**INTERNAL ORGANIZATIONS OF THE NETWORK LAYER**

* datagram
* virtual circuits

The internal organization of the network is orthogonal to the service that it provides, but most of the time a datagram organization is used to provide a connectionless service while a virtual circuit organization is used in networks that provide a connection-oriented service.

**1-DATAGRAM ORGANIZATION**

The first and most popular organization of the network layer is the datagram organization. This organization is inspired by the organization of the postal service. Each host is identified by a *network layer address*. To send information to a remote host, a host creates a packet that contains:

* the network layer address of the destination host
* its own network layer address
* the information to be sent

The network layer limits the maximum packet size. Thus, the information must have been divided in packets by the transport layer before being passed to the network layer.

To understand the datagram organization, let us consider the figure below. A network layer address, represented by a letter, has been assigned to each host and router. To send some information to host *J*, host *A* creates a packet containing its own address, the destination address and the information to be exchanged.

With the datagram organization, routers use *hop-by-hop forwarding*. This means that when a router receives a packet that is not destined to itself, it looks up the destination address of the packet in its *routing table*. A *routing table* is a data structure that maps each destination address (or set of destination addresses) to the outgoing interface over which a packet destined to this address must be forwarded to reach its final destination.

The main constraint imposed on the routing tables is that they must allow any host in the network to reach any other host. This implies that each router must know a route towards each destination, but also that the paths composed from the information stored in the routing tables must not contain loops. Otherwise, some destinations would be unreachable.

**2-VIRTUAL CIRCUIT ORGANIZATION**

The main advantage of the datagram organization is its simplicity. The principles of this organization can easily be understood. Furthermore, it allows a host to easily send a packet towards any destination at any time. However, as each packet is forwarded independently by intermediate routers, packets sent by a host may not follow the same path to reach a given destination. This may cause packet reordering, which may be annoying for transport protocols. Furthermore, as a router using **hop-by-hop** forwarding always forwards packets sent towards the same destination over the same outgoing interface, this may cause congestion over some links.

The **second organizatio**n of the network layer, called ***virtual circuits****,* has been inspired by the organization of telephone networks. Telephone networks have been designed to carry phone calls that usually last a few minutes. Each phone is identified by a telephone number and is attached to a telephone switch. To initiate a phone call, a telephone first needs to send the destination’s phone number to its local switch. The switch cooperates with the other switches in the network to create a bi-directional channel between the two telephones through the network. This channel will be used by the two telephones during the lifetime of the call and will be released at the end of the call. Until the 1960s, most of these channels were created manually, by telephone operators, upon request of the caller. Today’s telephone networks use automated switches and allow several channels to be carried over the same physical link, but the principles remain roughly the same.

In a network using virtual circuits, all hosts are identified with a network layer address. However, a host must explicitly request the establishment of a virtual circuit before being able to send packets to a destination host. The request to establish a virtual circuit is processed by the control plane, which installs state to create the virtual circuit between the source and the destination through intermediate routers. All the packets that are sent on the virtual circuit contain a virtual circuit identifier that allows the routers to determine to which virtual circuit each packet belongs. This is illustrated in the figure below with one virtual circuit between host A and host I and another one between host *A* and host.

**3-VIRTUAL CIRCUIT ESTABLISHMENT**

A second solution can be used if the routers know the entire topology of the network. In this case, the first router can use a technique called **source routing**. Upon reception of the signaling message, the first router chooses the path of the virtual circuit in the network. This path is encoded as the list of the addresses of all intermediate routers to reach the destination. It is included in the signaling message and intermediate routers can remove their address from the signaling message before forwarding it. This technique enables routers to spread the virtual circuits throughout the network better. If the routers know the load of remote links, they can also select the least loaded path when establishing a virtual circuit. This solution is illustrated with the blue circuit in the figure above.

The last point to be discussed about the virtual circuit organization is its data plane. The data plane mainly defines the format of the data packets and the algorithm used by routers to forward packets. The data packets contain a virtual circuit identifier, encoded as a fixed number of bits. These virtual circuit identifiers are usually called labels.

Each host maintains a flow table that associates a label with each virtual circuit that is has established. When a router receives a packet containing a label, it extracts the label and consults its label forwarding table. This table is a data structure that maps each couple (incoming interface, label) to the outgoing interface to be used to forward the packet as well as the label that must be placed in the outgoing packets. In practice, the label forwarding table can be implemented as a vector and the couple (incoming interface, label) is the index of the entry in the vector that contains the outgoing interface and the outgoing label. Thus a single memory access is sufficient to consult the label forwarding table. The utilization of the label forwarding table is illustrated in the figure below.

**4-THE CONTROL PLANE**

One of the objectives of the *control plane* in the network layer is to maintain the routing tables that are used on all routers. As indicated earlier, a routing table is a data structure that contains, for each destination address (or block of addresses) known by the router, the outgoing interface over which the router must forward a packet destined to this address. The routing table may also contain additional information such as the address of the next router on the path towards the destination or an estimation of the cost of this path.

In this section, we discuss the three main techniques that can be used to maintain the routing tables in a network.

**5-STATIC ROUTING**

The simplest solution is to pre-compute all the routing tables of all routers and to install them on each router. Several algorithms can be used to compute these tables.

A simple solution is to use shortest path routing and to minimize the number of intermediate routers to reach each destination. More complex algorithms can take into account the expected load on the links to ensure that congestion does not occur for a given traffic demand. These algorithms must all ensure that :

* all routers are configured with a route to reach each destination
* none of the paths composed with the entries found in the routing tables contain a cycle. Such a cycle would lead to a forwarding loop.

The figure below shows sample routing tables in a five routers network

**ROUTING TABLES IN A SIMPLE NETWORK**

The main drawback of static routing is that it does not adapt to the evolution of the network. When a new router or link is added, all routing tables must be recomputed. Furthermore, when a link or router fails, the routing tables must be updated as well.

**6-DISTANCE VECTOR ROUTING**

Distance vector routing is a simple distributed routing protocol. Distance vector routing allows routers to automatically discover the destinations reachable inside the network as well as the shortest path to reach each of these destinations. The shortest path is computed based on *metrics* or *costs* that are associated to each link. We use *l.cost* to represent the metric that has been configured for link *l* on a router.

Each router maintains a routing table. The routing table *R* can be modelled as a data structure that stores, for each known destination address *d*, the following attributes :

* *R[d].link* is the outgoing link that the router uses to forward packets towards destination *d*
* *R[d].cost* is the sum of the metrics of the links that compose the shortest path to reach destination *d*
* *R[d].time* is the timestamp of the last distance vector containing destination *d*

**7-P VERSION 4**

IP version 4 is the data plane protocol of the network layer in the TCP/IP protocol suite. The design of IP version 4 was based on the following assumptions :

* IP should provide an unreliable connectionless service (TCP provides reliability when required by the application)
* IP operates with the datagram transmission mode
* IP addresses have a fixed size of 32 bits
* IP must be usable above different types of datalink layers
* IP hosts exchange variable length packets

The addresses are an important part of any network layer protocol. In the late 1970s, the developers of IPv4 designed IPv4 for a research network that would interconnect some research labs and universities. For this utilization, 32 bits wide addresses were much larger than the expected number of hosts on the network. Furthermore, 32 bits was a nice address size for software-based routers. None of the developers of IPv4 were expecting that IPv4 would become as widely used as it is today.

IPv4 addresses are encoded as a 32 bits field. IPv4 addresses are often represented in *dotted-decimal* format as a sequence of four integers separated by a *dot*. The first integer is the decimal representation of the most significant byte of the 32 bits IPv4 address, ... For example,

* 1.2.3.4 corresponds to 00000001000000100000001100000100
* 127.0.0.1 corresponds to 01111111000000000000000000000001
* 255.255.255.255 corresponds to 11111111111111111111111111111111
* An IPv4 address is used to identify an interface on a router or a host. A router has thus as many IPv4 addresses as the number of interfaces that it has in the datalink layer. Most hosts have a single datalink layer interface and thus have a single IPv4 address. However, with the growth of wireless, more and more hosts have several datalink layer interfaces (e.g. an Ethernet interface and a Wi-Fi interface). These hosts are said to be *multihued*. A multihued host with two interfaces has thus two IPv4 addresses.
* An important point to be defined in a network layer protocol is the allocation of the network layer addresses. A naive allocation scheme would be to provide an IPv4 address to each host when the host is attached to the Internet on a first come first served basis. With this solution, a host in Belgium could have address 2.3.4.5 while another host located in Africa would use address 2.3.4.6. Unfortunately, this would force all routers to maintain a specific route towards each host. The figure below shows a simple enterprise network with two routers and three hosts and the associated routing tables if such isolated addresses were used.

## **WHAT IS A VPN & HOW DO YOU USE IT? (imp long)**

A **virtual private network (VPN)** provides a secure connection for your devices when you access the internet. When your connection is secure, your information stays private.

At this point, you might be asking how does a VPN protect you? And how does a VPN work?

VPNs act like a middle man between your internet service provider (ISP) and the internet. When you route your connection through a VPN, you access the internet through your VPN provider’s private server.

One of the main benefits of a VPN is that your data is encrypted before it’s transmitted. **Using a VPN also hides your IP address, which protects your identity while you’re online.**

### **ENCRYPTION BASICS**

**Encryption** hides your information by encoding it so it can only be read with the encryption key. Without the encryption key, your data appears nonsensical.

When you access the internet through a VPN, only your computer and the VPN have the key that can unscramble your encrypted data, otherwise known as decryption.

For example, if you enter your credit card information to make an online payment, that data stays encrypted until it reaches the seller or service provider. Your data remains encrypted and secure.

Each VPN provider has a slightly different process, but two main things happen each time you connect to a VPN:

1. our data passes through a secure tunnel where it is encrypted, making it unreadable when it travels between your device and the VPN server.
2. Your device’s IP address will then match the VPN server’s IP address, which masks your real IP address to protect your identity.

### **ADVANTAGES OF VPN**

Whether you’re considering a VPN for personal use or your company, there are various benefits to a VPN.

Using a VPN empowers you to share files securely, without worrying that the content will be exposed or compromised. Additionally, you can access the internet anonymously and protect your identity.

VPN services keep your IP address, passwords, location, and other identifying data [safe](https://www.bluehost.com/blog/10-fundamental-tips-stay-safe-internet/) from hackers or “big data” collectors. So, if you want to keep your information away from big tech companies and malicious attackers, a VPN might be right for you.

And some of the best benefits of a VPN? They’re **affordable and easy to use.**

VPN services cost as little as a few dollars a month. The software is intuitively designed, so you can use it even if you’re a beginner to internet privacy.

Understanding the pros and cons of VPN can help you decide if you should use one.

## **TYPES OF VPN**

There are [several types of VPNs](https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/), and it can be hard to understand how they’re different. However, VPNs fall into one of two categories, which makes it easier to figure out which VPN is right for you.

## **REMOTE ACCESS VPN**

A **remote access VPN**routes your connection through a secure remote server that permits you to establish a private connection. Additionally, it encrypts data to secure it.

Remote access VPNs are the most popular options for personal use. Additionally, they form the infrastructure of commercial VPN services. To use a remote access VPN, you typically have to install the VPN software on your computer and log in to secure your internet connection.

Ease of use is one of the main benefits of a VPN with the remote access model. This type of VPN is simple enough for new users, making it an optimal choice for personal use.

However, remote access VPNs usually aren’t a viable option for scaled operations or businesses.

## **SITE-TO-SITE VPN**

**Site-to-site** **VPNs** allow multiple users to access each other’s resources from fixed locations. For example, if you’re working in a company with office locations in various cities, they might use a site-to-site VPN to secure company data.

Site-to-site VPNs secure data by ensuring tall [local area connections](https://purple.ai/blogs/whats-the-difference-between-a-lan-and-a-wan/) (LAN) connect to the same wide area network (WAN). All the offices are connected to one another, and the data they share is encrypted and protected by the VPN.

Site-to-site VPNs encrypt all gateways, which means users don’t need to download VPN software to secure their data. Once a user logs into the company network, the VPN goes to work.

There are **two types** of site-to-site VPN services:

* Intranet VPNs are used when one company wants to securely connect multiple locations.
* Extranet VPNs connect multiple companies so they can securely share data and resources.

With site-to-site, the benefits of a VPN include security, efficiency, and scalability, which makes them ideal for corporations.

## **HOW SECURE IS A VPN?**

The primary benefits of a VPN are identity protection and data security. VPNs use encryption to [protect your data](https://www.bluehost.com/blog/how-to-keep-your-data-safe-and-secure-in-the-cloud/) from hackers and big tech companies. However, you can still be at risk of malware, trojans, and viruses when you use a VPN.

On the whole, a VPN is an excellent way to protect your personal data, but you still need to take other precautions on the internet.

If you visit a phishing website or download a compromised file, you’re at risk from malicious software (also known as [malware](https://us.norton.com/internetsecurity-malware-malware-101-how-do-i-get-malware-complex-attacks.html)).

**Malware**is software used by hackers to access your devices or network and damage them without your knowledge.

**Types of malware** include:

* Spyware
* Ransomware
* Trojan horses
* Viruses

**VPN PROTOCOLS**

The quality of your VPN depends on the VPN protocols your provider uses. [VPN protocols](https://www.cactusvpn.com/beginners-guide-to-vpn/vpn-protocol/) are how your VPN service encrypts your data and protects your information.

VPN protocols affect the speed and stability of your connection and your level of encryption.

The following types of protocols offer fast, stable connections and a high level of encryption:

* WireGuard
* SoftEther
* IKEv2/IPSec

**INTERNET TRACKING: WHAT DOES A VPN HIDES?**

Online privacy and anonymity are two main benefits of a VPN. But can people still track you when you use a VPN?

Let’s take a look.

A VPN masks your IP address and encrypts your data to protect your privacy.

However, there are other ways you can be [tracked online](https://surfshark.com/blog/can-you-be-tracked-if-you-use-a-vpn), including:

* Malware
* Cookies
* Digital fingerprinting
* DNS leaks
* Social media

# **IP SECURITY**

The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

**USES OF IP SECURITY –**  
IPsec can be used to do the following things:

* To encrypt application layer data.
* To provide security for routers sending routing data across the public internet.
* To provide authentication without encryption, like to authenticate that the data originates from a known sender.
* To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

**COMPONENTS Of IP SECURITY** –  
It has the following components:

**1- ENCAPSULATING SECURITY PAYLOAD (ESP) –**It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.

****2-AUTHENTICATION HEADER (AH) –****  
It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data’s confidentiality.

****INTERNET KEY EXCHANGE (IKE)** –**  
It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.

# **WHAT IS A SUBNET? | HOW SUBNETTING WORKS**

## **WHAT IS A SUBNET?**

## **SHORTEST PATH**

## A subnet, or subnetwork, is a [network](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/) inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary [routers](https://www.cloudflare.com/learning/network-layer/what-is-routing/) to reach its destination.

marine Alice puts a letter in the mail that is addressed to Bob, who lives in the town right next to hers. For the letter to reach Bob as quickly as possible, it should be delivered right from Alice's post office to the post office in Bob's town, and then to Bob. If the letter is first sent to a post office hundreds of miles away, Alice's letter could take a lot longer to reach Bob.

Like the postal service, networks are more efficient when messages travel as directly as possible. When a network receives data packets from another network, it will sort and route those packets by subnet so that the packets do not take an inefficient route to their destination.

**WHAT IS AN IP ADDRESS?**

In order to understand subnets, we must quickly define [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/). Every device that connects to the Internet is assigned a unique IP ([Internet Protocol](https://www.cloudflare.com/learning/ddos/glossary/internet-protocol/)) address, enabling data sent over the Internet to reach the right device out of the billions of devices connected to the Internet. While computers read IP addresses as binary code (a series of 1s and 0s), IP addresses are usually written as a series of alphanumeric characters.

**WHAT DO THE DIFFERENT PARTS OF AN IP ADDRESS MEAN?**

This section focuses on IPv4 addresses, which are presented in the form of four decimal numbers separated by periods, like 203.0.113.112. (IPv6 addresses are longer and use letters as well as numbers.)

Every IP address has two parts. The **first part** indicates which network the address belongs to. The **second part** specifies the device within that network. However, the length of the "first part" changes depending on the network's class.

Networks are categorized into different classes, labeled A through E. Class A networks can connect millions of devices. Class B networks and Class C networks are progressively smaller in size. (Class D and Class E networks are not commonly used.)

Let's break down how these classes affect IP address construction:

****CLASS A NETWORK:**** Everything before the first period indicates the network, and everything after it specifies the device within that network. Using 203.0.113.112 as an example, the network is indicated by "203" and the device by "0.113.112."

**CLASS B NETWORK:** Everything before the second period indicates the network. Again using 203.0.113.112 as an example, "203.0" indicates the network and "113.112" indicates the device within that network.

**CLASS C NETWORK:** For Class C networks, everything before the third period indicates the network. Using the same example, "203.0.113" indicates the Class C network, and "112" indicates the device.

**WHY IS SUBNETTING NECESSARY?**

As the previous example illustrates, the way IP addresses are constructed makes it relatively simple for Internet routers to find the right network to route data into. However, in a Class A network (for instance), there could be millions of connected devices, and it could take some time for the data to find the right device. This is why subnetting comes in handy: subnetting narrows down the IP address to usage within a range of devices.

Because an IP address is limited to indicating the network and the device address, IP addresses cannot be used to indicate which subnet an IP packet should go to. Routers within a network use something called a subnet mask to sort data into subnetworks.

## **WHAT IS A SUBNET MASK?**

A subnet mask is like an IP address, but for only internal usage within a network. Routers use subnet masks to route data packets to the right place. Subnet masks are not indicated within data packets traversing the Internet — those packets only indicate the destination IP address, which a router will match with a subnet.

Suppose Bob answers Alice's letter, but he sends his reply to Alice's place of employment rather than her home. Alice's office is quite large with many different departments. To ensure employees receive their correspondence quickly, the administrative team at Alice's workplace sorts mail by department rather than by individual employee. After receiving Bob's letter, they look up Alice's department and see she works in Customer Support. They send the letter to the Customer Support department instead of to Alice, and the customer support department gives it to Alice.

In this analogy, "Alice" is like an IP address and "Customer Support" is like a subnet mask. By matching Alice to her department, Bob's letter was quickly sorted into the right group of potential recipients. Without this step, office administrators would have to spend time laboriously looking for the exact location of Alice's desk, which could be anywhere in the building.

For a real-world example, suppose an IP packet is addressed to the IP address 192.0.2.15. This IP address is a Class C network, so the network is identified by "192.0.2" (or to be technically precise, 192.0.2.0/24). Network routers forward the packet to a host on the network indicated by "192.0.2."

Once the packet arrives at that network, a router within the network consults its routing table. It does some binary mathematics using its subnet mask of 255.255.255.0, sees the device address "15" (the rest of the IP address indicates the network), and calculates which subnet the packet should go to. It forwards the packet to the router or [switch](https://www.cloudflare.com/learning/network-layer/what-is-a-network-switch/) responsible for delivering packets within that subnet, and the packet arrives at IP address 192.0.2.15 (learn more about [routers](https://www.cloudflare.com/learning/network-layer/what-is-routing/) and [switches](https://www.cloudflare.com/learning/network-layer/what-is-a-network-switch/)).