ICMPv6

ICMP Background

- IP is connection less and unreliable
- Lagging of IP protocol:-
  - 1-Lack of Error Control (no error reporting & correcting mechanism)
  - 2-Lack of Assistance/ Query Mechanism

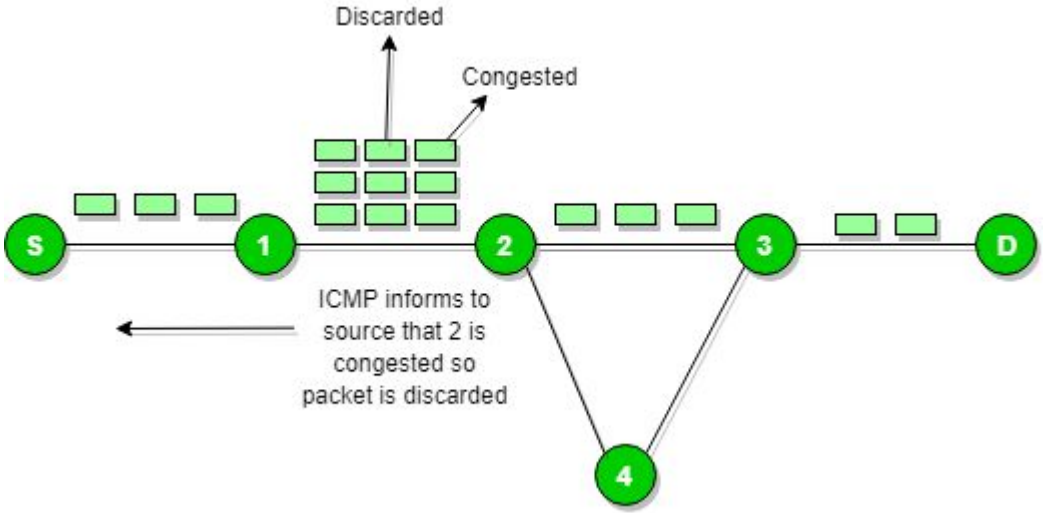
What happen if something goes wrong?

- It is network Layer Protocol
- **Purpose:-**
  - In order to **maintain the security** and safety of networks, maintaining a successful communication between devices is essential.
  - Being a **supporting protocol** in the **Internet protocol suite**, **ICMP** is often preferred by network devices to send error messages and similar information

So to Provide :

- Error Control & Assistance to datagram's

Internet Control Message protocol(ICMP)

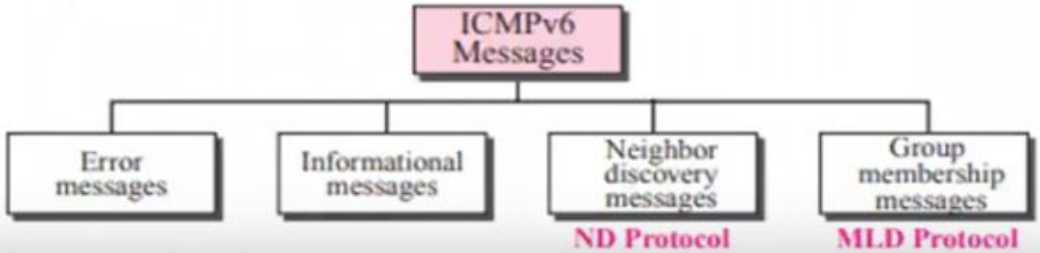


ICMPv6

- ICMP is one of the core protocols of the TCP/IP suite of protocols.
- Used by operating systems to send messages—either **informational or error messages**—between devices.
- Used by various applications such as **ping and traceroute** to test network connectivity between two devices

ICMPv6

- Protocols such as ND and MLD operate under the ICMPv6 protocol.
- Several extensions have been published, defining new ICMPv6 message types as well as new options for existing ICMPv6 message types.
- **ICMPv6 messages are grouped into two classes: error and informational messages.**
- Neighbor Discovery Protocol (NDP) is a node discovery protocol in IPv6 which replaces and enhances functions o ARP.
  - Secure Neighbor Discovery (SEND) is an extension of NDP with extra security.
- Multicast Listener Discovery (MLD) is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like
  - Internet Group Management Protocol (IGMP) is used in IPv4.
  - Multicast Router Discovery (MRD) allows discovery of multicast routers.



General Format of an ICMPv6 Message:

Every ICMPv6 message is preceded by an IPv6 header with/without an Extension header.

The ICMP message has a following message format-

Type- indicates the type of the message

Code- depends on message type. It provides additional level of granularity to the message.

Checksum- used for data-integrity of ICMPv6 messages

Type	Code 0	Checksum
Message Body		

ICMPv6 Fields

- Type (8 bits): Indicates the type of ICMPv6 message, such as Echo Request, Destination Unreachable, or Packet Too Big.
  - The Type field is used to group ICMPv6 messages into two classes:
    - Error messages: Type = 0 to 127
    - Informational messages: Type = 128 to 255
- Code (8 bits): Provides more granularity for the Type field. Its meaning depends on the message type.
- Checksum (16 bits): Used to detect data corruption in the ICMPv6 message and parts of the IPv6 header.

ICMPv6 Error Messages:

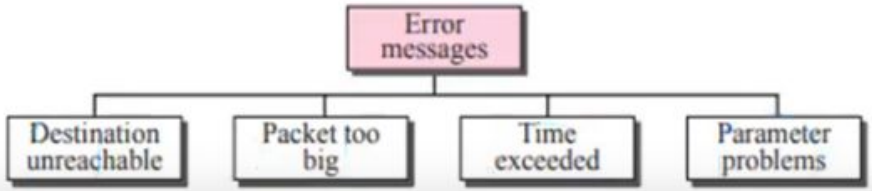
Type	Type Description	Code and Code Description
1	Destination Unreachable	0: No route to destination
		1: Communication with destination administratively prohibited
		2: Beyond scope of source address
		3: Address unreachable
		4: Port unreachable
		5: Source address failed ingress/egress policy
		6: Reject route to destination
2	Packet Too Big	0: Ignored by receiver
3	Time Exceeded	0: Hop limit exceeded in transit
		1: Fragment reassembly time exceeded
4	Parameter Problem	0: Erroneous header field encountered
		1: Unrecognized Next Header type encountered
		2: Unrecognized IPv6 option encountered
101	Private Experimentation	
107	Private Experimentation	
127	Reserved for expansion of ICMPv6 error messages	

ICMPv6 Informational Messages

Type	Type Description	Code and Code Description
Used by the **ping** *command (RFC 4443)*		
128	Echo Request	0: Ignored by receiver
129	Echo Reply	0: Ignored by receiver
Used for Multicast Listener Discovery (RFC 2710)		
130	Multicast Listener Query	0: Ignored by receiver
131	Multicast Listener Report	0: Ignored by receiver
132	Multicast Listener Done	0: Ignored by receiver
Used by Neighbor Discovery (RFC 4861)		
133	Router Solicitation	0: Ignored by receiver
134	Router Advertisement	0: Ignored by receiver
135	Neighbor Solicitation	0: Ignored by receiver
136	Neighbor Advertisement	0: Ignored by receiver
137	Redirect message	0: Ignored by receiver

Error Message

- As we know ICMP version 4, one of the main responsibilities of ICMP is to report errors.
- Four types of errors are handled: destination unreachable, packet too big, time exceeded, and parameter problems.
- Here the source-quenched message, which is used to control congestion in version 4, is eliminated in this version because the priority and flow label fields in IPv6 are supposed to take care of congestion.
- The redirection message has moved from the error-reporting category to the neighbor discovery category
- These messages are identified by the zero in the high-order bit of the Type field value.
- Hence, Type message from 0 to 127 are error messages and type messages from 128 to 255 are informational messages.



ICMPv6 messages

These ICMPv6 **error messages** are similar to ICMPv4 error messages:

- Destination Unreachable
- Packet Too Big
- Time Exceeded
- Parameter Problem

ICMPv6 Destination Unreachable

- The concept of the destination unreachable message is the same as described for ICMPv4.
- When a router cannot forward a datagram or a host cannot deliver the content of the datagram to the upper layer protocol
- Then router or the host discards the datagram and sends a destination-unreachable error message to the source host.

- Codes for DUM
  - *Code 0. No path to destination.*
  - *Code 1. Communication with the destination is administratively prohibited.*
  - *Code 2. Beyond the scope of source address.*
  - *Code 3. Destination address is unreachable.*
  - *Code 4. Port unreachable.*
  - *Code 5. Source address failed (filtering policy).*
  - *Code 6. Reject route to destination.*

Type :-1	Code 0 to 6	Checksum
Unused All(0)		
As much of received datagram as possible without exceeding the maximum IPv6 MTU		

ICMPv6 Packet Too Big Message

- This is a new type of message added to version 6.
- In IPv6 packets does not fragment at the router, if a router receives a datagram that is larger than the maximum transmission unit (MTU) size of the network through which the datagram should pass, two things happen.
  - First, the router discards the datagram.
  - Second, an ICMP error packet—a packet too-big message—is sent to the source.
- Here is only one code (0) and that the MTU field informs the sender of the maximum size packet accepted by the network.

Type :-2	Code 0	Checksum
MTU		
As much of received datagram as possible without exceeding the maximum IPv6 MTU		

ICMPv6 Time Exceeded Message

- Time-exceeded error message is generated in two cases:
  1. when the time to live value becomes zero and
  2. when not all fragments of a datagram have arrived in the time limit.
- The format of the time-exceeded message in version 6 is similar to the one in version 4.
- The only difference is that the type value has changed to 3.
- As in version 4, code 0 is used when the datagram is discarded by the router due to a hop-limit field value of zero. Code 1 is used when fragments of a datagram are discarded because other fragments have not arrived within the time limit.

Type :-3	Code 0 or 1	Checksum
Unused All(0)		
As much of received datagram as possible without exceeding the maximum IPv6 MTU		

ICMPv6 Parameter Problem

- Any ambiguity in the header of the datagram can create serious problems as the datagram travels through the Internet.
- If a router or the destination host discovers any ambiguous or missing value in any field, it discards the datagram and sends a parameter-problem message to the source.
- The message in ICMPv6 is similar to its version 4 counterpart.
- However, the type value has been changed to 4 and the size of the offset pointer field has been increased to 4 bytes.
- There are also three different codes instead of two.

  - Code 0. Erroneous header field.
  - Code 1. Unrecognized next header type.
  - Code 2. Unrecognized IPv6 option.

Type :-4	Code 0,1,2	Checksum
Offset pointer		
As much of received datagram as possible without exceeding the maximum IPv6 MTU		

ICMPv6 Informational messages

The following ICMPv6 informational messages used by ping are also similar to those in ICMPv4:

- Echo Request
- Echo Reply

ICMPv6 Informational messages:Echo Request

ICMPv6 Informational Messages:[These messages are usually used for diagnostic purposes.]

1. Type 128 Echo Request
2. Type 129 Echo Reply

Type :-128	Code 0	Checksum
Identifier		Sequence number
Optional data Sent by the request message; repeated by the reply message		

Type- 128

Code- 0

Identifier- An identifier that can help to matching Echo Replies. May be zero.

Sequence Number- An identifier that can help to matching Echo Replies. May be zero.

Data- any irrelevant information. May be zero.

ICMPv6 Informational messages:Echo Reply

- The message format is same as the Echo Request message. However, the values change as follows-

Type- 129
Code- 0
Identifier- Copied from Echo Request messages.
Sequence Number- Copied from Echo Request messages.
Data- data from invoking Echo Request message

These messages are sent in response to Echo Request messages.

Type :-129	Code 0	Checksum
Identifier		Sequence number
Optional data Sent by the request message; repeated by the reply message		

ICMPv6 messages

There are three ICMPv6 informational messages used for **Multicast Listener Discovery:**

- Multicast Listener Query
- Multicast Listener Report
- Multicast Listener Done

ICMPv6 message type	MLD message type
130	Multicast Listener Query
131	Multicast Listener Report
132	Multicast Listener Done

ICMPv6 messages

Neighbor Discovery uses the following ICMPv6 informational messages:

- Router Solicitation
- Router Advertisement
- Neighbor Solicitation
- Neighbor Advertisement
- Redirect

Neighbor Discovery (ND)

- Layer 2 protocol
- used for Stateless Address Autoconfiguration (SLAAC)
- used to find other hosts and their MAC addresses (replaces ARP)
- to find routers and DNS servers
- to find the prefix (network) used on the link
- used for Duplicate Address Detection (DAD)

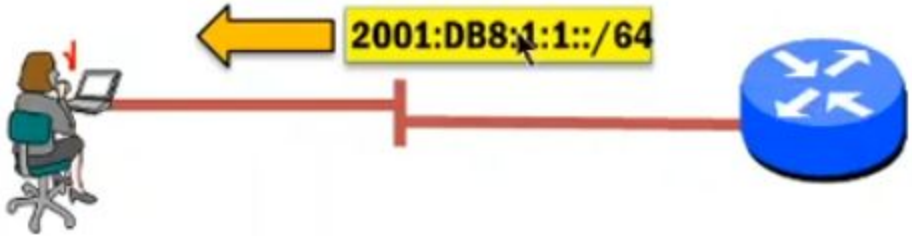
Stateless Address Auto-configuration (SLAAC)

Host learns prefix and prefix length from local router using Neighbor Discovery Protocol (NDP)

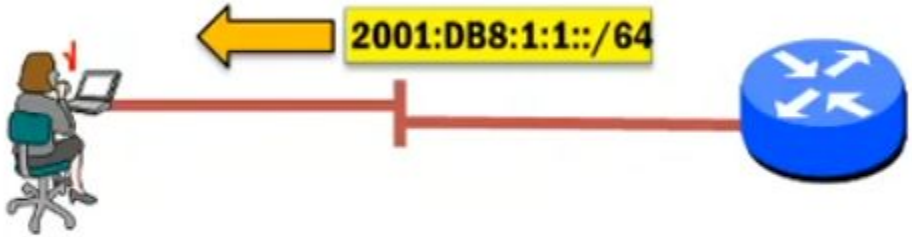
Stateless Address Auto-configuration (SLAAC)

Host learns prefix and prefix length from local router using Neighbor Discovery Protocol (NDP)

Router Advertisements (RA)



Router Advertisements (RA)
Router Solicitation (RS)



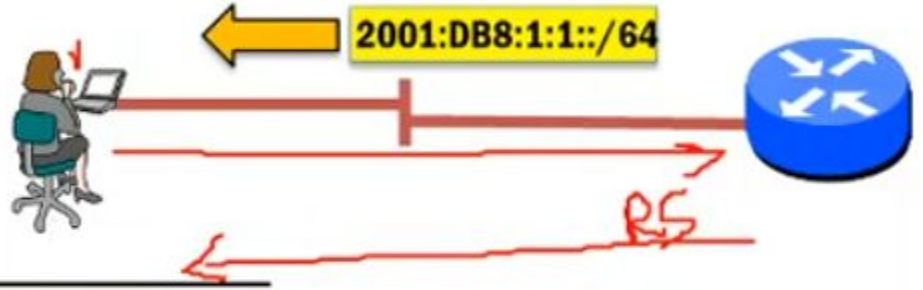
Prefix
(64 bits

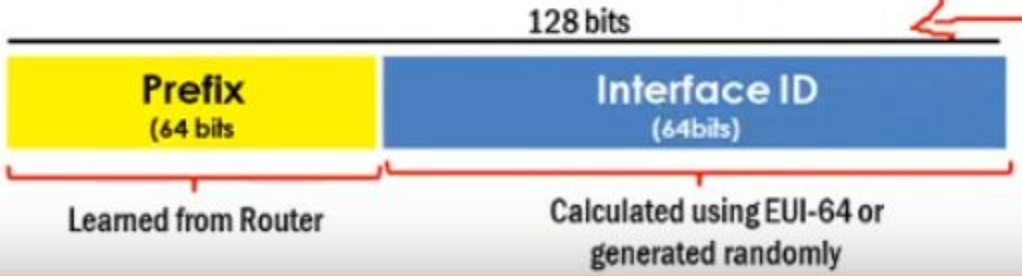
Learned from Router

A locally calculated or randomly generated interface ID is added with the the prefix part
To avoid duplication of its IPv6 with other nodes, uses Duplicate Address Detection (DAD)

Router Advertisements (RA)
Router Solicitation (RS)

(config)# interface FastEthernet0/0
(config-if)# ipv6 address autoconfig





Solicited-Node Multicast Address

- special multicast address defined in RFC4291
- for every IPv6 address, the specific multicast group must be joined
- also used for Neighbor Discovery (similar to ARP) and to make sure an address is unique
- prefix: ff02:0:0:0:0:1:ff00::/104 + last 24 bits of IPv6 address (ff02:0:0:0:0:1:ff00:0000 - ff02:0:0:0:0:1:ffff:ffff)

Router Solicitation ("RS", ICMPv6 Type 133)

host sends RS to "all routers" multicast group (ff02::2), to receive prefix (network) information and the address of routers

Router Advertisement ("RA", ICMPv6 Type 134)

router sends periodic RA to "all hosts" multicast group (ff02::1), to announce prefix (network) information and its own address

- also used as a reply to Router Solicitation (RS)
- preference can be set (low, medium, high), in case single router should be preferred by hosts on the link

Neighbor Solicitation ("NS", ICMPv6 Type 135)

to find Link Layer address (Layer 2 / MAC) of another host, a NS is sent to the solicited-node multicast address of the neighbor (like ARP in IPv4)

also, a NS is sent to unicast address of neighbor, to find out if it is still alive and reachable

Neighbor Advertisement ("NA", ICMPv6 Type 136)

is used to reply to Neighbor Solicitation (NS) message

Redirect (ICMPv6 Type 137)

sent by routers to tell hosts that there is a better next hop for a target

ICMPv6 Advantages

- If a wrong IP address is used for configuring a client to the DNS server, an ICMP message is sent by the destination device to indicate the error.
- If a client sends all communications to a particular router despite another router offering a best route, the particular router responds with the IP address of the router that provides a better route in the form of an ICMP message.
- All IP headers contain a Time to Live (TTL) value. This value is decremented as the IP packet is forwarded through each router. If a packet arrives at a router with a Time To Live (TTL) value of 1, the router cannot decrement the value any further and forward it. Instead, the router discards the packet and sends an ICMP message to indicate the expiry of the packet's TTL value.
- The Internet Control Message Protocol Version 6 (ICMPv6) also provides testing and diagnostics services for many utilities. In order to test the communication process,

ICMPv4 vs ICMPv6

Parameters	ICMPv4 Message	ICMPv6 Equivalent
Destination Unreachable	Network Unreachable (Type 3, Code 0)	Destination Unreachable-No Route to Destination (Type 1, Code 0)
	Host Unreachable (Type 3, Code 1)	Destination Unreachable-Address Unreachable (Type 1, Code 3)
	Protocol Unreachable (Type 3, Code 2)	Parameter Problem-Unrecognized Next Header Type Encountered (Type 4, Code 1)
	Port Unreachable (Type 3, Code 3)	Destination Unreachable-Port Unreachable (Type 1, Code 4)
	Communication with Destination Host Administratively Prohibited (Type 3, Code 10)	Destination Unreachable-Communication with Destination Administratively Prohibited (Type 1, Code 1)
Fragmentation	Fragmentation Needed and DF Set (Type 3, Code 4) (as specified in RFC 1191)[Source and Router]	Packet Too Big (Type 2, Code 0)[@only source]

ICMPv4 vs ICMPv6

Parameters	ICMPv4 Message	ICMPv6 Equivalent
Redirect	Redirect (Type 5, Code 0)	Neighbor Discovery Redirect message (Type 137, Code 0)
Time Exceeded	Time Exceeded-TTL Exceeded in Transit (Type 11, Code 0)	Time Exceeded-Hop Limit Exceeded in Transit (Type 3, Code 0)
	Time Exceeded-Fragment Reassembly Time Exceeded (Type 11, Code 1)	Time Exceeded-Fragment Reassembly Time Exceeded (Type 3, Code 1)
Parameter Problem	Parameter Problem (Type 12, Code 0)	Parameter Problem (Type 4, Code 0 or Code 2)
Header Size	IPv4 has header of 20-60 bytes.	IPv6 has header of 40 bytes fixed
Source Quench	Source Quench (Type 4, Code 0)	This message is not present in IPv6.
Message Types	Error and Query Message présents	Error and Informational Message présents

References

1. IPv6 Essentials : Silvia Hagen, 2nd Edition
2. Cisco IPv6 Fundamental - 2nd Edition, Rick Graziani
3. Internet Protocol, Version 6 (IPv6) Specification - RFC 8200
4. IPv6 Stateless Address Autoconfiguration - RFC 4862
5. Neighbor Discovery for IP version 6 (IPv6) - RFC 4861