IP Addresses, Domain Names, and URLs

by Sophia

WHAT'S COVERED

In this lesson, you will learn about the concepts of the Internet Protocol, IP addresses, and how they are used on the Internet. You will learn about Domain names and the purpose and functionality of DNS. Lastly, you will be introduced to the different parts of Universal Resource Locator addresses and their role in requesting resources from the World Wide Web.

Specifically, this lesson will cover the following:

1. IP Addresses

As you may recall, the Internet Protocol is a network protocol responsible for providing unique identifiers for devices and provides information for locating systems that are connected to other networks.

WATCH

View this video to learn more about subnetting.

One concept regarding IP addressing that is important to understand is the difference between public and private IP addresses. It is also important to understand how domain addresses, like google.com, are associated with IP addresses. There are currently two IP address versions, IPv4 and IPv6, two address types, public and private, and each address can be divided into two parts: the network portion and the host portion.

1a. Public Versus Private IP Addresses

Public addresses are required for any computer device to connect to and communicate on the Internet. Every public IP address must be unique in order for the Internet to function properly.

IN CONTEXT

Thinking back to the analogy of how the Internet is compared to the United States Postal Service. The public IP addresses of your computer serve the same purpose as the postal address of your house. In both cases, the parts of the address provide critical information about where your system is located and how to get the package to the destination.

Companies, organizations, and individuals need to purchase at least one IP address in order to access the Internet and the World Wide Web. Globally, public IP addresses are managed by the Internet Assigned Numbers Authority (IANA), which is a department of the ICANN. The ICANN organization is responsible for maintaining IP protocol standards. **Internet Service Providers (ISP)** are organizations that maintain the hardware needed to access the Internet and they sell IP addresses and connections to the Internet.

Private addresses are specific ranges of IP addresses that have been set aside by the IANA for use within private networks. These private addresses are non-routable, meaning that they only allow systems to communicate using a private (internal) network, but do not allow systems to communicate with the Internet. Special protocols called **Network Address Translation (NAT)** and **Port Address Translation (PAT)** operate on a router that connects the private network to the public Internet and allows multiple devices on a private network to share a single public IP address.

EXAMPLE
Private IPv4 Address Ranges:
010.000.000.000 to 10.255.255.255
172.016.000.000 to 172.31.255.255
192.168.000.000 to 192.168.255.255

Private IPv6 Address Range:
fc00::/7 or fc00:0000:0000:0000:0000:0000:0000:0000

Any variation of IP addresses within these private address ranges allows multiple devices on a private network to communicate without needing to purchase a public address. The network router then uses NAT and PAT along with a public IP address to grant the entire private network access to the Internet.

TERMS TO KNOW

Public Address

A unique IP address required for any computer device to connect to and communicate on the Internet.

Internet Service Provider (ISP)

An organization that provides access to the Internet in exchange for monthly fees.

Private Address

Specific ranges of IP addresses that only allow systems to communicate using an internal network, but do not allow systems to communicate with the Internet.

NAT (Network Address Translation)

A router-based protocol that swaps the private IP address of a packet originating from the private network with a public IP address before forwarding the packet onto the public Internet.

PAT (Port Address Translation)

A router-based protocol that extends the NAT protocol by using port numbers to allow multiple systems connected to the private network to use a single public IP address at the same time.

1b. IPv4 Versus IPv6

Internet Protocol version 4 (IPv4) was the original 32-bit addressing protocol used for communication on the Internet. Each address was 32 **binary** bits in length and was represented using four sets of decimal numbers (octets) ranging from 0 to 255 separated by periods. Each octet is a representation of 8 bits (or 1 byte) of the total 32 bits.

EXAMPLE

Binary: 10111001 . 01101011 . 01010000 . 11100111

Decimal: 185.107.080.231

Internet Protocol version 6 (IPv6) was introduced in 1995 to resolve a key problem with IPv4's 32-bit address; with only just over 4 billion addresses the world was running out of public IPv4 addresses. To solve the limited capacity of a 32-bit address scheme, IPv6 introduced the 128-bit address which provided a capacity of public addresses in the trillion trillion trillions (2128). Furthermore, IPv6 also incorporates **Internet Protocol Security (IPSec)** natively, whereas IPSec had to be enforced separately on IPv4 networks.

LEARN MORE

To learn more about IPv4 addresses, check out TutorialsPoint: IPv4 - Addressing.

TERMS TO KNOW

Internet Protocol version 4 (IPv4)

The fourth version of the internet protocol that uses 32 bit addresses to uniquely identify devices on a network.

Binary

A base 2 numbering system that only uses two symbols, 0 and 1, and is the only language understood by computer hardware.

Internet Protocol version 6 (IPv6)
The sixth version of the internet protocol that uses 128 bit addresses to uniquely identify devices on a network.

Internet Protocol Security (IPSec)
A communication protocol designed to incorporate authentication and encryption into an IPv4 network.

1c. Network and Host IDs

IP addresses, both IPv4 and IPv6, are made up of two parts, the network portion and the host portion. The network portion indicates the ID of the network to which the device is connected and the host portion uniquely identifies the individual device connected to the network. This separation is denoted using a **subnet-mask** which specifies how many bits, from the left-most bit, make up the network portion, and the remaining bits make up the host portion. IPv4 subnet masks typically appear in two forms, as an IP address where each octet is either a 0 or 255 or as a post-fix value using a forward slash and a number indicating the number of bits that make up the network portion.

➦ EXAMPLE
IP Address: 192.168.002.140
Subnet Mask: 255.255.255.000
Or
IP Address with subnet: 192.168.2.140/24

In the example, the first 3 octets have a value of 255, marking them as the network portion of the IP address.

➦ EXAMPLE
IP Address: **192.168.002.** 140
Subnet Mask: **255.255.255.**000

The fourth octet of the subnet mask is 0, marking it as the host portion of the IP Address.

➦ EXAMPLE
IP Address: 192.168.002.**140**
Subnet Mask: 255.255.255.**000**

KEY CONCEPT

IP Address: 192.168.002.**140**
Can be read as “host device 140 is connected to network 192.168.2.0”.

Additionally, some networking devices use a slash notation called a prefix to simplify address assignments by removing the need to enter a separate subnet-mask address.

➦ EXAMPLE
IP Address /w subnet: **192.168.2.** 140/**24**

The “/24” in the preceding example means the 24 leftmost bits are the network portion and make the network ID 192.168.2.0 . The IPv6 subnet mask is always represented as a prefix number.

Another concept to be aware of regarding IP addresses and **IP addressing schemes** for internal networks is **Variable-Length Subnet Mask (VLSM)** and **Classless Inter-Domain Routing (CIDR)**. IP addresses can be classified as A, B, and C (D and E classes exist but are not used).

- Class A addresses have a first octet value of 0 to 127 and only use a /8 bit mask.
- Class B addresses have a first octet value of 128 to 191 and use a /16 bit mask.
- Class C addresses have a first octet value of 192 to 223 and use a /24 bit mask.

Using only classful address schemes can cause a lot of wasted IP addresses since a network’s host address capacity is fixed by default. As a result, VLSM was introduced to provide administrators the ability to take their classful address scheme and further divide the networks into smaller networks. This is done by absorbing additional bits into the network mask and thus creating **subnetworks (subnet)**.

EXAMPLE

Class B

Subnet Mask:	255.255. 000.000
Bit Mask:	11111111.11111111 .00000000.00000000
IP Address /w subnet:	192.168.2 .140/**16**

Network ID	**Host Range**
192.168.0.0	**192.168.0.1 - 192.168.255.254**

VLSM

Subnet Mask:	255.255.252.000
Bit Mask:	11111111.11111111.111111 00.00000000
IP Address /w subnet:	192.168.2.140/**22**

Network ID	**Host Range**
192.168.0.0	**192.168.0.1 - 192.168.003.254**
192.168.4.0	**192.168.4.1 - 192.168.007.254**
192.168.8.0	**192.168.8.1 - 192.168.011.254**
...	**...**

The class B network using /16 bit mask originally allowed for 1 possible subnets with 65,534 hosts. That’s a lot of addresses for any one network!

We then changed the mask from /16 bits to /22 bits, borrowing 6 bits from the host portion to create subnets. We now have 64 possible subnets (which would be ideal for dividing the networks among different locations or departments), each with 1,022 host addresses.

VLSM is a great solution for managing address allocations; however, it affects network routers and how the router keeps track of where other networks are located. Network routers were originally built and programmed to only handle networks using the classes and their default subnet masks of /8, /16, and /24. To deal with this new technique of managing network and host addresses, CIDR was introduced to enable routers to understand VLSM addresses and subnets and be able to route data to and from classless and classful IP networks.

TERMS TO KNOW

Subnet-Mask
A component of Internet Protocol that indicates the network portion versus the host portion of an IP address.

IP Address Scheme
A planned configuration of network addresses and host addresses within IP-based networks.

Variable-Length Subnet Mask (VLSM)
A network design strategy that allows administrators to change the number of networks and host addresses to carefully control address allocation and avoid wasted addresses.

Classless Inter-Domain Routing (CIDR)
The implementation of VLSM in network devices and routers that improves the ability to allocate IP addresses and improves the router's efficiency of managing routes and routing decisions.

Subnetwork (Subnet)
A part of a larger network. Comes from "sub and "network."

2. Domain Names

A domain name is a unique, human-readable address that points to web servers and the IP address of devices connected to the Internet. Domain names are created by their prospective owner and are then registered through an ICANN-accredited registrar, such as hostgator.com or godaddy.com. **ICANN registrars** are organizations authorized to sell and register domain names on behalf of the customer.

EXAMPLE

- GOOGLE.COM
- MICROSOFT.COM
- TINYDANCINGDEER.COM

TERM TO KNOW

Internet Corporation for Assigned Names and Numbers (ICANN) Registrars
Organizations authorized to sell and register domain names on behalf of the customer.

2a. Domain Name System and Name Servers

Domain names provide the average user with an address that is easy to remember and type and that allows them to find websites and resources using human-friendly terms. This saves users from having to remember arbitrary numbers that make up IP addresses in order to find a website. However, from the perspective of networking devices, those human-friendly terms are useless without being translated into a public IP address.

⮫ EXAMPLE
When you type a domain name into your browser’s address bar, such as “google.com,” and press the Enter key to request Google’s homepage, the domain must first be translated into an IP address in order for your HTTP request to navigate the Internet and find the correct google web server.

Let’s examine the relationship between a domain name and an IP address. The Domain Name System (DNS) is the system architecture that translates domain names into IP addresses. It consists of DNS communication protocols as well as Name servers that are used to store DNS records, listen for DNS requests, and respond with a DNS response. Each domain name under the name server’s control is represented by one DNS record containing multiple types of entries. The DNS records are what the name servers examine when looking up the IP address of the domain being requested.

⮫ EXAMPLE
When you press Enter after typing a domain name into your browser, the browser sends a DNS request message to the IP address of a DNS name server. This address was assigned to your computer’s network card when it was connected to the network. In a typical home network, your router automatically assigns its own address as the name server. The router often forwards DNS requests to your Internet Service Provider’s (ISP) name server. Once the request reaches any DNS name server, the server will perform a lookup to see if it contains the DNS record for the requested domain name. If not, the name server will forward the request to another connected name server until the correct name server is reached. At that point, the name server finds matching DNS records from the request, reads the IP address, and responds with a DNS response containing the IP address. Your browser is able to send the actual HTTP GET request onto the target web server and the website is finally displayed.

2b. DNS Records

In the table below, you will find a sample DNS record of the domain name EDUREPOSITORY.COM. Notice that there are two Name Server (NS) type entries. These are the name servers that currently hold this DNS record. There are two name servers holding this record primarily for redundancy should one server go down and become unavailable. The two servers are ns73.domaincontrol.com and ns74.domaincontrol.com. Time to Live (TTL) is a field on DNS records that controls how long each record is valid. Longer TTLs mean that updates to records take longer to go into effect.

Type	Name	Data	TTL
A	@	50.62.160.137	600 seconds
A	mssql	50.62.160.137	600 seconds
NS	@	ns73.domaincontrol.com.	1 Hour
NS	@	ns74.domaincontrol.com.	1 Hour
CNAME	ftp	edurepository.com.	10800 seconds
CNAME	www	edurepository.com.	1 Hour
CNAME	_domainconnect	_domainconnect.gd.domaincontrol.com.	1 Hour

SOA	@	Primary nameserver: ns73.domaincontrol.com.	1 Hour

The A type record with the name “@” points to a specific IP address of 50.62.160.137. This is the address you would receive if you requested the root domain. AAAA records (not shown in the example) with a name of “@” is the same as an A record, but points to an IPv6 address.

Subdomains are created using A or AAAA records that use a name other than “@”. In the example, there is an A record with the name “mssql.” Therefore, when you enter mssql.edurepository.com into the address bar, it can be directed to a different address.

CNAME records are also used to create subdomains but can be directed to other domain names.

DNAME records, also not shown in the example, actually re-map the original domain to an external domain.

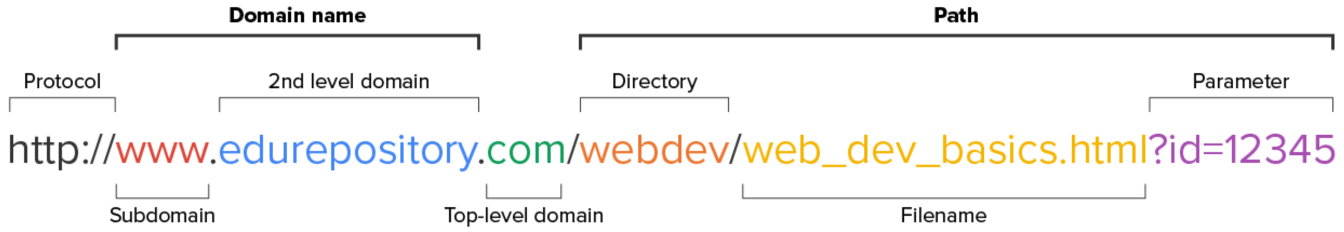
KEY CONCEPT

There are a number of additional DNS record types used for a variety of special purposes, however the above are the more common types.

3. Universal Resource Locator (URL)

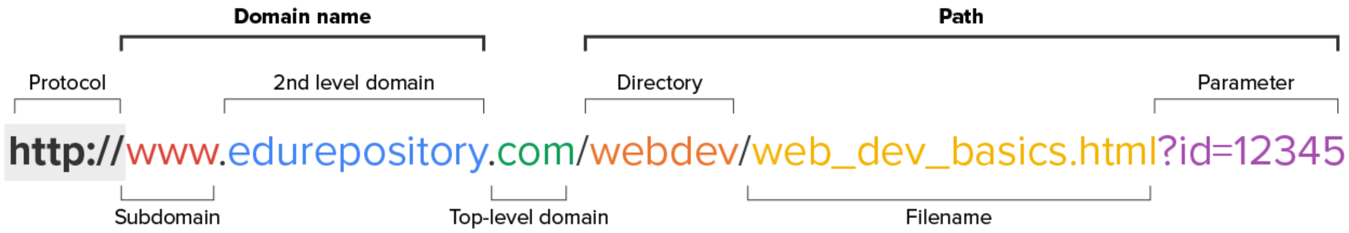
A **Universal Resource Locator (URL)** is a human-readable string of text used to request specific resources or access specific webpages on the World Wide Web. URLs consist of several parts.

EXAMPLE



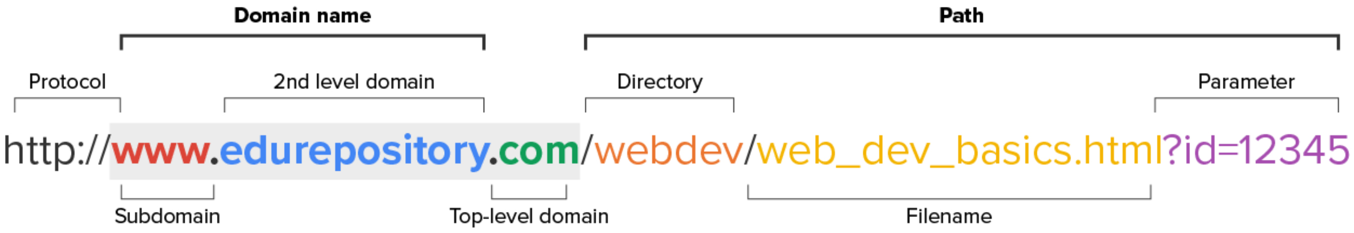
The leftmost part indicates the communication protocol being used. In this case, it is “HTTP” protocol demonstrated below.

EXAMPLE



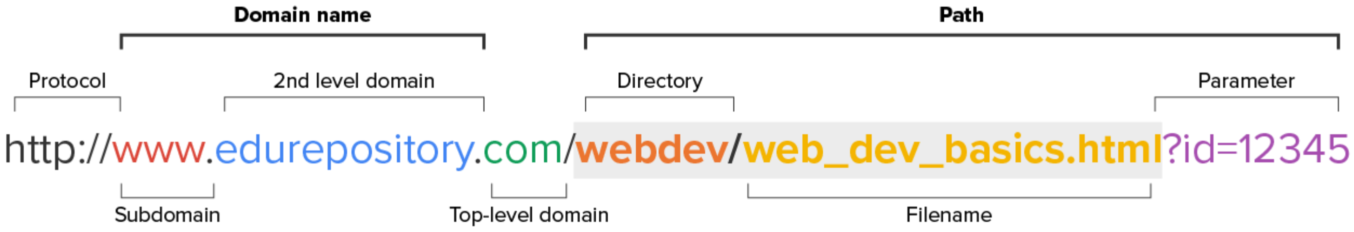
Next is the domain name which consists of an optional subdomain “www,” followed by the required root domain name “edurepository” and top-level domain “com.” The parts of the domain name are separated with periods.

EXAMPLE



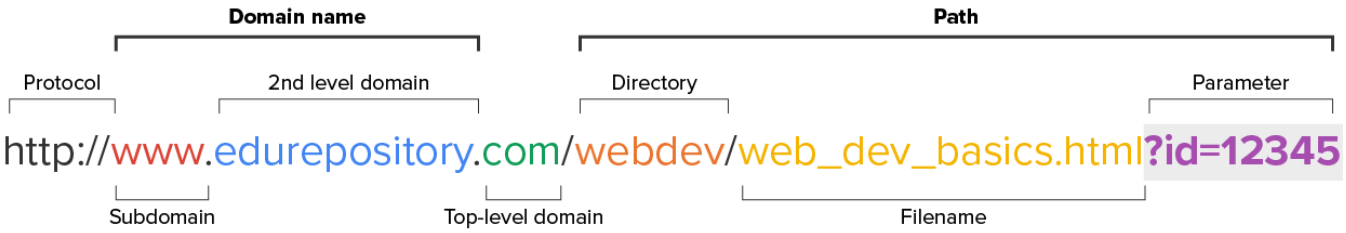
The next section after the domain name is the optional path indicator. This section is used to indicate what file or resource, located in which directories, you are requesting. In the example, we are looking for the “web_dev_basics.html” webpage which is located within the “webdev” directory of the site. If a path is omitted from the URL, then the web server will simply respond with the designated homepage of the website.

EXAMPLE



The final section contains optional parameters that get sent to the server along with the HTTP request to specify additional request parameters. The server uses the parameter values to make decisions on what specific content is being requested.

EXAMPLE



TERM TO KNOW

Universal Resource Locator (URL)

A human-readable string of text used to request specific resources or access specific webpages on the World Wide Web.

SUMMARY

In this lesson, you learned about the different versions of the IP protocol, how **IP addresses** are structured, and how **private IP addresses** differ from **public IP addresses**. You were introduced to the different versions of IP, IPv4 and IPv6, and how each IP address is divided into the **network ID and host ID**. You then learned about the **Domain Name System**, how name servers store the **DNS records** that associate domain names with IP addresses. Lastly, you learned about the different parts of a typical **Universal Resource Locator** and the role they play in requesting resources from the World Wide Web.

Source: THIS TUTORIAL WAS AUTHORED BY SOPHIA LEARNING. PLEASE SEE OUR TERMS OF USE.

TERMS TO KNOW

Binary

A base 2 numbering system that only uses two symbols, 0 and 1, and is the only language understood by computer hardware.

Classless Inter-Domain Routing (CIDR)

The implementation of VLSM in network devices and routers that improves the ability to allocate IP addresses and improves the router’s efficiency of managing routes and routing decisions.

IP Address Scheme

A planned configuration of network addresses and host addresses within IP-based networks.

Internet Corporation for Assigned Names and Numbers (ICANN) Registrars

Organizations authorized to sell and register domain names on behalf of the customer.

Internet Protocol Security (IPSec)

A communication protocol designed to incorporate authentication and encryption into an IPv4 network.

Internet Protocol version 4 (IPv4)

The fourth version of the internet protocol that uses 32 bit addresses to uniquely identify devices on a network.

Internet Protocol version 6 (IPv6)

The sixth version of the internet protocol that uses 128 bit addresses to uniquely identify devices on a network.

Internet Service Provider (ISP)

An organization that provides access to the Internet in exchange for monthly fees.

NAT (Network Address Translation)

A router-based protocol that swaps the private IP address of a packet originating from the private network with a public IP address before forwarding the packet onto the public Internet.

PAT (Port Address Translation)

A router-based protocol that extends the NAT protocol by using port numbers to allow multiple systems connected to the private network to use a single public IP address at the same time.

Private Address

Specific ranges of IP addresses that only allow systems to communicate using an internal network, but do not allow systems to communicate with the Internet.

Public Address

A unique IP address required for any computer device to connect to and communicate on the Internet.

Subnet-Mask

A component of Internet Protocol that indicates the network portion versus the host portion of an IP address.

Subnetwork (Subnet)

A part of a larger network. Comes from ‘sub’ and ‘network’.

Universal Resource Locator (URL)

A human-readable string of text used to request specific resources or access specific web pages on the World Wide Web.

Variable-Length Subnet Mask (VLSM)

A network design strategy that allows administrators to change the number of networks and host addresses to carefully control address allocation and avoid wasted addresses.