DNS Server Implementations: Resolving Domain Names to IP Addresses

VIKRANT SHENDE
ASSOCIATE PROFESSOR
KLS GIT

ANISH MAYANACHE
STUDENT
KLS GIT

CHETAN BADIGER
STUDENT
KLS GIT

HARSHEL MALAWADE
STUDENT
KLS GIT

Abstract—The Domain Name System (DNS) is a crucial software program or service that enables the resolution of domain names to their associated IP addresses. This paper discusses the importance of DNS servers in converting user-friendly domain names into machine-readable IP addresses, facilitating the connection to internet servers. It outlines the key steps involved in setting up a DNS server, including the DNS resolver, software options, DNS records and zones, caching, zone transfers, and security measures. By providing a reliable and secure DNS infrastructure, these implementations play a vital role in facilitating efficient internet communication and accessibility.

I. Introduction

The Domain Name System (DNS) is a critical component of the internet infrastructure, responsible for resolving domain names into their corresponding IP addresses. This process is essential for establishing connections to internet servers, enabling users to access websites and services through user-friendly domain names. DNS server implementations handle the resolution of domain names and play a crucial role in ensuring the accuracy and efficiency of this translation process.

DNS servers act as the backbone of the internet, serving as the intermediaries between users and the internet servers they wish to connect to. When a user enters a domain name, such as "www.example.com," the DNS server translates this user-friendly domain name into a machine-readable IP address, such as "192.0.2.1," which is used to locate and connect to the appropriate internet server. Without DNS servers, users would have to memorize and manually enter the IP addresses of websites, making internet usage much more complicated and less accessible.

Setting up a DNS server involves several important steps. The DNS resolver, located on the client side, initiates the DNS query by forwarding the user's request to a DNS server. Dedicated software for DNS servers, such as BIND, Microsoft DNS Server, or PowerDNS, handles the actual resolution process. DNS records and zones are used to store and organize information about domain names and their corresponding IP addresses. Caching is employed to improve performance by storing previously resolved queries and retrieving the information from the cache instead of repeating the resolution process for subsequent queries.

Furthermore, DNS servers can synchronize their records with other authoritative servers through zone transfers, ensuring consistent domain information across multiple DNS servers. Security measures, such as access control lists, DNSSEC, and rate limiting, are implemented to protect against DNS-based attacks, data tampering, and unauthorized access.

II. Future Scopes

The future scope for DNS can include the following:

1. Advanced Threat Intelligence: DNS server implementations can consolidate progressed danger knowledge capacities to proactively distinguish and moderate arising DNS-based attacks. This can include utilizing AI calculations to dissect examples and peculiarities in DNS traffic, empowering early discovery and counteraction of malicious activities.

2. Enhanced Privacy and Data Protection: DNS servers can additionally improve security and information insurance by carrying out highlights like DNS question encryption, zero-knowledge proofs, and differential privacy techniques. These actions can furnish clients with expanded command over their web-based exercises and shield delicate data from unauthorized access.

3. Integration with Decentralized Web Technologies: With the ascent of decentralized web innovations like blockchain-based area name frameworks (DNS), DNS server implementation can investigate integration possibilities. This can incorporate supporting decentralized naming frameworks and interoperability between customary DNS and blockchain-based DNS to guarantee a consistent and secure browsing experience.

4. Intelligent Traffic Management: DNS server implementation can use AI and ML calculations to enhance traffic management and improve resource allocation. By dissecting verifiable DNS information and organization conditions,the board frameworks can progressively change DNS responses to latency, optimize routing, and guarantee efficient utilization of network resources.

III. Methodology and Result

We have used the Cisco Packet Tracer Software for the Implementation of DNS. We can implement it in these following Steps:

Step-1: Add any number of Client PC's and any number of Servers, in this case I have added 3 PC's and 2 Servers to the workspace. Add a 2960 IOS-15 Switch.

Step-2: Make the connections using the Copper-Straight Through Wires. It has been highlighted in the menu.

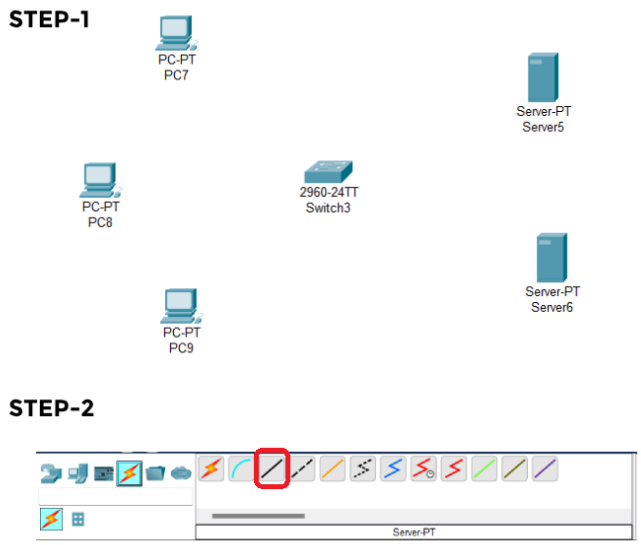

Fig. 1: Arranging the Components

Step-3: Using the Copper-Straight Through Wires, we have to connect the PC's to the switch and Switch to the Server. As shown below in the figure.

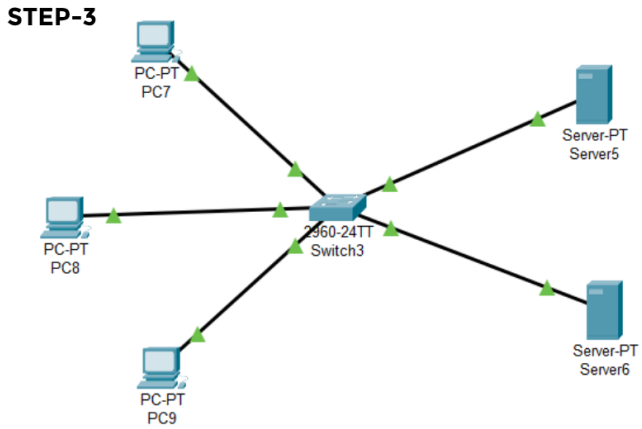

Fig. 2: Making the Connections

Step-4: By clicking on the server we can configure the server. Then Navigate yourself to Server/Desktop/IP Configuration. Then as we can see the IPv4 address has been set to 192.168.1.1 (Remember that we can set the IPv4 address to anything, for standard config we choose 192.168.1.1). Also make sure you set the DNS Server, put the same address as the IPv4 address.

Now we have to set up the DNS. Navigate yourself to Server/Services. Now under the Services tab, click on the DNS and turn on DNS Services. Here we have added a domain name as "www.mypage.com" with the address (192.168.1.1). [Optional: you can change the website under the HTTP tab, Navigate to HTTP/index.html and the change the HTML code to whatever you desire it to be].

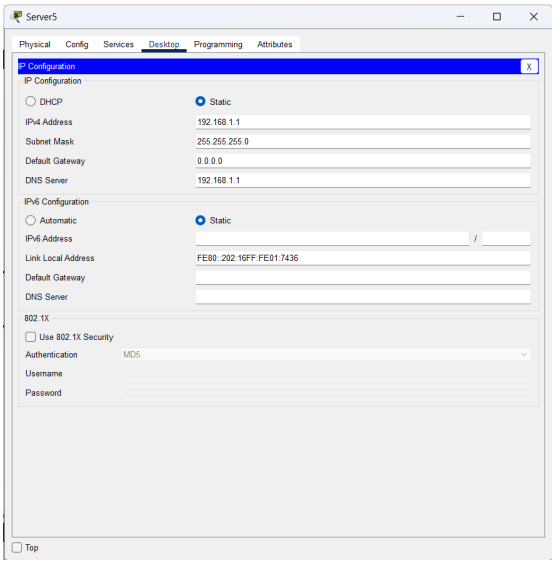

Fig. 3: Setting up Server-1

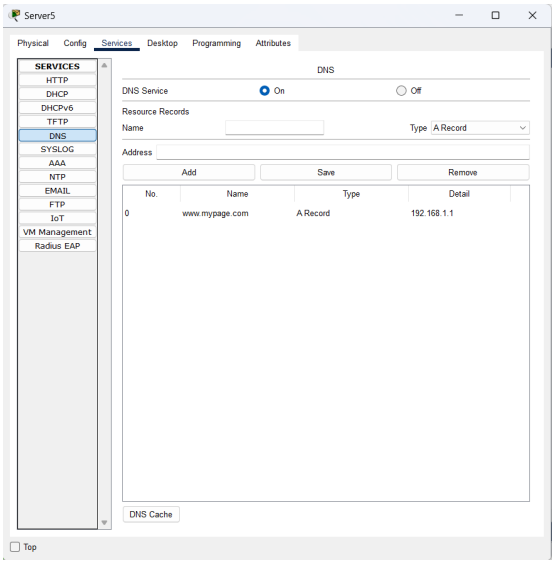

Fig. 4: Setting up Server-1

Similarly, we can configure the second server with an IPv4 address and DNS Server address as 192.168.1.2, and just as the first server add a domain name with the address

192.168.1.2. In this case, we have set the domain name to "www.basics.com" as shown in the below figures.

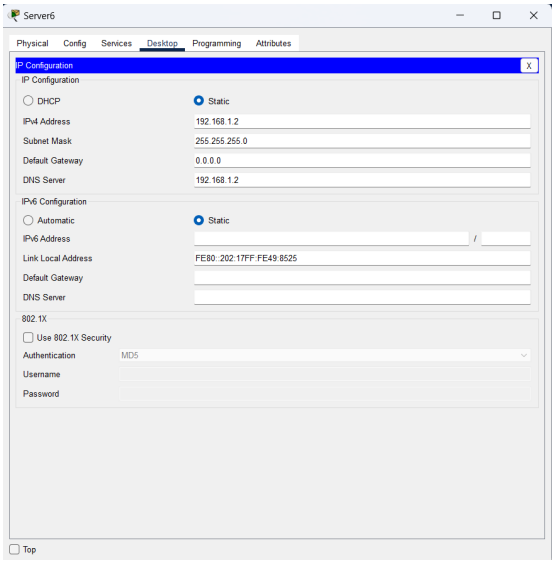

Fig. 5: Setting up Server-2

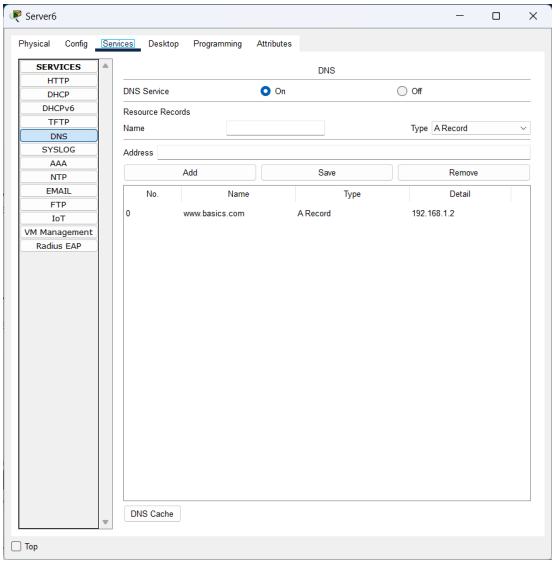

Fig. 6: Setting up Server-2

Step-5: Now, we have to set up the PC. Navigate to PC/Desktop/IP Configuration and set up the PC's by assigning the proper IPv4 addresses as shown in the below figures. PC7, PC8, PC9 get 192.168.1.3, 192.168.1.4, 192.168.1.5 respectively and then we can assign the DNS Server address randomly as we see fit. Here I have assigned the DNS Address 192.168.1.1 to PC7 and PC9, and the DNS Address 192.168.1.2 has been assigned to PC8.

Step-6: Now that we have set up the Servers and the PC's, we can check if these are working by using the Web Browser present in the PC. Navigate to PC7/Desktop/Web Browser and then search "www.mypage.com",

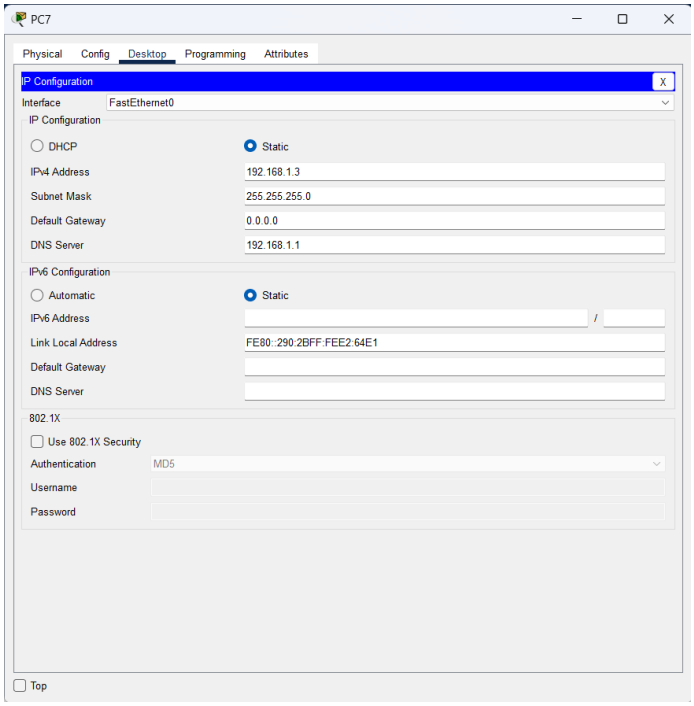

Fig. 7: Setting up PC7

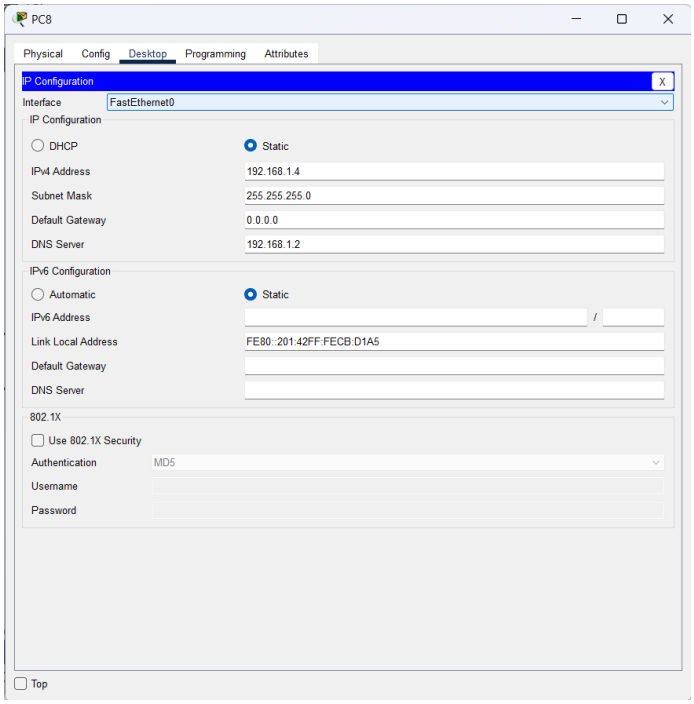

Fig. 8: Setting up PC8

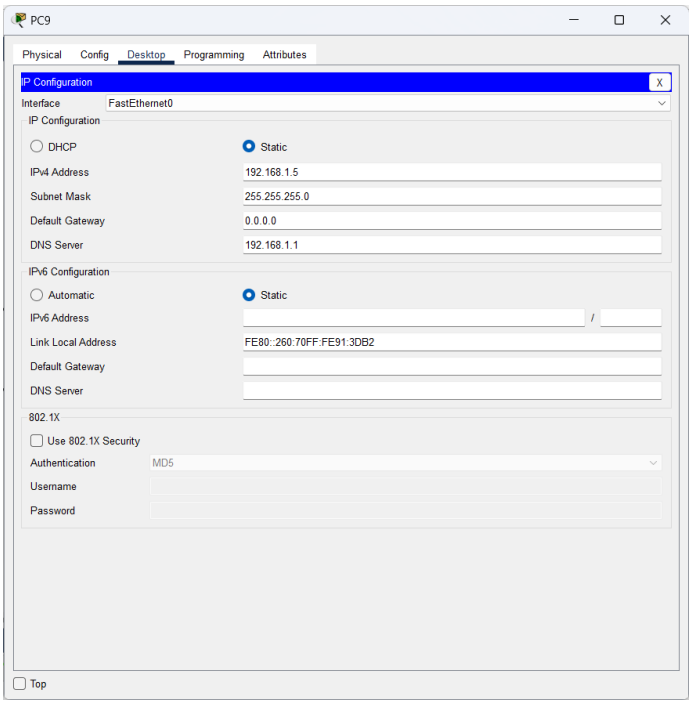

Fig. 9: Setting up PC9

we get the following result. Similarly we can check for PC8 and PC9. In Figure 13 we can see that if we search for any other domain name except to what it has been assigned we do not get any result. But if we search the Domain Address, we do get the result.

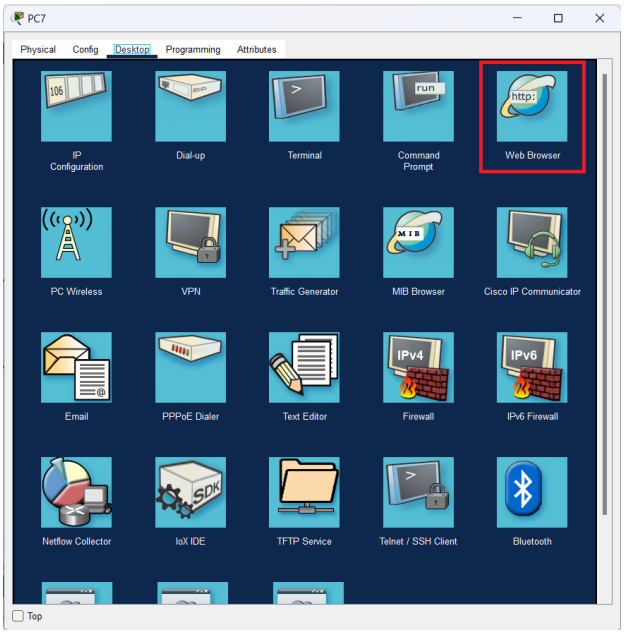

Fig. 10: PC7 Dialog box

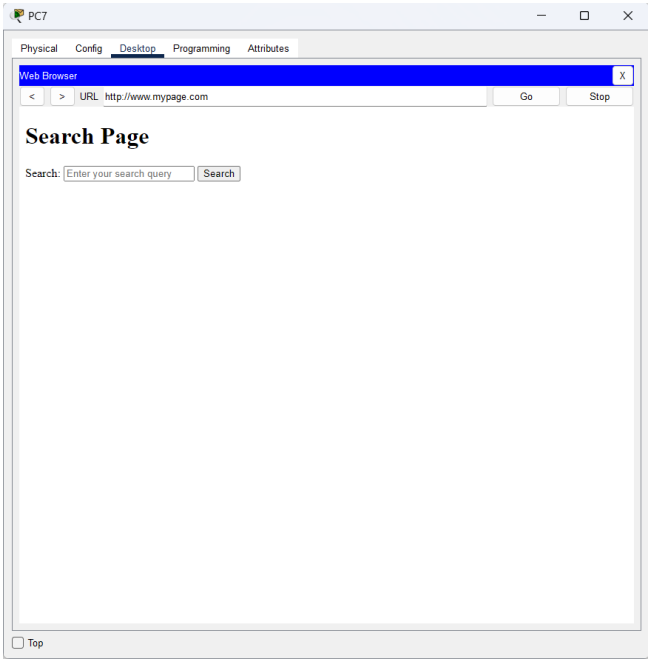

Fig. 11: PC7 Web Browser by using the domain-name specified.

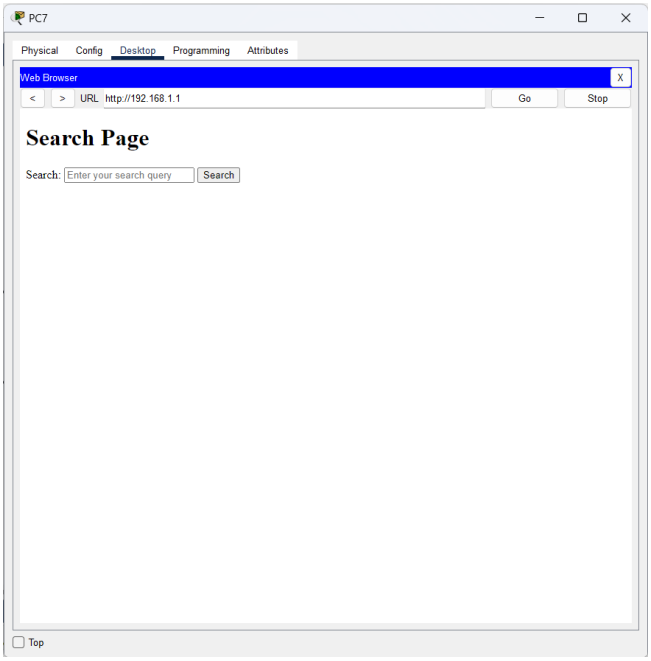

Fig. 12: PC7 Web Browser by using the DNS server address specified.

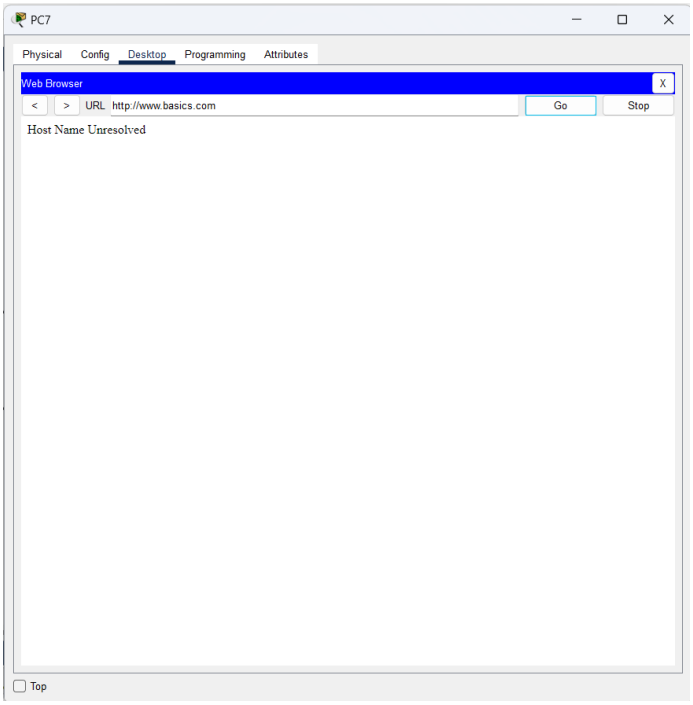

Fig. 13: PC7 Web Browser using "www.basics.com"

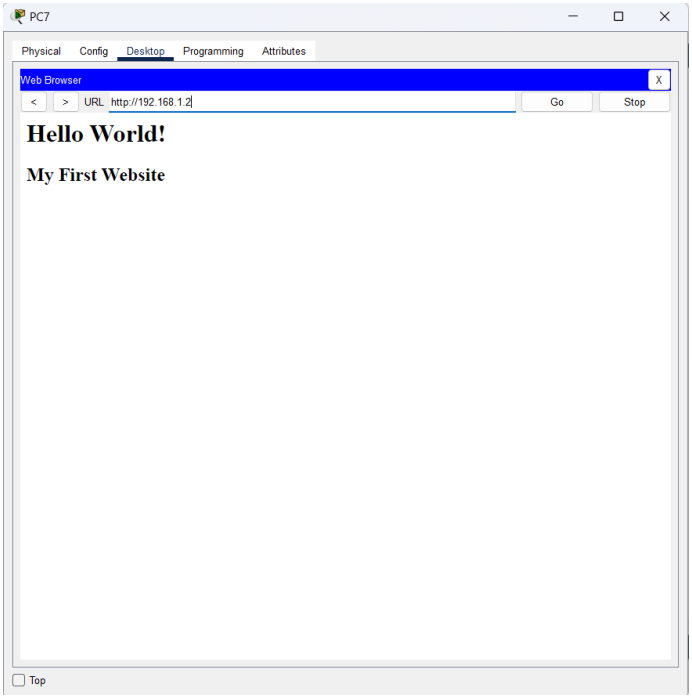

Fig. 14: PC7 Web Browser using 192.168.1.2

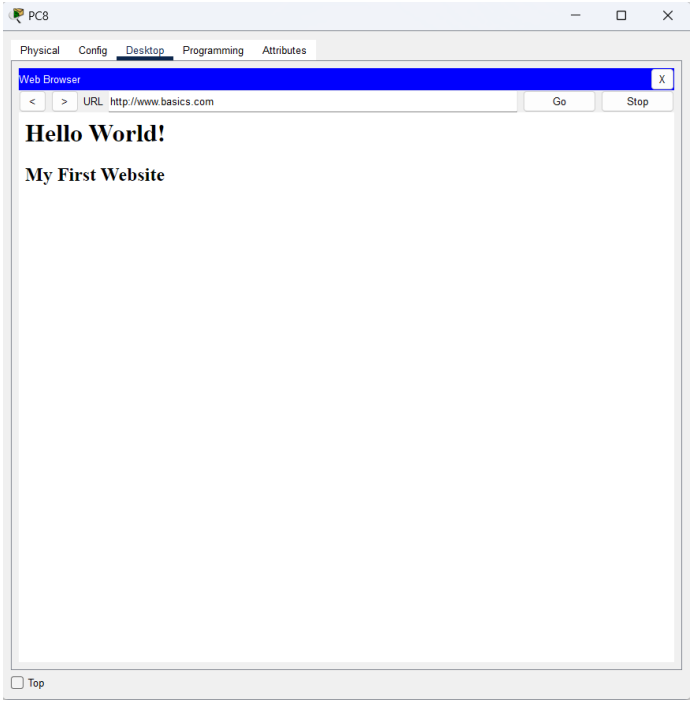

Fig. 15: PC8 Web Browser using the domain-name specified.

IV. Conclusion

All in all, the implementaion of the Domain Name System (DNS) assumes a pivotal part in the working of the web. DNS empowers the interpretation of intelligible domain names into IP addresses, working with the consistent navigation and communication among devices and servers. With DNS, users can easily access websites, send messages, and take part in different web-based activities. The proficient execution of DNS protocols and infrastructure guarantees dependable and quick goal of domain names, adding to the general strength and availability of the web. As innovation keeps on developing, the continuous turn of events and improvement of DNS execution stay fundamental for fulfill the developing needs of a connected world.