# IP Addressing

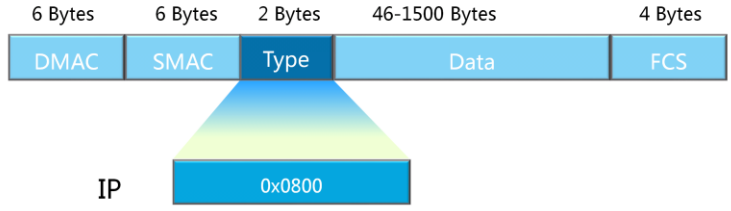
# Foreword

- The Internet Protocol (IP) is designed to provide a means for internetwork communication that is not supported by lower layer protocols such as Ethernet. The implementation of logical (IP) addressing enables the Internet Protocol to be employed by other protocols for the forwarding of data in the form of packets between networks. A strong knowledge of IP addressing must be attained for effective network design along with clear familiarity of the protocol behavior, to support a clear understanding of the implementation of IP as a routed protocol.

# Objectives

- Upon completion of this section, you will be able to:
  - Describe the fields and characteristics contained within IP.
  - Distinguish between public, private and special IP address ranges.
  - Successfully implement VLSM addressing.
  - Explain the function of an IP gateway.

# Next Header Processing

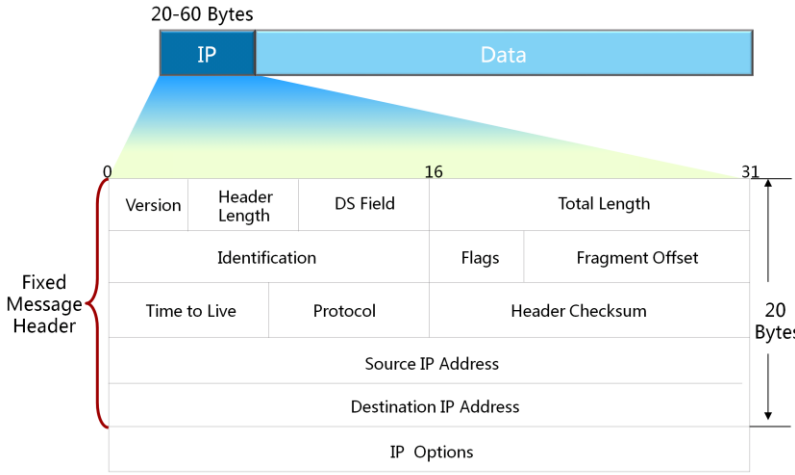



- The next set of instructions for processing are referenced in the type field of the frame header.

- Prior to discarding the frame header and trailer, it is necessary for the next set of instructions to be processed to be determined from the frame header. As highlighted, this is identified by determining the field value in the type field, which in this instance represents a frame that is destined for the IP protocol following completion of the frame process.
- The key function of the frame is to determine whether the intended physical destination has been reached, that the integrity of the frame has remained intact. The focus of this section will identify how data is processed following the discarding of the frame headers and propagation of the remaining data to the Internet Protocol.

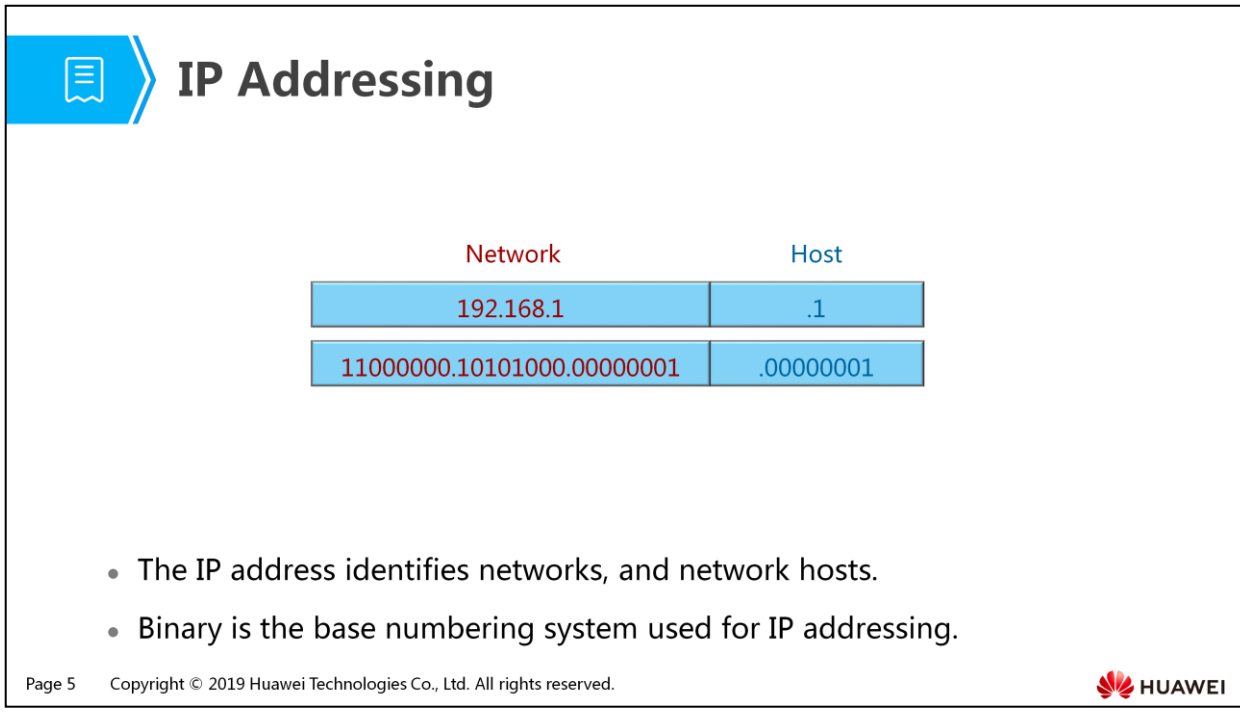
# IP Packet Header



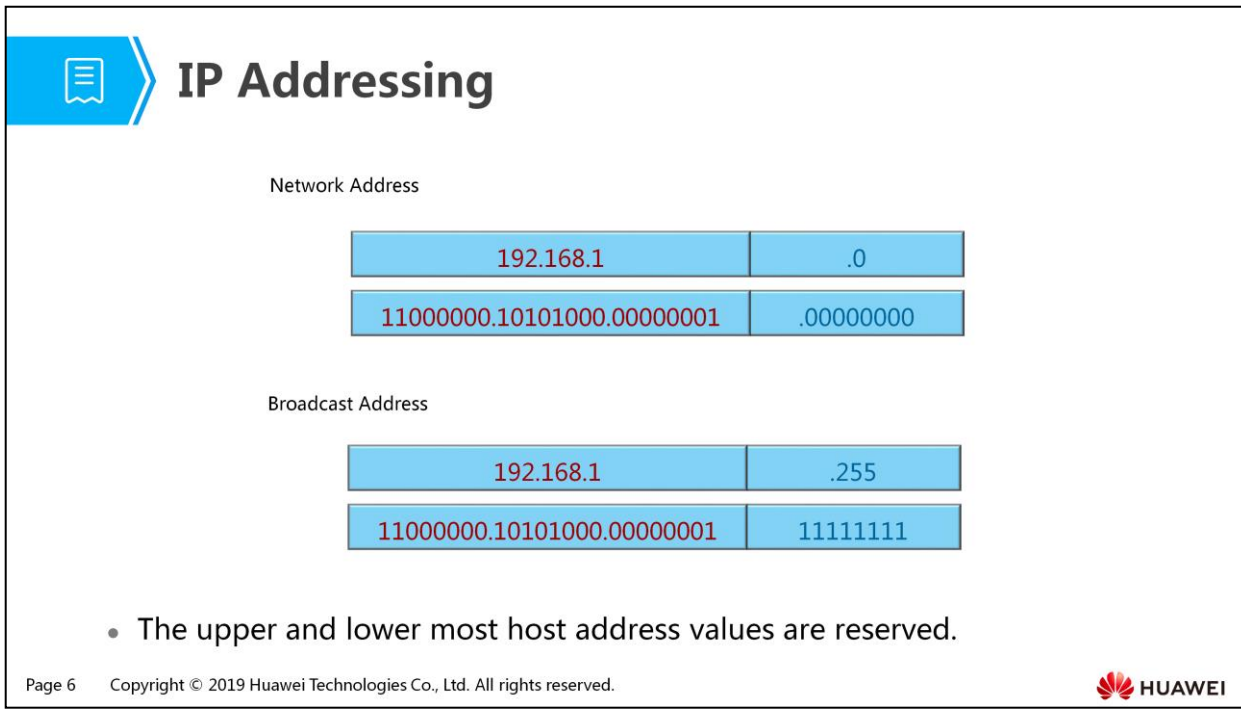



HUAWEI

- The IP header is used to support two key operations, routing and fragmentation. Routing is the mechanism that allows traffic from a given network to be forwarded to other networks, since the data link layer represents a single network for which network boundaries exist. Fragmentation refers to the breaking down of data into manageable blocks that can be transmitted over the network.
- The IP header is carried as part of the data and represents an overhead of at least 20 bytes that references how traffic can be forwarded between networks, where the intended destination exists within a network different from the network on which the data was originally transmitted. The version field identifies the version of IP that is currently being supported, in this case the version is known as version four or IPv4. The DS field was originally referred to as the type of service field however now operates as a field for supporting differentiated services, primarily used as a mechanism for applying quality of service (QoS) for network traffic optimization, and is considered to be outside of the scope of this training.
- The source and destination IP addressing are logical addresses assigned to hosts and used to reference the sender and the intended receiver at the network layer. IP addressing allows for assessment as to whether an intended destination exists within the same network or a different network as a means of aiding the routing process between networks in order to reach destinations beyond the local area network.




- Each IPv4 address represents a 32 bit value that is often displayed in a dotted decimal format but for detailed understanding of the underlying behavior is also represented in a binary (Base 2) format. IP addresses act as identifiers for end systems as well as other devices within the network, as a means of allowing such devices to be reachable both locally and by sources that are located remotely, beyond the boundaries of the current network.
- The IP address consists of two fields of information that are used to clearly specify the network to which an IP address belongs as well as a host identifier within the network range, that is for the most part unique within the given network.




- Each network range contains two important addresses that are excluded from the assignable network range to hosts or other devices. The first of these excluded addresses is the network address that represents a given network as opposed to a specific host within the network. The network address is identifiable by referring to the host field of the network address, in which the binary values within this range are all set to 0, for which it should also be noted that an all 0 binary value may not always represent a 0 value in the dotted decimal notation.
- The second excluded address is the broadcast address that is used by the network layer to refer to any transmission that is expected to be sent to all destinations within a given network. The broadcast address is represented within the host field of the IP address where the binary values within this range are all set to 1. Host addresses make up the range that exists between the network and broadcast addresses.

# Decimal, Binary and Hexadecimal

| Format | Value Range | Base Value |
|---|---|---|
| Binary | 0 — 1 | 2 |
| Decimal | 0 — 9 | 10 |
| Hexadecimal | 0 — F | 16 |

- Binary and Hexadecimal are common numbering systems used within IP networks.





- The use of binary, decimal and hexadecimal notations are commonly applied throughout IP networks to represent addressing schemes, protocols and parameters, and therefore knowledge of the fundamental construction of these base forms is important to understanding the behavior and application of values within IP networks.
- Each numbering system is represented by a different base value that highlights the number of values used as part of the base notations range. In the case of binary, only two values are ever used, 0 and 1, which in combination can provide for an increasing number of values, often represented as 2 to the power of x, where x denotes the number of binary values. Hexadecimal represents a base 16 notation with values ranging from 0 to F, (0-9 and A-F) where A represents the next value following 9 and F thus represents a value equivalent to 15 in decimal, or 1111 in binary.

# Binary vs. Decimal Conversion

| Bit Order | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|
| Binary Power | $2^7$ | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ |
| Binary | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

| Decimal | Binary | Hexadecimal |
|---|---|---|
| 0 | 00000000 | 00 |
| 1 | 00000001 | 01 |
| 2 | 00000010 | 02 |
| 3 | 00000011 | 03 |
| 4 | 00000100 | 04 |
| 5 | 00000101 | 05 |
| 6 | 00000110 | 06 |
| 7 | 00000111 | 07 |
| 8 | 00001000 | 08 |

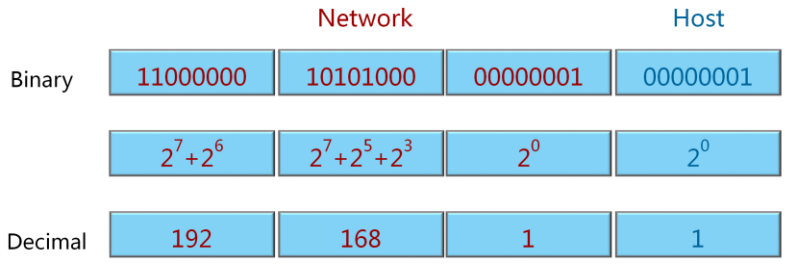
| Decimal | Binary | Hexadecimal |
|---|---|---|
| 9 | 00001001 | 09 |
| 10 | 00001010 | 0A |
| 11 | 00001011 | 0B |
| 12 | 00001100 | 0C |
| 13 | 00001101 | 0D |
| 14 | 00001110 | 0E |
| 15 | 00001111 | 0F |
| ... | ... | ... |
| 255 | 11111111 | FF |





- A byte is understood to contain 8 bits and acts as a common notation within IP networks, thus a byte represents a bit value of 256, ranging from 0 through to 255. This information is clearly represented through translation of decimal notation to binary, and application of the base power to each binary value, to achieve the 256 bit value range. A translation of the numbering system for binary can be seen given in the example to allow familiarization with the numbering patterns associated with binary. The example also clearly demonstrates how broadcast address values in decimal, binary and hexadecimal are represented to allow for broadcasts to be achieved in both IP and MAC addressing at the network and data link layers.

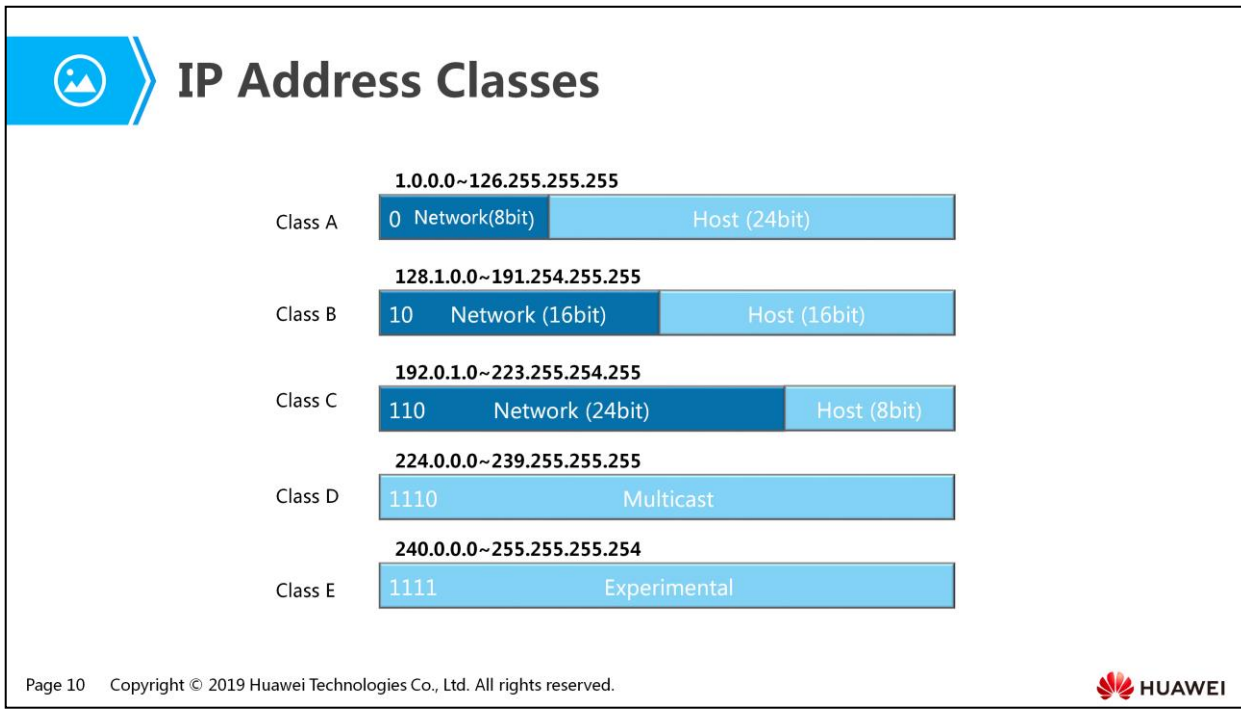
# Binary Conversion








- The combination of 32 bits within an IP address correlates to four octets or bytes for which each can represent a value range of 256, giving a theoretical number of 4’ 294’ 967’ 296 possible IP addresses, however in truth only a fraction of the total number of addresses are able to be assigned to hosts. Each bit within a byte represents a base power and as such each octet can represent a specific network class, with each network class being based on either a single octet or a combination of octets. Three octets have been used as part of this example to represent the network with the fourth octet representing the host range that is supported by the network.




- The number of octets supported by a network address is determined by address classes that break down the address scope of IPv4. Classes A, B and C are assignable address ranges, each of which supports a varied number of networks, and a number of hosts that are assignable to a given network. Class A for instance consist of 126 potential networks, each of which can support $2^{24}$, or 16’ 777’ 216 potential host addresses, bearing in mind that network and broadcast addresses of a class range are not assignable to hosts.
- In truth, a single Ethernet network could never support such a large number of hosts since Ethernet does not scale well, due in part to broadcasts that generate excessive network traffic within a single local area network. Class C address ranges allow for a much more balanced network that scales well to Ethernet networks, supplying just over 2 million potential networks, with each network capable of supporting around 256 addresses, of which 254 are assignable to hosts.
- Class D is a range reserved for multicast, to allow hosts to listen for a specific address within this range, and should the destination address of a packet contain a multicast address for which the host is listening, the packet shall be processed in the same way as a packet destined for the hosts assigned IP address. Each class is easily distinguishable in binary by observing the bit value within the first octet, where a class A address for instance will always begin with a 0 for the high order bit, whereas in a Class B the first two high order bits are always set as 1 and 0, allowing all classes to be easily determined in binary.

# IP Address Types

| Private Address Ranges | |
|---|---|
| Class A | 10.0.0.0~10.255.255.255 |
| Class B | 172.16.0.0~172.31.255.255 |
| Class C | 192.168.0.0~192.168.255.255 |

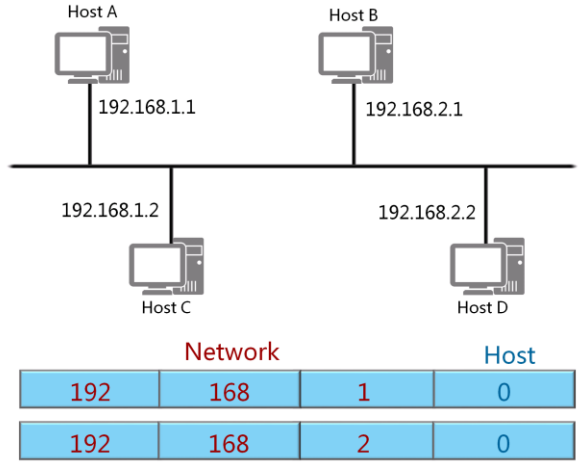
| Special Addresses | |
|---|---|
| Diagnostic | 127.0.0.0 ~ 127.255.255.255 |
| Any Network | 0.0.0.0 |
| Network Broadcast | 255.255.255.255 |

- The IP network address range has been divided, and certain addresses and ranges assigned special functions in the network.

  HUAWEI

- Within IPv4, specific addresses and address ranges have been reserved for special purposes. Private address ranges exist within the class A, B and C address ranges to prolong the rapid decline in the number of available IP addresses. The number of actual end systems and devices that require IP addressing in the world today exceeds the 4’ 294’ 967’ 296 addresses of the 32 bit IPv4 address range, and therefore a solution to this escalating problem was to allocate private address ranges that could be assigned to private networks, to allow for conservation of public network addresses that facilitate communication over public network infrastructures such as the Internet.
- Private networks have become common throughout the enterprise network but hosts are unable to interact with the public network, meaning that address ranges can be reused in many disparate enterprise networks. Traffic bound for public networks however must undergo a translation of addresses before data can reach the intended destination.
- Other special addresses include a diagnostic range denoted by the 127.0.0.0 network address, as well as the first and last addresses within the IPv4 address range, for which 0.0.0.0 represents any network and for which its application shall be introduced in more detail along with principles of routing. The address 255.255.255.255 represents a broadcast address for the IPv4 (0.0.0.0) network, however the scope of any broadcast in IP is restricted to the boundaries of the local area network from which the broadcast is generated.

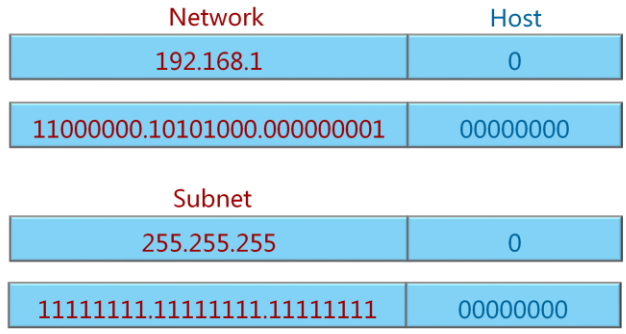
# IP Communication



- In order for a host to forward traffic to a destination, it is necessary for a host to have knowledge of the destination network. A host is naturally aware of the network to which it belongs but is not generally aware of other networks, even when those networks may be considered part of the same physical network. As such hosts will not forward data intended for a given destination until the host learns of the network and thus with it the interface via which the destination can be reached.
- For a host to forward traffic to another host, it must firstly determine whether the destination is part of the same IP network. This is achieved through comparison of the destination network to the source network (host IP address) from which the data is originating. Where the network ranges match, the packet can be forwarded to the lower layers where Ethernet framing presides, for processing. In the case where the intended destination network varies from the originating network, the host is expected to have knowledge of the intended network and the interface via which a packet/frame should be forwarded before the packet can be processed by the lower layers. Without this information, the host will proceed to drop the packet before it even reaches the data link layer.

## Subnet Mask

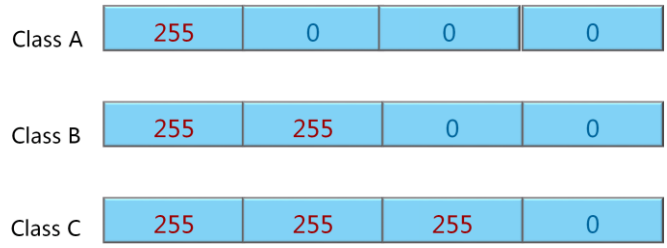



- Subnet masks distinguish between the binary values that represent each (sub)network and those that represent each host.

- The identification of a unique network segment is governed by the implementation of a mask value that is used to distinguish the number of bits that represent the network segment, for which the remaining bits are understood as representing the number of hosts supported within a given network segment. A network administrator can divide a network address into sub-networks so that broadcast packets are transmitted within the boundaries of a single subnet. The subnet mask consists of a string of continuous and unbroken 1 values followed by a similar unbroken string of 0 values. The 1 values correspond to the network ID field whereas the 0 values correspond to the host ID field.

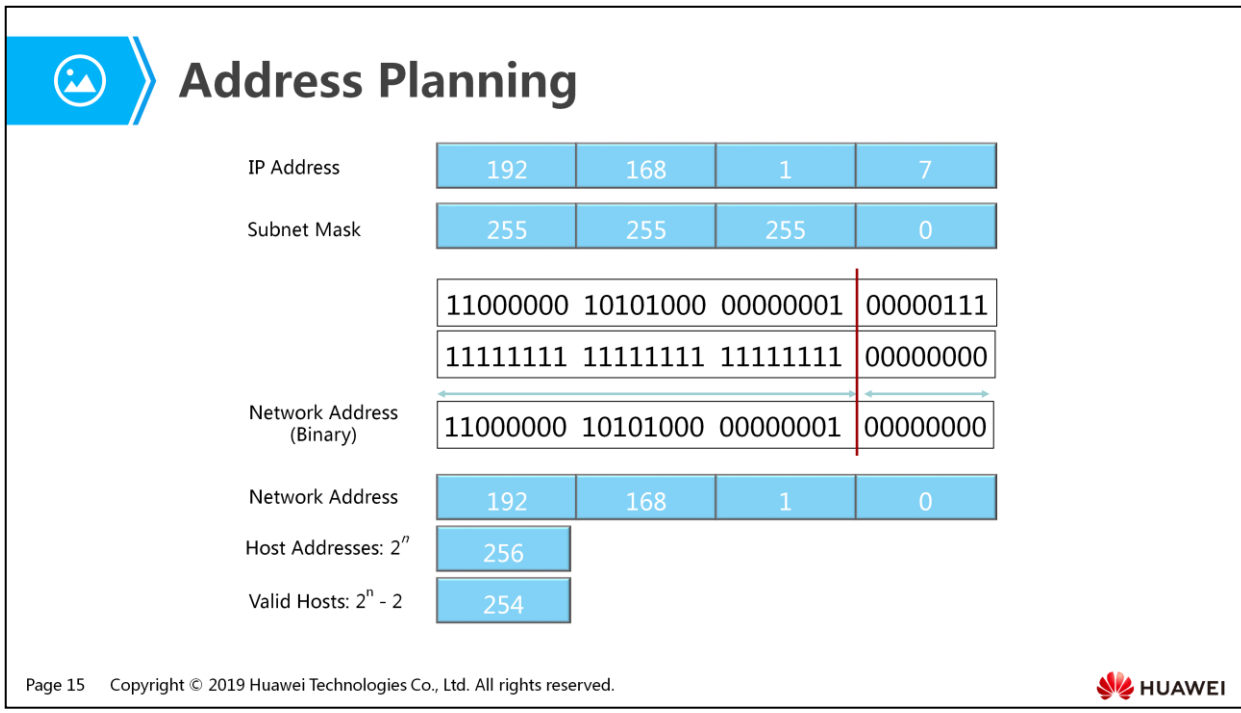
# Default Subnet Mask




- Certain subnet masks are applied to address ranges by default to denote the fixed range that is used for each network class.

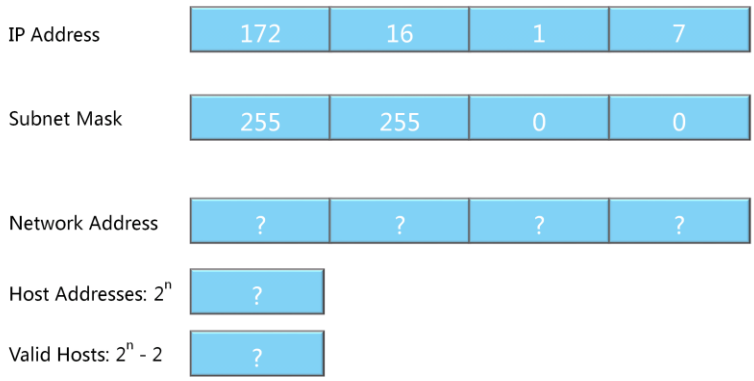
 

- For each class of network address, a corresponding subnet mask is applied to specify the default size of the network segment. Any network considered to be part of the class A address range is fixed with a default subnet mask pertaining to 8 leftmost bits which comprise of the first octet of the IP address, with the remaining three octets remaining available for host ID assignment.
- In a similar manner, the class B network reflects a default subnet mask of 16 bits, allowing a greater number of networks within the class B range at the cost of the number of hosts that can be assigned per default network. The class C network defaults to a 24 bit mask that provides a large number of potential networks but limits greatly the number of hosts that can be assigned within the default network. The default networks provide a common boundary to address ranges, however in the case of class A and class B address ranges, do not provide a practical scale for address allocation for Ethernet based networks.




- Application of the subnet mask to a given IP address enables identification of the network to which the host belongs. The subnet mask will also identify the broadcast address for the network as well as the number of hosts that can be supported as part of the network range. Such information provides the basis for effective network address planning. In the example given, a host has been identified with the address of 192.168.1.7 as part of a network with a 24 bit default (class C) subnet mask applied. In distinguishing which part of the IP address constitutes the network and host segments, the default network address can be determined for the segment.
- This is understood as the address where all host bit values are set to 0, in this case generating a default network address of 192.168.1.0. Where the host values are represented by a continuous string of 1 values, the broadcast address for the network can be determined. Where the last octet contains a string of 1 values, it represents a decimal value of 255, for which a broadcast address of 192.168.1.255 can be derived.
- Possible host addresses are calculated based on a formula of $2^n$ where n represents the number of host bits defined by the subnet mask. In this instance n represents a value of 8 host bits, where $2^8$ gives a resulting value of 256. The number of usable host addresses however requires that the network and broadcast addresses be deducted from this result to give a number of valid host addresses of 254.

## Case Scenario

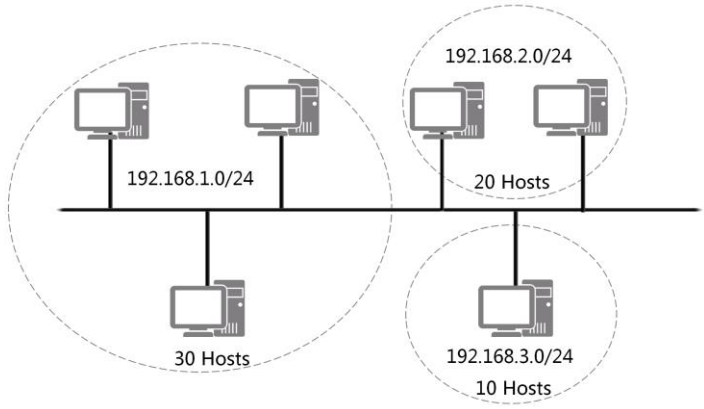



- Determine the network for the given IP address, and the number of actual, and valid host addresses in the network.

- The case scenario provides a common class B address range to which it is necessary to determine the network to which the specified host belongs, along with the broadcast address and the number of valid hosts that are supported by the given network. Applying the same principles as with the class C address range, it is possible for the network address of the host to be determined, along with the range of hosts within the given network.

# Addressing Limitations

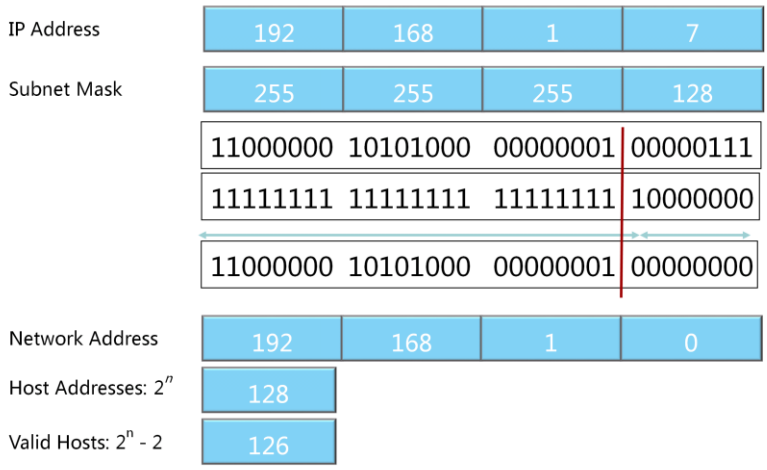



- Network design using the default subnet mask results in address wastage.

- One of the main constraints of the default subnet mask occurs when multiple network address ranges are applied to a given enterprise in order to generate logical boundaries between the hosts within the physical enterprise network. The application of a basic addressing scheme may require a limited number of hosts to be associated with a given network, for which multiple networks are applied to provide the logical segmentation of the network. In doing so however, a great deal of address space remains unused, displaying the inefficiency of default subnet mask application.

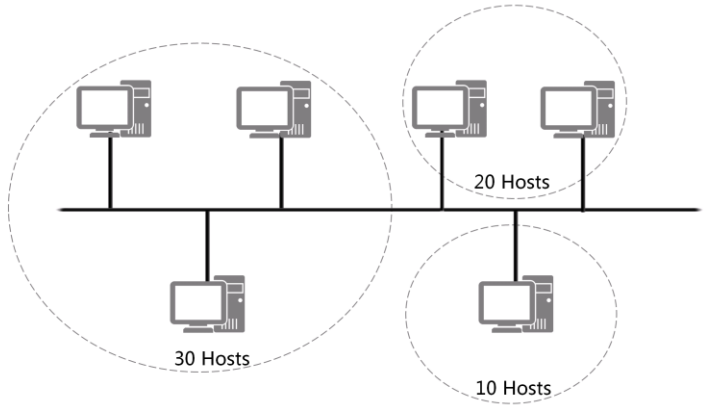
# VLSM Calculation



- As a means of resolving the limitations of default subnet masks, the concept of variable length subnet masks are introduced, which enable a default subnet mask to be broken down into multiple sub-networks, which may be of a fixed length (a.k.a. fixed length subnet masks or FLSM) or of a variable length known commonly by the term VLSM. The implementation of such subnet masks consists of taking a default class based network and dividing the network through manipulation of the subnet mask.
- In the example given, a simple variation has been made to the default class C network which by default is governed by a 24 bit mask. The variation comes in the form of a borrowed bit from the host ID which has been applied as part of the network address. Where the deviation of bits occurs in comparison to the default network, the additional bits represent what is known as the subnet ID.
- In this case a single bit has been taken to represent the sub-network for which two sub-networks can be derived, since a single bit value can only represent two states of either 1 or 0. Where the bit is set to 0 it represents a value of 0, where it is set to 1 it represents a value of 128. In setting the host bits to 0, the sub-network address can be found for each sub-network, by setting the host bits to 1, the broadcast address for each sub-network is identifiable. The number of supported hosts in this case represents a value of $2^7$ minus the sub-network address and broadcast address for each sub-network, resulting in each sub-network supporting a total of 126 valid host addresses.

## VLSM Case Scenario

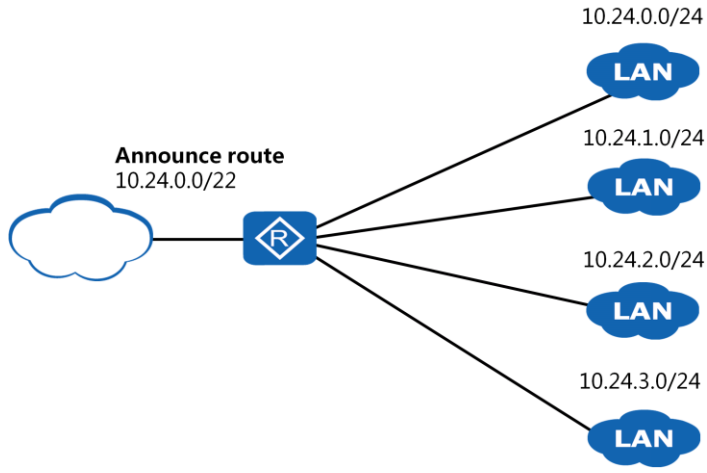



- Using only the network 192.168.1.0/24, implement VLSM for the given number of hosts in each network segment.

- In relation to problem of address limitations in which default networks resulted in excessive address wastage, the concept of variable length subnet masks can be applied to reduce the address wastage and provide a more effective addressing scheme to the enterprise network.
- A single default class C address range has been defined, for which variable length subnet masks are required to accommodate each of the logical networks within a single default address range. Effective subnet mask assignment requires that the number of host bits necessary to accommodate the required number of hosts be determined, for which the remaining host bits can be applied as part of the subnet ID, that represents the variation in the network ID from the default network address.

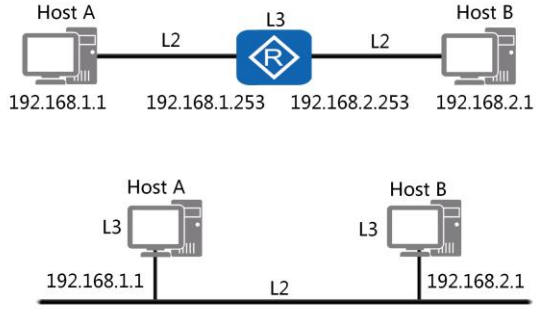
# Classless Inter-Domain Routing



- Classless inter-domain routing was initially introduced as a solution to handle problems that were occurring as a result of the rapid growth of what is now known as the Internet. The primary concerns were to the imminent exhaustion of the class B address space that was commonly adopted by mid-sized organizations as the most suited address range, where class C was inadequate and where class A was too vast, and management of the 65534 host addresses could be achieved through VLSM. Additionally, the continued growth meant that gateway devices such as routers were beginning to struggle to keep up with the growing number of networks that such devices were expected to handle. The solution given involves transitioning to a classless addressing system in which classful boundaries were replaced with address prefixes.
- This notation works on the principle that classful address ranges such as that of class C can be understood to have a 24 bit prefix that represents the subnet or major network boundary, and for which it is possible to summarize multiple network prefixes into a single larger network address prefix that represents the same networks but as a single address prefix. This has helped to alleviate the number of routes that are contained particularly within large scale routing devices that operate on a global scale, and has provided a more effective means of address management. The result of CIDR has had far reaching effects and is understood to have effectively slowed the overall exhaustion rate of the IPv4 address space.

# IP Gateways

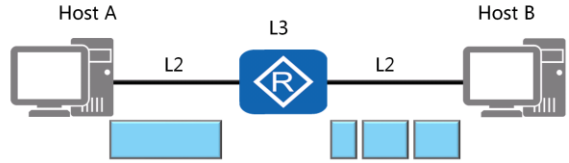



- Gateways use IP to forward packets between networks.
- Hosts may act as gateways between networks in a LAN.

- The forwarding of packets requires that the packet first determine a forwarding path to a given network, and the interface via which a packet should be forwarded from, before being encapsulated as a frame and forwarded from the physical interface. In the case where the intended network is different from the originating network, the packet must be forwarded to a gateway via which the packet is able to reach it’ s intended destination.
- In all networks, the gateway is a device that is capable of handling packets and making decisions as to how packets should be routed, in order to reach their intended destination. The device in question however must be aware of a route to the intended destination IP network before the routing of packets can take place. Where networks are divided by a physical gateway, the interface IP address (in the same network or sub-network) via which that gateway can be reached is considered to be the gateway address.
- In the case of hosts that belong to different networks that are not divided by a physical gateway, it is the responsibility of the host to function as the gateway, for which the host must firstly be aware of the route for the network to which packets are to be forwarded, and should specify the hosts own interface IP address as the gateway IP address, via which the intended destination network can be reached.

# IP Fragmentation

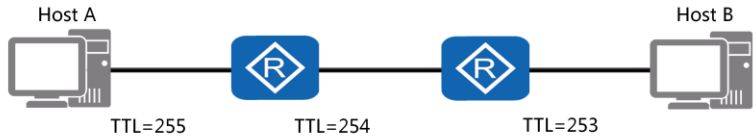



| Version | Header Length | DS Field | Total Length |
|---|---|---|---|
| **Identification** | | **Flags** | **Fragment Offset** |
| Time to Live | Protocol | Header Checksum | |
| Source IP Address | | | |
| Destination IP Address | | | |
| IP Options | | | |

- The data of forwarded packets exists in many formats and consists of varying sizes, often the size of data to be transmitted exceeds the size that is supported for transmission. Where this occurs it is necessary for the data block to be broken down into smaller blocks of data before transmission can occur. The process of breaking down this data into manageable blocks is known as fragmentation.
- The identification, flags and fragment offset fields are used to manage reassembly of fragments of data once they are received at their final intended destination. Identification distinguishes between data blocks of traffic flows which may originate from the same host or different hosts. The flags field determines which of a number of fragments represents the last fragment at which time initiation of a timer is started prior to reassembly, and to notify that reassembly of the packet should commence.
- Finally the fragment offset labels the bit value for each fragment as part of a number of fragments, the first fragment is set with a value of 0 and subsequent fragments specify the value of first bit following the previous fragment, for example where the initial fragment contains data bits 0 through to 1259, the following fragment will be assigned an offset value of 1260.

# Time To Live



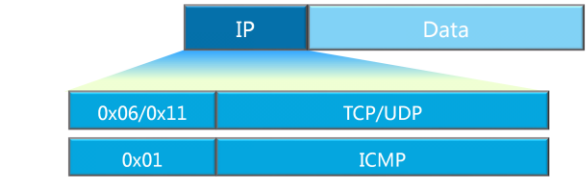

| Version | Header Length | DS Field | Total Length |
|---|---|---|---|
| Identification | | Flags | Fragment Offset |
| **Time to Live** | Protocol | Header Checksum | |
| Source IP Address | | | |
| Destination IP Address | | | |
| IP Options | | | |





- As packets are forwarded between networks, it is possible for packets to fall into loops where routes to IP networks have not been correctly defined within devices responsible for the routing of traffic between multiple networks. This can result in packets becoming lost within a cycle of packet forwarding that does not allow a packet to reach its intended destination. Where this occurs, congestion on the network will ensue as more and more packets intended for the same destination become subject to the same fate, until such time as the network becomes flooded with erroneous packets.
- In order to prevent such congestion occurring in the event of such loops, a time to live (TTL) field is defined as part of the IP header, that decrements by a value of 1 each time a packet traverses a layer 3 device in order to reach a given network. The starting TTL value may vary depending on the originating source, however should the TTL value decrement to a value of 0, the packet will be discarded and an (ICMP) error message is returned to the source, based on the source IP address that can be found in the IP header of the wandering packet.

# Protocol Field




| Version | Header Length | DS Field | Total Length |
|---|---|---|---|
| Identification | | Flags | Fragment Offset |
| Time to Live | **Protocol** | Header Checksum | |
| Source IP Address | | | |
| Destination IP Address | | | |
| IP Options | | | |





- Upon verification that the packet has reached its intended destination, the network layer must determine the next set of instructions that are to be processed. This is determined by analyzing the protocol field of the IP header. As with the type field of the frame header, a hexadecimal value is used to specify the next set of instructions to be processed.
- It should be understood that the protocol field may refer to protocols at either the network layer, such as in the case of the Internet Control Message Protocol (ICMP), but may also refer to upper layer protocols such as the Transmission Control Protocol (06/0x06) or User Datagram Protocol (17/0x11), both of which exist as part of the transport layer within both the TCP/IP and OSI reference models.

# Summary

- What is the IP subnet mask used for?
- What is the purpose of the TTL field in the IP header?
- How are gateways used in an IP network?

HUAWEI

- The IP subnet mask is a 32 bit value that describes the logical division between the bit values of an IP address. The IP address is as such divided into two parts for which bit values represent either a network or sub-network, and the host within a given network or sub-network.
- IP packets that are unable to reach the intended network are susceptible to being indefinitely forwarded between networks in an attempt to discover their ultimate destination. The Time To Live (TTL) feature is used to ensure that a lifetime is applied to all IP packets, so as to ensure that in the event that an IP packet is unable to reach it’ s destination, it will eventually be terminated. The TTL value may vary depending on the original source.
- Gateways represent points of access between IP networks to which traffic can be redirected, or routed in the event that the intended destination network varies from the network on which the packet originated.


Thank You
www.huawei.com