Assignment 3: **Concept of TCP/IP with studying the addressing mechanism used in the network system**

The **Internet Protocol Suite** (commonly known as **TCP/IP**) is the set of communications protocols used for the Internet and other similar networks. It is named from two of the most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which were the first two networking protocols defined in this standard. The Internet Protocol Suite, like many protocol suites, may be viewed as a set of layers. Each layer solves a set of problems involving the transmission of data, and provides a well-defined service to the upper layer protocols based on using services from some lower layers. Upper layers are logically closer to the user and deal with more abstract data, relying on lower layer protocols to translate data into forms that can eventually be physically transmitted.

TCP/IP is composed of layers:

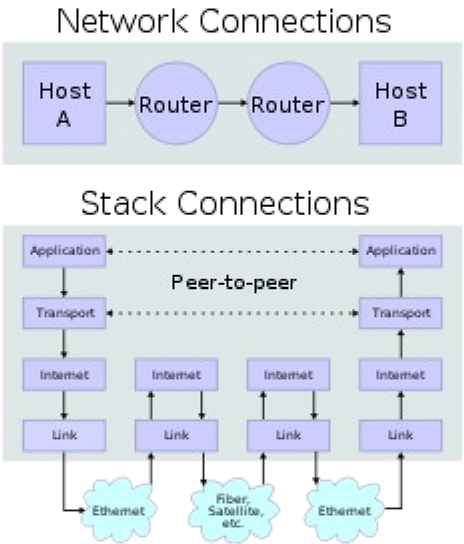
- **IP** - is responsible for moving packet of data from node to node. IP forwards each packet based on a four byte destination address (the IP number). The Internet authorities assign ranges of numbers to different organizations. The organizations assign groups of their numbers to departments. IP operates on gateway machines that move data from department to organization to region and then around the world.
- **TCP** - is responsible for verifying the correct delivery of data from client to server. Data can be lost in the intermediate network. TCP adds support to detect errors or lost data and to trigger retransmission until the data is correctly and completely received.
- **Sockets -** is a name given to the package of subroutines that provide access to TCP/IP on most systems.

The TCP/IP model consists of four layers (RFC 1122). From lowest to highest, these are the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer.

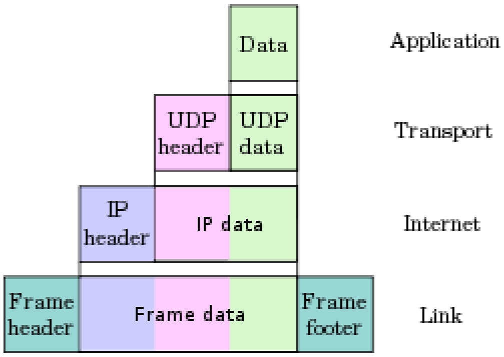
Layers in the Internet Protocol Suite

The TCP/IP suite uses encapsulation to provide abstraction of protocols and services. Such encapsulation usually is aligned with the division of the protocol suite into layers of general functionality. In general, an application (the highest level of the model) uses a set of protocols to send its data down the layers, being further encapsulated at each level.

This may be illustrated by an example network scenario, in which two Internet host computers communicate across local network boundaries constituted by their internetworking gateways (routers).



TCP/IP stack operating on two hosts connected via two routers and the corresponding layers used at each hop



Encapsulation of application data descending through the protocol stack.

The functional groups of protocols and methods are the Application Layer, the Transport Layer, the Internet Layer, and the Link Layer (RFC 1122). It should be noted that this model was not intended to be a rigid reference model into which new protocols have to fit in order to be accepted as a standard.

The following table provides some examples of the protocols grouped in their respective layers.

Application	DNS, TFTP, TLS/SSL, FTP, Gopher, HTTP, IMAP, IRC, NNTP, POP3, SIP, SMTP,SMPP, SNMP, SSH, Telnet, Echo, RTP, PNRP, rlogin, ENRP
	Routing protocols like BGP and RIP which run over TCP/UDP, may also be considered part of the Internet Layer.
Transport	TCP, UDP, DCCP, SCTP, IL, RUDP, RSVP
Internet	IP (IPv4, IPv6) ICMP, IGMP, and ICMPv6

	OSPF for IPv4 was initially considered IP layer protocol since it runs per IP-subnet, but has been placed on the Link since RFC 2740.
Link	ARP, RARP, OSPF (IPv4/IPv6), IS-IS, NDP

Different authors have interpreted the RFCs differently regarding whether the **Link Layer** (and the four-layer TCP/IP model) covers physical layer issues or a "hardware layer" is assumed below the link layer. Some authors have tried to use other names for the link layer, such as *Network interface layer*, in effort to avoid confusion with the Data link layer of the seven-layer OSI model. Others have attempted to map the Internet Protocol model onto the seven-layer OSI Model. The mapping often results in a five-layer TCP/IP model, wherein the Link Layer is split into a Data Link Layer on top of a Physical Layer. Especially in literature with a bottom-up approach to computer networking, where physical layer issues are emphasized, an evolution towards a five-layer Internet model can be observed out of pedagogical reasons.

The **Internet Layer** is usually directly mapped to the OSI's Network Layer. At the top of the hierarchy, the **Transport Layer** is always mapped directly into OSI Layer 4 of the same name. OSIs Application Layer, Presentation Layer, and Session Layer are collapsed into TCP/IP's **Application Layer**. As a result, these efforts result in either a four- or five-layer scheme with a variety of layer names. This has caused considerable confusion in the application of these models. Other authors dispense with rigid pedagogy[17] focusing instead on functionality and behavior.

1)MAC Addressing:

A MAC address (Media Access Control) is a unique address given to each network host (this includes computers, PLCs - prorammable logic controllers, routers, and wireless devices. This does not include hubs and switches that are not managable). In other words anything that you can browse, telnet, e-mail, FTP, or otherwise connect to using an ethernet network has a MAC address.

In computer networking, a Media Access Control address (MAC address), Ethernet Hardware Address (EHA), hardware address, adapter address or physical address is a quasi-unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number.

Three numbering spaces, managed by the Institute of Electrical and Electronics Engineers (IEEE), are in common use for formulating a MAC address: MAC-48, EUI-48, and EUI-64. The IEEE claims trademarks on the names "EUI-48" and " EUI-64", where "EUI" stands for Extended Unique Identifier.

Although intended to be a permanent and globally unique identification, it is possible to change the MAC address on most of today's hardware, an action often referred to as MAC spoofing. A host cannot determine from the MAC address of another host whether that host is on the same OSI Layer 2 network segment as the sending host or a network segment bridged to that network segment.

In TCP/IP networks, the MAC address of a subnet interface can be queried with the IP address using the Address Resolution Protocol (ARP) for Internet Protocol Version 4 (IPv4) or the Neighbor Discovery Protocol (NDP) for IPv6. On broadcast networks, such as Ethernet, the MAC address uniquely identifies each node and allows frames to be marked for specific hosts. It thus forms the basis of most of the Link layer (OSI Layer 2) networking upon which upper layer protocols rely to produce complex, functioning networks.

Notational conventions

The standard (IEEE 802) format for printing MAC-48 addresses in human-friendly form is six groups of two hexadecimal digits, separated by hyphens (`-`) or colons (`:`), in transmission order, e.g. `01-23-45-67-89-ab`, `01:23:45:67:89:ab`. This form is also commonly used for EUI-64. Other less common conventions use three groups of four hexadecimal digits separated by dots (`.`), e.g. `0123.4567.89ab`; again in transmission order.

MAC Address details

The original IEEE 802 **MAC address** comes from the original Xerox Ethernet addressing scheme.[1] This 48-bit address space contains potentially 2^{48} or 281,474,976,710,656 possible MAC addresses.

All three numbering systems use the same format and differ only in the length of the identifier. Addresses can either be "universally administered addresses" or "locally administered addresses."

A **universally administered address** is uniquely assigned to a device by its manufacturer; these are sometimes called "burned-in addresses" (BIA). The first three octets (in transmission order) identify the organization that issued the identifier and are known as the Organizationally Unique Identifier (OUI).[2] The following three (MAC-48 and EUI-48) or five (EUI-64) octets are assigned by that organization in nearly any manner they please, subject to the constraint of uniqueness. The IEEE expects the MAC-48 space to be exhausted no sooner than the year 2100; EUI-64s are not expected to run out in the foreseeable future.

A **locally administered address** is assigned to a device by a network administrator, overriding the burned-in address. Locally administered addresses do not contain OUIs.

Universally administered and locally administered addresses are distinguished by setting the second least significant bit of the most significant byte of the address. In EUI-64 addresses, if the bit is 0, the address is universally locally administered. If it is 1, the address is locally globally administered. The bit is 0 in all OUIs. For example, 02-00-00-00-00-01. The most significant byte is 02h. The binary is 000000**1**0 and the second least significant bit is 1. Therefore, it is a locally administered address.

If the least significant bit of the most significant byte is set to a 0, the packet is meant to reach only one receiving NIC. This is called unicast. If the least significant bit of the most significant byte is set to a 1, the packet is meant to be sent only once but still reach several NICs. This is called multicast.

The following technologies use the MAC-48 identifier format:

- Ethernet
- 802.11 wireless networks
- Bluetooth
- IEEE 802.5 token ring
- most other IEEE 802 networks
- FDDI
- ATM (switched virtual connections only, as part of an NSAP address)
- Fibre Channel and Serial Attached SCSI (as part of a World Wide Name)

The distinction between EUI-48 and MAC-48 identifiers is purely semantic: MAC-48 is used for network hardware; EUI-48 is used to identify other devices and software. (Thus, by definition, an EUI-48 is not in fact a "MAC address", although it is syntactically indistinguishable from one and assigned from the same numbering space.)

The IEEE now considers the label MAC-48 to be an obsolete term which was previously used to refer to a specific type of EUI-48 identifier used to address hardware interfaces within existing 802-based networking applications and should not be used in the future. Instead, the term EUI-48 should be used for this purpose.

EUI-64 identifiers are used in:

- FireWire
- IPv6 (as the least-significant 64 bits of a unicast network address or link-local address when stateless autoconfiguration is used)
- ZigBee / 802.15.4 wireless personal-area networks

The IEEE has built in several special address types to allow more than one network interface card to be addressed at one time:

- Packets sent to the **broadcast address**, all one bits, are received by all stations on a local area network. In hexadecimal the broadcast address would be "FF:FF:FF:FF:FF:FF".

- Packets sent to a **multicast address** are received by all stations on a LAN that have been configured to receive packets sent to that address.
- **Functional addresses** identify one or more Token Ring NICs that provide a particular service, defined in IEEE 802.5.

These are "group addresses", as opposed to "individual addresses"; the least significant bit of the first octet of a MAC address distinguishes individual addresses from group addresses. That bit is set to 0 in individual addresses and 1 in group addresses. Group addresses, like individual addresses, can be universally administered or locally administered.

In addition, the EUI-64 numbering system encompasses both MAC-48 and EUI-48 identifiers by a simple translation mechanism. To convert a MAC-48 into an EUI-64, copy the OUI, append the two octets "FF-FF", and then copy the organization-specified part. To convert an EUI-48 into an EUI-64, the same process is used, but the sequence inserted is "FF-FE". In both cases, the process can be trivially reversed when necessary. Organizations issuing EUI-64s are cautioned against issuing identifiers that could be confused with these forms. The IEEE policy is to discourage new uses of 48-bit identifiers in favor of the EUI-64 system.

2)IP Addressing

The IP address provides the grouping capability that MAC addresses do not. An IP address not only provides a grouping hierarchy but can be freely assigned and moved from one host to another. This grouping capability allows a host to differentiate local computers and distant ones so that communication to a host that is local could be direct and communication to a distant host could be efficiently routed.

IP addressing is assigning a 32-bit logical numeric address to a network device. Every IP address on the network must be unique. IP addresses are assigned manually (i.e. by an administrator) or automatically (i.e. dynamically by DHCP or APIPA). These addressing methods will be covered more extensively in the *Network Services* TechNotes. An IP address is represented in a dotted decimal format, for example: 159.101.6.8

As you can see, the address is divided in 4 parts, which are called *octets* . Each octet in an IP address represents 8 bits. The IP address mentioned above can also be displayed in dotted binary format: 10011111.01100101.00000110.00001000

Converting the decimal address to a binary format (and vice versa) is a fairly easy process. The highest decimal number you can represent with 8 bits is 255. This is the case when all bits in an octet are set to 1.

1	1	1	1	1	1	1	1	
128 +	64 +	32 +	16 +	8 +	4 +	2 +	1	= 255
(2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0)	

The following are examples of binary values and their decimal counterparts:

Binary	*Decima l*
00000010	2
00000011	3
10000000	128
10000001	129
11111010	250

The currently available addressing space in IP version 4 is divided in 5 classes:

Class A - 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh

- First bit 0; 7 network bits; 24 host bits
- Initial byte: 0 - 127
- 126 Class As exist (0 and 127 are reserved)
- 16,777,214 hosts on each Class A

Class B - 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh

- First two bits 10; 14 network bits; 16 host bits
- Initial byte: 128 - 191
- 16,384 Class Bs exist
- 65,532 hosts on each Class B

Class C - 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh

- First three bits 110; 21 network bits; 8 host bits
- Initial byte: 192 - 223
- 2,097,152 Class Cs exist
- 254 hosts on each Class C

Class D - 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm

- First four bits 1110; 28 multicast address bits
- Initial byte: 224 - 247
- Class Ds are multicast addresses

Class E - 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr

- First four bits 1111; 28 reserved address bits
- Initial byte: 248 - 255
- Reserved for experimental use

<u>Private vs. Public addresses</u> IANA reserved four address ranges to be used in private networks only. This prevents address conflict between addresses on private corporate or home networks and the Internet:

- 10.0.0.0 through 10.255.255.255 from the Class A range
- 172.16.0.0 through 172.31.255.255 from the Class B range
- 192.168.0.0 through 192.168.255.255 from the Class C range
- 169.254.0.1 through 169.254.255.254 (reserved for Automatic Private IP Addressing)

The range 127.0.0.0 to 127.255.255.255 is reserved for IP loopback addresses, which are mainly intended for testing purposes and for checking if the TCP/IP stack has correctly loaded.

To function properly in a TCP/IP internetwork, a network device needs an IP address, a subnet mask, and a default gateway. The latter two are discussed below.

a)**Subnetting:**

Subnetting, originally referred to the subdivision of a class-based network into subnetworks, but now refers more generally to the subdivision of a CIDR block into smaller CIDR blocks. Subnetting allows single routing entries to refer either to the larger block or to its individual constituents. This permits a single, general routing entry to be used through most of the Internet, more specific routes only being required for routers in the subnetted block.

A *subnet mask* is a 32-bit number that determines how an IP address is split into network and host portions, on a bitwise basis. For example, 255.255.0.0 is a standard class B subnet mask, since the first two bytes are all ones (network), and the last two bytes are all zeros (host). In a subnetted network, the network portion is extended. For example, a subnet mask of 255.255.255.0 would subnet a class B address space using its third byte. Using this scheme, the first two bytes of an IP address would identify the class B network, the next byte would identify the subnet within that network, and the final byte would select an individual host. Since subnet masks are used on a bit-by-bit basis, masks like 255.255.240.0 (4 bits of subnet; 12 bits of host) are perfectly normal.

In a traditional subnetted network, several restrictions apply, which have been lifted by CIDR. However, if older, non-CIDR routing protocols (such as RIP version 1) are in use, these restrictions must still be observed.

1. **Identical subnet masks.** Since non-CIDR routing updates do not include subnet masks, a router must assume that the subnet mask it has been configured with is valid for all subnets. Therefore, a single mask must be used for all subnets with a network. Different masks can be used for different networks.

   Based on this assumption, a router can exchange subnet routes with other routers within the network. Since the subnet masks are identical across the network, the routers will interpret these routes in the same manner. However, routers not attached to the subnetted network can't interpret these subnet routes, since they lack the subnet mask. Therefore, subnet routes are not relayed to routers on other networks. This leads to our second restriction.

2. **Contiguous subnets.** A subnetted network can't be split into isolated portions. All the subnets must be contiguous, since routing information can't be passed to non-members. Within a network, all subnets must be able to reach all other subnets without passing traffic through other networks.

Subnetting is used to break the network into smaller more efficient *subnets* to prevent excessive rates of Ethernet packet collision in a large network. Such subnets can be arranged hierarchically, with the organization's network address space (see also Autonomous System) partitioned into a tree-like structure. Routers are used to manage traffic and constitute borders between subnets.

A routing prefix is the sequence of leading bits of an IP address that precede the portion of the address used as host identifier. The routing prefix is often expressed as a "subnet mask", which is a bit mask covering the number of bits used in the prefix. It is frequently expressed in quad-dotted decimal representation, e.g., 255.255.255.0 is the subnet mask for the 192.168.1.0 network with a 24-bit routing prefix (192.168.1.0/24).

All hosts within a subnet can be reached in one "hop" (time to live = 1), implying that all hosts in a subnet are connected to the same link.

A typical subnet is a physical network served by one router, for instance an Ethernet network (consisting of one or several Ethernet segments or local area networks, interconnected by network switches and network bridges) or a Virtual Local Area Network (VLAN). However, subnetting allows the network to be logically divided regardless of the physical layout of a network, since it is possible to divide a physical network into several subnets by configuring different host computers to use different routers.

.b) **Supernetting**

Supernetting is synonymous with Classless Inter-Domain Routing (CIDR) although CIDR is rather just the concept that is implemented when subnetting or supernetting.

In Internet networking terminology, a supernet is a block of contiguous subnetworks addressed as a single subnet. Supernets always have masks that are smaller than the classful mask, otherwise it isn't a supernet. One purpose of this is to free up millions of wasted IP addresses on the Internet that classful addressing consumed.

Supernetting alleviates some of the issues with the original classful addressing scheme for IP addresses by allowing multiple networks address ranges to be combined, either to create a single larger network, or just for route aggregation to keep the "Internet Routing Table" (or any routing table) from growing too large.

For supernetting to work, you must be using static routing everywhere or be using a routing protocol which supports classless routing, such as RIPv2 or OSPF (or BGP for Exterior Routing) which can carry subnet mask information with the routing update. The older RIPv1 (or EGP for Exterior Routing) protocol only understands classful addressing, and therefore cannot transmit subnet mask information.

EIGRP is also a Classless Routing Protocol capable of support for CIDR or VLSM (Variable Length Subnet Masking). By default EIGRP will summarize the routes within the routing table and forward these summarized routes to its peers. This can be disastrous within heterogeneous routing environments if VLSM has been used with Discontiguous Subnets and therefore Auto-Summarization should be disabled unless VLSM has been carefully designed and implemented.

The family of Classfull Routing Protocols are RIPv1, and IGRP - these protocols can not support CIDR as they do not have the ability to include subnet info within the Routing Updates.

The Family of Classless Routing Protocols are RIPv2, OSPF, EIGRP and BGP. EIGRP can handle multiple Routed Protocols such as IPX and Appletalk. RTP (Reliable Transport Protocol) is used by EIGRP as it's layer 4 protocol as opposed to TCP. This keeps EIGRP Protocol Independent because RTP is not native to THE TCP/IP ip stack like TCP.

Another way to look at supernetting is:

Let's take a class B mask of 255.255.0.0 - If we borrow 2 network bits, the mask changes to 255.252.0.0, this is called Supernetting. If on the other hand we borrow two host bits, the mask changes to 255.255.192.0, this is called subnetting.

This same method can be used on class A and C addresses.

Supernetting is the idea of combining two or more blocks of IP addresses that together compose a continuous range of addresses (no missing addresses in the middle). You create a supernet when you have a need to place more hosts on a single network than currently will work in a classful configuration.

The term supernetting stems from the idea that at one time there were 'classes' of IP addresses and that certain classes of addresses were a certain size. By adding two sets of addresses of one size using supernetting, you created a larger set of addresses--a super subnet that contained both of the smaller classful subnets.

Classful addressing identifies a *class C* addresses as being in the range of 192.0.0.0 through 223.255.255.255. A single class C block such as 192.168.1.0 - 192.168.1.255 has at most, 254 addresses. If you have more than 254 computers that need to be on the same network (to get Windows Domain Browsing working for instance). then you need to create a supernet.