Introduction to IP Addressing and Networking

By Olusola Kolebaje

Contents

Networking Basics

A network can be defined as the interconnection of autonomous computers linked together to facilitate communication while networking is the simple concept of connected computers.

Networks and networking have grown exponentially over the last 15 years; they have evolved at light speed just to keep up with huge increases in basic critical user needs such as sharing data and printers, as well as more advanced demands such as video conferencing.

Contents

Types of Networks

Local Area Network (LAN)

A LAN (Local Area Network) is a group of computers and network devices connected together, usually within the same building. A Local Area Network (LAN) is a high-speed communication system designed to link computers and other data processing devices together within a small geographical area, such as a workgroup, department, or building. Local Area Networks implement shared access technology. This means that all the devices attached to the LAN share a single communications medium, usually a coaxial, twisted pair or fibre optic cable.

Metropolitan Area Network (MAN)

Metropolitan area networks or MANs are large computer networks usually spanning a city or a town. They typically use wireless infrastructure or optical fibre connections to link their sites.

The IEEE 802-2001 standard describes a MAN as being: "A MAN is optimized for a larger geographical area than is a LAN, ranging from several blocks of buildings to entire cities. MANs

can also depend on communications channels of moderate to high data rates. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. MANs might also be owned and operated as public utilities. They will often provide means for internetworking of local networks. Metropolitan area networks can span up to 50km."

Wide Area Network (WAN)

Wide Area Network (WAN) is a computer network that covers a broad area. A WAN in compares to a MAN, is not restricted to a geographical location, although it might be restricted to a geographical locations, it might also be confined within the bounds of a state or country. A WAN connects several LANs, and may be limited to an enterprise (a corporation or organization) or accessible to the public.

The technology is high speed and relatively expensive. The *Internet* is an example of a worldwide public WAN.

Contents

Networking Devices

Router

Routers are used to connect networks together and route packets of data from one network to another. Routers, by default break up a broadcast domain, which is the set of all devices on a network segment that hear all broadcasts sent on that segment.

Routers also break up collision domains. This is an Ethernet term used to describe a network scenario where one particular device sends a packet on a network segment, forcing every other device on that segment to pay attention to it. At the same time, a different device tries to transmit, leading to a collision, after which both devices must retransmit one at a time.

Routers run on the layer 3 of the OSI (Open System Interconnection) reference model.

Switch

Switches are used for network segmentation based on the MAC addresses. Switches look at the incoming frame's hardware addresses before deciding to either forward the frame or drop it. Switches break up collision domains but the hosts on the switch are still members of one big broadcast domain.

Hub

A hub is really a multiple port repeater. A repeater receives a digital signal and re-amplifies or regenerates that signal, and then forwards the digital signal out all active ports without looking at any data. An active hub does the same thing. This means all devices plugged into a hub are in the same collision domain as well as in the same broadcast domain, which means that devices share the same bandwidth. Hubs operate at the physical layer of the OSI model.

Contents

IP Addressing

An IP address is a numeric identifier assigned to each machine on an IP network. It designates the specific location of a device on the network. An IP address is a software address and designed to allow host on one network to communicate with a host on a different network regardless of the type of LANs the hosts are participating in.

IP Terminologies

Bit: A bit is one digit, either a 1 or a 0.

Byte: A byte is 7 or 8 bits, depending on whether parity is used.

Octet: An octet, made up of 8 bits is just an ordinary 8 bit binary number. In most cases byte and octet are completely interchangeable.

Network address: This is the designation used in routing to send packets to a remote network. For example 10.0.0.0, 172.16.0.0, and 192.168.10.0 are network addresses.

Broadcast address: The address used by applications and hosts to send information to all nodes on a network is called the broadcast address. Examples include 255.255.255.255 which is all networks, all nodes; 172.16.255.255, which is all subnets and hosts on network 172.16.0.0.

Heirarchical IP Addressing Scheme

An IP address consists of 32 bits of information (IPV4). IPV6, a new version of IP consists of 128 bits of information. The 32 bits IP is divided into four sections referred to as octet or bytes each containing 1 byte (8bits).

An IP address is depicted using any of these three methods.

Dotted decimal, as in 172.16.30.56
Binary, as in 10101100.00010000.00011110.00111000
Hexadecimal, as in AC.10.1E.38

All this examples represent the same IP address. But the most commonly used is the dotted decimal. The Windows Registry stores a machine's IP address in hex.

The 32 bit IP address is a structured or hierarchical address, as opposed to a flat non hierarchical address. Although either type of addressing scheme could have been used, hierarchical addressing was chosen for a good reason. The advantage of this scheme is that it can handle a large number of addresses, namely 4.3 billion (a 32 bit address space with two possible values for each position that is either 1 or 0 gives 237, or 4,294,967,296).

The disadvantage of the flat addressing scheme relates to routing. If every address were unique, all routers on the internet would need to store the address of each and every machine on the internet. This would make efficient routing impossible.

Network Address Range

The network address uniquely identifies each network. Every machine on the same network shares that network address as part of its IP address. In the IP address of 172.16.30.56, 172.16 is the network address.

The node address is assigned to and uniquely identifies each machine on a network. This number can also be referred to as host address. In 172.16.30.56, 30.56 is the node address. Class A network is used when a small number of networks possessing a very large number of nodes are needed. Class C network is used when numerous networks with a small number of node is needed.

Class A Addresses

The first bit of the first byte in a class A network address must always be off or 0. This means a class A address must be between 0 and 127, inclusive.

0xxxxxxx.hhhhhhhh.hhhhhhhh.hhhhhhhh

If we turn the other 7 bits all off and then turn them all on, we'll find the class A range of network addresses.

00000000 = 0

01111111 = 127

Class A format is *network.node.node.node*, so for example in the IP address 49.22.102.70, the 49 is the network address and 22.102.70 is the node address. Every machine on this particular network would have the distinctive network address of 49.

Class B Addresses

The first bit of the first byte must always be turned on, but the second bit must always be turned off.

01xxxxxx.xxxxxxxx.hhhhhhhh.hhhhhhhh

If we can turn the first bit on and the second bit off and if the other 6 bits all off and then all on, we'll find the class B range of network addresses.

10000000 = 128

10111111 = 191

Class B format is *network.network.node.node*, so far in the IP address 132.163.40.57, the 132.163 is the network address and 40.57 is the node address.

Class C Addresses

The first and second bit of the first byte must always be turned on, but the third bit can never be on.

110xxxxx.xxxxxxxx.xxxxxxxx.hhhhhhhh

If we turn the first and second bit on and the third bit off and then all other 5 bits all off and all on, we'll find the class C range of network address.

11000000 = 192

11011111 = 223

Class C format is *network.network.network.node*, for example in the IP address 195.166.231.75, the 195.166.231 is the network address and 75 is the node address.

Class D and Class E Addresses

The address between 224 and 255 are reserved for class D and E networks. Class D (224-239) is used for multicast addresses and class E (240-255) for scientific purposes.

Private IP Addresses

Private IP addresses are those that can be used on a private network, but they're not routable through the internet. This is designed for the purpose of creating a measure of well-needed security, but it also conveniently saves valuable IP address space. If every host on every network had to have real routable IP addresses, we would have run out of IP addresses to hand out years ago.

Class A 10.0.0.0 through 10.255.255.255

Class B 172.16.0.0 through 172.31.255.255

Class C 192.168.0.0 through 192.168.255.255

Contents

Troubleshooting IP Addressing

Here are the troubleshooting steps in resolving a problem on an IP network.

1. Open a DOS window and ping 127.0.0.1. This is the diagnostic or loopback address, and if you get a successful ping, your IP stack is considered to be initialized. If it fails, then you have an IP stack failure and need to reinstall TCP/IP on the host.

2. From the DOS window, ping the IP addresses of the local host. If that's successful, then your Network Interface Card (NIC) card is functioning. If it fails, then there is a problem with the NIC card. This doesn't mean that a cable is plugged into the NIC, only that the IP protocol stack on the host can communicate to the NIC.

3. From the DOS window, ping the default gateway. If the ping works, it means that the NIC is plugged into the network and can communicate on the local network. If it fails, then you have a local physical network problem that could be happening anywhere from the NIC to the gateway.

4. If steps 1 through 3 were successful, try to ping the remote server. If that works then you have IP communication between then local host and the remote server, you also know that the remote physical network is working.

5. If the user still can't communicate with the server after steps 1 through 4 were successful, then there's probably a resolution problem and there is need to check the Domain Name Server (DNS) settings.

Contents

Network Address Translation

Network Address Translation (NAT) is used mainly to translate private inside addresses on a network to a global outside address. The main idea is to conserve internet global address space, but it also increases network security by hiding internal IP addresses from external networks.

NAT ADVANTAGES

- Conserves legally registered addresses.
- Reduces address overlap occurrence.
- Increases flexibility when connecting to internet.
- Eliminates address renumbering as network changes.
- Translation introduces switching path delays.

NAT Disadvantages

- Loss of end-to-end traceability
- Certain applications will not function with NAT enabled.

Types of NAT

Static NAT: This type of NAT is designed to allow one-to-one mapping between local and global addresses. Static NAT requires that there is one real internet IP address for every host on your network.

Dynamic NAT: This version gives one the ability to map an unregistered IP address to a registered IP address from out of a pool of registered IP addresses.

Overloading: This is also known as Port Address Translation (PAT). It is the most popular type of NAT configuration. Overloading is a form of dynamic NAT that maps multiple unregistered IP address to a single registered IP address by using different ports. With overloading thousands of users can connect to the internet using only one real global IP address.

NAT Terminologies

- Local addresses: Name of local hosts before translation.
- Global addresses: Name of addresses after translation.
- Inside local: Name of inside source address before translation.
- Outside local: Name of destination host before translation.
- Inside global: Name of inside hosts after translation.
- Outside global: Name of outside destination host after translation.

Contents

Layer2 Switching

Layer2 switching is the process of using the hardware address of devices on a LAN to segment a network. The term layer2 switching is used because switches operate on the data-link layer which is the second layer of the OSI reference model.

Layer2 switching is considered hardware-based bridging because it uses specialized hardware

called an application-specific integrated circuit (ASIC). ASICs can run up to gigabit speeds with very low latency rates.

Switches read each frame as it passes through the network, the layer2 device then puts the source hardware address in a filter table and keeps track of which port the frame was received on. The information (logged in the switch's filter table) is what helps the machine determine the location of a specific sending device. After a filter table is built on the layer2 device, it will only forward frames to the segment where the destination hardware is located. If the destination device is on the same segment as the frame, the layer2 device will block the frame from going to any other segments. If the destination is on a different segment, the frame can only be transmitted to that segment. This is called TRANSPARENT BRIDGING.

When a switch interface receives a frame with a destination hardware address that isn't found in the device filter table, it will forward the frame to all connected segments. If the unknown device that was sent the frame replies to this forwarding action, the switch updates its filter table regarding that device's location.

Advantages of Layer2 Switching

The biggest benefit of LAN switching over hub-centered implementations is that each device on every segment plugged into a switch can transmit simultaneously whereas hubs only allow one device per network segment to communicate at a time.

Switches are faster than routers because they don't take time looking at the Network layer header information. Instead, they look at the frame's hardware address before deciding to either forward the frame or drop it.

Switches create private dedicated collision domains and provide independent bandwidth on each port unlike hubs. The figure below shows five hosts connected to a switch, all running 10Mbps half-duplex to the server. Unlike the hub, each host has 10Mbps dedicated communication to the server.

Limitations of Layer2 Switching

Switched networks break up collision domains but the network is still one large broadcast domain. This does not only limits your network's size and growth potential, but can also reduce its overall performance.

Functions of Layer2 Switching

There are three distinct functions of layer2 switching, these are:

- Address learning.
- Forward/filter decision.
- Loop avoidance.

Address Learning

When a switch is first powered on, the MAC forward/filter table is empty. When a device transmits and an interface receives the frame, the switch places the frame source address in the MAC forward/filter table, allowing it to remember which interface the sending device is located on. The switch then has no choice but to flood the network with this frame out of every port except the source port because it has no idea where the destination device is actually located.

If a device answers the flooded frame and sends a frame back, then the switch will take source address from that frame and place that MAC address in its database as well, associating this address with the interface that received the frame. Since the switch now has both of the relevant MAC addresses in its filtering table, the two devices can now make a point to point connection. The switch doesn't need to flood the frame as it did the first time.

If there is no communication to a particular address within a certain amount of time, the switch will flush the entry from the database to keep it as current as possible.

Forward/Filter Decisions

When a frame arrives at a switch interface, the destination hardware address is compared to the forward/filter MAC database. If the destination hardware address is known and listed in the database, the frame is sent out only the correct exit interface.

The switch doesn't transmit the frame out any interface except for the destination interface. This preserves bandwidth on the other network segments and is called *Frame Filtering*.

Loop Avoidance

When two switches are connected together, redundant links between the switches are a good idea because they help prevent complete network failures in the event one link stops working.

Redundant links are extremely helpful but they often cause more problems than they solve, this is because frames can be flooded down all redundant links simultaneously creating network loops.

Switches use a protocol called STP (Spanning Tree Protocol) created by Digital Equipment Corporation (DEC) now Compaq to avoid network loops by shutting down redundant links. With STP running, frames will be forwarded only on the premium STP-picked link.

Contents

Configuring the Cisco 2950 Catalyst Switch Family

The 2950 switch is one of the Cisco Catalyst switch family's high-end model. The 2950 comes in many flavors and run 10Mbps all the way up to 1Gbps switched ports with either twisted-pair or fiber. They can provide basic data, video and voice services.

2950 Switch Startup

When the 2950 switch is first powered on, it runs through a Power-on-Self-test (POST). At first all port LEDs are green, and if upon completion the post determines that all ports are in good shape, all the LEDs blink and then turn off. But if the POST finds a port that has failed both the system's LED and the port's LEDs turn amber.

However, unlike a router, the switch is actually usable in Fresh-out-of-the-box condition. You can just plug the switch into your network and connect network segment together without any configuration.

To connect to the Cisco switch, use a rolled Ethernet cable to connect a host to a switch console serial communication port. Once you have the correct cable connected from your PC to the Cisco switch, you can start HyperTerminal to create a console connection and configure the

device as follows:

1. Open HyperTerminal by clicking on start button and then All programs, then Accessories, then Communication, then click on HyperTerminal. Enter a name for the connection. It is irrelevant what you name it. Then click OK.

2. Choose the communication port either COM1 or COM2, whichever is open on your PC.

3. Now at the port settings. The default values (2400bps and no flow control hardware) will not work, you must set the port settings as shown in the figure below.

Notice that the bit rate is set to 9600 and the flow control is set to none. At this point click OK and press the Enter key, and you should be connected to your Cisco switch console port.

Here's the 2950 switch's initial output:

```
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [Yes/no]: no

Press RETURN to get started!

00:04:53: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively down

00:04:54: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to
down
Switch>
```

The Configuration

The switch> prompt is called the user exec mode and it's mostly used to view statistics. You can only view and change configuration of a Cisco switch in privileged exec mode which you get into with the enable command.

Switch>

Switch> enable

Switch#

Switch# disable

Switch>

The global configuration mode can be entered from the privileged mode by using the configure terminal command or config t for short.

Switch# config t

Enter the configuration commands, one per line, End with CNTL/Z.

Switch(config)# hostname zenith

Zenith(config)#

The hostname command is used in naming the switch. The hostname of a switch is only locally significant but it's still helpful to set a hostname on a switch so that you can identify the switch when connecting to it.

Setting the ENABLE MODE Passwords and LINE Password

Zenith> enable

Zenith# config t

Enter the configuration commands, one per line, End with CNTL/Z.

Zenith(config)# enable password bank

Zenith(config)# enable secret middle

The enable password bank command sets the enable password as bank and the enable secret middle command sets the enable secret password as middle. The enable secret password is more secure and it supersedes the enable password if it is set. The enable secret password and the enable password cannot be the same on the 2950 switch.

Zenith(config)# line ?

First line number

console Primary terminal line

vty Virtual terminal

Zenith(config)# line vty ?

First line number

Zenith(config)# line vty 0 15

Zenith(config-line)# login

Zenith(config-line)# password alex

Zenith(config-line)# line con 0

Zenith(config-line)# login

Zenith(config-line)# password malouda

Zenith(config-line)# exit

Zenith(config)# exit

Zenith#

The line vty 0 15, login and password alex commands set the telnet password to alex and the line con 0, login, and password malouda commands sets the console password to malouda.

Setting IP Information

You don't have to set any IP configuration on the switch to make it work. You can just plug it in.

But there are two reasons we set IP address information on the switch.

To manage the switch via Telnet or other management software.

To configure the switch with different VLANs and other network functions.

Zenith(config)# int vlan 1

Zenith(config-if)# ip address 172.16.10.17 255.255.255.0

Zenith(config-if)# no shutdown

Zenith(config-if)# exit

Zenith(config)# ip default-gateway 172.16.10.1

Zenith(config)#

The IP address is set to 172.16.10.17 and the no shutdown command must be applied to enable the interface.

Configuring Interface Descripions

You can administratively set a name for each interface on the switches with the description command.

Zenith(config)# int fastethernet 0/ ?

FastEthernet Interface number.

Zenith(config)# int fastethernet 0/1

Zenith(config-if)# description Sales LAN

Zenith(config-if)# int f0/12

Zenith(config-if)# description Connection to Mail server

Zenith(config-if)# CNTL/Z

Zenith#

You can look at the descriptions at any time with either the show interface command or the show running-config command from the global configuration mode.

ERASING AND SAVING THE SWITCH CONFIGURATION
Zenith# copy running-config startup-config
Zenith# erase startup-config

The first command copies the configuration into the NVRAM (Non-volatile RAM) while the erase startup-config command erases the switch configuration.

Zenith# erase startup-config Erasing the nvram filesystem will remove all files! Continue? [confirm] [Enter]

```
[OK]

Erase of nvram: complete

Zenith#
```

Contents

Virtual LAN (VLAN)

A Virtual LAN (VLAN) is a logical grouping of network users and resources connected to administratively defined ports on a switch. When one create VLANs, one creates smaller broadcast domains within a switched internetwork by assigning different ports on the switch to different subnetworks. A VLAN is treated like its own subnet or broadcast domain, which means that frames broadcast onto the network are only switched between ports logically grouped within the same VLAN. By default, no hosts in a specific VLAN can communicate with any other hosts that are members of another VLAN.

Advantages of VLAN

o A group of users needing security can be put into a VLAN so that no user outside the VLAN can communicate with them.
o As a logical grouping of users by function, VLANs can be considered independent from their physical or geographical locations..
o VLANs can enhance network security..
o It can block broadcast storms caused by a faulty NIC (Network Interface Card) card..
o VLANs increase the number of broadcast domains while decreasing their sizes.

VLAN Membership

VLANs are usually created by the administrator, who then assigns switch ports to each VLAN. Such a VLAN is called a static VLAN. If the administrator wants to do a little more work up front and assign all the host devices hardware addresses into a database, then the switch can be configured to assign VLANs dynamically whenever a host is plugged into a switch. This is called dynamic VLAN.

Static VLANs

Static VLANs are the usual way of creating VLANs, and they're also the most secure. The switch port that you assign a VLAN association to always maintain that association until an administrator manually changes that port assignment.

Dynamic VLANs

A dynamic VLAN determines a node's VLAN assignment automatically. Using intelligent management software, you can base assignment on hardware addresses, protocols, or even applications to create dynamic VLANs.

An example is the VLAN Management Policy Server (VMPS) service used to set up a database of MAC addresses that can be used for dynamic addressing of VLANs. A VMPS database maps MAC addresses to VLANs.

Frame Tagging

As frames are switched through the network, switches must be able to keep track of all the frames. Frames are handled differently according to the type of link they are traversing. The frame identification method uniquely assigns user defined ID to each frame. This is sometimes referred to as the "VLAN ID".

Each switch that the frame reaches must first identify the VLAN ID from the frame tag, and then it finds out what to do with the frame by looking at the information in the filter table. If the frame reaches a switch that has another trunked link, the frame will be forwarded out the trunk-link port.

Once the frame reaches an exit to an access link matching the frame's VLAN ID, the switch removes the VLAN identifier. This is so the destination device can receive the frame without having to understand their VLAN identification.

There are two different types of links in a switched environment, they are:

Access links: This type of link is only part of one VLAN. Any device attached to an access link is unaware of a VLAN membership; the device just assumes its part of a broadcast domain. Access link devices cannot communicate with devices outside their VLAN unless the packet is routed.

Trunk links: Trunk links can carry multiple VLANs. A trunk link is a 100 or 1000Mbps point to point link between two switches, between a switch and server. These carry the traffic of multiple VLANs from 1 to 1005 at a time. Trunking allows you to make a single port part of multiple VLANS at the same time. It also allows VLANs to span across multiple switches.

VLAN Identification Methods

There are basically two ways of frame tagging.

Inter-Switch Link (ISL)

IEEE 802.1Q

The main purpose of ISL and 802.1Q frame tagging methods is to provide interswitch VLAN communication.

Inter-switch Link (ISL) Protocol: This is proprietary to Cisco switches, and it is used for fast Ethernet and gigabit Ethernet links only. ISL routing can be used on a switch port, router interfaces and server interface cards to trunk a server.

IEEE 802.1Q: Created by the IEEE as a standard method of frame tagging, it isn't Cisco proprietary so if you're trunking between a Cisco switched link and a different brand of switch; you have to use 802.1Q for the trunk link to work.

VLAN TRUNKING PROTOCOL (VTP)

This protocol was created by Cisco but it is not proprietary. The basic goals of VLAN Trunking protocol (VTP) are to manage all configured VLANs across a switched internetwork and to maintain consistency through the network. VTP allows an administrator to add, delete and rename VLANs on a switch, information that is then propagated to all other switches in the VTP domain.

Before one can get VTP to manage VLANs across the network, one has to create a VTP server.

All switches sharing the same VLAN information must be in the same VTP domain.

One can use a VTP domain if there is more than one switch connected in a network, but if all the switches are in only one VLAN, there is no need to use VTP. VTP information is set between switches via trunk port.

This report exposes one to various aspects of computer networking, IP routing and IP switching and how to manage a network from an office network to larger networks. Areas covered in this report includes IP addressing, Network Address Translation (NAT), IP switching and Virtual Private Network (VPN).

Contents

Contents