INTERNET CONTROL PROTOCOLS

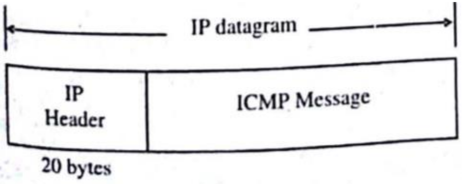
At the network layer (or more accurately the Internetwork layer), TCP/IP supports the internetwork
Protocol (IP). IP contains four supporting protocols:
1: Address Resolution Protocol (ARP)
2: Reverse Address Resolution Protocol (RARP)
3: Internet Control Message Protocol (ICMP)
4: Internet Group Message Protocol (IGMP)
5: BOOTP

INTERNET CONTROL MESSAGE PROTOCOL (ICMP) : is a mechanism used by hosts and routers to send notification of datagram problems back to the sender. ICMP uses echo test/reply to test whether a destination is reachable and responding.

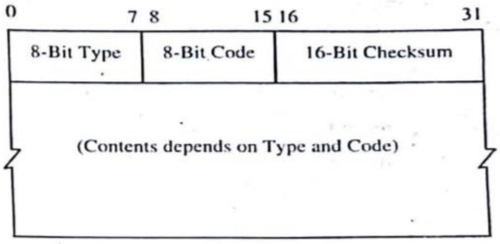
It also handles both control and error messages, but its sole function is to report problems, not correct them. Responsibility for correction lies with the sender.

A datagram carries only the addresses of the original sender and the final destination. It does not know the addresses of the previous router(s) that passed it along. For this reason ICMP can send messages only to the source, not to an intermediate router. ICMP is often considered part of the IP layer.

It communicates error messages and other conditions that require attention. ICMP messages are usually acted on by either the IP layer or the higher layer protocol (TCP or UDP). Some ICMP messages cause errors to be returned to User processes. ICMP messages are transmitted within IP datagrams

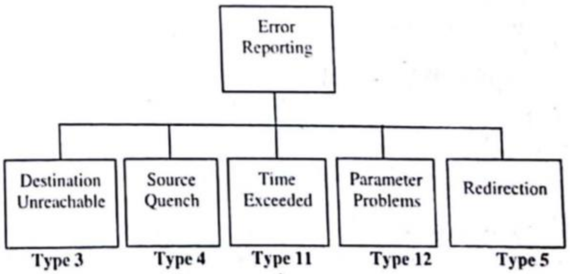


Shows the format of an ICMP message. The first 4 bytes have the same format for all messages, but the remainder differs from one message to the next.



Error Reporting In ICMP

ICMP always reports error messages to the original source. Five types of errors are handled



The following are important points about ICMP error messages:
1: No ICMP error message will be generated in response to a datagram carrying an ICMP error message.
2: No ICMP error message will be generated for a fragmented datagram that is not the first fragment
3: No ICMP error message will he generated for n datagram having a multicast address.
4: No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

All error messages contain a data section that includes the IP header of the original datagram plus the first 8 bytes of data in that datagram. The original datagram header is added to give the original source. Which receives the error message, information about the datagram itself.

ADDRESS RESOLUTION PROTOCOL (ARP)

ARP is used to find the physical address of the node when its Internet address is known. Anytime a host. or a router needs to find the physical address of another host on its network. it formats an ARP query packet that includes the IP address and broaden ts in over the network. Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes its internet address and sends back its physical address

The host holding the datagram adds the address of the target host both to its cache memory and to the datagram header, then sends the datagram on its way.

ARP is a low level protocol that uses the services of the MAC (Data Link) Layer, and as with all protocols, is then encapsulated in a physical network frame.

WORKING OF ARP

Step1: When a source device want to communicate with another device, source device checks its Address Resolution Protocol (ARP) cache to find it already has a resolved MAC address of the destination device.

If it is there, it will use that address for communication. To view your local address resolution protocol(ARP) cache, Open command prompt and type command "arp a"

Step2: If ARP resolution is not there in local cache, the source machine will generate an ARP request message, it puts its own data link layer address as the sender hardware address and its own IP Address as the sender protocol Address

Step3: the source broadcast the ARP request message to the local network

Step4: The message is received by each device on the LAN since it is A broadcast. each device compare the target protocol address with its own protocol address. Those who do not match will drop the packet without any action

Step5: when the target device checks the target protocol address, it will find a match and will generate an ARP reply message

Step6: The destination device will update its Address Resolution protocol (ARP) cache. since it need to contact the sender machine soon.

Step7: Destination device send the ARP reply message and it will not be a broadcast, but a unicast

Step8: The source machine will process the ARP reply from destination, it store the Sender Hardware Address as the layer 2 address or the destination

Step9: The source machine will update its ARP cache with the Sender Hardware Address and Sender Protocol Address it received from the ARP reply message.

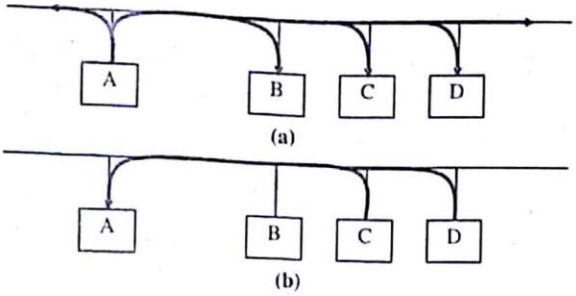
REVERSE ADDRESS RESOLUTION PROTOCOL (RARP)

RARP works much like ARP. The host wishing to retrieve its internet address broadcast an RARP query packet that contains its physical address to every host on its physical network.

A server on the network recognizes the RARP packet and returns the host's internet address The TCP/IP protocol that allows a computer to obtain its IP address from a server is known as the Reverse Address Resolution Protocol (RARP).

RARP is adapted from the ARP protocol and uses the same message format. Like an ARP message, a RARP message is sent from one machine to another encapsulated in the data portion of a network frame.

Figure shows how a host uses RARP. The sender broadcasts a RARP request that specifics itself as both the sender and target machine, and supplies its physical network address in the target hardware address field. All computers on the network receive the request, but only those authorized to supply the RARP service process the request and send a reply such computers are known informally as RARP servers. For RARP to succeed. the network must common at least one RARP server



Server answer requests by filling in the target protocol address field, changing the message type from request to reply, and sending the reply back directly to the machine making the request. The original machine receives replies from all RARP servers, even though only the first is needed

BOOT STRAP PROTOCOL

To overcome some of the drawback of RARP, researcher developed the BOOT strap Protocol (BOOTP). Later, the Dynamic Host Configuration Protocol (DHCP) was developed as a successor to BOOTP. Because the two protocol are closely related. Because it uses UDP uses IP,BOOTP can be implemented with an application program. Like RARP. BOOTP operates in tJ1e client-server paradigm and requires only a single packet exchange. However, BOOTP is more efficient than RARP because a single BOOTP message specific many items needed at start-up. including a computer IP address, the address of a router, and the address of a server.

BOOTP also includes a vender-specific field in the reply that allows hardware vendors to send additional information used only for their computers.

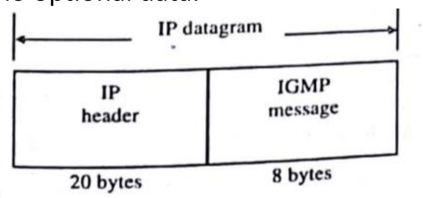
BOOTP places all responsibility for reliable communication on the client. Because UDP uses IP for delivery. messages can be delayed. lost, delivered out of order or duplicated. Furthermore, because IP docs not provide a checksum for data, the UDP datagram could arrive with some bits corrupted.
If no reply arrives before the timer expires, the client must re-transmit the request. Of course, after a power failure all machines on a network will re-boot simultaneously possibly over-running the BOOTP server(s) with requests
If all clients use exactly the same re-transmission timeout, many or all of them will attempt to re-transmit simultaneously. To avoid the resulting collision, the BOOTP specification recommends using a random delay.

MULTICASTING In multicast communication, there is one source and a group of destination. The relationship is one-to-many. In this type of communication, the source address is a unicast address. But the destination address is a group address which defines one or more destinations. The group address identifies the members of the group.
A multicast packet start from the source S1 and goes to all destinations that belong to group G1
In multicasting, when a router receives a packet, it may forward it through severl of its interfaces

Applications of Multicasting

1: Access to Distributed Databases: Most of the large databases today are distributed. That is, the information is stored in more than one location, usually at the time of production.
2: Information Dissemination: Businesses often need to send information to their customers. If the nature of the information is the same for each customer, it can be multicast
3: Dissemination of News: In a similar manner news can be easily disseminated through multicasting. one single message can be sent to those interested in a particular topic
4: Teleconferencing: It Involves multicasting. the individuals attending a Teleconference all need to receive the same information at the same time. temporary or permanent groups can be formed for this purpose
5: Distance Learning: One growing area in the use of multicasting is Distance Learning. Lesson taught by one single professor can be received by a specific group of students

INTERNET GROUP MESSAGE PROTOCOL (IGMP) which is used by hosts and routers that support multicasting. It lets all the systems on a physical network know which hosts currently belong to which multicast groups
This information is required by the multicast routers, so they know which multicast datagrams to forward onto which interfaces. Like ICMP, IGMP is considered part of the IP layer. Also like ICMP, IGMP messages are transmitted in IP datagrams. Unlike other protocols, IGMP has a fixed-size message, with no optional data.



IGMP Message

shows the format of the 8-byte

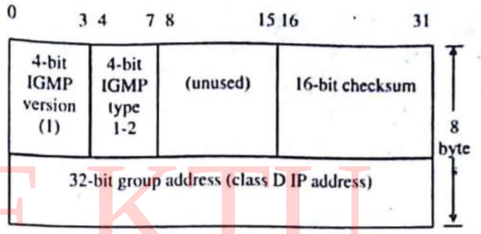


Figure 5.8: Format of Fields in IGMP Message

The IGMP version is 1. An IGMP type of 1 is a query sent by a multicast router, and 2 is a response sent by a host. The checksum is calculated in the same manner as the ICMP checksum
The group address is a class D IP address. In a query the group address is set to O. and in a report it contains the group address being reported

EXTERIOR ROUTING PROTOCOL

Protocols used between autonomous systems are called exterior routing protocols. Although interior routing protocols are usually designed to provide detailed routing information about all or most computers inside the autonomous systems, exterior protocols are designed to be more careful in the information they provide. Usually, exterior protocols provide information about only the preferred or tJ1e best routes rather than all possible routes.
Border Gateway Protocol (BGP) is the most common exterior routing protocol in use today.

BORDER GATEWAY PROTOCOL (BGP)

BGP is a complex, advanced distance Exterior Gateway Protocol (EGP). BGP exchange routing information between Autonomous Systems (ASs). BGP is especially used for exchanging routing information between all of the major internet Service Providers (1SPs) as well between larger client sites and their respective ISPs. And. in some large enterprise networks. BGP is used to interconnect different geographical or administrative regions.

Some of the primary attributes of BGP is the use of pieces of information about a known route. where it came from and how to reach it, A BGP router will also generate an error message if it receives a route that is missing these are mandatory attributes

The border Gateway Protocol (BGP) was developed for use in conjunction with elements that employ the TCP/IP suite, although the concepts are applicable to any internet BGP has become the preferred exterior router protocol for the internet. Functions BGP was designed to allow routers called gateways in the standard, in different Autonomous systems. (ASs) to cooperate in the exchange of routing information. The protocol operates in terms of messages which are sent over TCP connections

Characteristics of BGP

1: It is an advanced distance vector protocol

2: It sends full routing updates at the start of the session, trigger updates are sent afterward

3: It maintains connections by sending periodic keep lives

4: It sends a triggered update when a keep alive, an update, or a notification is not received

5: It creates and maintains connections between peers using TCP port 179

6: It Has its own routing table, although it is capable of both sharing and inquiring of the interior IP routing table

7: BGP uses a very complex metric, and is the source of its strength. The metric, referred to as attributes, allows great flexibility in path selection

IPV6 (INTERNET PROTOCOL VERSION 6)

is a set of specifications from the Internet Engineering Task Force (IETF) that's essentially an upgrade of IP version 4 (IPv4). The basics of IPv6 are similar to those of IPv4 -- devices can use IPv6 as source and destination addresses to pass packets over a network, and tools like ping work for network testing as they do in IPv4, with some slight variations.

A main advantage of IPv6 is increased address space. The 128-bit length of IPv6 addresses is a significant gain over the 32-bit length of IPv4 addresses, allowing for an almost limitless number of unique IP addresses. The size of the IPv6 address space makes it less vulnerable to malicious activities such as IP scanning. IPv6 packets can support a larger payload than IPv4 packets resulting in increased throughput and transport efficiency. IPv6 also support auto-configuration to help correct most of the shortcomings in version 4, and it has integrated security and mobility features.

IPv6 features include:

1. Supports source and destination addresses that are 128 bits (16 bytes) long.
2. Requires IPSec support.
3. Uses Flow Label field to identify packet flow for QoS handling by router.
4. Allows the host to send fragments packets but not routers.
5. Doesn't include a checksum in the header.
6. Uses a link-local scope all-nodes multicast address.

Structure of IPv6

The only header that is required is referred to simply as the 1Pv6 header. This is of fixed size with a length of 40 octets. Compared to 20 octet. for the mandatory portion of the 1Pv4 header. The following extension headers have been defined:

1: Hop-by-Hop Options Header: Defines special options that require hop-by-hop processing.

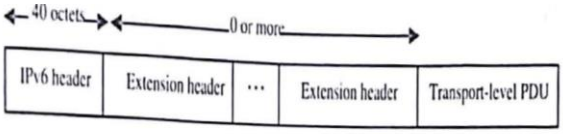
2: Routing Header: Provides extended routing, similar to IPv4 source routing.

3: fragment Header: Contains fragmentation and reassembly information.

4: Authentication Header: Provides packet integrity and authentication.

5: Encapsulating Security Pay-load Header: Provides privacy.

6: Destination Options Header: Contains optional infon11a1ion to be examined by the destination node.



ISSUES RELATED TO IPV6

1: Lack of IPv6 Security Training/Education: The biggest risk today is the lack of IPv6 security knowledge. Enterprises must invest lime and money in IPv6 security training upfront, before deploying. Network security is more effective as part of the planning stage rather than after deployment.

2: security Device Bypass via Unfiltered IPv6 and Tunnelled Traffic: Only a lack of knowledge is considered a bigger risk than the security products themselves. Conceptually it's simple, security products need to do two things recognize suspicious IPv6 packets and apply controls when they do. However in practice this is hardly possible in IPv4 let alone an environment that may have rogue or unknown runnel traffic.

3: Lack of IPv6 Support at ISPs and Vendors: Thorough testing is critical until IPv6 security functionality and Stability are on par with that of IPv4. A test network and a test plan for all protocols involved must be devised to test all equipment especially new security tech from vendors. Every network is unique and requires a unique test plan. Further complicating the issues is not having a native IPv6 connection from provider. A tunnel connected to interface further increases security complexity and provides an opening for man in the middle and denial of service attacks

4: Congruence of security policies in IPv4 & IPv6: Weak IPv6 security policies are direct result of the current deficit In IPv6 security knowledge, Not only do the depth of the IPv6 security policies need to be equal to that of their IPv4 Counterparts but their breadth must be wider to encompass new vulnerabilities that didn't need to be considered in an IPv4 homogeneous environment

Advantage of IPv6 over IPv4

1: Larger Address Space: Address filed in IPv6 is 128 bits long while the address filed of IPv4 is only 32 bit in length IPv6 offers very large, i.e. 296 address space as compared to IPv4

2: Better Header Format: The header of IPv6 has been designed in a way to speed up the routing process. In header of IPv6 options are separated from the base header. options are inserted into base header only when required by the upper-layer data

3: Provision for Extension: IPv6 has been designed in a way that a protocol can be extended easily to meet the requirements of emerging technologies or new applications

4: Resource Allocation Support in IPv6: IPv6 provides a mechanism called flow label for resource Allocation. Flow label enables source to send request for the special handling of a packet. This mechanism is really helpful in real -time audio and video transmission

5: Security Features: To ensure confidentiality and packet's integrity encryption and authentication options are included in IPv6

ICMPv6

Internet Control Message Protocol (both ICMPv4 and ICMPv6) is a protocol which acts as a communication messenger protocol between the communicating devices in IP network. ICMP messages provide feedback, error reporting and network diagnostic functions in IP network which are necessary for the smooth operation of IPv6

ICMPv6 is a new version of the ICMP that forms an integral pan of the IPv6 architecture. ICMPv6 message are transported within an IPv6 packet that may include IPv6 extension within header

Function of ICMPv6

1: Error Reporting, 2: Network Diagnostics

3: Neighbour Discovery

4: Multicasting Membership Reporting

5: Router Solicitation and router Advertisements

ICMPv6 Messages

ICMPv6 is a multipurpose protocol and is used for a variety of activities including error reporting in packet processing, diagnostic activities, Neighbour Discovery process and IPv6 multicast membership reporting. To perform these activities, ICMPv6 messages are subdivided into two classes

1: Error Messages: ICMPv6 error messages are used to report errors in the forwarding or delivery of IPv6 packets. The ICMPv6 "Type field'' values for the error message are between O and 127.

ICMPv6 error messages belong to four different categories:

1: Destination Unreachable: Destination Unreachable ICMPv6 error message is generated by the source host or a router when an IPv6 datagram packet cannot be delivered for any reason other than congestion.

2: Packet Too Big: Packet Ton Dig ICMPv6 error messages are generated by the router when a packet cannot be forwarded to the next hop link because the size of the IPv6 datagram is larger than the MTU (Maximum Transmission Unit) of the link. Packet Too Dig ICMPv6 error message includes the MTU of the next link also. MTU is the size of the largest protocol data unit that is supported over the link.

3: Time Exceeded: Similar to the Time-to-Live field value in 1Pv4 datagram header, IPv6 header includes a Hop Limit field. The Hop Limit field value in IPv6 header is used to prevent routing loops. Hop Limit field in IPv6 datagram header is decremented by each router that forwards the packet. When the Hop Limit field value in IPv6 header reaches zero, the router discards the IPv6 datagram packet and returns a "Time Exceeded'' ICMPv6 error message to the source host.

4: Parameter Problems: Parameter Problem ICMPv6 error message is typically related with the problems and mistakes related with IPv6 header itself. When a problem or mistake with an IPv6 header make a router cannot process the packet, the router stops processing the IPv6 datagram packet discards the packet and returns a "Parameter Problem" ICMPv6 error message to the source host

2: information Messages: ICMPv6 informational messages are used for network diagnostic functions and additional critical network functions like Neighbour Discovery. Router Solicitation & Router Advertisement, Multicasting Memberships. Echo Request and Echo Reply are also ICMPv6 information messages. ICMPv6 informational messages have values for the Type field (8 bit binary number) between 128 and 255.

1: Diagnostic Messages: ICMPv6 Echo request and Echo reply are the Diagnos1ic messages. Every IPv6 host must return an ICMPv6 Echo reply when it receives an ICMPv6 Echo request. Echo request and Echo reply messages are used by the ping command to check the network connectivity between two IPv6 hosts

2: MLD (Multicast Listener Discovery) Messages: ICMPv6 MLD Messages are used by an IPv6 enabled router to discover hosts who are interested in multicast packers, and the multicast addresses they are interested. MLD messages are used by MLD Protocol. MLD (Multicast Listener Discovery) Protocol is the IPv6 equivalent of IGMP (Internet Group Management) Protocol in IPv4.

3: **ND (Neighbour Discovery) Messages**: ICMPv6 ND Messages are used for the Neighbour. Discovery Protocol (NDP). ND Messages includes Router Solicitation & Router Advertisement, Neighbour Solicitation and Neighbour Advertisement

ICMPv6 ADVANTAGES

✓ provides more address space (which is being needed in larger business scales-example Comcast)

✓ More powerful internet (128bit versus IPv4's current 32 bit)

✓ Offers and overall larger scale internet-which again will be needed in the future

✓ Address allocation is done by the device itself

✓ Support for security using (IPsec) Internet Protocol Security

DISADVANTAGES

✓ It will be much harder to remember IP addresses (compared to the addresses now)

✓ Creating a smooth transition from IPv4 to IPv6

✓ IPv6 is not available to machines that run IPv4

✓ Any consumer costs in having to replace an IPv4 machine

✓ Time to convert over to IPv6

Checksum

ICMPv6 provides a minimal level of message integrity verification by the inclusion of a 16-bit checksum in its header. The checksum is calculated starting with a pseudo-header of IPv6 header fields according to the IPv6 standard, which consists of the source and destination addresses, the packet length and the next header field, the latter of which is set to the value 58.