



Romel Cabiling ▾



Home

Home > My courses > Network Attacks: Detection, Analysis & Counter... > 09 Internet Protocol Address (Ip Address)  
> Lesson Proper for Week 9

# Lesson Proper for Week 9

## INTERNET PROTOCOL ADDRESS (IP ADDRESS)

### IP ADDRESS

Stands for internet protocol address; it is an identifying number that is associated with a specific computer or computer network. When connected to the internet, the IP address allows the computers to send and receive information.

Allows information to be sent and received by the correct parties, which means they can also be used to track down a user's physical location.

The **internet protocol** suite governs rules for packetizing, addressing, transmitting, routing, and receiving data over networks.

**IP** addressing is a logical means of assigning addresses to devices on a network. Each device connected to the internet requires a unique IP address.

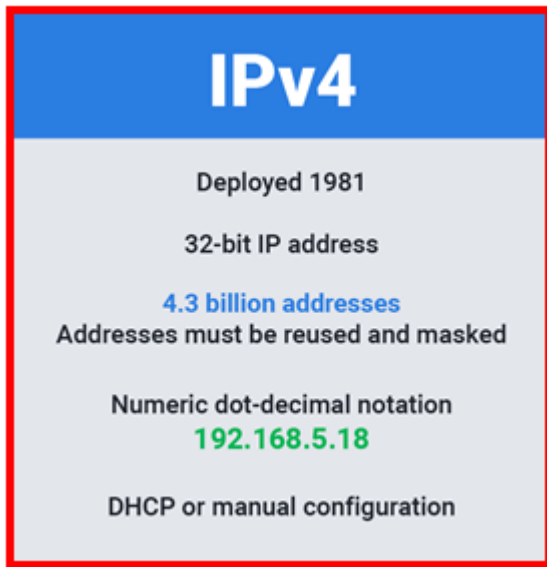
*\*An IP address serves two principal functions:*

- o Host or network interface identification
- o Location addressing



## IP VERSIONS

**a. IPv4 stands for Internet Protocol version 4.** It is the underlying technology that makes it possible for us to connect our devices to the web. Whenever a device accesses the Internet, it is assigned a unique, numerical IP address. To send data from one computer to another through the web, a data packet must be transferred across the network containing the IP addresses of both devices.



**b. IPv6 stands for Internet Protocol version 6.** It is the latest version of the Internet Protocol, which identifies devices across the internet so they can be located. Every device that uses the internet is identified through its own IP address in order for internet communication to work.

The IPv6 protocol can handle packets more efficiently, improve performance and increase security. It enables internet service providers to reduce the size of their routing tables by making them more hierarchical.



Internet Protocol works the same way as any other language, by communicating using set guidelines to pass information. All devices find, send, and exchange information with other connected devices using this protocol. By speaking the same language, any computer in any location can talk to one another.

The process works like this:

1. Your device indirectly connects to the internet by connecting at first to a network connected to the internet, which then grants your device access to the internet.
2. When you are at home, that network will probably be your Internet Service Provider (ISP). At work, it will be your company network.
3. Your IP address is assigned to your device by your ISP.
4. Your internet activity goes through the ISP, and they route it back to you, using your IP address. Since they are giving you access to the internet, it is their role to assign an IP address to your device.
5. However, your IP address can change. For example, turning your modem or router on or off can change it. Or you can contact your ISP, and they can change it for you.
6. When you are out and about – for example, traveling – and you take your device with you, your home IP address does not come with you. This is because you will be using another network (Wi-Fi at a hotel, airport, or coffee shop, etc.) to access the internet and will be using a different (and temporary) IP address, assigned to you by the ISP of the hotel, airport or coffee shop.

## TYPES OF IP ADDRESSES

There are different categories of IP addresses, and within each category, different types.

**Consumer IP address.** Every individual or business with an internet service plan will have two types of IP addresses: their private IP addresses and their public IP address. The terms public and private relate to the network location — that is, a private IP address is used inside a network, while a public one is used outside a network.

**Private IP address.** Every device that connects to your internet network has a private IP address. This includes computers, smartphones, and tablets but also any Bluetooth-enabled devices like speakers, printers, or smart TVs. With the growing internet of things, the number of private IP addresses you have at home is probably growing. Your router needs a way to identify these items separately, and many items need a way to recognize each other. Therefore, your router generates private IP addresses that are unique identifiers for each device that differentiate them on the network.



**Public IP address.** A public IP address is the primary address associated with your whole network. While each connected device has its own IP address, they are also included within the main IP address for your network. As described above, your public IP address is provided to your router by your ISP. Typically, ISPs have a large pool of IP addresses that they distribute to their customers. Your public IP address is the address that all the devices outside your internet network will use to recognize your network.

*Public IP addresses come in two forms – dynamic and static.*

## **1. Dynamic IP addresses**

Dynamic IP addresses change automatically and regularly. ISPs buy a large pool of IP addresses and assign them automatically to their customers. Periodically, they re-assign them and put the older IP addresses back into the pool to be used for other customers. The rationale for this approach is to generate cost savings for the ISP. Automating the regular movement of IP addresses means they don't have to carry out specific actions to re-establish a customer's IP address if they move home, for example. There are security benefits, too, because a changing IP address makes it harder for criminals to hack into your network interface.

## **2. Static IP addresses**

In contrast to dynamic IP addresses, static addresses remain consistent. Once the network assigns an IP address, it remains the same. Most individuals and businesses do not need a static IP address, but for businesses that plan to host their own server, it is crucial to have one. This is because a static IP address ensures that websites and email addresses tied to it will have a consistent IP address — vital if you want other devices to be able to find them consistently on the web.

*This leads to the next point – which is the two types of website IP addresses.*

## **There are two types of website IP addresses**

For website owners who don't host their own server, and instead rely on a web hosting package – which is the case for most websites – there are two types of website IP addresses. These are shared and dedicated.

### **1. Shared IP addresses**

Websites that rely on shared hosting plans from web hosting providers will typically be one of many websites hosted on the same server. This tends to be the case for individual websites or SME websites, where traffic volumes are manageable, and the sites themselves are limited in terms of the number of pages, etc. Websites hosted in this way will have shared IP addresses.



## 2. Dedicated IP addresses

Some web hosting plans have the option to purchase a dedicated IP address (or addresses). This can make obtaining an SSL certificate easier and allows you to run your own File Transfer Protocol (FTP) server. This makes it easier to share and transfer files with multiple people within an organization and allow anonymous FTP sharing options. A dedicated IP address also allows you to access your website using the IP address alone rather than the domain name — useful if you want to build and test it before registering your domain.

### IP ADDRESS SECURITY THREATS

Cybercriminals can use various techniques to obtain your IP address. Two of the most common are social engineering and online stalking.

Attackers can use **social engineering** to deceive you into revealing your IP address. For example, they can find you through Skype or a similar instant messaging application, which uses IP addresses to communicate. If you chat with strangers using these apps, it is important to note that they can see your IP address. Attackers can use a Skype Resolver tool, where they can find your IP address from your username.

Criminals can track down your IP address by merely **stalking** your online activity. Any number of online activities can reveal your IP address, from playing video games to commenting on websites and forums.

Once they have your IP address, attackers can go to an IP address tracking website, such as [whatismyipaddress.com](http://whatismyipaddress.com), type it in, and then get an idea of your location. They can then cross-reference other open-source data if they want to validate whether the IP address is associated with you specifically. They can then use LinkedIn, Facebook, or other social networks that show where you live, and then see if that matches the area given.

If a Facebook stalker uses a phishing attack against people with your name to install spying malware, the IP address associated with your system would likely confirm your identity to the stalker.

### IP ADDRESS PROTECTION

Hiding your IP address is a way to protect your personal information and online identity. The two primary ways to hide your IP address are:

#### 1. Using a proxy server



## 2. Using a virtual private network (VPN)

A **proxy server** is an intermediary server through which your traffic is routed:

§ The internet servers you visit see only the IP address of that proxy server and not your IP address.

§ When those servers send information back to you, it goes to the proxy server, which then routes it to you.

A drawback of proxy servers is that some of the services can spy on you — so you need to trust it. Depending on which one you use, they can also insert ads into your browser.

*VPN offers a better solution:*

§ When you connect your computer – or smartphone or tablet – to a VPN, the device acts as if it is on the same local network as the VPN.

§ All your network traffic is sent over a secure connection to the VPN.

§ Because your computer behaves as if it is on the network, you can securely access local network resources even when you are in another country.

§ You can also use the internet as if you were present at the VPN's location, which has benefits if you are using public Wi-Fi or want to access geo-blocked websites.

◀ Preliminary Activity for Week 9

Jump to...



Analysis, Application, and Exploration for Week 9 ▶



### Navigation

Home



Dashboard

Site pages

My courses

Capstone Project 1

Network Attacks: Detection, Analysis & Counter...

Participants

General

06 - Preliminary Examination


08 Wireless And Wi-Fi Security



09 Internet Protocol Address (Ip Address)

 Preliminary Activity for Week 9

 **Lesson Proper for Week 9**

 Analysis, Application, and Exploration for Week 9

 Generalization for Week 9

 Evaluation for Week 9

 Assignment for Week 9

Ojt/Practicum 1

Social And Professional Issues

System Integration And Architecture 2

Courses

---

## Fair Warning

**NOTICE:** Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

**PROSECUTION:** Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

**COURSE OF ACTION:** Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

---

## Activities

 Assignments

 Forums

 Quizzes

 Resources



