Lecture 4.2

Network Layer: Error Reporting Protocol ICMP

Dr. Vandana Kushwaha

Department of Computer Science

Institute of Science, BHU, Varanasi

Error Reporting

- **IP** provides **unreliable** **and** **connectionless** **datagram delivery**.
- The **IP protocol** is a **best-effort delivery service** that delivers a **datagram** from its **original source** to its **final destination.**
- However, **IP protocol** **has** **two deficiencies**: **lack of** **error control** and **lack of** **assistance mechanisms**.
- The **IP protocol** has **no error-reporting** **or** **error-correcting mechanism**.
- **What** happens if something goes **wrong**?
- **What** happens if a **router** must **discard** a **datagram** because it cannot find a **router** to the **final destination**, or because the **time-to-live** field has a **zero value**?
- **What** happens if the **final destination** host must **discard** **all fragments** of a **datagram** because it has **not received** all **fragments** within a **predetermined time limit?**

Error Reporting

- These are situations where an **error has occurred** and the **IP protocol** has **no built-in mechanism to notify the original host.**
- The **IP protocol** also **lacks a mechanism** for **host and management queries**.
- A **host** sometimes **needs to determine** if a **router** or another **host** is **alive**.
- And sometimes a **network administrator needs information** from another host or router.
- The **Internet Control Message Protocol (ICMP)** has been designed to **compensate** for the above **deficiencies.**
- It is a **companion to the IP protocol**.

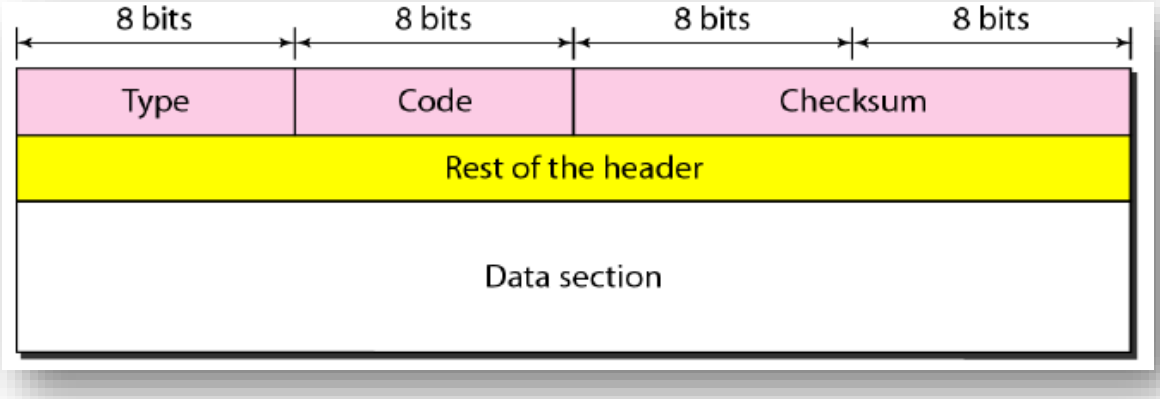
Types of Messages in ICMP

- **ICMP messages** are divided into **two broad categories**:
    1. ***Error-reporting messages***
    2. ***Query messages***
- The **Error-reporting messages report problems** that a **router or a host (destination)** may **encounter** when it processes an **IP packet**.
- The **Query messages**, which **occur in pairs**, help a **host** or a **network manager** get specific information from a **router** or **another host.**

ICMP Message Format

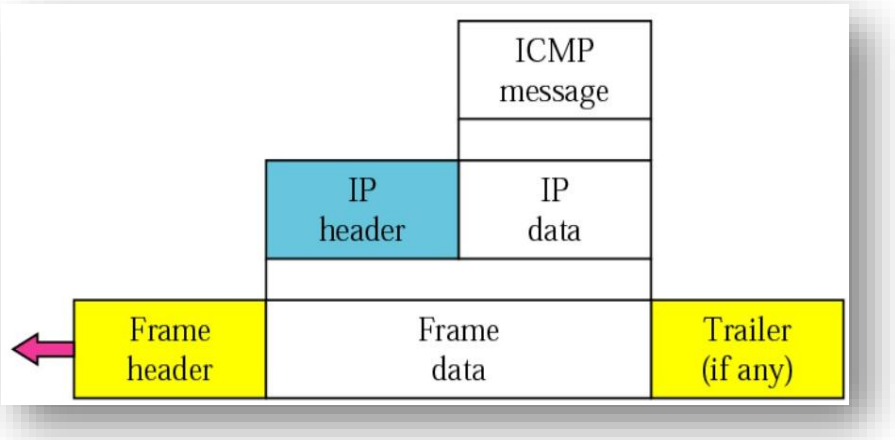
- An **ICMP message** has an **8-byte header** and a **variable-size data section**.
- The first field, **ICMP type**, defines the **type** of the **message.**
- The **code field** specifies the **reason** for the particular message type.
- The last common field is the **checksum field** used for **securing ICMP header**.
- The **rest** of the **header** is **specific** for each **message type**.
- The **data section** in **error messages** carries information for finding the **original packet** that had the **error.**
- In **ICMP query messages**, the **data section** carries **extra information** based on the **type of the query.**

ICMP Message Format



ICMP Encapsulation

- **ICMP** itself is a **network layer protocol**.
- However it's messages are **not passed directly to data link layer**.
- Instead the **messages** are **first encapsulated inside IP datagrams** before going to the **lower layer.**

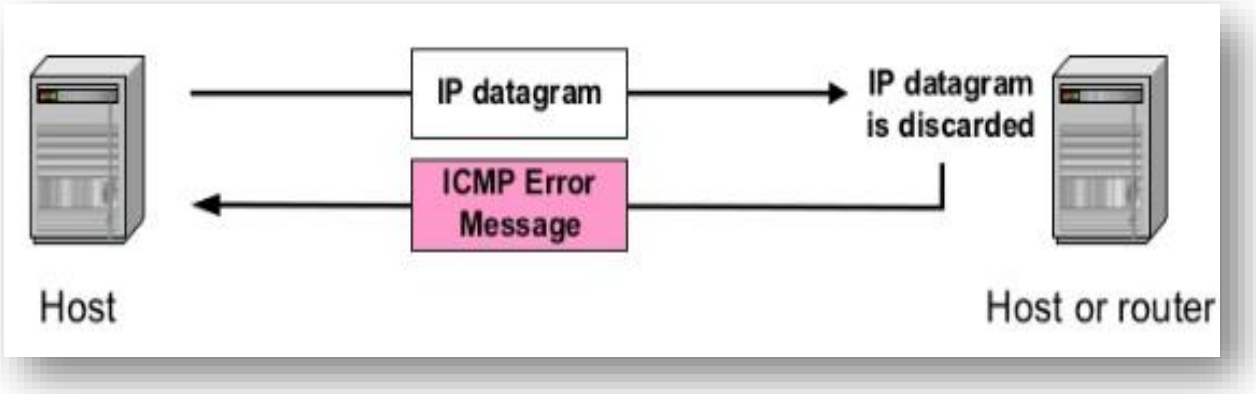


Error Reporting Messages

- One of the **main responsibilities** of **ICMP** is to **report errors**. Although technology has produced increasingly reliable transmission media, **errors still exist** and must be **handled.**
- **IP** is an **unreliable protocol**. This means that **error checking** and error control are not a concern of **IP**.
- **ICMP** was designed, in part, to **compensate** for this **shortcoming.**
- However, ***ICMP does not correct errors-it simply reports them***.
- **Error correction** is **left** to the **higher-level protocols**.

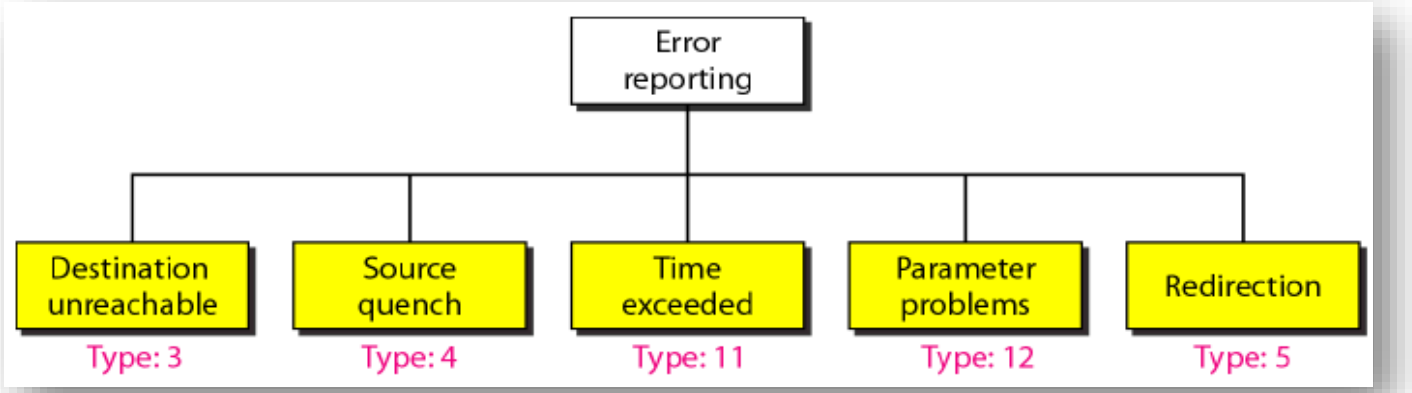
Error Reporting Messages

- **Example**



Error Reporting Messages

- **Error messages** are **typically sent** when a **datagram is discarded due to some error**.
- **Error messages** are **always sent to the original source** because the only information available in the datagram about the route is the source and destination IP addresses.
- **Five types of errors** are handled: *destination unreachable, source quench, time exceeded, parameter problems, and redirection*.



Destination Unreachable

- When a **router** **cannot route** a **datagram** or a **host** **cannot deliver a datagram**, the **datagram** is **discarded.**
- Some of the **reasons** for a **datagram** not to be delivered are: **Net/Host Unreachable,** **Fragmentation Needed** and **DF flag was set**, Communication with **destination network** is **administratively prohibited** etc.
- And the **router** or the **host** sends a **destination-unreachable** message **back** to the **source host** that initiated the datagram.
- Note that **destination-unreachable** messages can be **created** by either a **router** or the **destination host.**
- The **Type field** is set to **one**, which is the value for the **Destination Unreachable** message.
- The **Code field** supplies **more information** about the **reason** why the datagram was not delivered.

Source Quench

- The **IP protocol** is a **connectionless protocol**. IP does not have a **flow control** mechanism **embedded** in the protocol.
- The **lack of flow control** can create a **major problem** in the **operation of IP.**
- The **source host never knows** if the **routers** or the **destination host** has been **overwhelmed** with **datagrams.**
- The **source host never knows** if it is **producing datagrams faster** than can be forwarded by **routers** or **processed** by the **destination host.**
- The **lack of flow control** can create **congestion** in **routers** or the **destination host.**
- In this case, the **router** or the **host** has **no choice** but to **discard** some of the **datagrams**.
- The **Source-quench** message in **ICMP** was designed to add a kind of **flow control** to the **IP.**

Source Quench

- When a **router** or **host** **discards a datagram** due to **congestion,** **it sends a** **source-quench message** to the **sender** of the **datagram**.
- This message has **two purposes**:
  - **First**, it informs the **source** that the **datagram** has been **discarded.**
  - **Second**, it warns the **source** that there is **congestion** somewhere in the path and that the **source** should **slow down** (quench) the **sending process**.

Time Exceeded

- The **time-exceeded message** is generated in **two cases**:
- **Case1**:
- As **routers** use **routing tables** to find the **next hop** (next router) that must receive the packet.
- If there are **errors** in one or more **routing tables**, a **packet** can travel in a **loop** or a **cycle**, going from one **router** to the **next** or visiting a series of routers **endlessly**.
- Each **datagram** contains a field called ***time to live*** that controls this situation.
- When a **datagram** visits a **router**, the value of this **field** is **decremented** by **1.** When the time-to-live value **reaches 0,** after **decrementing,** the router **discards** the datagram.
- However, when the **datagram** is **discarded,** a **time-exceeded** message must be **sent** by the **router** to the **original source**.

Time Exceeded

- **Case2**:
- A **time-exceeded message** is also generated when not **all fragments** that make up a message arrive at the **destination host within** a **certain time limit.**

Parameter Problem

- Any **ambiguity** **in the** **header part** of a **datagram** can create **serious problems** as the **datagram** travels through the **Internet.**
- If a **router** or the **destination host** discovers an **ambiguous** **or** **missing value** in any **field** of the datagram, it **discards** **the datagram** and sends a **parameter-problem** **message** back to the **source**.
- **ICMP Parameter Problem** message also has an option for a **special pointer** to inform the sender **where** in the original **IPv4 header** the **error** had **occurred.**

Redirection

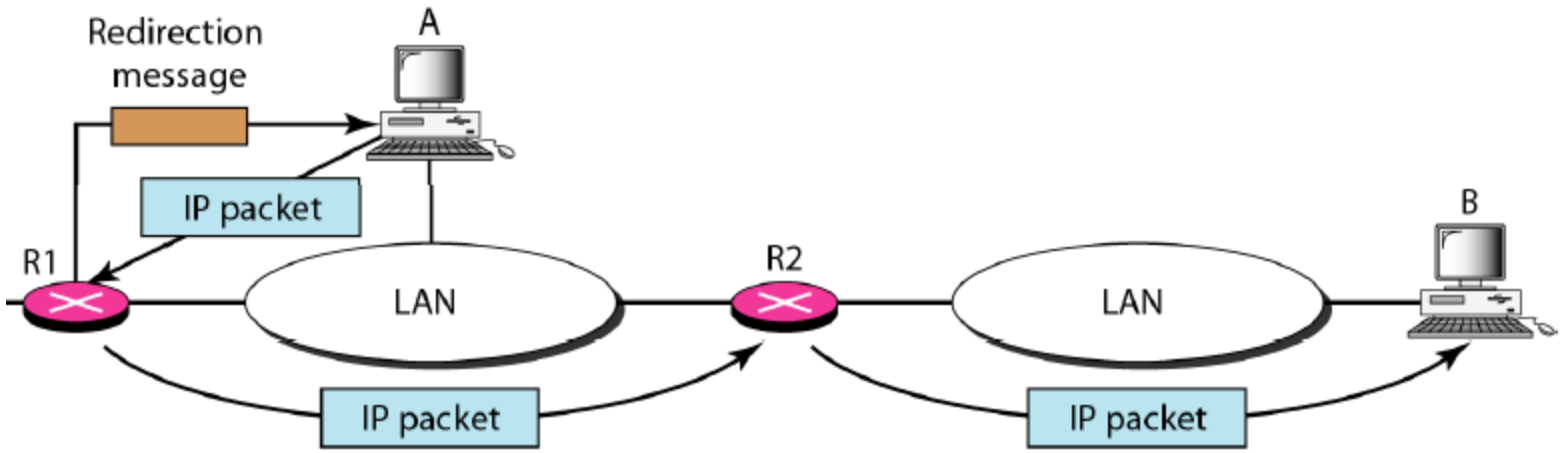
- When a **router** needs to **send a packet** destined for **another network**, it must know the **IP address** of the **next appropriate router**.
- The same is **true** if the **sender** **is a host**.
- Both **routers** **and** **hosts**, then, must have a **routing table** to find the **address** of the **router** or the **next router.**
- **Routers** take part in the **routing update** process, and are **supposed** to be **updated constantly.**
- **Routing** is **dynamic**. However, for efficiency, **hosts do not take part** in the **routing update process** because there are many more hosts in an internet than routers.
- **Updating** the **routing tables** of **hosts** dynamically produces **unacceptable traffic**.
- **The** **hosts** usually use **Static routing**.
- When a **host comes up**, its **routing table** has a **limited number** of **entries.**

Redirection

- It usually knows the **IP address** of **only one router**, the **default router**.
- For this reason, the **host may send** a **datagram,** which is destined for another network, to the **wrong router**.
- In this case, the **router** that **receives** the **datagram** will **forward the datagram to the correct router.**
- However, to **update the routing table of the host**, it sends a **redirection message** to the **host.**
- This concept of **redirection is** shown in Figure on next slide.

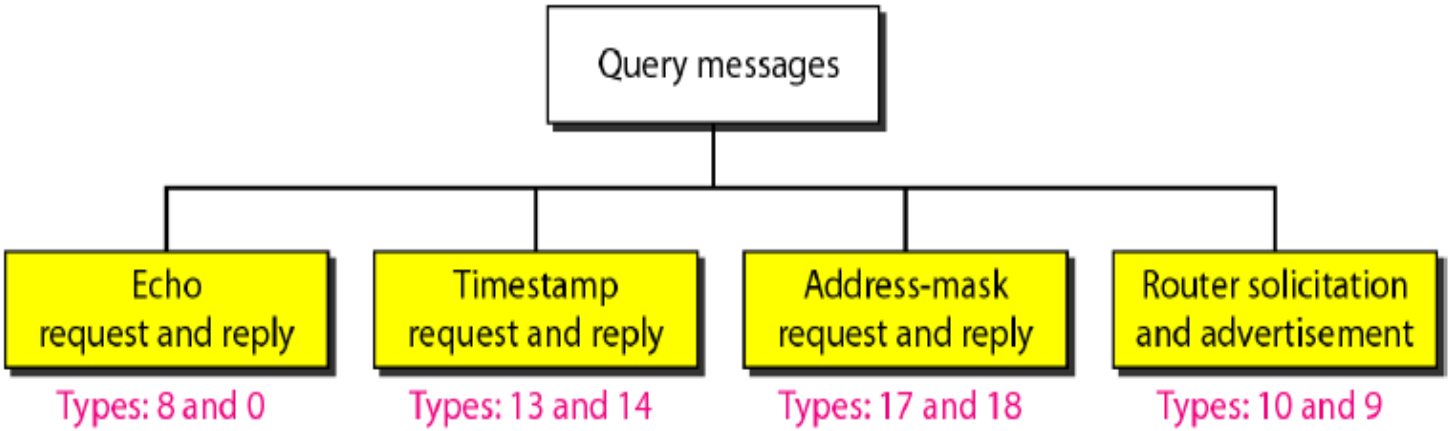
Redirection

- **Host A** wants to send a datagram to **host B.**
- **Router R2** is obviously the **most efficient routing choice**, but **host A** did not choose **router R2**. The **datagram** goes to **R1** instead.
- **Router R1**, after consulting its **table,** finds that the **packet** should have gone to **R2.**
- It **sends** the **packet** to **R2** and, at the **same time**, **sends** a **redirection message** to **host A.**
- **Host A's routing table** can now be **updated.**



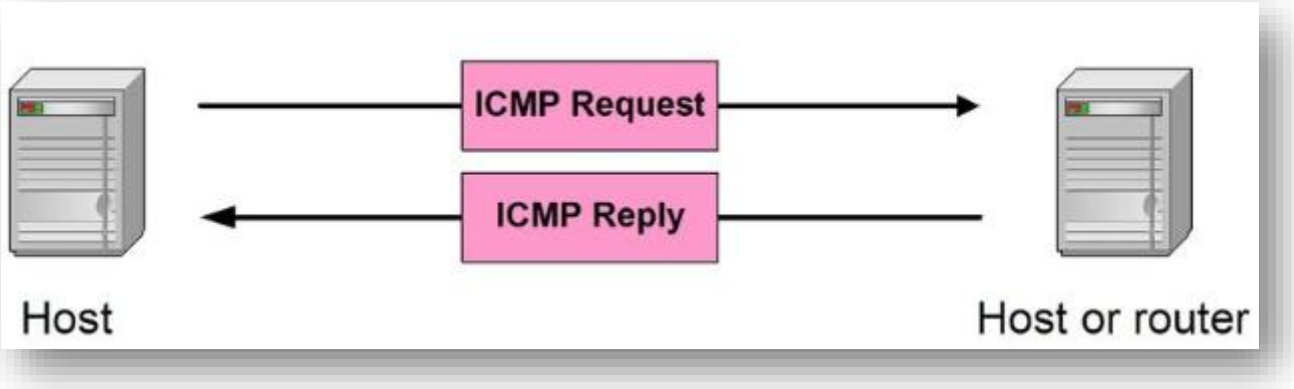
ICMP Query Messages

- In addition to error reporting, **ICMP** can **diagnose** **some network problems**.
- This is accomplished through the **query messages**, a group of **four** **different pairs** of **messages**.

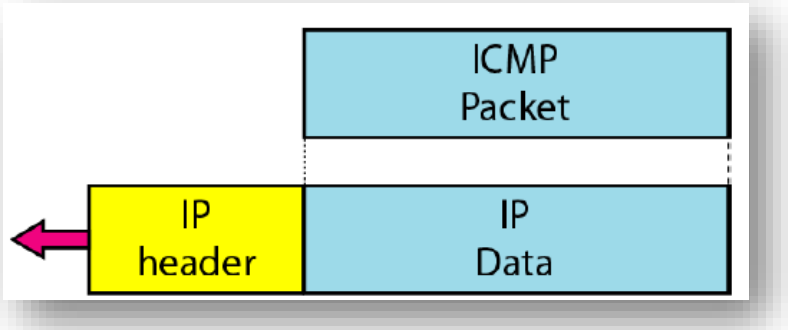


- In this type of **ICMP message**, a **node** sends a **ICMP request** message that is **answered** in a specific format as **ICMP reply** by the **destination node.**

ICMP Query Messages



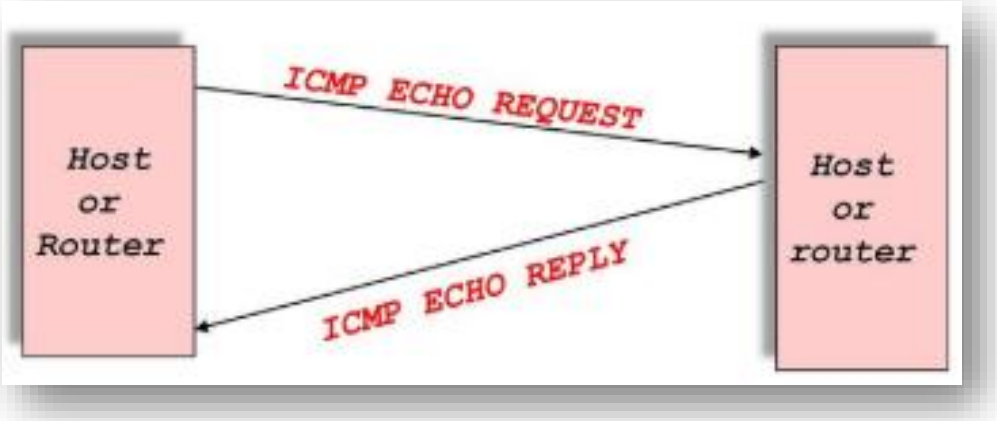
- A **query message** is **encapsulated** **in an** **IP packet**, which in turn is **encapsulated** **in a data link layer** **frame.**
- However, in this case, no bytes of the **original IP** are **included** in the **message**, as shown in **Figure** below:



Echo Request and Echo Reply

- The **echo-request** and **echo-reply** messages are designed for **diagnostic purposes**.
- The **combination** of **echo-request** and **echo-reply** messages determines whether **two systems (hosts or routers)** can **communicate** with **each other.**
- It also confirms that the **intermediate routers** are **receiving, processing**, and **forwarding IP datagrams**.
- Today, most systems provide a version of the ***ping* command** that can create a **series** (instead of just one) of **echo-request** and **echo-reply** messages, providing **statistical information.**
- We can use the ***ping*** program to find if a **host is alive** and responding.

Echo Request and Echo Reply



Timestamp Request and Timestamp Reply

- **Two machines** (hosts or routers) can use the **timestamp request** and **timestamp reply** messages to determine the **round-trip time(RTT)** needed for an **IP datagram** to **travel** between them.
- It can also be used to **synchronize** the **clocks** in **two machines.**

Address-Mask Request and Address-Mask Reply

- A **host** may know its **IP address**, but it **may not know** the corresponding **mask.**
- For **example,** a **host** may know its **IP address** as **159.31.17.24**, but it **may not know** that the **corresponding mask** is **/24.**
- To **obtain its mask**, a **host** sends an **address-mask-request message** to a **router** on the **LAN.**
- If the **host** knows the **address** of the **router,** it **sends** the **request directly** to the **router.**
- If it **does not know**, it **broadcasts** the message.
- The **router** receiving the **address-mask-request message** responds with an **address-mask-reply message**, providing the necessary **mask** for the host.
- This can be applied to its **IP address** to get its **subnet address**.

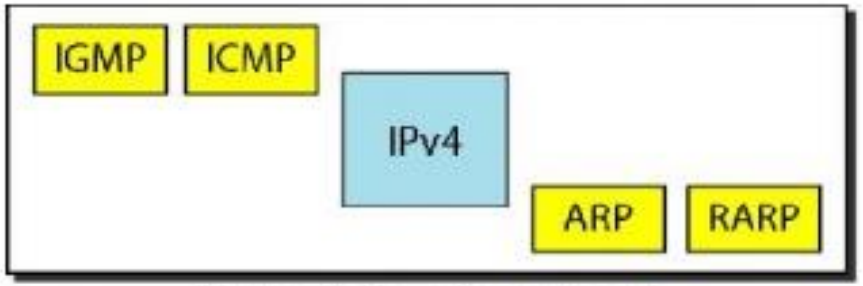
Router Solicitation and Router Advertisement

- The **router-solicitation** and **router-advertisement** messages can **help** a **host** to **check** whether the **neighboring routers** are **alive** and **functioning**.
- A **host** can **broadcast** (or multicast) a **router-solicitation message.**
- The **router** or **routers** that **receive** the **solicitation message broadcast their routing information** using the **router-advertisement message.**
- A **router** can also **periodically** send **router-advertisement messages** even if **no host has solicited.**
- Note that when a **router** sends out an **advertisement**, it **announces** not only its **own presence** but also the **presence of all routers** on the **network** of which it is aware.

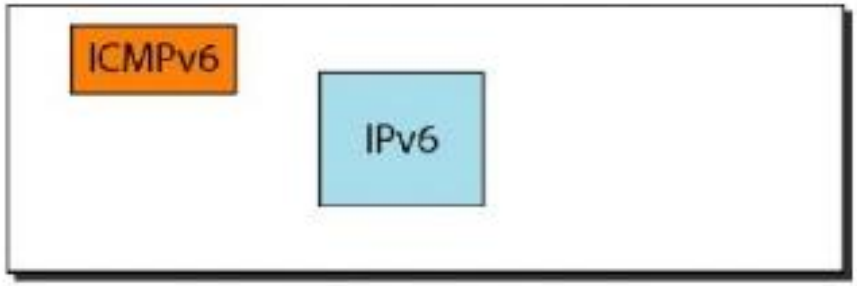
ICMPv6

- **ICMPv4** protocol that has been **modified** in **version 6** of the **TCP/IP protocol suite** is **ICMPv6.**
- This **new version** follows the **same strategy** and **purposes** of **version 4.**
- **ICMPv4** has been **modified** to make it more **suitable** for **IPv6.**
- In addition, some **protocols** that were **independent** in **version 4** are now **part** of **Internetworking Control Message Protocol** (**ICMPv6**).
- The **ARP** and **IGMP protocols** in **version 4** are **combined** in **ICMPv6.**
- The **RARP protocol** is **dropped** from the **suite** because it was **rarely used** and **BOOTP/DHCP** has the same functionality.
- Just as in **ICMPv4,** we divide the **ICMPv6 messages** into **two categories**.
- However, each category has **more types** of messages than before.

Comparison of network layers in version 4 and version 6



Network layer in version 4



Network layer in version 6