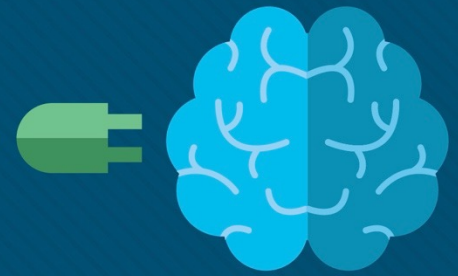


Chapter 3: Network Protocols and Services

Information Security

Dr. Ayman Aljarbouh

3.6 Network Services

Module Objectives

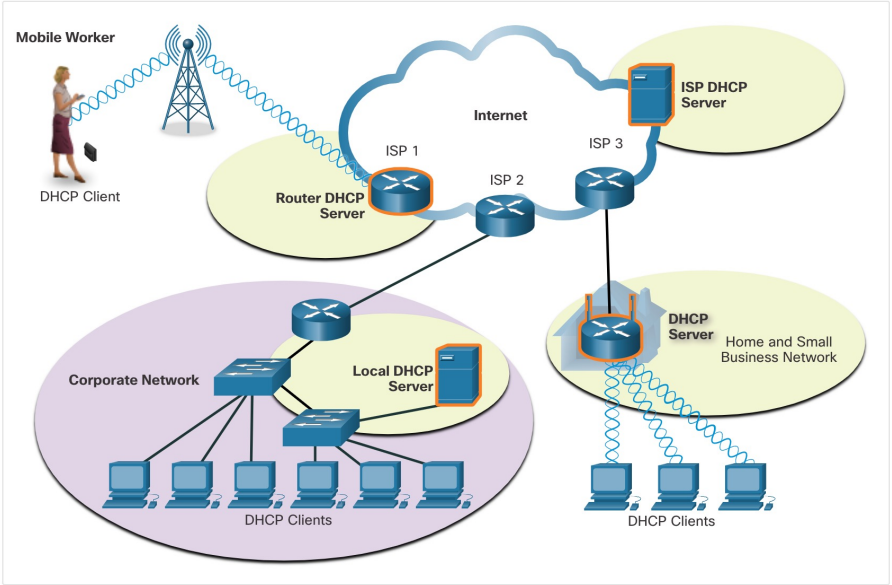
Module Title: Network Services

Module Objective: Explain how network services enable network functionality

Topic Title	Topic Objective
DHCP	Explain how DHCP services enable network functionality.
DNS	Explain how DNS services enable network functionality.
NAT	Explain how NAT services enable network functionality.

Dynamic Host Configuration Protocol

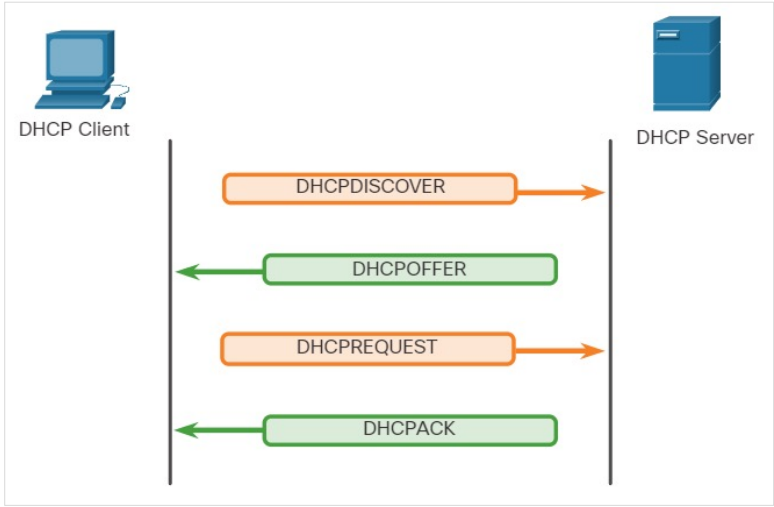
- Two types of addressing:
  - **Dynamic** – Dynamic Host Configuration Protocol (DHCP) for IPv4 service automates the assignment of IPv4 addresses, subnet masks, gateways, and other IPv4 networking parameters.
  - **Static** – The network administrator manually enters IP address information on hosts.
- When a host connects to the network, the DHCP server chooses an address from a configured range of addresses called a pool and assigns it to the host.
- DHCP can allocate IP addresses for a configurable period of time, called a lease period.



Medium-to-large networks – DHCP server is a local PC-based server
Home network – DHCP server is on the local router connecting the home network to the ISP.

DHCP Operation

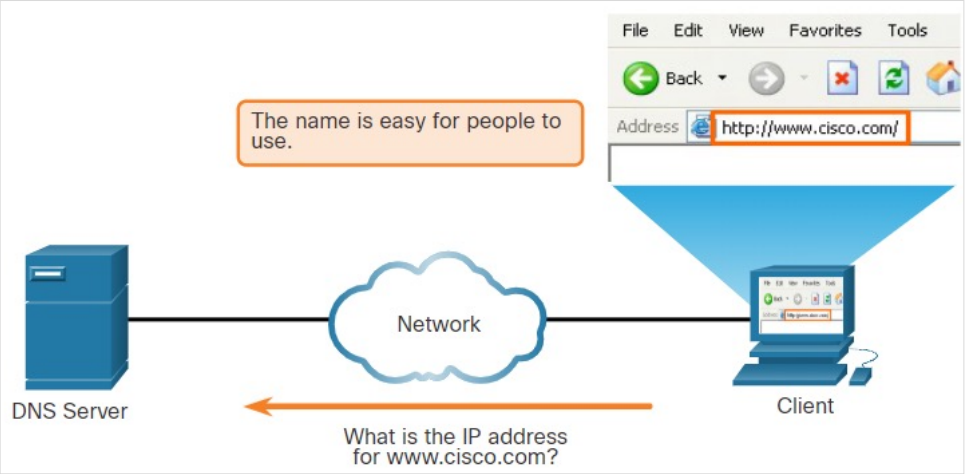
- DHCP operation includes: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK, and DHCPNAK.
- When DHCP-configured device connects to the network, the client broadcasts a **DHCPDISCOVER** message to identify any available DHCP servers on the network.
- A DHCP server replies with a **DHCPOFFER** message, which offers a lease to the client.
- The client sends a **DHCPREQUEST** message that identifies the explicit server and lease offer that the client is accepting.



- If the IPv4 address requested by the client, or offered by the server, is still available, the server returns the **DHCPACK** message. If the offer is no longer valid, then the selected server responds with a **DHCPNAK** message. If a **DHCPNAK** message is returned, then the selection process begins again with a new **DHCPDISCOVER** message being transmitted.

DNS Overview

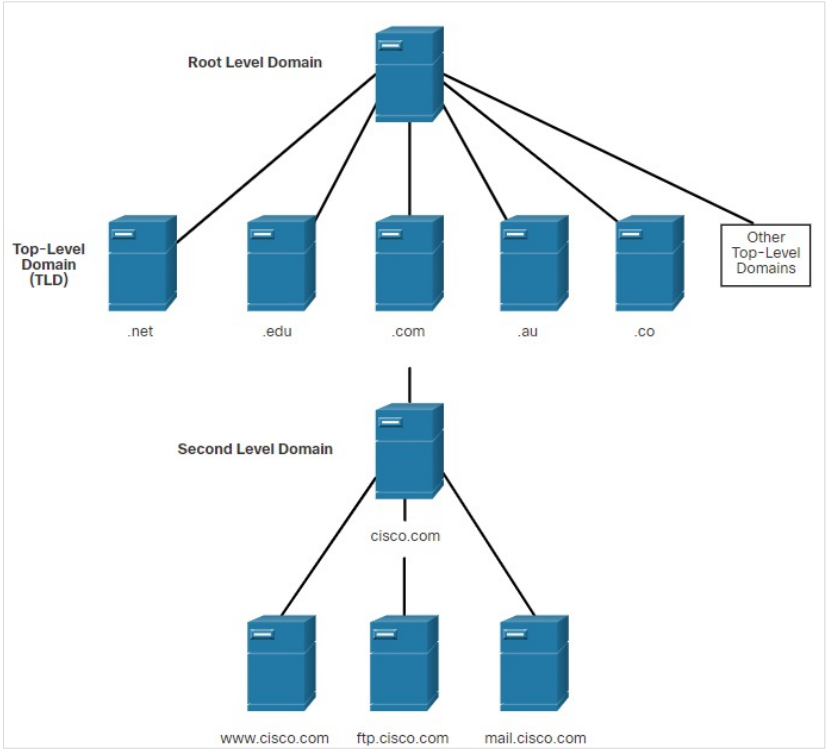
- Domain Name System (DNS) provides domain names and their associated IP addresses.
- The DNS system consists of a global hierarchy of distributed servers that contain databases of name to IP address mappings.
- Malicious DNS traffic can be detected through protocol analysis and the inspection of DNS monitoring information.



DNS Resolves Names to IP Addresses

The DNS Domain Hierarchy

- DNS consists of a hierarchy of generic top-level domains and numerous country-level domains.
- The second-level domains are represented by a domain name that is followed by a top-level domain.
- Subdomains are found at the next level of the DNS hierarchy and represent some division of the second-level domain.
- Fourth level domain can represent a host in a subdomain.
- Top-level domains represent either the type of organization or country of origin. Examples: (**.org)** - a non-profit organization, **(.au)** – Australia.

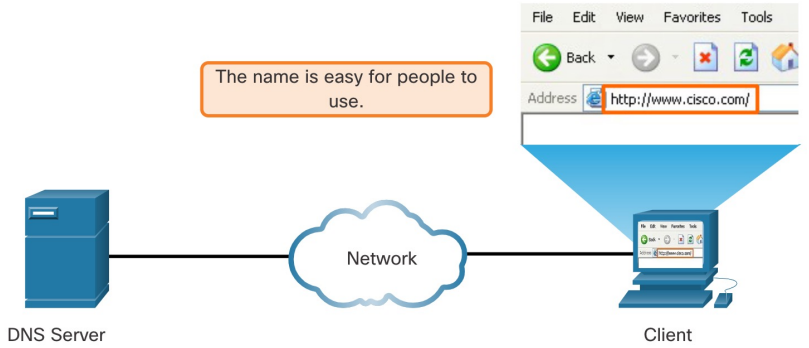


DNS Hierarchy

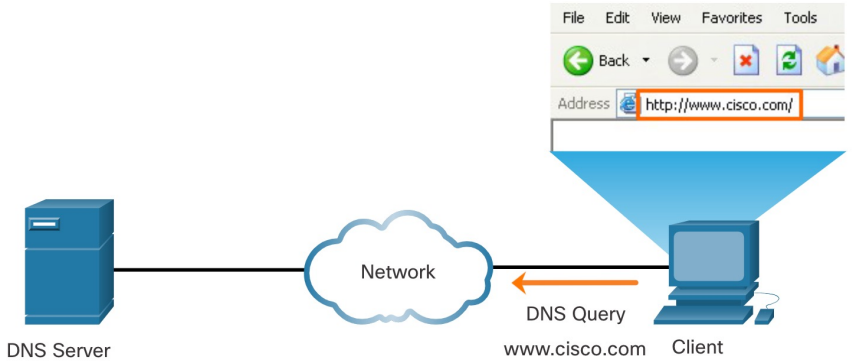
The DNS Lookup Process

Steps involved in DNS resolution:

Step 1 - The user types an FQDN (Fully Qualified Domain Name) into a browser application Address field.



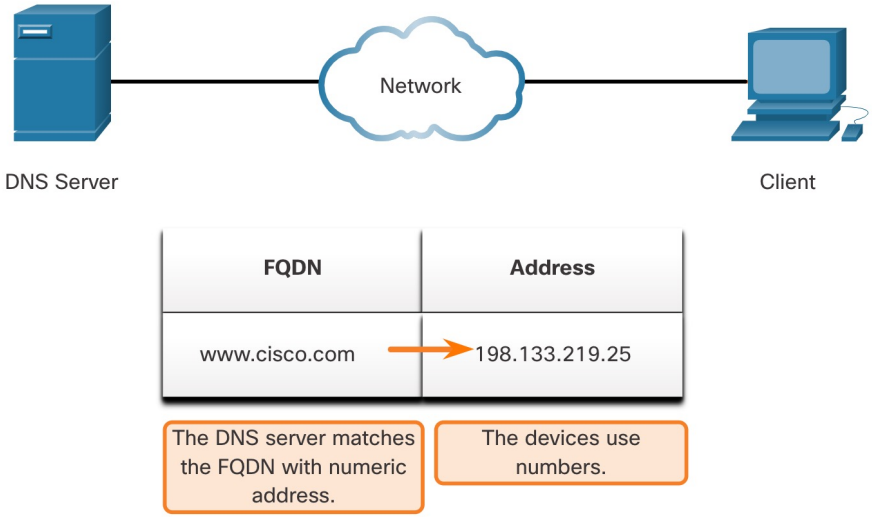
Step 2 - A DNS query is sent to the designated DNS server for the client computer.



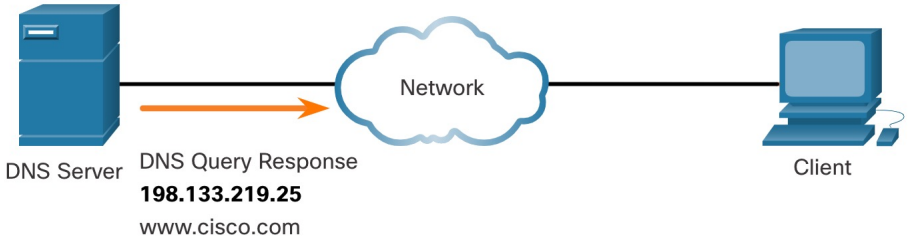
The DNS Lookup Process (Contd.)

Steps involved in DNS resolution:

Step 3 - The DNS server matches the FQDN with its IP address.



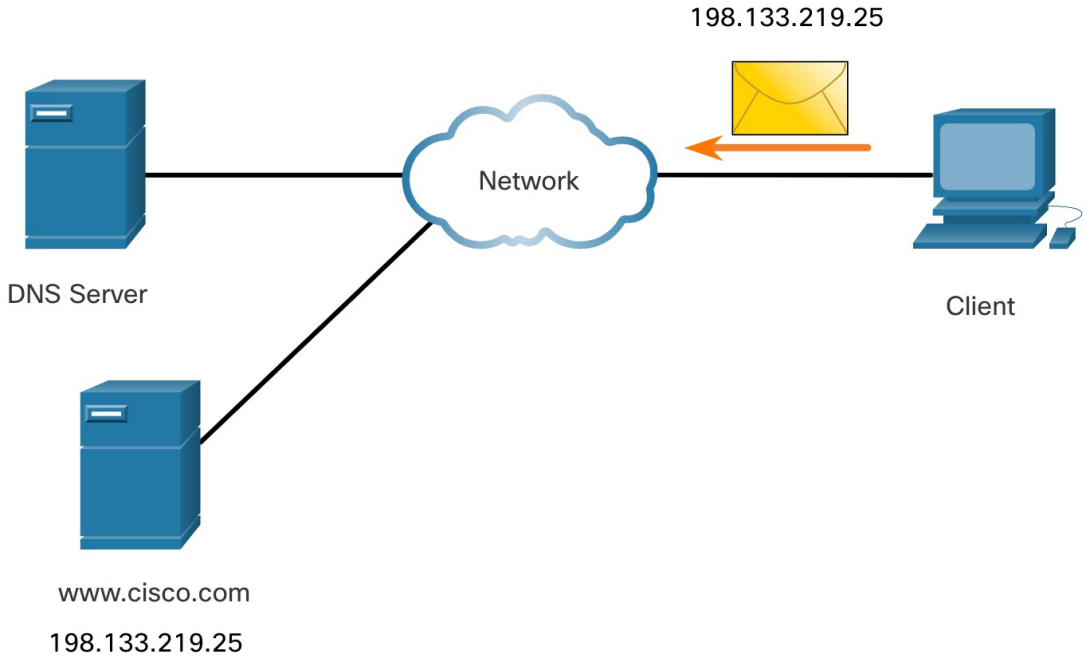
Step 4 - The DNS query response is sent back to the client with the IP address for the FQDN.



The DNS Lookup Process (Contd.)

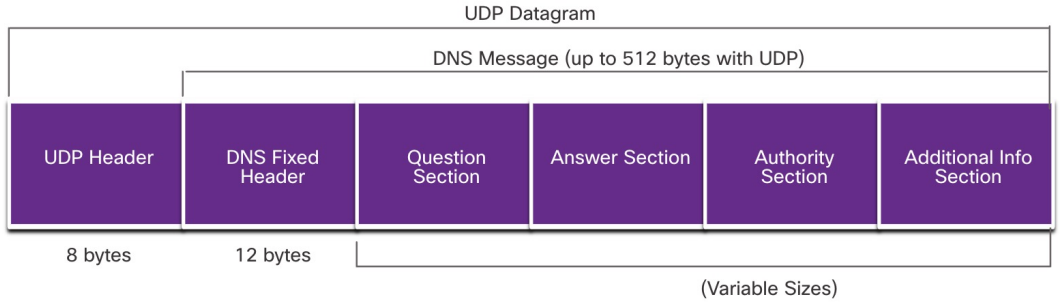
Steps involved in DNS resolution:

Step 5 – The client receives the IP address of the FQDN.



DNS Message Format

- DNS uses UDP port 53 for DNS queries and responses.
- If a DNS response exceeds 512 bytes, Dynamic DNS (DDNS) is used.
- The DNS protocol communications use a single format called a **message**.
- DNS uses the same message format for all types of client queries and server responses, error messages, and transfer of resource record information.



DNS Uses the Same Message For

- All types of client queries and server responses
- Error messages
- The transfer of resource records between servers

DNS Message Format (Contd.)

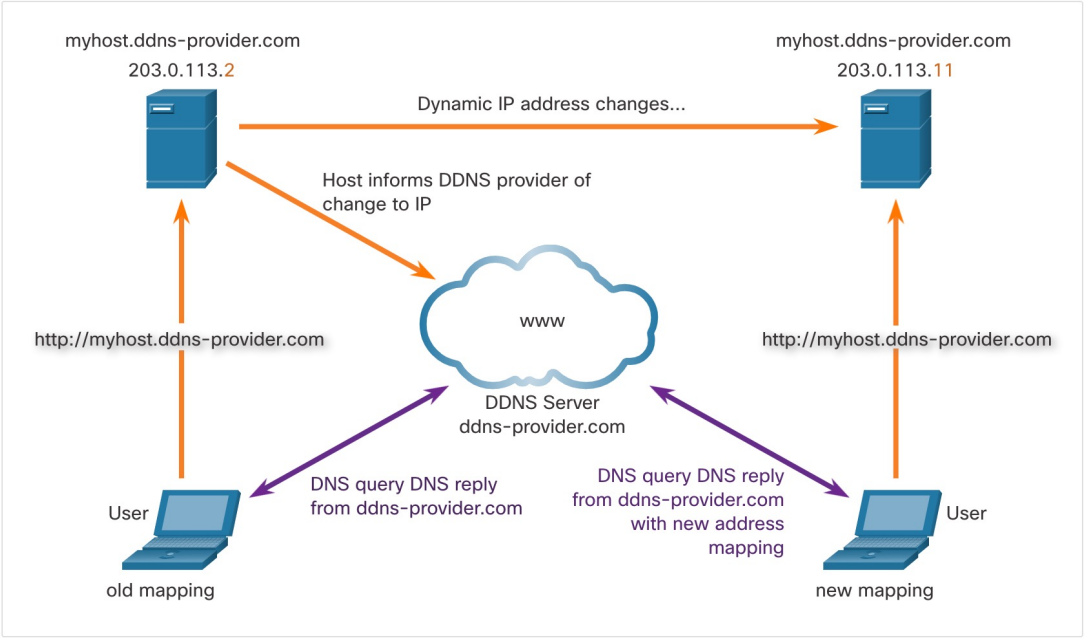
Sections of DNS message format :

DNS message section	Description
Question	The question for the server. It contains the domain name to be resolved, the class of domain, and the query type.
Answer	The DNS resource record, or RR, for the query including the resolved IP address depending on the RR type.
Authority	Contains the RRs for the domain authority.
Additional	Relevant to query responses only. Consists of RRs that hold additional information that will make query resolution more efficient

Dynamic DNS

Dynamic DNS (DDNS)

- Allows a user or organization to register an IP address with a domain name as in DNS.
- When the IP address of the mapping changes, the new mapping can be propagated through the DNS almost instantaneously.

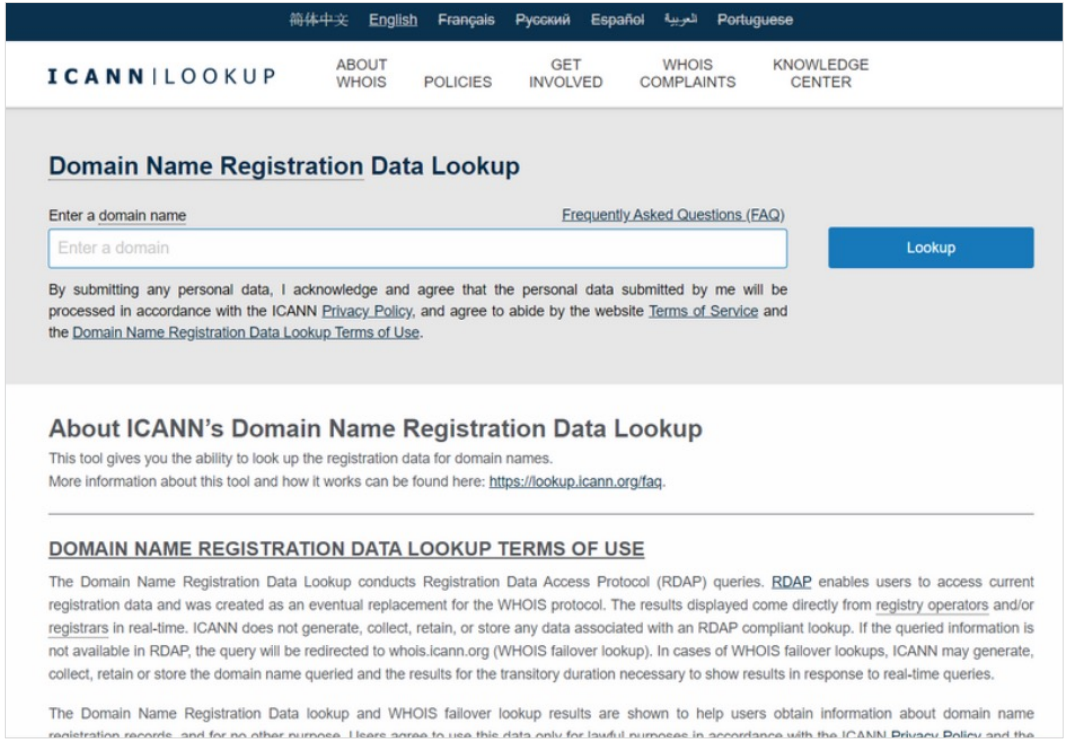


https://www.youtube.com/watch?v=rOLGvZagdC0

The WHOIS Protocol

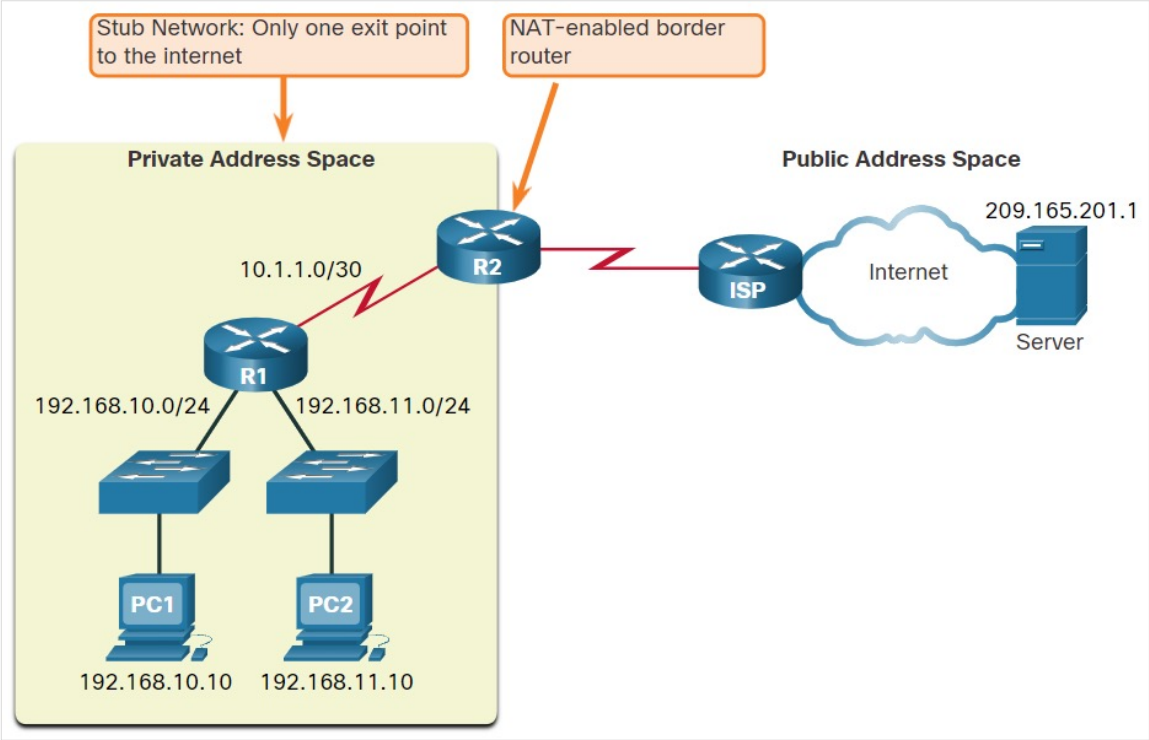
WHOIS Protocol:

- WHOIS is a TCP-based protocol that is used to identify the owners of Internet domains through the DNS system.



Network Address Translation (NAT) – Enabled Routers

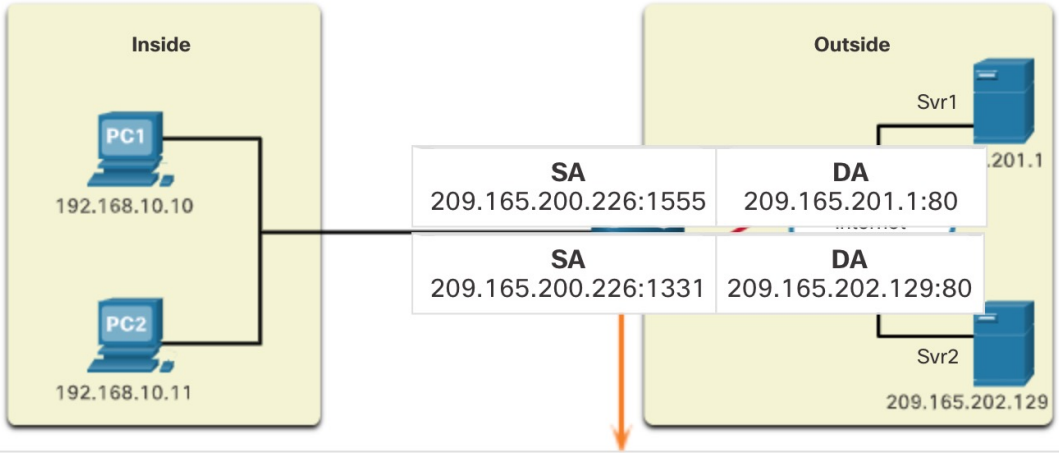
- NAT is used to conserve public IPv4 addresses.
- NAT-enabled routers can be configured with one or more valid public IPv4 addresses which are known as the **NAT pool**.
- A NAT router typically operates at the border of a stub network.



https://www.youtube.com/watch?v=FTUV0t6JaDA

Port Address Translation

- Port Address Translation (PAT)
  - One-to-many – Many internal address translations to one or more public IP addresses.



NAT Table with Overload

Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global IP Address
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80

New Terms and Commands

• DHCP(Dynamic Host Configuration protocol) • Lease period • DNS (Domain Name System) • DDNS (Dynamic DNS)	• WHOIS • FQDN • NAT

Lab 14 - Using Wireshark to Examine a UDP DNS Capture

- In this lab, you will complete the following objectives:
  - Communicate with a DNS server by sending a DNS query using the UDP transport protocol.
  - Use Wireshark to examine the DNS query and response exchanges with the same server.