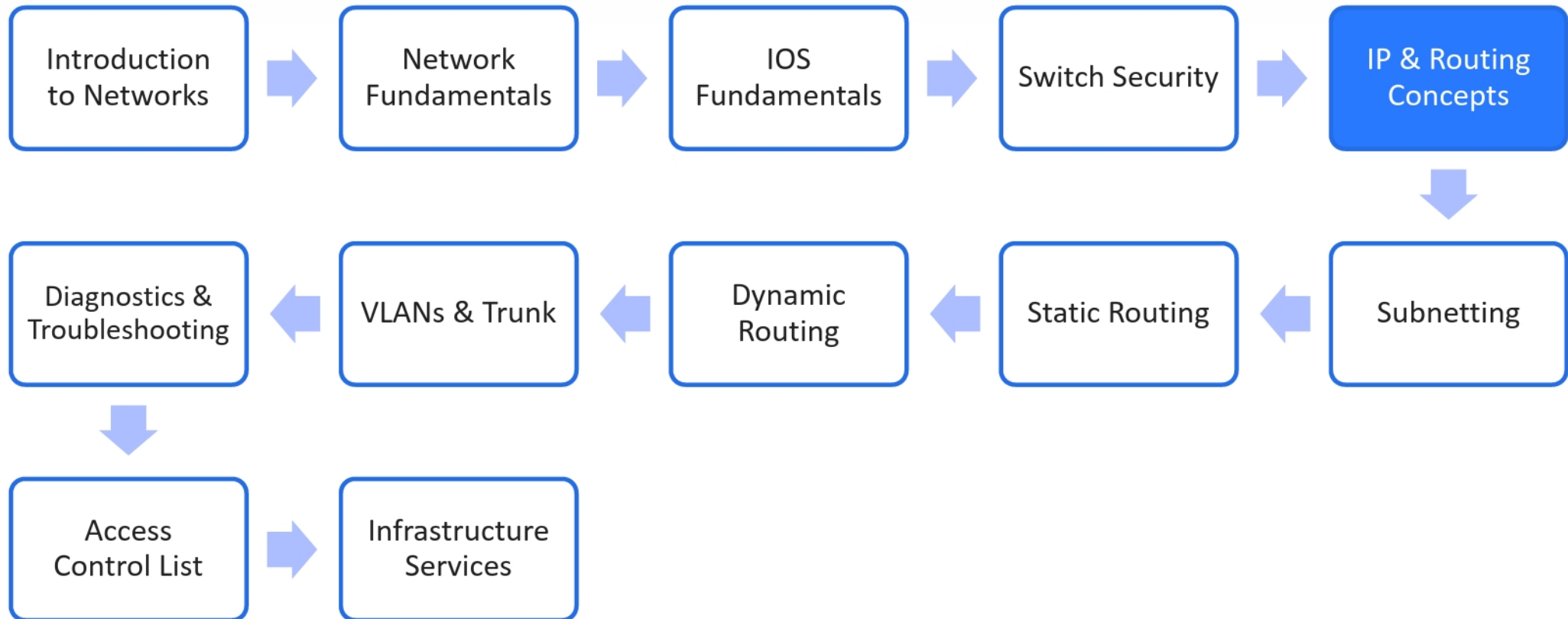


Cyber Security Professional Program

IP & ROUTING CONCEPTS

Computer Networking

Program Path



Overview

Lesson Objective

In a network, IP addresses are used to identify a device's source and destination. The object of this lesson is to understand routers, how they work, their processes, and the logic involved in IPv4/6 configuration.



Decimal, Binary, and Hex

The Router

Routing Process

IPv4

IPv6

IP & Routing Concepts

DECIMAL, BINARY, AND HEX

Number Systems

Decimal



The most common numbering system consists of ten numbers, 0-9, and it is called the decimal system. The system is based on the 10 fingers we use to count and is known as the *base-10 numeral system*.



Binary



Binary is an alternative number system that consists of only two numbers: **0** and **1**. This system is used by computers, which communicate by transmitting negative and positive electrical currents. Because there are only two numbers, the system is known as the *base-2 numeral system*.



Hexadecimal



Hex, or Hexadecimal, is a number system that consists of 16 characters, and is known as the *base-16 numeral system*. Hex uses the numbers 0-9, followed by the letters A-F. Hex is widely used as an alternative representation to binary, since it is a more human-oriented system.



Positional Notation

When learning about number systems, a good way to approach them is to consider numbers a result of their positions.

Each number's value can be calculated as a result of a function.

The function is the same regardless of the base being used, making it easier to perform base transitions.

The function is:
[number] = [digit] * [base] ^ [position].

Positional Conversion

02

Base 2

The Digits:

The Positions:

The Result:

1	0	1	1
2^3	2^2	2^1	2^0
8	0	2	1

10

Base 10

The Digits:

The Positions:

The Result:

1	0	2	4
10^3	10^2	10^1	10^0
1000	0	20	4

16

Base 16

The Digits:

The Positions:

The Result:

B	1	0	5
16^3	16^2	16^1	16^0
45056	256	0	5



Binary to Decimal

After the Positional Notation method is used to map a number's value, the positional value of each digit can be found. The next step is conversion, summarizing each of the individual values to get the result.

Conversion Formula

Positional Value	128	64	32	16	8	4	2	1
Radix (Base)	2	2	2	2	2	2	2	2
Position	1	1	0	1	0	1	0	0
Calculation	1x128	1x64	0x32	1x16	0x8	1x4	0x2	0x1
Positional Value	128	64	0	16	0	4	0	0
Result	128 + 64 + 0 + 16 + 0 + 4 + 0 + 0 = 212							



Decimal To Binary

While the aim of conversion to decimal is to solve a formula, the aim of conversion from decimal is to find the missing variable.

The operation can be summed up as **find the X** that will result in the closest number.

For example, when converting the number 1994 to binary, the first step is to find **X**, where 2^x is the closest to 1994.

Continuing this process, the number should be written down and the calculation should be repeated for the remainder.

Positional Conversion

$$\begin{array}{r}
 1994 \\
 - 1024 \\
 \hline
 970 \\
 - 512 \\
 \hline
 458 \\
 - 256 \\
 \hline
 202 \\
 - 128 \\
 \hline
 74 \\
 - 64 \\
 \hline
 10
 \end{array}$$

$$2^{10}=1024$$

$$2^9=512$$

$$2^8=256$$

$$2^7=128$$

$$2^6=64$$

$$2^3=8$$

$$\begin{array}{r}
 10 \\
 - 8 \\
 \hline
 2 \\
 - 2 \\
 \hline
 0
 \end{array}$$

$$2^3=8$$

$$2^1=2$$

32	16	8	4	2	1
0	0	1	0	1	0
2048	1024	512	256	128	64
0	1	1	1	1	1



Calculation Tricks

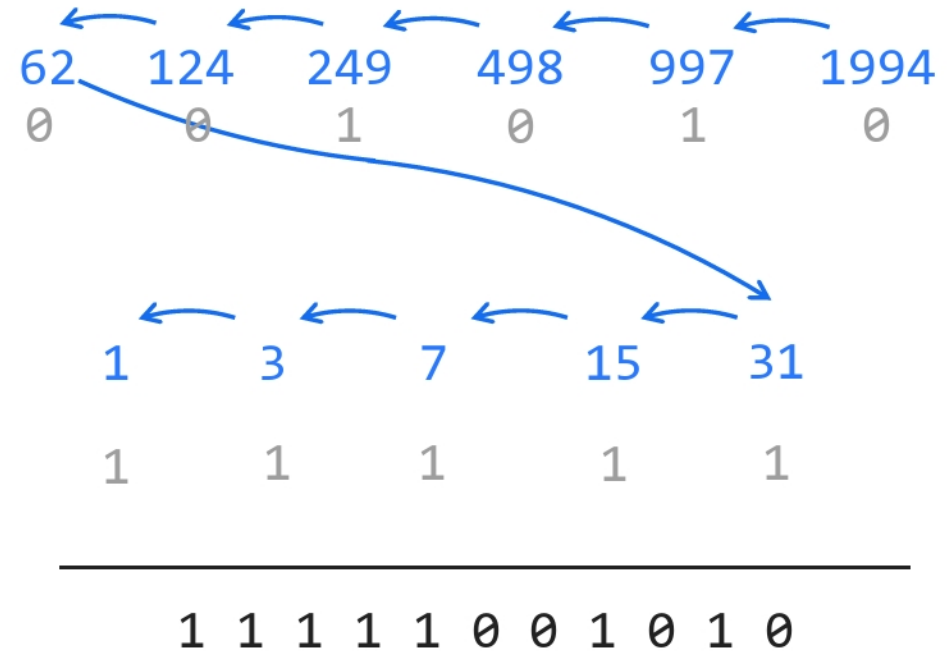
For binary, there are some tricks that can make the calculation easier, instead of having to guess.

One trick is to take the desired number and divide it, without the remainder, while recording each operation.

If the result is even, write a 0. If it is odd, write a 1. The binary representation will appear when the operations are done.

For other bases, there are other tricks and mathematical methods.

Division Calculation



Binary to Hexadecimal

Because 16 is technically 2^4 , conversion from base-2 to base-16 is rather easy. Each hexadecimal digit can be considered a representation of 4 binary digits. For example, 101110 is 0010 + 1110, making it 2E in hexadecimal.

Conversion Formula

Number	0	1	2	3	4	5	6	7
Binary	0000	0001	0010	0011	0100	0101	0110	0111
Hexadecimal	0	1	2	3	4	5	6	7
Number	8	9	10	11	12	13	14	15
Binary	1000	1001	1010	1011	1100	1101	1110	1111
Hexadecimal	8	9	A	B	C	D	E	F



Hexadecimal Conversion

Here is how binary is converted to hex, with an example.

Binary to Hex



- Divide the binary number into groups of 4 digits.
- Convert each group to its equivalent hex value using the Base Comparison table.
- Merge the results of each group.



Example



Convert 0111111111010100 to hex.

- 0111 1111 1101 0100
- 0111 = 7, 1111 = F, 1101 = D, 0100 = 4
- Answer is 7FD4



Other Bases

Base-X



There are other bases besides binary, decimal, and hexadecimal. Throughout history, other counting systems, such as base-6, base-8, and base-12 were developed.

Old British measurements, such as dozen (12), gross (144), and feet (12 inches) are suspected to have been originated by a base-12 number system.



Most of those bases are no longer in use today.

LAB NET-05-L1

Converting Decimal, Binary, and Hex
30–60 Min.



Mission

The objectives of this exercise are to understand numbering systems and how to convert between them.

Steps

- Convert Decimal to Binary
- Convert Binary to Decimal
- Convert Binary to Hex
- Convert Hex to Binary

Environment & Tools

- Calculator

Related Files

- NET-05-L1 Converting Decimal ,Binary, and Hex

IP & Routing Concepts

THE ROUTER

Overview

Router



A router is a device designed to receive, forward, and analyze packets transmitted to and from other devices on a network, and other networks.

Routers enable inter-network communication, and can provide services such as ACL and NAT, which are required in any networking scheme.



A router is a Layer 3 device that communicates using IP addresses.

Default Gateway

Default Gateway



The default gateway is a network device that can route traffic to and from other networks. A router typically fulfills this role.

The default gateway is similar to the door of a room. If a desired object is in another room, the object can be reached only by exiting through the door.



If the destination is on the same network, there is no need to pass through the router.

The Router

Default Gateway Configuration

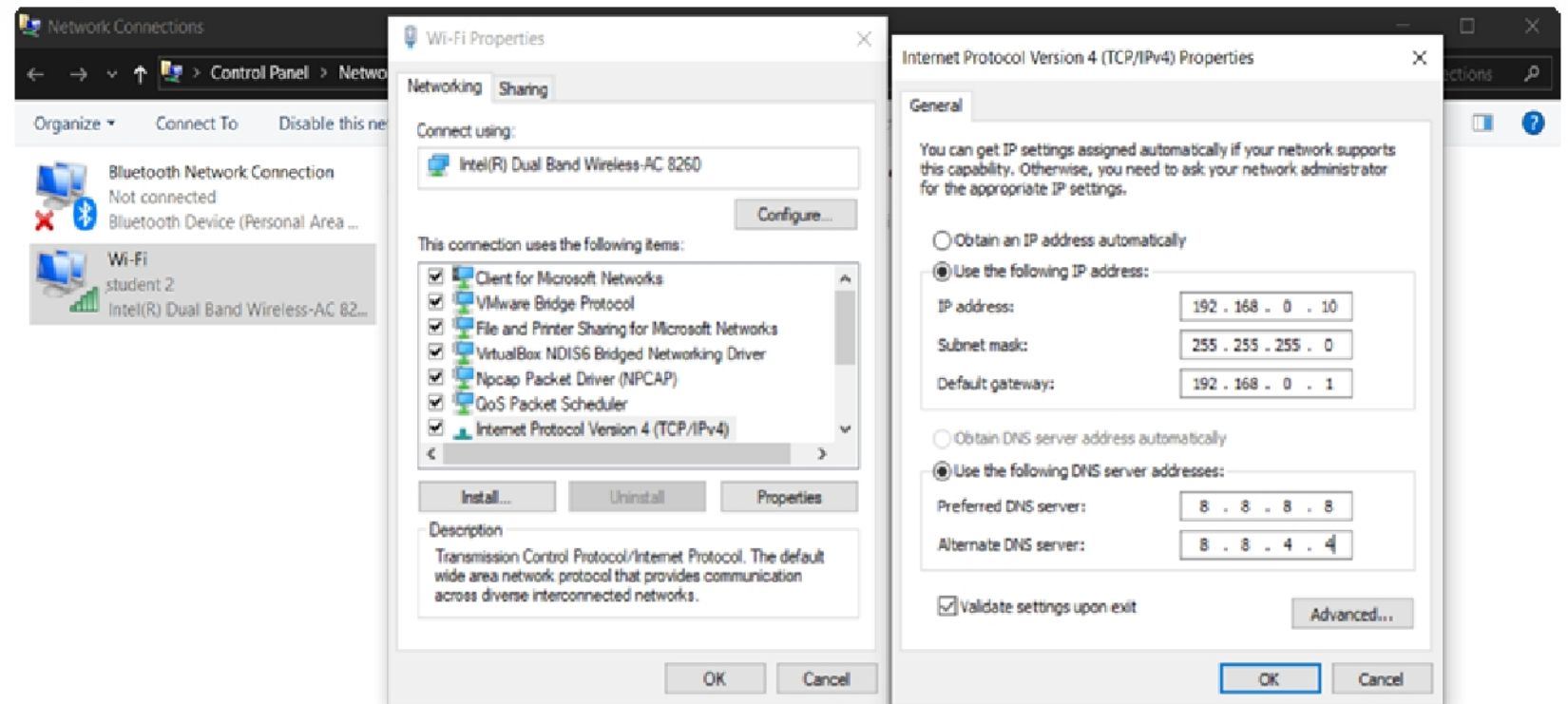
Default gateway configuration options are typically located together with other adapter configuration options.

In Windows, the settings are located under **Network & Internet Settings** in **Change Adapter Options**.

By default, the gateway should be received from the DHCP.

However, if manual IPs were configured, the gateway should also be configured manually.

NIC Configuration



Router Interfaces

Fast Ethernet Interface



Fast Ethernet was first made public in 1995. Ethernet operates at a speed of 100 Mbps and uses the media standard 100BaseT.



Gigabit Ethernet Interface



Gigabit Ethernet was introduced in 1999, and it supports a faster speed of 1000 Mbps. It uses the media standard 1000BaseT, but can also support 100 Mbps.



Serial Interface



Serial interfaces are used for long distance transmissions. If two serial ports need to communicate with each other, they must be synchronized with the same clock frequency and allocate the necessary bandwidth.



Logical Ports



Other Router Interfaces

Other common interfaces on a router include the Console and AUX (not the one used for audio).

Console



This is a physical management port, visually similar to Ethernet ports, that provides out-of-band access to a Cisco device. Out-of-band refers to access via a dedicated management channel used only for device maintenance.



AUX



The auxiliary port mainly functions as a backup console port, although it can also be used as a dial-up port for remote management, and other purposes. The main difference between Console and AUX is that AUX pushes output to the port after power-up, while a Console does so during the power-up process itself.



The Router

Interface Configuration

Router interfaces need to be set up with IP addresses, similar to computer network interfaces.

The **interface [type] [id]** command selects the desired interface.

To use an interface, it must be set up with

ip address [ip] [subnet mask] and enabled using the **no shutdown** command.

Use **show ip interface brief** to verify interface settings on the router.

Router Interface Configuration

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
R1(config-if)#exit
R1(config)#exit
R1#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.0.1	YES	manual	up	up



Loopback Interface

What it is used for ...



Loopback is a logical interface that is not assigned to a physical port. The interface can be used to test and manage Cisco IOS devices, because it ensures that at least one interface will always be available. It can also be used in the OSPF identification process.



A loopback interface should not be confused with a loopback address.

Loopback Interface Configuration

A Loopback Interface is often configured during the initial router configuration, mainly for testing purposes.

The interface is configured to automatically be ready for operation.

A router can have more than one loopback interface enabled simultaneously, but each interface must have a unique IP.

A loopback interface is created using the command **interface loopback <ID>** via the configuration terminal.

Loopback Interface Configuration

```
Router(config)#interface loopback 0
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
```

```
Router(config-if)#ip address 10.10.10.10 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)# exit
```



IP & Routing Concepts

ROUTING PROCESS

Overview

The Routing Process



The routing process involves selecting a path for the delivery of packets across different networks, from source to destination, through Layer 3 devices.

It is important to note that routers can route packets to directly connected networks, without requiring configuration. However, if the networks are not connected, the route needs to be learned.



Routing decisions are made based on a *routing table*.

Routing Process

Examination

In the first step, the router decides whether to process a packet or ignore it. Routers will ignore packets with errors, or packets they don't know how to process.

1

Decision-Making

The router decides where to forward the packet to, based on its destination IP address and the routing table.

3

Forwarding

After a decision is made, the router forwards the packet to the interface from which the packet must exit.

5

Decapsulation

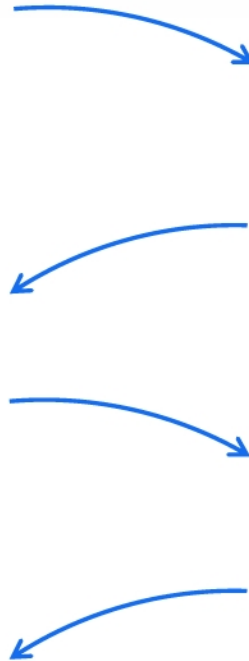
The router examines the Layer 2 address to decide if the packet was intended for itself (the default gateway), and verifies the integrity of the frame using the FCS (Layer 2 trailer).

2

Encapsulation

The router re-encapsulates the packet with new Layer 2 headers for the next hop, according to the decision made in step 3.

4



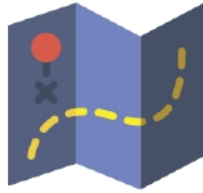
Routing Choices

Same LAN



If the destination IP is on the same LAN as the source device, there is no need for routing. The frame will get to the destination via the switch.

Known Route



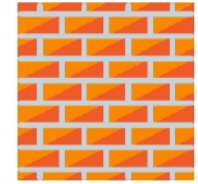
If the destination IP is on a different LAN, but the network device has a static or dynamic route to the destination IP, it will forward the packet to the next hop, based on the route.

No Route



If there is no static or dynamic route in the network device's routing table, it will forward the packet to its default 'gateway of last resort'.

No Gateway



If there is no 'gateway of last resort' and the destination packet is not listed, the router will discard the packet.

Routing Table

The Routing Table contains data stored in the router, with lists of routes to possible network destinations.

The table includes information about the network topology.

The codes on the left side of a route show how the network is learned by the router.

The command **show ip route** displays the routing table and is run in the Enable mode.

Routing Table

```
Router# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
        * - candidate default, U - per-user static route, o - ODR  
        P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks  
D       172.16.0.0/16 [90/5376] via 192.168.4.2, 00:02:24, GigabitEthernet4/0  
C       172.16.0.0/24 is directly connected, GigabitEthernet0/0  
S       172.16.1.0/24 [1/0] via 192.168.1.2  
R       172.16.2.0/24 [120/1] via 192.168.2.2, 00:00:15, GigabitEthernet2/0  
O       172.16.3.0/24 [110/2] via 192.168.3.2, 00:01:26, GigabitEthernet3/0  
C      192.168.1.0/24 is directly connected, GigabitEthernet1/0  
C      192.168.2.0/24 is directly connected, GigabitEthernet2/0  
C      192.168.3.0/24 is directly connected, GigabitEthernet3/0  
C      192.168.4.0/24 is directly connected, GigabitEthernet4/0
```

Routing Table Codes

Directly Connected / Local Route



When inspecting the routing table, records identified by the codes **C** or **L** indicate directly connected networks. The codes mean that the devices are connected to the physical layer. The **C** and **L** records are automatically created.



Static Route



Static routes are configured and recorded manually, and are identified in the routing table by the letter **S**.



Dynamic Route



Dynamic routes are identified with unique letters that indicate the dynamic protocol, as follows:

- D** - EIGRP routing protocol
- O** - OSPF routing protocol
- R** - RIP routing protocol



IP & Routing Concepts

IPV4

Overview

IP



An Internet Protocol (IP) is a numerical label assigned to devices connected to a network. It is used for host identification and communication.

The IP address space is managed by IANA (Internet Assigned Numbers Authority) and divided into five regional Internet registries (RIRs), each responsible for their designated territories.



Each RIR is responsible for address assignment to users and service providers.

IPv4 Addresses



IPv4 addresses consist of 32 bits and are divided into four octets, each containing 8 bits. This addressing method provides 4,294,967,296 (2^{32}) IPv4 addresses in total.

An IP address represented in binary will appear as follows:

192.168.1.1 = 11000000.10101000.00000001.00000001



IPv4 Structure



An IPv4 address consists of two parts: network and host, defined by the subnet mask.

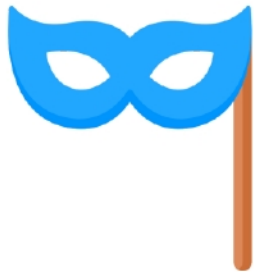
Network - Represents the network part of the IP address.

Host - Represents the specific device on the network segment.



Subnet Mask

Subnet Mask



A subnet mask is a 32-bit address, same as an IP address.

Like an IPv4 address, a subnet mask consists of 4 octets, separated by dots (.).

Subnet masks will be further explained in the next module.



Two similar IP addresses can belong to completely different networks, depending on the subnet mask.

Classful Addressing

A classful network is an addressing architecture that began in 1981, and was used until the introduction of Classless Inter-Domain Routing in 1993. It divides IPv4 address space into 5 classes, based on the 4 leading address bits.

Classful Table

NETMASK	RANGES	PREFIX	CLASS
255.0.0.0	1.0.0.0 - 127.255.255.255	/8	A
255.255.0.0	128.0.0.0 - 191.255.255.255	/16	B
255.255.255.0	192.0.0.0 - 223.255.255.255	/24	C
* Reserved for multicasting	224.0.0.0 - 239.255.255.255		D
* Experimental	240.0.0.0 - 255.255.255.255		E

NOTE: 255.255.255.255 is reserved as the IPv4 [Broadcast address](#).



Communication Types

Unicast



The most basic form of IP communication is *one-on-one*, where a packet is sent directly from one device on the network to another device on the network. A single source communicates with a single destination.



Multicast



Multicast is when a single source communicates with multiple destinations. A packet is sent from one device on the network to a group comprised of one or more devices, using Class D addresses.



Broadcast



Broadcast is when a packet is sent from one device on the network to all other devices on the network, using a generic broadcast address (255.255.255.255 or FF:FF:FF:FF:FF:FF).



IPv4

IPv4 Link Local

Link-Local



Link-Local addresses, also known as APIPA addresses, are valid only for communication within the network broadcast domain. The entire 169.254.0.0/16 address range is reserved for Link-Local.

If the DHCP is not available or an IP is not statically configured, the OS will randomly generate a Link-Local address.

Link-Local addresses are not guaranteed to be unique outside their network segment, which is the reason why routers do not forward their packets.



IPv4

Loopback Address

Loopback Address



Loopback addresses represent the same interface in a computer. In IPv4, an entire network (127.0.0.0/8) is reserved for loopback addresses.

Almost all leading operating systems use the name "localhost" to represent IPv4 loopback address 127.0.0.1.



The IPv6 address reserved for loopback is 0000:0000:0000:0000:0000:0000:0000:0001/128

Public vs Private

IP addresses are typically divided into two groups: private and public.

Private



Private IPs are non-unique addresses that can belong to one of three IP address ranges. They are used to create networks that do not communicate over the Internet. The same private IPs can be found in multiple separate networks and are free to use.



Public



Public addresses are used for communication over the Internet. These IP addresses must be unique, require a fee, and are purchased from service providers. A router will typically have both a private and public IP. For example, the address 8.8.8.8 is a public address used by Google.



IPv4

Private IP Ranges

Private addresses are used in networks designed for homes and organizations. The ranges differ according to the amount of separate networks and computers in each network, and there are no enforced rules.

Ranges

RANGE	TARGET	CLASS
10.0.0.0 – 10.255.255.255	A few large networks with many computers.	A
172.16.0.0 – 172.31.255.255	A considerable amount of medium-size networks.	B
192.168.0.0 - 192.168.255.255	Many small networks with only a few computers.	C



IPv4

LAB NET-05-L2

IPv4 & initial Router Configuration
30–60 Min.



Mission

The objective of this exercise is to learn how to configure initial settings on a Cisco Router.

Steps

- Initial Router Configuration
- Configure IPv4

Environment & Tools

- OS
 - All platforms
- Tools
 - Cisco Packet Tracer 7.2.2

Related Files

- NET-05-L2 IPv4 and Initial Router Configuration
- NET-05-L2.pka

IP & Routing Concepts

IPV6

Overview

The Need for IPv6



Over the years, the IPv4 address space was depleted, since technical progress meant that many more devices around the world were connected to the Internet.

IPv6 was designed to solve the IPv4 address space limitation and provide some additional enhancements. IPv6 has a larger 128-bit address space, with the number of available addresses being 340×10^{36} .



Example of an IPv6 address: 2001:0000:3238:0001:0063:0000:0000:FEFB

Compressing IPv6 Addresses

IPv6 addresses are long and difficult to read. Some rules exist to omit specific numbers to simplify the addresses.

Leading Zeros

The first rule allows us to discard leading zeros in a block, making the address a bit shorter:

2001:0:3238:1:63:0000:0000:FEFB

2

Zero Block

If there is a block that consists of 4 zeros, but without a consecutive zero-filled block, it can be replaced with a single zero, and the final address will be: **2001:0:3238:1:63::FEFB**

4

Full Address

A full address contains all 8 blocks, with 4 hexadecimal digits.

Example of a full IPv6 address:

2001:0000:3238:0001:0063:0000:0000:FEFB

1

Consecutive Zeros

If two or more blocks contain consecutive zeros, they can be omitted and replaced with double colon signs (::) resulting in: **2001:0:3238:1:63::FEFB**

Note that omitting is allowed only once in the address.

3

IPv6

IPv6 Address Breakdown

IPv6 Address

2001:0ABC:00BB:0000:0000:0000:0000:0001 /64

1 2 3 4



The prefix represents the prefix portion of the address. IPv6 does not use notation subnet masks like IPv4. The prefix length indicates the network portion.

1. Because the prefix is /64, the first 64 bits in the address represent the network portion.
2. The 16 bits from the 49th to the 64th are for defining subnets.
3. The remaining 64 bits represent the host portion in the IPv6 address.
4. The range can be from 0 to 128, with the most common being /64.

Configuration Example

```
Router(config-if)#ipv6 address  
2001:0ABC:00BB:0000:0000:0000:  
0000:0001/64
```



IPv6

Configure and Verify IPv6

To enable IPv6 routing, enter the configuration terminal mode, and run the command

ipv6 unicast-routing

Configure IPv6 on the router interface using the command **ipv6 address**

Verify the configuration using the command

show ipv6 interface brief

IPv6 Configuration on a Router

```
Router(config)#ipv6 unicast-routing
Router(config)#interface gigabitEthernet0/0/0
Router(config-if)#ipv6 address 2001:0ABC:00BB:0000:0000:0000:0000:0001/64
Router(config-if)#no shutdown
Router(config-if)#exit
Router#show ipv6 interface brief
GigabitEthernet0/0/0      [up/down]
    FE80::201:97FF:FE13:A801
    2001:ABC:BB::1
GigabitEthernet0/0/1      [administratively down/down]
    unassigned
Vlan1                     [administratively down/down]
    unassigned
```



Device Communication Types

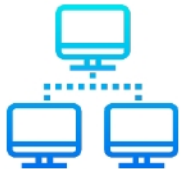
Unicast



Unicast addresses represent specific network interfaces that support IPv6.
Unicast addresses have 3 sub-types (described in the following slide).



Multicast



Addresses used to send IPv6 packets from a single host to multiple destinations.



Anycast



IPv6 unicast addresses that can be assigned to multiple devices. Packets sent to an Anycast address are routed to the nearest device that has that address (which is why Anycast is also known as "one to the nearest"). This method operates similar to IPv4 broadcast.



IPv6 Unicast Types

Global Unicast



IPv6 global unicast addresses are similar to IPv4 public addresses. They are unique and can be routed via the Internet. IANA currently assigns only 2000::/3 addresses.



Link-Local



Addresses that enable communication between devices in the same local link (LAN). Link Local addresses must be unique only within the link. They are not guaranteed to be unique beyond their network segment, and begin with FE80::/10.



Unique-Local



Similar to IPv4 private addresses, with minor differences.

Unique addresses should not be routable in the global IPv6, and should not be translated to global IPv6 addresses. They begin with FC00::/8.



IPv6 Address Example

The table below lists examples of commonly used IPv6 addresses of various types.

Common IPv6 Addresses

Type	Address Example	Notes
Global Unicast	2001:0ABC:1111:0000:1111:0000:0000:0200	The address range is from 2000 to 3FFF.
Global Unicast	2001:0ABC:0000:00BB:DCBA:0000:0000:0200	The address range is from 2000 to 3FFF.
Link-Local	FE80:0000:0000:0000:3211:5412:ECDC:FE11	Link-local address prefix is FE80::/10.
Link-Local	FE80:0000:0000:0000:3211:5412:CAD1:FE12	Link-local address prefix is FE80::/10.
Multicast	FF02:0000:0000:0000:0000:000F:FF00:120F	Multicast addresses use the prefix ff00::/8.
Anycast	xxxx.xxxx:xxxx:xxxx:0000:0000:0000:0000	Similar to broadcast addresses in IPv4.



IPv4 and IPv6 Coexistence

IPv4 and IPv6 can coexist using protocols and tools created by IETF, which are known as: Dual Stack, Tunneling, and Translation.

Dual Stack



Dual Stack means that a device runs both IPv4 and IPv6 protocols simultaneously. Using two stacks allows both IP versions to coexist.



Tunneling



Tunneling is used when IPv6 addresses are to be sent over IPv4 networks, or vice versa. In this method, the IPv6 packet is encapsulated within an IPv4 packet.



Translation



Translation allows IPv6 to communicate with IPv4-enabled devices using techniques similar to those used by NAT.



LAB NET-05-L3

Configure IPv6 Addressing
30–60 Min.



Mission

The objective of this exercise is to practice configuring IPv6 addresses on a router and clients.

The lab also covers practicing verification of IPv6 addressing implementation.

Steps

- Configure IPv6 Unicast Global address on R1 interfaces
- Configure IPv6 on Users PC's and verify connectivity
- Configure IPv6 Link -local address on R1 interfaces and PC's (Optional)

Environment & Tools

- OS
 - All platforms
- Tools
 - Cisco Packet Tracer 7.2.2

Related Files

- NET-05-L3 Configure IPv6 Addressing
- NET-05-L3.pka

An overhead, high-angle shot of a group of people working at a rustic wooden table. The scene is bathed in a cool blue light. In the upper left, a person's hand is visible pointing at a laptop screen. Another person's head and shoulders are in the lower left, looking towards the center. A third person is in the lower right, typing on a laptop. The table is cluttered with various items: two laptops, a smartphone, a disposable coffee cup, and several sheets of paper, one of which features a diagram with blue and yellow bars. The background shows a patterned rug and the legs of other people, suggesting a collaborative workspace or meeting.

QUESTIONS?



THANK YOU
