

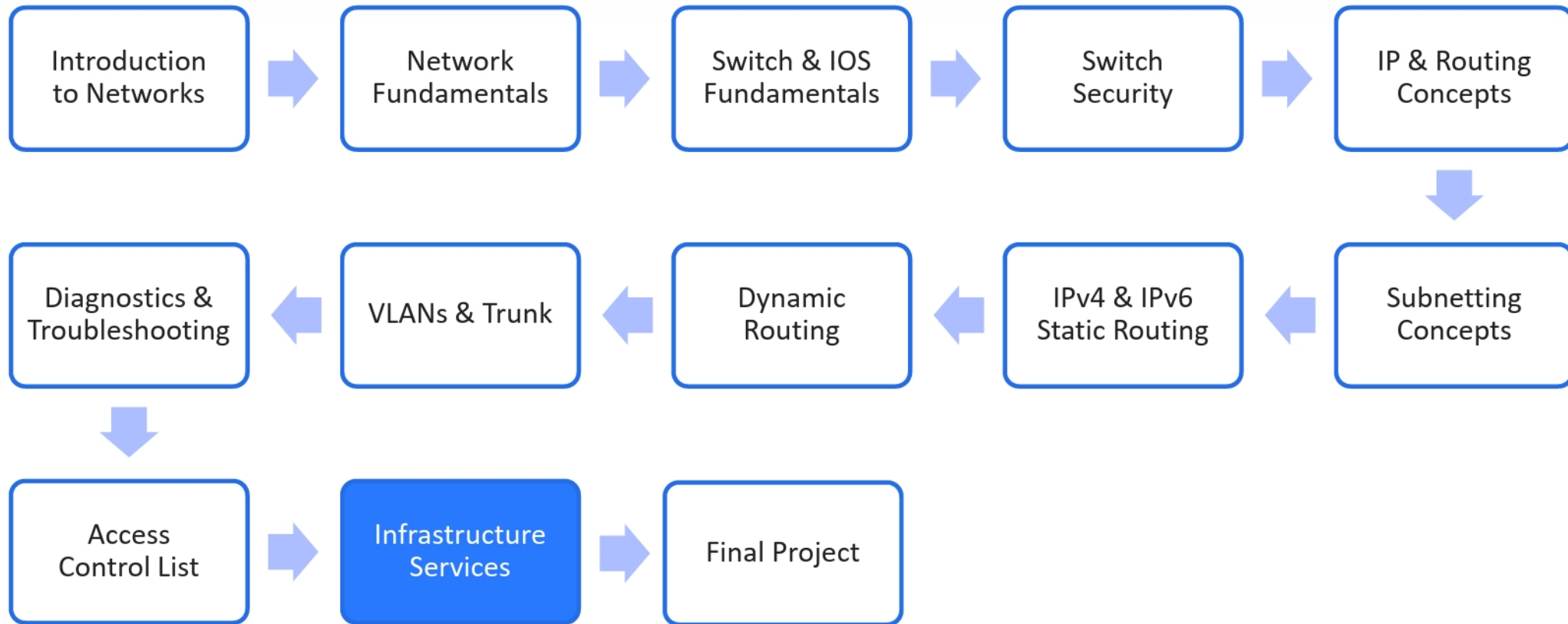


Cybersecurity Professional Program

Infrastructure Services

Computer Networking

Computer Networking Course Path



Overview

Lesson Objective

The objective of this lesson is to become familiar with infrastructure services, such as NAT, and how they are configured.

In addition, this lesson covers how to configure and implement DHCP.



DHCP Overview

DHCP Implementation

NAT Overview

NAT Implementation

Infrastructure Services

DHCP OVERVIEW

DHCP Purpose

Why Use DHCP?



To communicate with each other, all devices on a network must have a unique IP address.

Network administrators will often be responsible for assigning static IP addresses to network components, such as routers, servers, firewalls, etc.

Assigning a static IP address for every endpoint in an organization can be time consuming. Many endpoints do not require a static IP address.



What Is DHCP?

DHCP



The solution is to use Dynamic Host Configuration Protocol (DHCP).

DHCP was designed to manage IP address allocation automatically on any network or device. It operates as a server with a range of IP addresses that it allocates dynamically to devices on the network.

It also includes additional network information, such as the DNS server address, default gateway address, and more.

Routers can also operate as DHCP servers.



DHCP is defined in RFC 2131.

DHCP Characteristics

OSI Model Layer

DHCP operates in the **application layer** of the OSI and TCP/IP models.

Logical Ports

DHCP operates on UDP ports **67** (server) and **68** (client).

Versions

DHCP supports both **IPv4** (DHCPv4) and **IPv6** (DHCPv6).

DHCP Allocation Methods

Dynamic Allocation

The DHCP server assigns an available IP address to the client from its address pool for a limited amount of time.

This means that the client “leases” the address from the server for a period set by the administrator.

At the end of the lease, the client requests an extension or a new address.

Automatic Allocation

As in the dynamic allocation method, the client receives a random available IP address. But in this case, there is no time limit for the address.

The client does not have to renew the lease for the address it was assigned.

Reservation Address

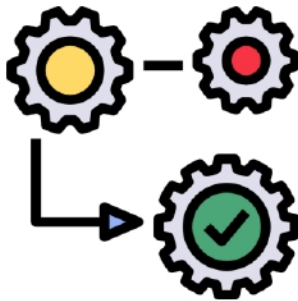
The network administrator configures the DHCP server to allocate a specific IP address to a selected client device.

The address is reserved for a specific device in advance based on its MAC address.

This method is useful for devices such as network printers and others.

DHCP Operation

How DHCP Works



The DHCP process includes four basic steps:

Discover, Offer, Request, and Acknowledgment (DORA).

The client device typically starts the process by contacting the server.

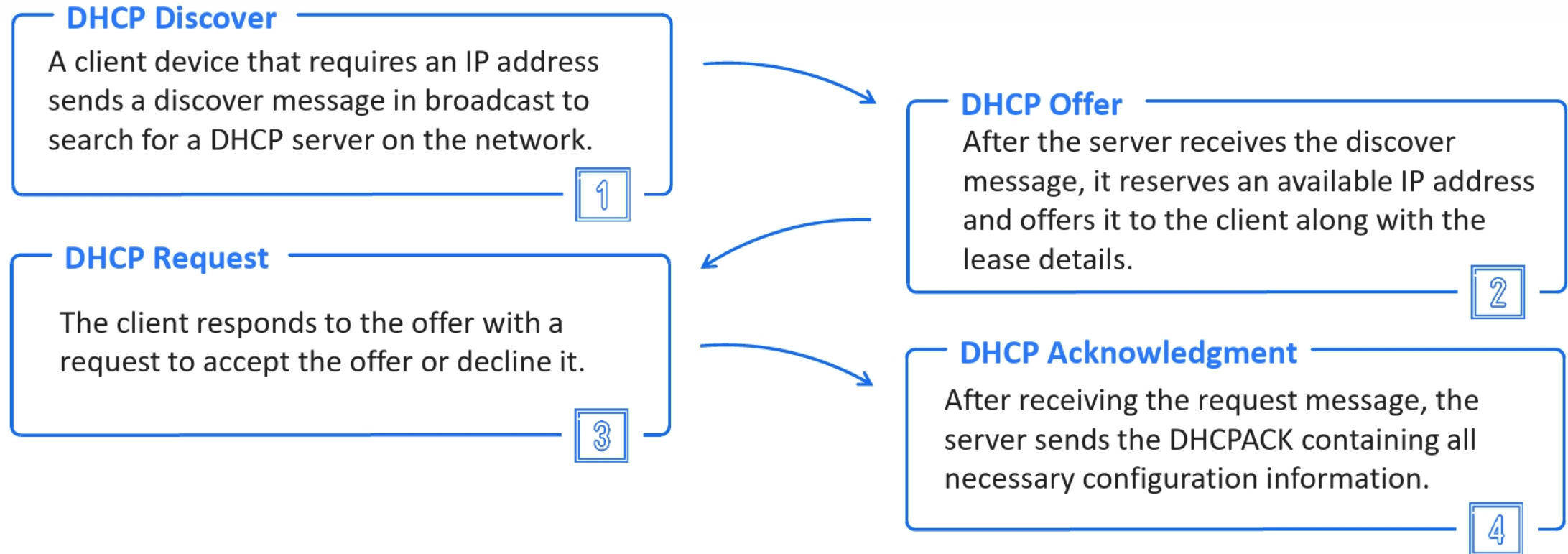
The information passing between the client and server is encapsulated in dedicated DHCP packets.

The DHCP server allocates the IP address and other information according to the chosen allocation method (dynamic, automatic, etc.).



The DHCP process is known as DORA.

DHCP Process



DHCP Lease Renewal Process

DHCP Request



Before a lease expires, the client sends a DHCPREQUEST message directly to the DHCPv4 server that originally offered the IPv4 address.



DHCP Acknowledgment



Upon receiving the DHCPREQUEST message, the server verifies it and, if possible, extends the lease information by returning a DHCPACK.



Messages can be sent in unicast or broadcast.

Router vs. Server

Router

Used in small and medium-sized businesses

Easy to manage

Requires knowledge of Cisco IOS and the relevant configuration

Relatively low cost, as no device is required other than the existing router



VS.

Server

Used in larger networks and enterprises

Easy to manage

Requires general knowledge of servers, especially DHCP servers

Relatively expensive, especially if the organization needs to buy a dedicated server to act as the DHCP server



DHCPv6

DHCP for IPv6



Unlike IPv4, IPv6 uses multiple types of addresses from different hosts. DHCPv6 was developed due to the usage in networks of various address formats and prefixes instead of subnet masks. DHCPv6 also supports more allocation methods than DHCPv4. For example, an IPv6 host can automatically generate an IP address internally using stateless address auto-configuration (SLAAC) or the EUI-64 process for link-local addresses.



DHCPv6 is defined in RFC 2460.

DHCPv6 Allocation Methods

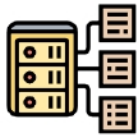
SLAAC



In this method, the device can obtain an IPv6 global address without the services of a DHCP server. The device uses ICMPv6 for advertisement messages to provide addressing and other configuration information that would normally be provided by a DHCP server.



Stateless DHCPv6



The stateless DHCPv6 method informs the client to use the information in the router advertisement (RA) message for addressing, while additional configuration parameters are available from a DHCPv6 server. The client will then communicate with a stateless DHCPv6 server to obtain additional information not provided in the RA message, such as a DNS server address.



Stateful DHCPv6



Like DHCPv4, addressing information and configuration need to be obtained from a DHCPv6 server.



Infrastructure Services

DHCP IMPLEMENTATION

Configure a DHCPv4 Server

Configuration Steps

Step 1: Exclude addresses from the DHCP pool.

Run *ip dhcp excluded-address* to reserve an IP address for the default gateway or statically configured servers.

Step 2: Set up a DHCP pool of addresses using *ip dhcp pool*

Step 3: Configure specific tasks, such as the default gateway, DNS server, domain name, etc.

Note: The *lease 0 4 30* (days, hours, minutes) will not work in Packet Tracer, but it does work on real Cisco devices.

Set R1 as a DHCP Server

```
R1(config)#ip dhcp excluded-address 192.168.0.1
R1(config)#ip dhcp excluded-address 192.168.0.100 192.168.0.150
R1(config)#ip dhcp pool LAN1
R1(dhcp-config)#network 192.168.0.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.0.1
R1(dhcp-config)#dns-server 192.168.0.105
R1(dhcp-config)#domain-name Cyber.com
R1(dhcp-config)#lease 0 4 30
R1(dhcp-config)#exit
```

Verify DHCP Settings

Several commands can be used to verify and troubleshoot DHCP settings:

show ip dhcp pool: Displays pool settings

show ip dhcp binding: Displays the client list, with IP, MAC address, and lease expiration

show ip dhcp conflict: Displays IP conflicts detected during DHCP negotiation

Verify Settings on R1

```
R1#show ip dhcp pool
```

Pool LAN1 :

```
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)          : 0 / 0
Total addresses                   : 254
Leased addresses                  : 3
Excluded addresses                : 2
Pending event                     : none
```

1 subnet is currently in the pool

Current index	IP address range	Leased/Excluded/Total
192.168.0.1	192.168.0.1 - 192.168.0.254	3 / 2 / 254



Configure DHCPv4 Relay

DHCP relay is a technique that allows devices to obtain addresses from a DHCP server on a remote network.

Note: Broadcast messages are not transmitted to other networks. When a client sends DHCPDiscover, the router acts as a relay and forwards the message directly to the server in unicast.

Enable the *ip helper-address* command and DHCP server address on the interface that receives the requests.

Relay Setting on R1

```
R1(config)#interface gigabitethernet 0/0
#The IP of the DHCP Server.
R1(config-if)#ip helper-address 10.0.0.250
R1(config-if)#exit
```

Configuring a DHCPv4 Client

A router can also act as a DHCP client. Its interface can be set manually or dynamically.

Use the *ip address dhcp* command on the interface to enable dynamic allocation.

For example, an interface facing the ISP typically gets an IP from the ISP DHCP server.

Set R1 as a DHCP Client

```
R1(config)#interface gigabitethernet 0/0
R1(config)#ip address dhcp
R1(config)#exit
*Aug 18 12:42:22.507: %DHCP-6-ADDRESS-ASSIGN: Interface
GigabitEthernet0/0 assigned DHCP address 209.165.201.12, mask
255.255.55.0, hostname R1
R1(config)#do show ip interface brief
```

Interface	IP-Address	OK?	Method	Status
Protocol				
GigabitEthernet0/0	209.168.201.12	YES	DHCP	up up
GigabitEthernet0/1	unassigned	YES	unset	administratively

Lab NET-12-L1

Configure DHCPv4 on a Cisco Router
30–60 Min.



Mission

The objective of this lab is to set up a DHCP service on a Cisco router and make sure all devices on the network receive addresses dynamically. The lab also promotes understanding of the DHCP relay concept.

Steps

- Answer the questions.
- Configure DHCPv4 on R1.
- Verify DHCP configuration.
- Configure DHCP relay.

Environment & Tools

- OS: All platforms
- Tools: Cisco Packet Tracer 7.2.2 or higher

Related Files

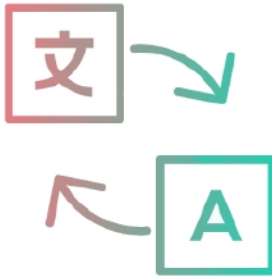
- Lab document
- NET-12-L1.pka

Infrastructure Services

NAT OVERVIEW

What Is NAT?

NAT Protocol



Network address translation (NAT) is an essential protocol and service that converts a private address to a public address and vice versa.

NAT is usually enabled on a firewall or router device at the edge of the local network and the beginning of the outside network.

Access to the internet from any home-based, corporate, or local network is only possible through NAT.



NAT is defined in RFC 2663.

Why Use NAT?

NAT's Usefulness



Although IPv4 is required for a device to communicate properly, the number of available addresses is being depleted rapidly, and, at this rate, a worldwide address shortage is imminent.

To save addresses and slow the depletion, private addresses were separated from public addresses.

Private addresses uniquely identify devices within a network, such as a computer connected to an internal server.

Public addresses identify groups of computers outside of a local network.



Private IP addresses are defined in RFC 1918.

Private IP Space

According to RFC 1918, three address spaces are reserved for devices in a private network (LAN). Their usage is unlimited, and they can be freely implemented.

Private IP Range

IP	Subnet
10.0.0.0–10.255.255.255/8	255.0.0.0
172.16.0.0–172.31.255.255/12	255.240.0.0
192.168.0.0–192.168.255.255/16	255.255.0.0



NAT Operation

How NAT Works



The NAT process is transparent to users, and any evidence of its operation is stored in a special table in the NAT-enabled device. This helps hide the internal network from the internet and adds an extra layer of security.

NAT operates in one of three methods: static, dynamic, or port address translation (PAT).

Each method uses a specific address terminology to describe its operation.



Theoretically, the maximum number of private addresses that can be translated into one public address is 65,536.

NAT Advantages and Disadvantages

Advantages

Prevents IPv4 address depletion (PAT)

Flexible network design and address scheme

Provides an additional layer of security



VS.

Disadvantages

Accessing internal resources requires special configuration and makes troubleshooting more challenging.

Reduces network performance and resource availability. Difficult to troubleshoot issues remotely.

NAT interferes with integrity checks because it modifies values in the headers.



NAT Address Terminology

Inside Local



The source IP address of the local device in the private network

For example: **10.0.0.5/24**

Outside Local



The IP address of the destination device as viewed from the inside local device (the destination LAN)

For example: A remote web server

Inside Global



The public IP address used by the inside local device for identification and access to the internet

For example: The IP address on an interface facing a WAN

Outside Global



The IP address of the destination device as viewed from the outside network (the NAT-enabled router)

For example: A remote web server

NAT Operation Steps

Step 1

A host on the local network sends a request to an external destination (outside local), such as a web server.

1

Step 3

The mapped address pair is saved in the device's NAT table and forwarded to the external destination IP (outside global) on the internet.

3

Step 5

The NAT-enabled device receives the reply from the web server and converts the public destination address to the original private address (based on the NAT table). The local host then receives the server's reply.

5

Step 2

The NAT-enabled device receives the request and changes the local device source address (inside local) to the public IP configured on the WAN interface (inside global).

2

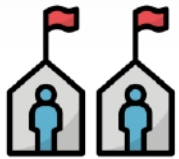
Step 4

The web server receives the request and replies with a public source IP.

4

NAT Methods

Static NAT



One-to-One NAT

This is a permanent mapping of a single private IP to a specific single public address. This method is not meant to conserve IPv4 addresses but to allow access to internal resources from an outside network.



Dynamic NAT

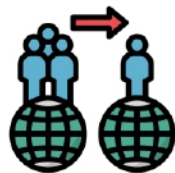


Many-to-Many NAT

This method is also not meant to conserve addresses. Multiple IP addresses are mapped dynamically by the router to a pool of public addresses. The conversion is done on a first-come, first-served basis.



NAT Overload



Many-to-One NAT

NAT overload or port address translation (PAT) is the most common method and is used to conserve addresses. In this method, multiple private IP addresses are converted into a single public address. To distinguish the traffic from different devices, the source port number is also used for the inside global address.



NAT64

What Is NAT64?



Network address translation **IPv6** to **IPv4** (NAT64) technology facilitates communication between IPv6-only and IPv4-only hosts and networks.

The solution allows enterprises and ISPs to accelerate IPv6 adoption while simultaneously handling IPv4 address depletion.



Infrastructure Services

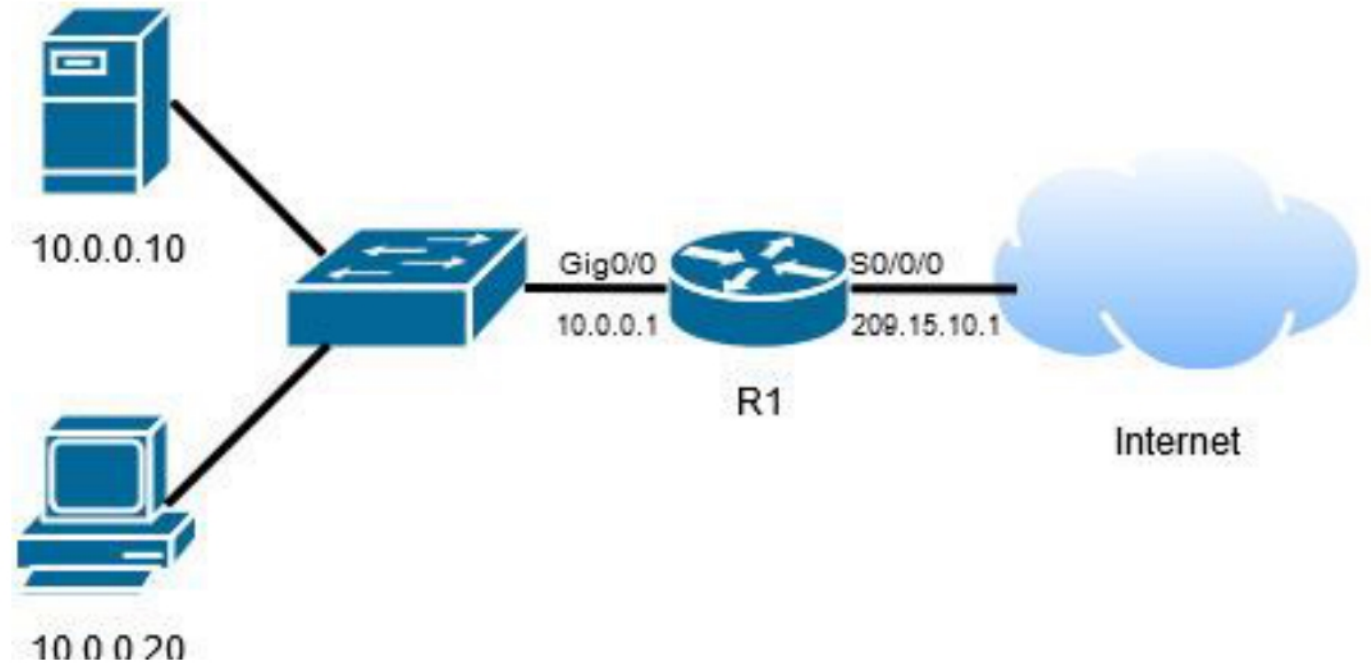
NAT IMPLEMENTATION

NAT Topology

The example on the right illustrates the simple topology of a router connecting a small corporate network to the internet.

The next slide shows how each NAT method is configured and verified on R1.

Network Example



NAT Interface Configuration

The first step in configuring NAT is to set the router's interfaces for the translation process.

The `ip nat inside\outside` command tells the router which interfaces will participate in the NAT process and their direction based on the network topology.

Each interface connected to the private network is defined as `inside`, and each interface connected to the internet is defined as `outside`.

Setting Interfaces on R1

```
#The interface facing the LAN.
Edge-R1(config)#interface gigabitEthernet 0/0
Edge-R1(config-if)#ip add 10.0.0.1 255.255.255.0
Edge-R1(config-if)#ip nat inside
Edge-R1(config-if)#no shutdown
Edge-R1(config-if)#exit

#The interface facing the WAN.
Edge-R1(config)#interface serial 0/0/0
Edge-R1(config-if)#ip add 209.15.10.1 255.255.255.0
Edge-R1(config-if)#ip nat outside
Edge-R1(config-if)#no shutdown
Edge-R1(config-if)#exit
```

Static NAT Configuration

Command

```
ip nat inside source static <local-ip> <global-ip>
```



In this example, a user wants to connect to the internal server from somewhere on the internet.

The user cannot access the LAN directly, so it sends the request to public router interface **209.15.10.1**, and the router uses the NAT static map to forward the request to the **10.0.0.10** server.

The second section in the example on the right is for port forwarding. It forwards only SSH traffic from outside to the server.

Static Map on R1

```
#Map all traffic between 10.0.0.10 and 209.15.10.1
Edge-R1(config)#ip nat inside source static 10.0.0.10 209.15.10.1

#Map only SSH connection between 10.0.0.10 and 209.15.10.1 on tcp
port 8080 of the outside
Edge-R1(config)# ip nat inside source static tcp 10.0.0.10 22
209.15.10.1 8080
```



Dynamic NAT Configuration

Assume the ISP defined 10 public addresses on the WAN interface:

Step 1: Create a public address pool using *ip nat pool*.

Step 2: Configure standard ACL to identify local addresses that need to be translated using *access-list*.

Step 3: Bind the ACL and the pool using *ip nat inside source list*.

Note: Using this method, the pool should contain enough available addresses: one for each device.

Set Dynamic NAT on R1

#Dynamic NAT allows local hosts access to the outside network, using a randomly selected public address from the pool.

```
Edge-R1(config)#ip nat pool ToFreedom 209.15.10.1 209.15.10.10  
netmask 255.255.255.0
```

```
Edge-R1(config)#access-list 1 permit 10.0.0.0 0.0.0.255
```

```
Edge-R1(config)#ip nat inside source list 1 pool ToFreedom
```

NAT Overload Configuration

NAT overload or port address translation (PAT) allows a router to use a single public address for multiple inside local addresses.

Methods to configure PAT:

1. Use an address pool.
2. Use a single address defined on the interface.

An important part of the command is the **overload** option.

Set PAT on R1

#Method 1

```
Edge-R1(config)#ip nat pool ToFreedom 209.15.10.1 209.15.10.10  
netmask 255.255.255.0  
Edge-R1(config)#access-list 1 permit 10.0.0.0 0.0.0.255  
Edge-R1(config)#ip nat inside source list 1 pool ToFreedom overload
```

#Method 2

```
Edge-R1(config)#access-list 1 permit 10.0.0.0 0.0.0.255  
Edge-R1(config)#ip nat inside source list 1 interface serial 0/0/0  
overload
```

Verify NAT Settings

Two commands can be used to fully verify a NAT operation.

The `show ip nat statistics` command displays NAT parameter and pool configuration, pool status, and interface configuration.

The `show ip nat translations` command shows the active NAT translation (inside local and inside global address pairing, when they occur).

Note: Static NAT translation is always shown in the table.

Verify NAT on R1

```
Edge-R1#show ip nat statistics
Total translations: 5 (1 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: GigabitEthernet0/0
Hits: 5   Misses: 13
Expired translations: 1
Dynamic mappings:
-- Inside Source
access-list 1 pool ToFreedom refCount 0
  pool ToFreedom: netmask 255.255.255.0
                  start 209.15.10.1 end 209.15.10.1
                  type generic, total addresses 1 , allocated 0 (0%), misses 8

Edge-R1#show ip nat translations
Pro  Inside global      Inside local       Outside local      Outside global
---  ---                ---                ---                ---
tcp  209.15.10.1:50016   10.0.0.10:50016    8.8.8.8:53         8.8.8.8:53
tcp  209.15.10.1:50017   10.0.0.10:50017    200.10.0.254:80    200.10.0.254:80
tcp  209.15.10.1:50018   10.0.0.20:50018    157.160.27.8:80    157.160.27.8:80
tcp  209.15.10.1:50019   10.0.0.20:50019    82.11.0.2:443      82.11.0.2:443
```



QUESTIONS?



THANK YOU
