WHAT IS NETWORK ARCHITECTURE?

the way network devices and services are structured to serve the connectivity needs of client devices. Network devices typically include switches and routers.

how computers are organized in a system and how tasks are allocated between these computers. Two of the most widely used types of network architecture are peer-to-peer and client/server. Client/server architecture is also called 'tiered' because it uses multiple levels.

What are the kinds of network architecture?



Types of Networking Architecture  
  
While there are myriads ways to design your network architecture, you'll find that most fall into one of two types. These are the **peer-to-peer and client/server architectures**. In a peer-to-peer model, all devices in a network have equal responsibilities and privileges with each other.

**Network architecture** is the design of a [computer network](https://en.wikipedia.org/wiki/Computer_network). It is a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as [communication protocols](https://en.wikipedia.org/wiki/Communication_protocol) used.

In [telecommunication](https://en.wikipedia.org/wiki/Telecommunication), the specification of a network architecture may also include a detailed description of products and services delivered via a communications network, as well as detailed rate and billing structures under which services are compensated.

The network architecture of the [Internet](https://en.wikipedia.org/wiki/Internet) is predominantly expressed by its use of the [Internet protocol suite](https://en.wikipedia.org/wiki/Internet_protocol_suite), rather than a specific model for interconnecting networks or nodes in the network, or the usage of specific types of hardware links.

What is Network Architecture? And, How Does It Work?

There is infinite knowledge sitting in the palm of our hands. With a few swipes, we can log on to any website and get the information we want in seconds. It’s so convenient that we often take for granted the complex and incredible mechanisms – the wires, cables, and servers – that make it all possible.

This is what network architecture is all about. It’s how data flows efficiently from one computer to another. And for businesses with an online component, it’s an important concept that has a significant impact on their operation. Let’s start with the networking architecture definition.

There are many ways to approach network architecture design, which depend on the purpose and size of the network. Wide area networks (WAN), for example, refer to a group of interconnected networks often spanning large distances. Its network architecture will be vastly different from that of a local area network (LAN) of a smaller office branch.

Planning the network architecture is vital because it either enhances or hinders the performance of the entire system. Choosing the wrong transmission media or equipment for a particular expected server load, for instance, can cause slowdowns on the network.

Network architecture can also facilitate security, becoming increasingly important as more user devices connect to the network. The design and protocols of the network need to support quick and efficient user recognition and authorization.

Most network architectures adopt the Open Systems Interconnection Model or OSI. This conceptual model separates the network tasks into seven logical layers, from lowest to highest abstraction.

The Physical layer, for instance, deals with the wire and cable connections of the network. The highest layer, the Application layer, involves APIs that deal with application-specific functions like chat and file sharing.

The OSI model makes it easier to troubleshoot the network by isolating problem areas from each other.

Network Architecture Design

The design of any digital network architecture involves optimizing its building blocks. These include:

* **Hardware**  
  These are the equipment that forms the components of a network, such as user devices (laptops, computers, mobile phones), routers, servers, and gateways. So, in a way, the goal of any network architecture is to find the most efficient way to get data from one hardware point to another.
* **Transmission Media**  
  Transmission media refers to the physical connections between the hardware devices on a network. Different media have various properties that determine how fast data travels from one point to another.

They come in two forms: wired and wireless. Wired media involve physical cables for connection. Examples include coaxial and fiber optic. Wireless media, on the other hand, relies on microwave or radio signals. The most popular examples are WiFi and cellular.

* **Protocols**  
  Protocols are the rules and models that govern how data transfers between devices in a network. It’s also the common language that allows different machines in a network to communicate with each other. Without protocols, your iPhone couldn’t access a web page stored on a Linux server.

There are many network protocols, depending on the nature of the data. Examples include the Transmission Control Protocol / Internet Protocol (TCP/IP) used by networks to connect to the Internet, the Ethernet protocol for connecting one computer to another, and the File Transfer Protocol for sending and receiving files to and from a server.

* **Topology**  
  How the network is wired together is just as important as its parts. Optimizing this is the goal of network topology.

Topology is the structure of the network. This is important because factors like distance between network devices will affect how fast data can reach its destination, impacting performance. There are various network topologies, each with strengths and weaknesses.

A star topology, for example, describes a layout where all devices in the network are connected to a central hub. The advantage of this layout is that it’s easy to connect devices to the network. However, if the central hub fails, the whole network goes down.

On the other hand, a bus topology is where all network devices are connected to a single pathway, called the bus. The bus acts like a highway that carries data from one part of the network to the other. While cheap and easy to implement, its performance tends to slow down as more devices are added to the network.

Today, most network architectures use a hybrid topology, combining different topologies to compensate for each individual’s weakness.

Advantages and Disadvantages of Network Architecture

Different network architectures have their pros and cons; and knowing them is the key to picking out the right one for your needs.

Peer-to-peer models are often inexpensive and easy to put up because you don’t need to invest in a powerful server. Theoretically, all you need are network cables or a router, and you’re good to go. It’s also quite robust; if one computer goes down, the network stays up. The distributed nature also lessens or at least spreads out the network load to prevent congestions.

However, peer-to-peer models are harder to manage. Since there’s no centralized hub, you’d need to configure each computer individually to set up, for example, security software. Thus, peer-to-peer networks are also less secure. One hacked computer is all it takes to hijack the network.

Client/server models, on the other hand, are easier to manage because they take on a centralized approach. You can set up access privileges, firewalls, and proxy servers to boost the network’s security. Thus, a client/server setup is best for large networks over larger distances.

The disadvantage of this approach is that a client/server architecture is more expensive to set up, as you need a powerful server to handle the network load. It also requires a dedicated administrator to manage the server, which adds to payroll.

But the biggest con of a client/server model is that the server is a weak link. If the server goes down, the entire network shuts down. Thus, security is often the most robust at and near the server.

Computer Network Architecture Examples

Let’s take a look at how network architecture works in practice. Let’s use a manufacturing company with various locations globally as an example.

Each location, such as a factory, will have its own network. If the manufacturing site uses Internet of Things (IoT) sensors on its equipment, it will most likely use edge computing. These sensors will be connected via WiFi to an edge gateway device or an on-site server. This can also accept user devices on the factory, such as employee workstations and mobile phones.

These mini networks will then be connected to the company’s wide area network (WAN), often using a client/server architecture. Corporate headquarters will often house the central server, although a server on the cloud is also a possibility these days. Regardless, network administrators on HQ can monitor and manage the whole WAN infrastructure.

The enterprise WAN is also connected to the Internet via a broadband connection, courtesy of their service provider.

Network Architecture Starts with the Right Equipment

Protocols and software matter, but the heart of any good network is quality equipment. Regardless of which architecture you choose, trust Fusion Connect to provide you with the best routers, [SD-WAN](https://www.fusionconnect.com/services/connectivity/sd-wan), wireless access points, and other devices to power up your network.

WHAT ARE THE DIFFERENT COMPONENTS OF NETWORK ARCHITECTURE?



In today’s business environment, a network serves as the operational glue holding the company together. It enables communication, collaboration, and data storage. However, if that “glue” isn’t strong, it weakens a company’s infrastructure, endangering critical assets. From remote workstations to personal devices, the multifaceted nature of a network means the threats are ever-evolving. Learn about the different components of network architecture with our informative guide. Discover more here.

**Networks 101**

Two or more computers that communicate to share resources, messages, or exchange files are [considered a network](https://fcit.usf.edu/network/chap1/chap1.htm). A typical example would be two computers sending emails over the network, but networks go beyond exchanging communicative messages to more command-like functions. For example, a wireless printer (a resource) may receive a command from a computer over a network, either with a direct connection or wirelessly. Networks enable shared storage across multiple devices.

Understanding different network types and what they share or store will help assess what potential targets and how a threat actor might conduct an attack. For example, infiltrating a minor network may lead to larger network access. The two most well-known types of networks are a [Local Area Network (LAN)](https://en.wikipedia.org/wiki/Local_area_network) and a [Wide Area Network (WAN)](https://en.wikipedia.org/wiki/Wide_area_network), but more network options have emerged as technology has improved. Below is a quick guide to each type of network.

**Basic Network Types**

**Local Area Networks**

Local area networks cover small geographical areas, such as rooms or buildings. Servers, workstations/desktops, and laptops will be connected via cables or use Wireless Access Points (WAPs).

**Wide Area Networks**

Wide area networks extend between larger geographical swaths, like counties, states, and countries. Generally, WANs rely on transoceanic cabling or satellite uplinks. The equipment infrastructure necessary for WANs is more complex and utilizes many multiplexers, bridges, and routers. However, WANs are not independent of LANs; rather, WANs build off of  LANs and metropolitan networks.

[Assess your Network Security](https://www.rsisecurity.com/managed-security-services/)

**Other Network Types**

Beyond these common types, others include Personal Area Networks (PANs), Metropolitan Area Networks (MANs), Storage Area Networks (SANs), and Campus Area Networks (CANs). It’s important to cover the basic network terminology because many company networks are complex and include a variety of different network types.

**Personal Area Network** – PANs cover very small distances, even less than local networks, and, as the name indicates, are personal to a user. PANs can connect to other devices through Bluetooth, infrared, Near Field Communication (NFC), or a wired connection. PANs are suitable for small file-sharing, such as music.

**Campus Area Network** – CANs join two or more LANs together in a limited area that then forms a larger network. These may be present at college campuses or a company campus/complex.

**Metropolitan Area Network** – MANs span the distances between city government buildings. Connectivity stems from a high-speed connection, such as fiber-optic cables. Thus, city resources are easily shareable within different departmental facilities.

**Storage Area Network** – SANs refer to dedicated, high-speed networks used for data storage. They include multiple switches, servers, and disk arrays. Because of their partitioned nature, SANs offer the benefit of avoiding high-traffic backups that LANs sometimes experience.



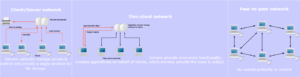
**Network Architecture Options**

The architecture of a network depends on how computers are organized and how tasks are distributed to those devices. A [network architecture](https://www.rsisecurity.com/architecture-implementation/) rendering, often helpful when conducting a threat assessment, may include the transmission equipment, software, and communication protocols, and infrastructure (wired or wireless) that enables devices to communicate and transfer data. The two most common architecture types are Peer-to-Peer (P2P) and tiered, also referred to as client-server. However, thin-client networks are gaining popularity, especially when it comes to securing personal work devices.

**Peer-to-Peer** – This type of architecture treats all devices equally. Tasks are allocated equally without a hierarchy, which is why P2P can also be called a distributed network. Rather than relying on a central server, each computer possesses software enabling communication. One benefit of this arrangement is that if one device fails, others will still maintain the network of communication. Peer-to-peer architecture caters specifically to file sharing.

**Tiered** – In a tiered network, also known as a client-server network, the clients are the computers and the computers depend on the server. The network server(s) manages the data and distributes it based on client requests. Some servers focus on one type of task, such as email or printing, while others support multiple services. The network servers utilize their own operating systems and have more processing and storage capacity compared to regular computers. Within a tiered network, if a server goes down, clients are more vulnerable because the network is not as distributed as in a P2P network.

**Thin-Client Network** – This architecture gives the server more responsibilities, such as running applications for the clients. Rather than the software running on the client, the server runs the programs and the client’s main job is simply to display and accept inputs. For example, users would access a virtual machine on their device but none of the applications are actually run on the personal device. Because of this, thin-client architecture [offers more security](http://www.castellan.net/Castellan_INSIGHTS_0806.pdf) and protection for proprietary information. While the initial upfront cost of switching to a thin-client architecture can be significant, the manageability it provides makes it worth the cost for large companies.



**Components of Network Architecture**

Whether building a network or updating network security, knowing and assessing [network architecture](https://blog.rsisecurity.com/enterprise-information-security-architecture-what-you-need-to-know/) components will help IT teams evaluate the weak links or discover new ways to improve network functionality.

**Essential Network Components**

**Switches** – Switches connect devices, allowing them to communicate over the network. On-premise and cloud-based switches are the two main options. An on-premise switch requires a company/IT department to configure, maintain, and monitor the LAN, giving companies greater control over their network operations. For larger companies, this is completely feasible, but smaller companies may be better off using a cloud-based switch, where a cloud provider manages it, pushes updates, and provides a user interface.

**Routers** – Routers connect networks and devices on the networks to the Internet. This means instead of each device having a direct connection, multiple devices, via the router, share one Internet connection. A router also determines the best route for data transmission by analyzing other data traveling over the network. The router has the power to prioritize certain computers. More complex routers allow consumers and companies to use a built-in firewall or VPN.

**Wireless Access Points (WAPs)**– WAPs allow devices to connect to the Internet without a cable, making it easier to add multiple devices or move about within a building. Routers provide the initial bandwidth, but WAPs expand the covered area. Additionally, WAPs show data about connected devices, which can be used for security assessments.

**Other Odds and Ends**

While the above three architecture components compose the core of a network, other components often come up when discussing [network security.](https://blog.rsisecurity.com/network-security-best-practices-a-complete-checklist/)

**Repeaters** – Repeaters regenerate network signals that are distorted. They also relay messages between subnetworks and may be analog or digital. While an analog repeater mainly amplifies a signal, a digital repeater has better quality and can almost duplicate a signal to the original level.

**Hubs** – Hubs allow computers to talk with each other; however, they do not perform any complex tasks. Hubs must be physically plugged into the network with a wired connection.

**Bridges** – Bridges divide a LAN into multiple segments and assist in reducing traffic. They store the addresses of devices and know which segment they are in. As a result, when a computer tries to send information to another computer, the request is first sent to a bridge, which then determines the segment in which the recipient computer is located.

**Evolving Network Architecture**

[Network architecture](https://www.rsisecurity.com/architecture-implementation/) matters not just for internal operations but also for consumer interaction with companies. Consumerization and increased use of technology have made it crucial that companies provide platforms that are user-friendly and, for the most part, glitch-free. Consumers do not want slow and cumbersome shopping experiences or processes that require many steps. For example, many companies now offer auto fill-in capabilities so repeat customers have less hassle when checking out. Cloud architecture enables better market agility through traffic partitioning.



**Cloud Architecture**

When constructing a network, [ORACLE recommends](https://docs.oracle.com/cd/E65465_01/html/E66877/gqahk.html) studying the different traffic patterns over the network. [Cloud computing](https://www.rsisecurity.com/services/cloud-security/) offers many benefits, but if constructed poorly, a cloud infrastructure can be inefficient. For example, a single network interface used with a multi-node configuration will not be able to accommodate high cloud network traffic. Utilizing different networks/subnetworks to isolate traffic maximizes efficiency and improves functionality. Types of traffic may include guests, storage, or management.

**Benefits of Traffic Partitioning**

**Network reliability and availability**– Integrating multiple networks reduces the likelihood of total network failure that can occur with single-network configurations. If an issue occurs in a single-network configuration, all traffic may cease or be compromised.

**Performance and scalability** – Unlike a single network interface, multiple interfaces guide network traffic routes while decreasing network congestion and improving overall performance, both qualities consumers highly value.

**Security** – Network separation is more beneficial than a single network traffic flow because that architecture enables IT managers to isolate a security issue more easily. Additionally, if a security breach occurs, some operations/traffic may remain functional while the vulnerable section is dealt with.

**Manageability** – Network management becomes easier the more organized you are. For example, a personal planner with daily columns and sections provides greater organization than one with only a large block of blank space. It’s easier to manage tasks when they are clearly categorized.

**How to Design a Secure Network**

Just as consumers highly value efficiency and reliability, they also expect companies to [implement secure networks](https://blog.rsisecurity.com/how-to-set-up-a-secure-network/). The Internet is an integral part of any functioning business in modern society, but connecting to it adds a door for hackers to potentially enter. Consequently, security should be at the forefront when considering network infrastructure. The Infosec Institute offers the following suggestions when [designing a network with security in mind](https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/communications-and-network-security/secure-network-architecture-design/).

1. **Don’t overlook the supposedly insignificant**. This means that even simple information or policy pages can be weak links in a network’s architecture. Areas of a network that consumers overlook may be a prime target for hackers.
2. **Implement fail safes**. When developing a network architecture, implement fail-safes so that if systems fail information and company applications do not become vulnerable at the same time.
3. **Limit access**. While it may be easier to grant total access to an individual or entity, it’s not secure and goes against the least privilege model. If a third-party needs network access, only grant them access for what they need or the least amount of access necessary. Then, if a security risk occurs, the vulnerability will hopefully not endanger the entire network.
4. **Encryption** – [Encryption](https://blog.rsisecurity.com/importance-of-encryption-in-the-business-world/) should be included in any network security model. Moreover, many compliance models list encryption as a requirement. Typically, encryption occurs over the network layer of the Open System Interconnection (OSI) model but on an IP-based network, the [network encryption process](https://www.techopedia.com/definition/16121/network-encryption) will involve IP protocols and keys versus the OSI algorithm process.
5. **Test before total implementation**. Once a network is set up the work isn’t over. Companies should run [vulnerability tests](https://www.rsisecurity.com/marketing/vulnerability-assessment/) to ensure major vulnerabilities are addressed prior to the network going live.

**Network Security Checklist For Personal/Small Businesses**

[Network security](https://blog.rsisecurity.com/network-security-best-practices-a-complete-checklist/) isn’t just something for companies to consider. Consumers can also take proactive steps to safeguard their networks. [PC Magazine recommends](https://www.herzing.edu/blog/what-network-security-and-why-it-important) the following steps for securing a home network.

* Change your router admin username and password
* Change the network name
* Activate encryption
* Double up on firewalls
* Turn off guest networks
* Update router firmware

These considerations apply to small businesses as well. For example, a cafe offering WiFi should reset passwords frequently and use a separate network for business operations.

**For Larger Companies**

[Penetration testing](https://www.rsisecurity.com/penetration-testing/) and computer forensics will help strengthen network security. The following [categories provide a baseline](https://www.titanhq.com/complete-network-security-checklist/) for conducting a network security audit.

* Policies – including network configuration, patching
* Provisioning Servers
* Deploying Workstations
* Network Equipment
* Vulnerability Scans
* Redundancy
* Remote Access
* Wireless networking – such as guest networks, BYOD procedures, and encryption
* Email
* Internet Access
* File Sharing
* Server Log Monitoring