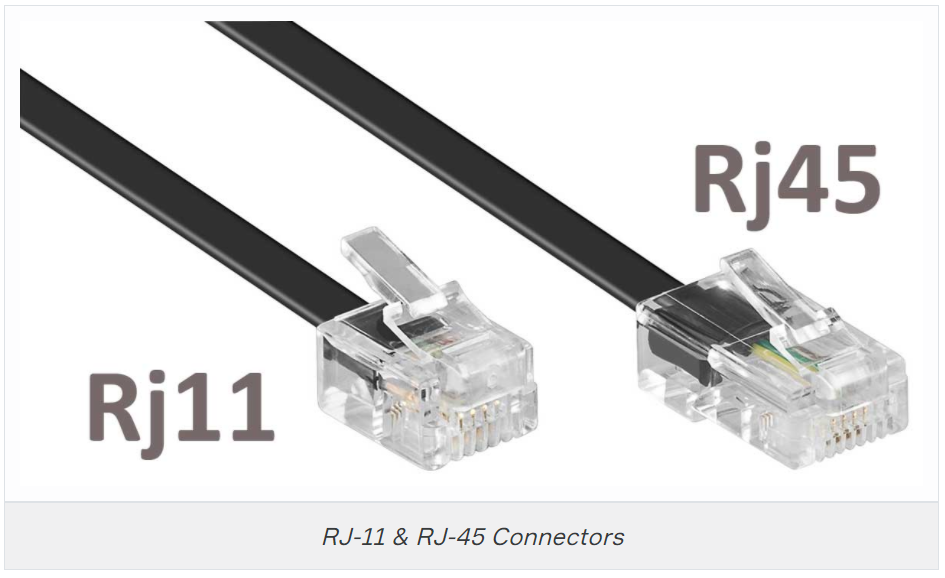
Here’s a common example: 100BaseX. The 100 tells us that the transmission speed is 100 Mb or 100 megabits. The X value can mean several different things; for example, a T is short for twisted-pair. This is the standard for running 100-megabit Ethernet over two pairs (four wires) of Category 5, 5e, or 6 UTP.

So why are the wires in this cable type twisted? Because when electromagnetic signals are conducted on copper wires in close proximity—like inside a cable—it causes interference called crosstalk. Twisting two wires together as a pair minimizes interference and even protects against interference from outside sources. This cable type is the most common today for the following reasons:

* It’s cheaper than other types of cabling.
* It’s easy to work with.
* It allows transmission rates that were impossible 10 years ago.



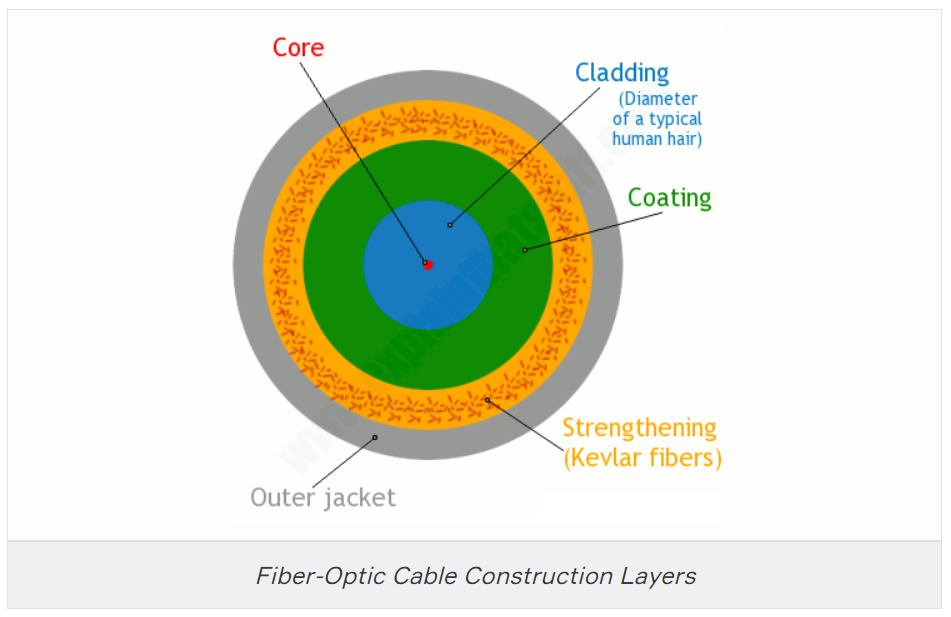
**BNC connectors** won’t fit very well on *UTP cable*, so a **registered jack (RJ)** connector should be used. The connector used with UTP cable is called **RJ-11** for phones that use four wires; **RJ-45** has four pairs (eight wires), as shown in the below figure.



Fiber-Optic Cable

**Optical fiber** is a very thin strand of pure glass that acts as a waveguide for light over long distances. It uses a principle known as *total internal reflection*.

Fiber optic cable is actually composed of two layers of glass: The **core** which is thinner than hair *carries the actual light signal*, and the **cladding** is a *layer of glass surrounding the core*. Most fibers operate in duplex pairs: one fiber is used to transmit and the other is used to receive. But it is possible to send both signals over a single strand.



Because fiber-optic cable transmits digital signals using light impulses rather than electricity, it’s **immune to EMI and RFI**. Fiber cable allows light impulses to be carried on either a glass or a plastic core. Glass can carry the signal a *greater distance*, but plastic *costs less*.

Although fiber-optic cable may sound like the solution to many problems, it has advantages and disadvantages just like the other cable types.

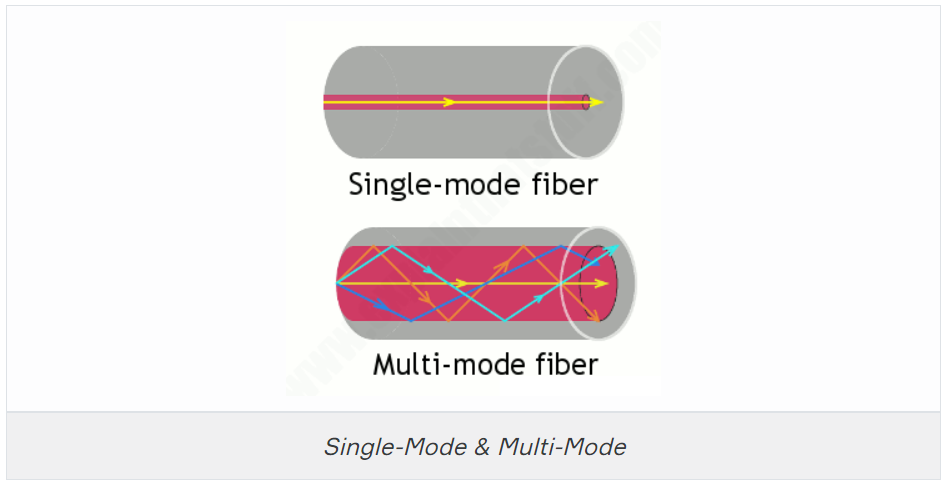
Here are the advantages:

* It’s completely immune to EMI and RFI.
* It can transmit up to 40 kilometers (about 25 miles).
* It has high carrying capacity (very broad bandwidth, THz or Tbits/s)
* It has very low transmission losses (<0.2dB/km, cf1dB/km microwave, 10db/km twisted copper pair)
* It does not produce heat

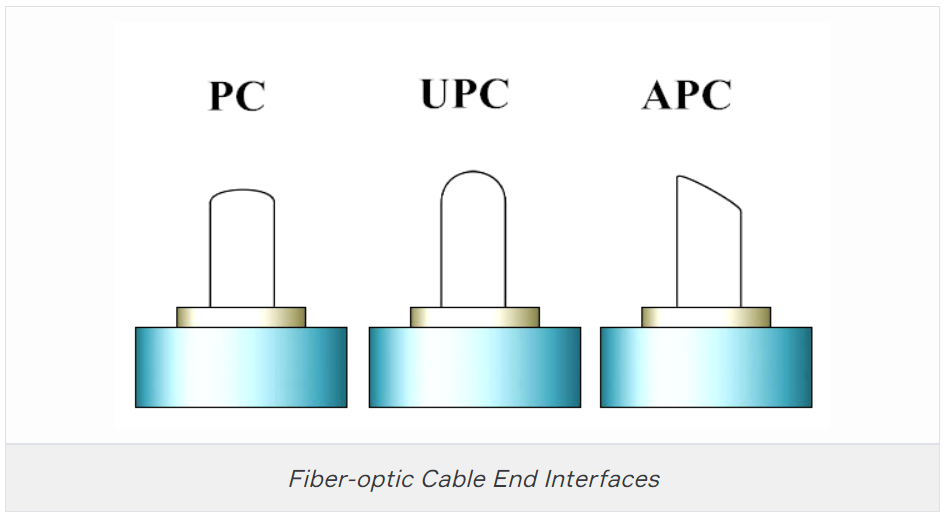
And here are the disadvantages:

* It’s difficult to install.
* It’s more expensive than twisted-pair.
* Troubleshooting equipment is more expensive than twisted-pair test equipment.
* It’s harder to troubleshoot.

There are two main types of fiber optic cables: **Single-Mode Fiber (SMF)** and **Multi-Mode Fiber (MMF)**. The difference is basically in the *size of the core*. **MMF** has a much wider core, allowing multiple modes (or “rays”) of light to propagate. **SMF** has a very narrow core which allows only a single mode of light to propagate. Each type of fiber has different properties with its own advantages and disadvantages.



Fiber optic cables have mainly 2 types of cable end interfaces. **Angled Physical Contact (APC)** and **Ultra Physical Contact (UPC)** (and there is also Physical Contact (PC) that is similar to UPC).

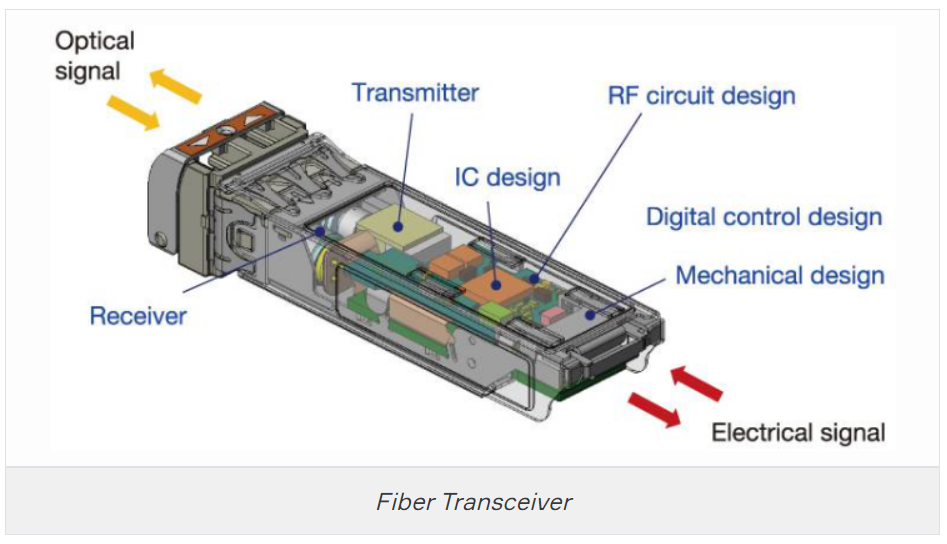


A whole bunch of different types of *connectors* are available to use with fiber-optic cables, but the two most popular are the **straight tip (ST)** and the **subscriber (or square) connector (SC)**.Formun Üstü

### Transceivers

A **transceiver (TRX)** is a device that can transmit and receive signals. Usually, a transceiver contains both a transmitter and a receiver, both of which share common circuitry. However, if the transmitter and receiver only share a common housing and nothing else, the device is called a **transmitter-receiver**. Transceivers are extremely important in the history of technology, as they have paved the way for many inventions such as two-way radios, mobile phones, and the internet.

Alıcı-verici (TRX), sinyalleri iletebilen ve alabilen bir cihazdır. Genellikle bir alıcı-verici, her ikisi de ortak devreyi paylaşan hem bir verici hem de bir alıcı içerir. Bununla birlikte, verici ve alıcı yalnızca ortak bir muhafazayı paylaşır ve başka hiçbir şeyi paylaşmazsa, cihaza verici-alıcı denir. Alıcı-vericiler, iki yönlü telsizler, cep telefonları ve internet gibi birçok icadın önünü açtıkları için teknoloji tarihinde son derece önemlidir.



Transceivers can be found in radio technology, telephony as well as Ethernet in which transceivers are called **Medium Attachment Units (MAUs)**.

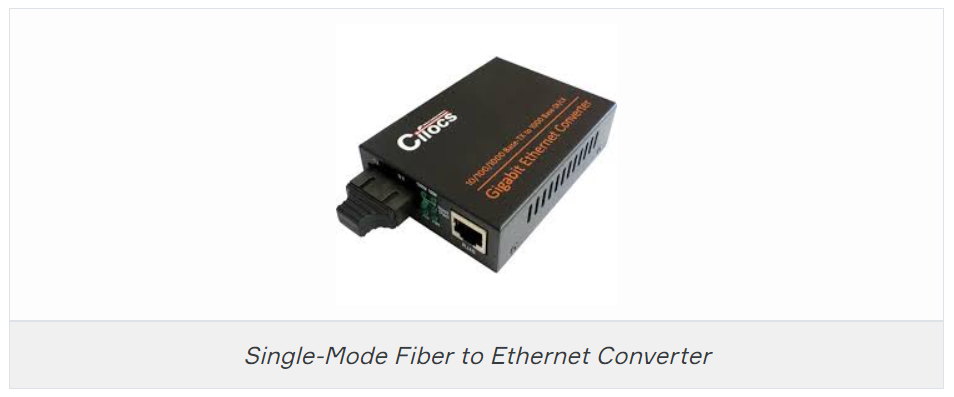
The **small form-factor pluggable (SFP)** is a *compact, hot-pluggable* optical module transceiver used for both *telecommunication* and *data communications* applications.

**The Quad Small Form-factor Pluggable (QSFP)** is another compact, hot-pluggable transceiver used for data communications applications. It interfaces networking hardware (such as servers and switches) to a fiber optic cable or active or passive electrical copper connection.

Media Converters

Sometimes, you’ll need to convert from one media type to another. Maybe you need to go from one mode of fiber to another mode, or in an even more extreme case, you need to go from fiber to Ethernet. If you’re faced with situations like these, you’ll need to be familiar with some of the more common media converters:

* **Single-Mode Fiber to Ethernet** - These devices accept a fiber connector and an Ethernet connector and convert the signal from Ethernet and single-mode fiber.



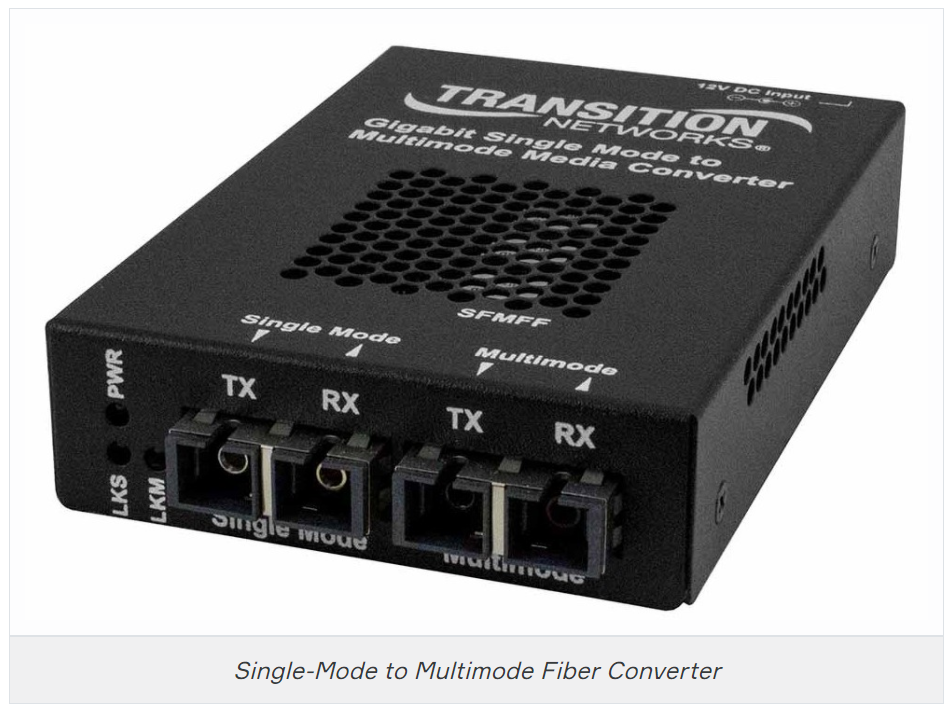
**Multimode Fiber to Ethernet** - These devices accept a fiber connector and an Ethernet connector and convert the signal from Ethernet and multi-mode fiber.



**Fiber to Coaxial** - These devices accept a fiber connector and a coaxial connector and convert digital signals from optical to coax.



**Single-Mode to Multimode Fiber** - These devices accept a single-mode fiber connector and a multimode fiber connector and convert the signals between the two.



### Transmission Speeds

Network administrators can control the speed of a network to meet the network’s traffic demands based on the selected cable or fiber type and the network topology.

Admins usually permit or would like to have, transmission speeds of up to 10 Gbps or higher on the core areas of their networks that connect various network segments. In the distribution and access areas, where users connect to switches, it’s typically 100 Mbps per connection, but transmission speeds are creeping up because the traffic demand is getting higher.

### Distance

Decision factors used in choosing what type of cable to use often come down to the topology of a network and the distance between its components. Some network technologies can run much farther than others without communication errors, but all network communication technologies are prone to attenuation—the degradation of a signal due to the medium itself and the distance signals have to travel. Some cable types suffer from attenuation more than others. For instance, any network using twisted-pair cable should have a maximum segment length of only 328 feet (100 meters).

### Duplex

All communications are either **half-duplex** or **full-duplex**. The difference is whether the communicating devices can “talk” and “listen” at the same time.

During **half-duplex** communication, a device can either send communication or receive communication, but not both at the same time. Think walkie-talkie—when you press the button on the walkie-talkie, you turn the speaker off and you can’t hear anything the other side is saying.

In **full-duplex** communication, both devices can send and receive communication at the same time. This means that the effective throughput is doubled and communication is much more efficient. Full duplex is typical in most of today’s switched networks. We'll discuss full and half-duplex in more detail in the section “The Current Ethernet Specifications.”

Frequency

Each cable type has a specified maximum frequency that gives you the transmission bandwidth it can handle. Cat5e cable is tested to 100 MHz maximum frequency and can run 1 Gbps signals for relatively short distances. That’s maxing it out, but it’s still good for connecting desktop hosts at high speeds. On the other hand, Cat6 is a 250 MHz cable that can handle 1 Gbps data flow all day long with ease. Cat 6 has a lot more twists and thicker cables, so it’s best used when connecting floors of a building.

**💡Tips:**

* Although a signal is measured as **bandwidth**, the capacity to carry the signal in a cable is measured as **frequency**.

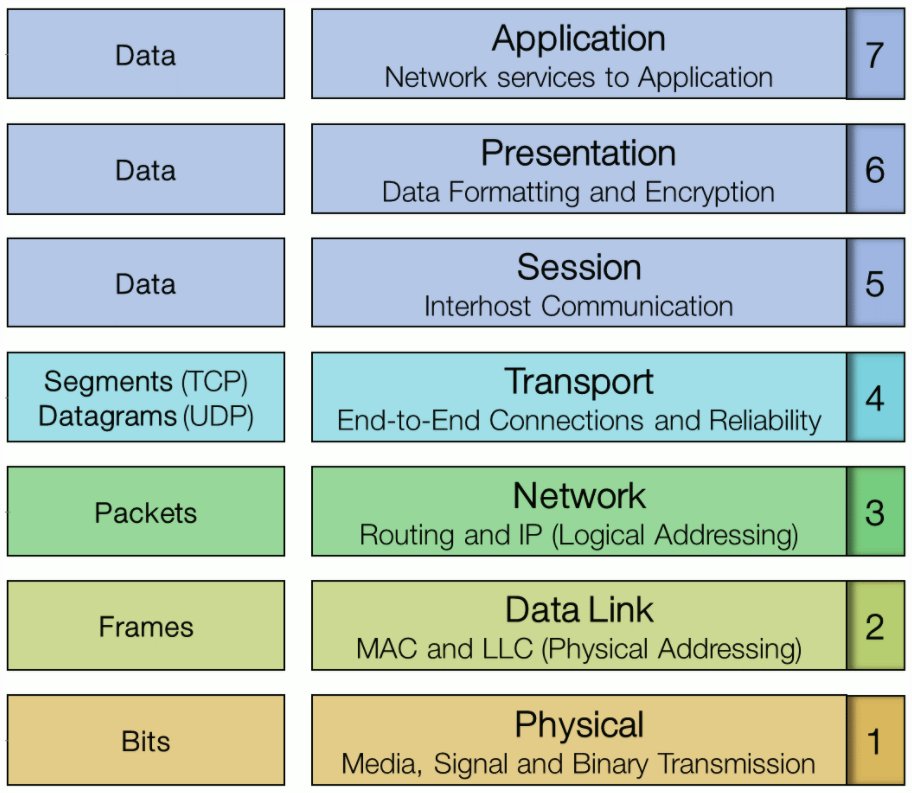
## **The OSI Reference Model**

### What is the OSI Reference Model?

**OSI Model** stands for the Open System Interconnection model. **OSI Model** defines how **data is transferred** from one computer to another computer regardless of the operating system or vendor of the hardware.

In a very basic scenario, two computers connected with a LAN and transfer data using the Network Interface Card (NIC or Network Adapter). This forms a computer network, however, if both systems use different operating systems, for example, one system runs on Windows and the other one runs on macOS then how can data be exchanged between these two different systems? Here comes the role of an OSI model which is a seven-layered model that defines how data can be exchanged between different systems.

OSI model was introduced by the International Organisation for standardization (ISO) in 1984. There are seven layers in an OSI model.



As the complexity of computer hardware and software increases, the problem of successfully communicating between these systems becomes more difficult. Dividing these difficult problems into "sub-tasks" allows them to be readily understood and solved more easily. Using this layered approach means that a vendor can work on the design and debugging for a particular layer without affecting any of the others.

Each layer performs a different group of tasks required for network communication. Although not all network systems implement layers using this structure, they all implement each task in some way. The OSI model is not a standard or a specification; it serves as a **functional guideline** for designing network protocols, software, and appliances and for troubleshooting networks.

The OSI’s seven layers are divided into two groups. The top three layers (**upper layers**) define the rules of how the applications working within host machines communicate with each other as well as with end-users. The bottom four layers (**lower layers**) define how the actual data is transmitted from end to end.

Advantages of OSI Reference Model

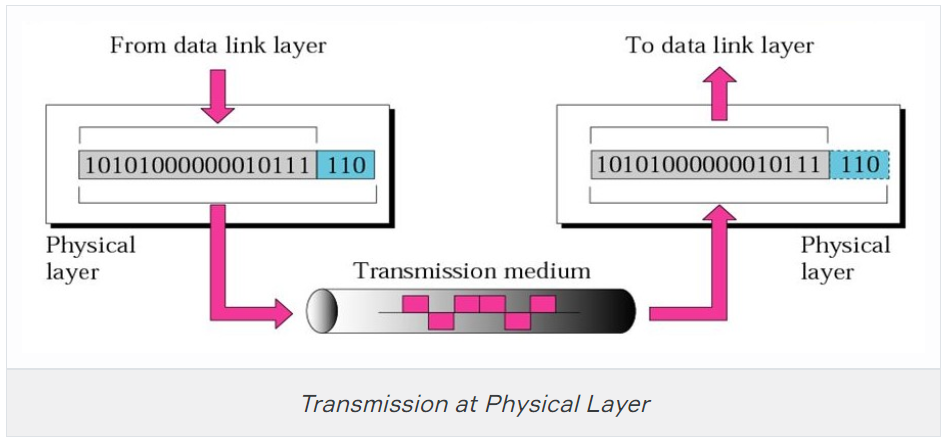
The OSI model is hierarchical. Understand that the central purpose of the OSI, and all networking models, is to allow different vendors’ networks to interoperate smoothly. This short-list depicts some of the most important advantages we gain by using the OSI layered model:

* The OSI model divides network communication processes into smaller and simpler components, thus aiding component development, design, and troubleshooting.
* It allows multiple-vendor development through the standardization of network components.
* It encourages industry standardization by defining the specific functions that occur at each layer of the model.
* It allows various types of network hardware and software to communicate.
* It prevents changes in one layer from affecting other layers, facilitating development and making application programming much easier.

1-Physical Layer

The physical layer of the OSI model (layer 1) is responsible for the transmission and receipt of bits from one node to another node. It specifies the following:

* Physical network topology - mechanical specifications for the network medium, such as cable specifications, the medium connector and pin-out details (the number and functions of the various pins in a network connector), or radio transceiver specifications.
* The process of transmitting and receiving signals from the network medium including modulation schemes and timing/synchronization.

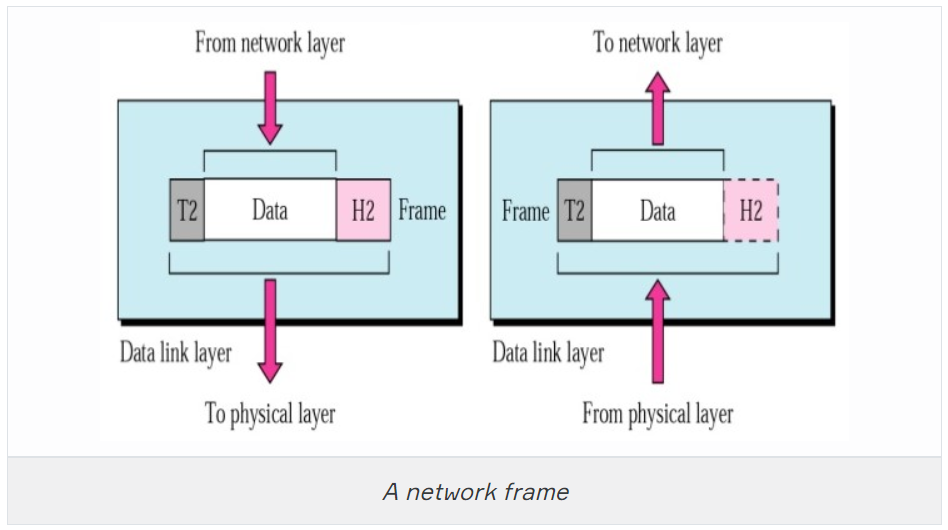


Devices operating at the physical layer include:

* **Transceiver** - the part of a network interface that sends and receives signals over the network media.
* **Media Converter** - converts one media signaling type to another.
* **Repeater** - amplifies the signal to extend the maximum allowable distance for a media type.
* **Hub** - a multiport repeater, deployed as the central point of connection for nodes wired in a star topology.
* **Modem** - a device that converts between digital and analog signal transmissions.

### 2-Data Link Layer

The data link layer (layer 2) is responsible for transferring data between nodes on the same network segment. The data link layer splits the message into pieces, each called a data frame, and adds a customized header. This header contains a source and destination hardware (MAC) address and error checking values. Other information includes the frame length and network layer protocol identifier.



Some network products use multiple different frame types. For example, Ethernet specifies four frame types. The basic structure remains the same but each frame type contains a slightly different header structure. Devices must communicate using the same frame type.

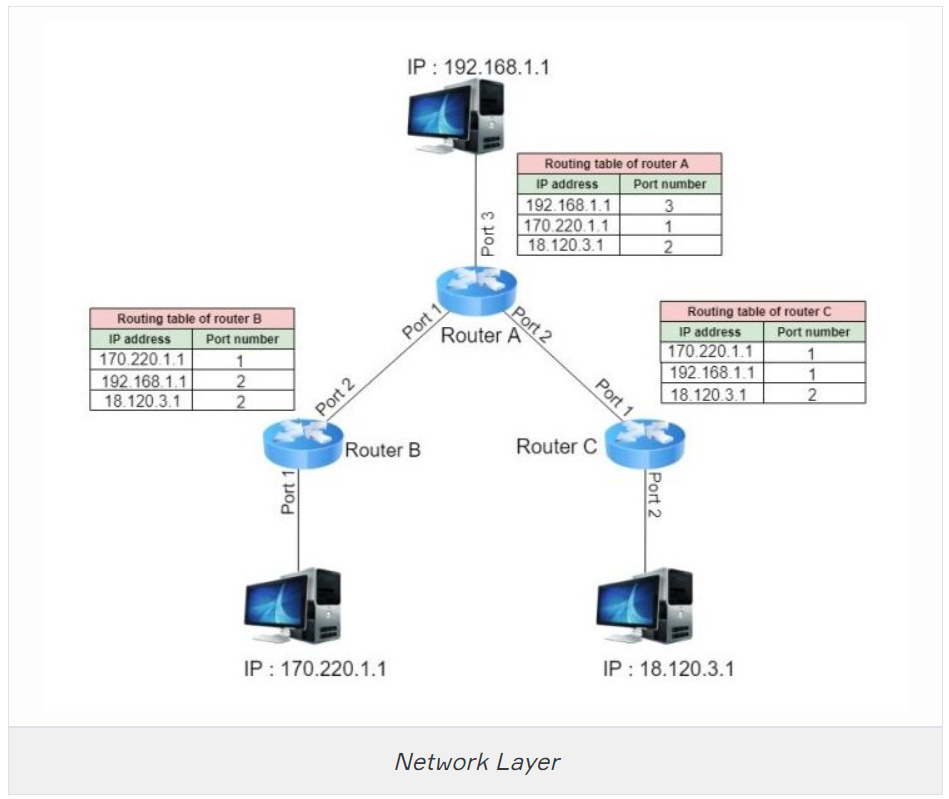
The last part of the frame usually contains some sort of error checking. Protocols at almost every layer perform a consistency check to verify that data has been transferred correctly. The data link layer is only capable of very basic error checking, such as identifying truncated or corrupted frames. There is no function to acknowledge or retransmit damaged frames. That function is handled at higher layers of the OSI model.

Connectivity devices found at the data link layer include:

* **Network adapter (or Network Interface Card [NIC])** - joins a host computer to network media (cabling or wireless) and enables it to communicate over the network by assembling and disassembling frames.
* **Bridge** - joins two network segments while minimizing the performance reduction of having more nodes on the same network.
* **Basic switch** - a multiport bridge that creates links between nodes more efficiently.
* **Wireless Access Point (AP)** - allows nodes with wireless network cards to communicate and joins wireless networks to wired ones.

### 3-Network Layer

The network layer (layer 3) is responsible for moving data around a network of networks, known as an internetwork or internet. While the data link layer moves data using hardware addresses within a single network segment, the network layer moves information around an internetwork using a logical network and host IDs.



The network layer transfers information between networks by examining the destination network layer address or logical network address and routing the packet through the internetwork using intermediate systems (routers). The packet moves, hop by hop, through the internetwork to the target network. Once it has reached the destination network, the hardware address can be used to move the packet to the target node. This process requires each logically separate network to have a unique network address.

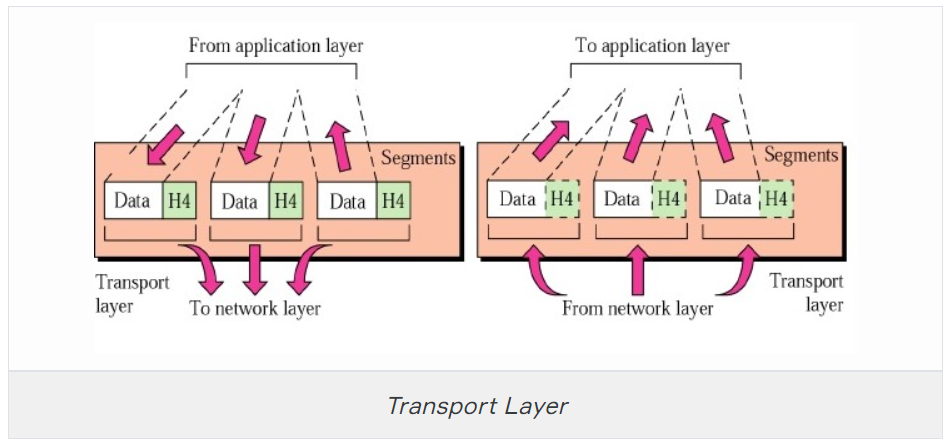
The main appliance working at layer 3 is the router. Other devices include Layer 3 switches (combining the function of switches and routers) and basic firewalls.

### 4-Transport Layer

The first three layers of the OSI model are primarily concerned with moving frames and datagrams between nodes and networks. At the transport layer (also known as the end-to-end or host-to-host layer) the content of the packets starts to become significant.

Any given host on a network will be communicating with many other hosts using many different types of networking data. One of the critical functions of the transport layer is to identify each type of network application by assigning it a port number. For example, data from the HTTP web browsing application can be identified as port 80 while data from an email server can be identified as port 25.

At the transport layer, on the sending host, data from the upper layers are packaged as a series of segments and each segment is tagged with the application's port number. The segment is then passed to the network layer for delivery. The host could be transmitting multiple HTTP and email segments at the same time.



At the network and data link layers, the port number is not significant - it becomes part of the data payload and is "invisible" to routers and switches working at the network and data link layers. At the receiving host, each segment is extracted from its frame and then identified by its port number and passed up to the relevant handler at the upper session and application layers.

The transport layer is also responsible for ensuring reliable data delivery so that packets arrive error-free and without loss. The transport layer can overcome any lack of reliability in the lower level protocols. This reliability is achieved using **acknowledgment** messages that inform the sender the data was successfully received. The kinds of problems that may occur during the delivery of the data are non-delivery and delivery in a damaged state. In the first case, the lack of acknowledgment results in the retransmission of the data and, in the second case, a **Negative Acknowledgement (NACK)** forces retransmission.

Devices working at the transport layer (or above) include multilayer switches and security appliances such as more advanced firewalls and Intrusion Detection Systems (IDS).

### 5-Session Layer

Most application protocols require the exchange of multiple messages between the client and the server. This exchange of such a sequence of messages is called a **session** or **dialog**. The session layer (layer 5) represents the dialog control functions that administer the process of establishing the dialog, managing data transfer, and then ending (or "tearing down") the session.



Sessions can work in three modes:

* **One-way/simplex** - only one system is allowed to send messages; the other receives only.
* **Two-Way Alternate (TWA)/half-duplex** - the hosts establish some system for taking turns to send messages, such as exchanging a token.
* **Two-Way Simultaneous (TWS)/duplex** - either host can send messages at any time.

The session layer can also provide a synchronization service for long transactions in which checkpoints are inserted into the data stream (dialog separation). If a problem occurs, only the data transferred after the last checkpoint is re-sent.

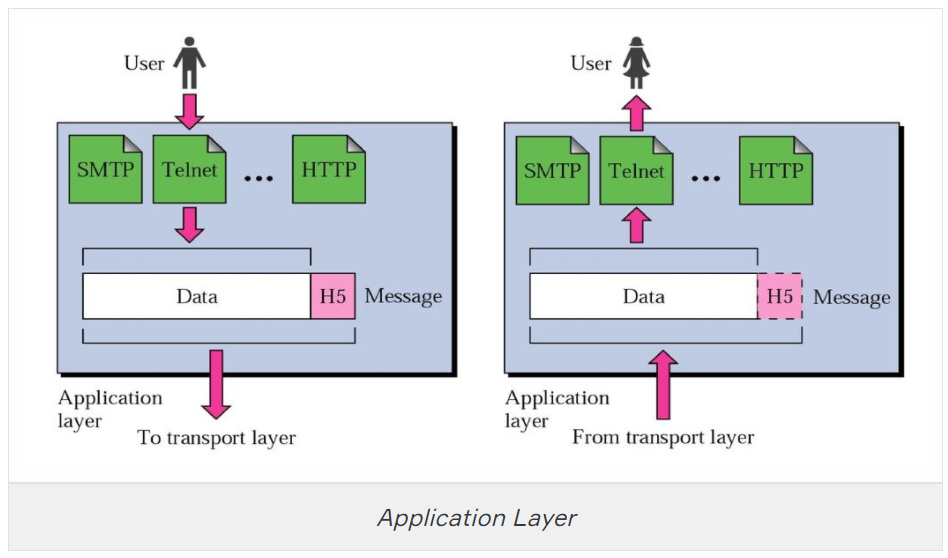
In summary, this layer primarily manages applications’ data by separating from each other application. For instance, multiple web browser sessions at the same time on your desktop are handled by the help of session layer.

### 6-Presentation Layer

The presentation layer (layer 6) transforms data between the format required for the network and the format required for the application. For example, the presentation layer is used for character set conversion. The communicating computers may use different character coding systems (such as American Standard Code for Information Interchange [ASCII] and Unicode); the peer presentation layers agree to translate the data into one of the formats or they will both translate the data into a third format. The presentation layer can also be conceived as supporting data compression and encryption (scrambling a message so that it can only be read in conjunction with a valid "key"). However, in practical terms, these functions are often implemented by encryption devices and protocols running at lower layers of the stack.

### 7-Application Layer

The application layer (layer 7) is at the top. An application layer protocol doesn’t encapsulate any other protocols or provide services to any protocol. An application layer protocol provides an interface for software applications on network hosts that have established a communication channel using the lower-level protocols to exchange data. For example, one of the most utilized services provided by the application layer is file transfer. Different file systems may use entirely different file naming conventions and data syntax and the application layer must overcome these differences. More widely, upper-layer protocols provide most of the services that make a network useful, rather than just functional, including network printing, electronic mail and communications, directory lookup, and database services.



It is important to distinguish between network application protocols and the software application code (programs and shared programming libraries) that run on computers. Software programs and operating systems make use of the Application Programming Interface (API) to call functions of the relevant part of the network stack. Examples of APIs include:

* Network card drivers could use the Network Driver Interface Specification (NDIS) API to implement functions at the data link layer.
* The Sockets / WinSock APIs implement transport and session layer functions.
* High-level APIs implement functions for services such as file transfer, email, web browsing, or name resolution.

### Summary

### 

### Data Encapsulation

When a host transmits data across a network to another device, the data goes through **encapsulation**: It’s wrapped with protocol information at each layer of the OSI model. Each layer communicates only with its peer layer on the receiving device.

To communicate and exchange information, each layer uses **Protocol Data Units (PDUs)**. These hold the control information attached to the data at each layer of the model. They’re usually attached to the header in front of the data field but can also be in the trailer, or end, of it.

Each **PDU** attaches to the data by encapsulating it at each layer of the OSI model, and each has a specific name depending on the information provided in each header. This PDU information is read-only by the peer layer on the receiving device. After it’s read, it’s stripped off, and the data is then handed to the next layer up.

The below figure shows the PDUs and how they attach control information to each layer. This figure demonstrates how the upper-layer user data is converted for transmission on the network. The data stream is then handed down to the Transport layer, which sets up a virtual circuit to the receiving device by sending over a synch packet. Next, the data stream is broken up into smaller pieces, and a Transport layer header (a PDU) is created and attached to the header of the data field; now the piece of data is called a segment. Each segment is sequenced so the data stream can be put back together on the receiving side exactly as it was transmitted.

### 

In summary, at a transmitting device, the data-encapsulation method works like this:

1. User information is converted to data for transmission on the network.
2. Data is converted to segments, and a reliable connection is set up between the transmitting and receiving hosts.
3. Segments are converted to packets or datagrams, and a logical address is placed in the header so each packet can be routed through an internetwork.
4. Packets or datagrams are converted to frames for transmission on the local network. Hardware (Ethernet) addresses are used to uniquely identify hosts on a local network segment.
5. Frames are converted to bits, and a digital encoding and clocking scheme is used.

Q: What is data encapsulation?  
A: Data encapsulation is the process of breaking down information into smaller manageable chunks before it is transmitted across the network. These chunks are wrapped with protocol information at each layer of the OSI model. In this process, the source and destination addresses are attached into the headers, along with parity checks.

Formun Altı