**Chapter 3**

**Unicast IP**

A unicast address is an address that identifies a unique node on a network. Unicast addressing is available in IPv4 and IPv6 and typically refers to a single sender or a single receiver, although it can be used in both sending and receiving.  
A unicast address packet is transferred to a network node, which includes an interface address. The unicast address is then inserted into the destination's packet header, which is sent to the network device destination.  
Unicast is the most common form of IP addressing.

A unicast address identifies a network device, such as a workstation or a server. A unicast address on a local area network (LAN) contains a subnet prefix and an interface ID.

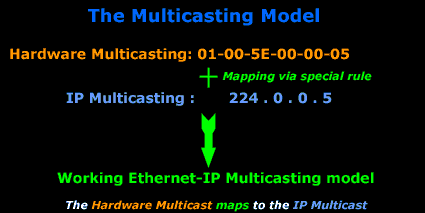
**Multicast IP and Multicast Streaming**

A multicast is similar to a broadcast in the sense that its target is a number of machines on a network, but not all. Where a broadcast is directed to all hosts on the network, a multicast is directed to a group of hosts. The hosts can choose whether they wish to participate in the multicast group (often done with the Internet Group Management Protocol), whereas in a broadcast, all hosts are part of the broadcast group whether they like it or not!

1) Hardware/Ethernet Multicasting

2) IP Multicasting

3) Mapping IP Multicast to Ethernet Multicast



HARDWARE/ETHERNET MULTICASTING

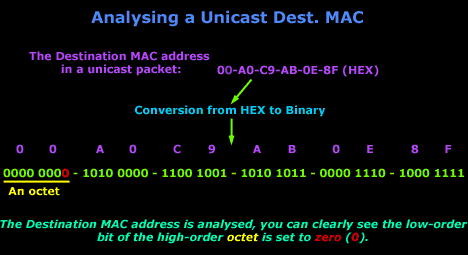
When a computer joins a multicast group, it needs to be able to distinguish between normal unicasts (which are packets directed to one computer or one MAC address) and multicasts. With hardware multicasting, the network card is configured, via its drivers, to watch out for particular MAC addresses (in this case, multicast MAC addresses) apart from its own. When the network card picks up a packet which has a destination MAC that matches any of the multicast MAC addresses, it will pass it to the upper layers for further processing.

To understand this, we need to analyse the destination MAC address of a unicast and multicast packet, so you can see what we are talking about:

When a normal (unicast) packet is put on the network by a computer, it contains the Source and Destination MAC address, found in the 2nd Layer of the OSI model. The following picture is an example of my workstation (192.168.0.6) sending a packet to my network's gateway (192.168.0.5):

multicast-intro-3

Now let's analyse the destination MAC address:

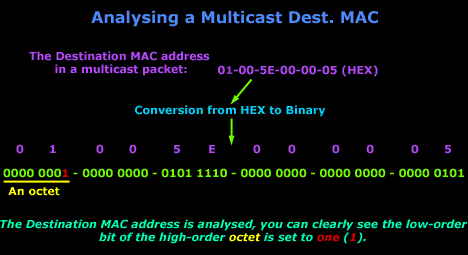


a multicast packet is not directed to one host but a number of hosts, so the destination MAC address will not match the unique MAC address of any computer, but the computers which are part of the multicast group will recognise the destination MAC address and accept it for processing.

The following multicast packet was sent from my NetWare server. Notice the destination MAC address (it's a multicast):

multicast-intro-5

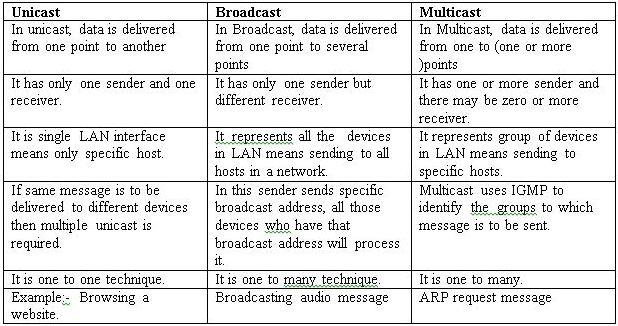
Analysis of a multicast destination MAC address:

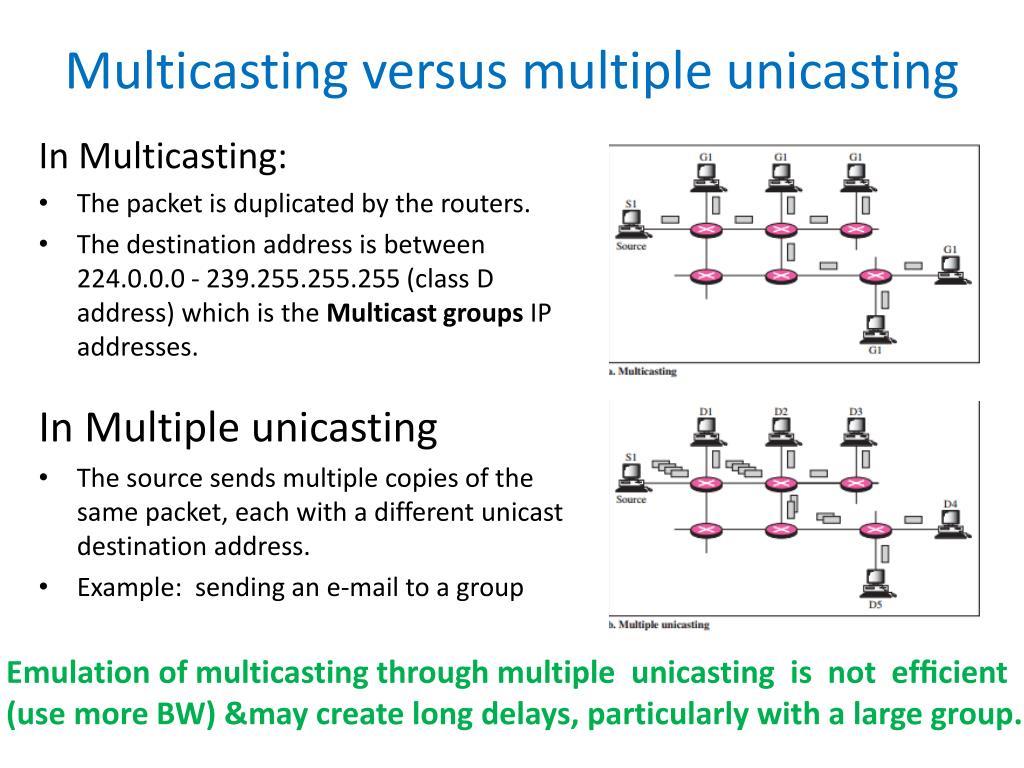


**Broadcast IP**

Broadcast is the term used to describe communication where a piece of information is sent from one point to all other points. In this case there is just one sender, but the information is sent to all connected receivers.

Broadcast transmission is supported on most LANs (e.g. [Ethernet](https://erg.abdn.ac.uk/users/gorry/course/lan-pages/enet.html)), and may be used to send the same message to all computers on the LAN (e.g. the [address resolution protocol (arp)](https://erg.abdn.ac.uk/users/gorry/course/inet-pages/icmp.html) uses this to send an address resolution query to all computers on a LAN). Network layer protocols (such as [IPv4](https://erg.abdn.ac.uk/users/gorry/course/inet-pages/ip.html)) also support a form of broadcast that allows the same packet to be sent to every system in a logical network (in IPv4 this consists of the IP network ID and an all 1's host number).





**TCP/IP Port Numbers**

A port is a physical docking point using which an external device can be connected to the computer. It can also be programmatic docking point through which information flows from a program to the computer or over the Internet.

A network port which is provided by the Transport Layer protocols of Internet Protocol suite, such as Transmission Control Protocol (TCP) and User Diagram Protocol (UDP) is a number which serving endpoint communication between two computers.

To determine what protocol incoming traffic should be directed to, different port numbers are used. They allow a single host with a single IP address to run network services. Each port number have a distinct service, and for each host can have 65535 ports per IP address. **Internet Assigned Numbers Authority  (IANA)** is responsible for managing the uses of these ports. There are three categories for ports by IANA −

* 0 to 1023 – well known ports or system ports.

Some well-known ports are −

|  |  |  |
| --- | --- | --- |
| **Port number** | **Transport protocol** | **Service name** |
| 20,21 | TCP | File Transfer Protocol |
| 23 | TCP | Telnet |
| 25 | TCP | Simple Mail Transfer Protocol(SMTP) |
| 53 | TCP and UDP | Domain Name System(DNS) |
| 110 | TCP | Post Office Protocol(POP3) |
| 123 | UDP | Network Time Protocol(NTP) |

* **1024 to 49151** – registered ports assigned by IANA to a specific service upon application by a requesting entity.
* **49152 to 65 535**– dynamic (private, high) ports range from 49,152 to 65,535. Can be used by private or customer service or temporal purposes.