网络协议分析与实现

鲍青
杭州电子科技大学网络空间安全学院
E-mail： qbao@hdu.edu.cn

目录

- ICMP 原理
- ICMP 报文格式
- ICMP 软件整体结构
- PING 程序实现

Overview

a router cannot find a route to the final destination
Time-to-live field has a 0 value
destination discards all fragments of a datagram

- IP lack of
  - error control
    - IP has no error-reporting or error-correcting mechanism
  - assistance mechanism
    - A mechanism for host and management requires
- ICMP （ Internet Control Message Protocol ）
  - A companion to the IP, to compensate for the above two deficiencies
    - Provide error reporting（而不是 error-correcting!) for IP
    - Provide assistance mechanism for other layers （TCP/UDP and application）
      - 主机可以通过使用 ICMP 与 Internet 中路由器或者主机实现控制报文的通信

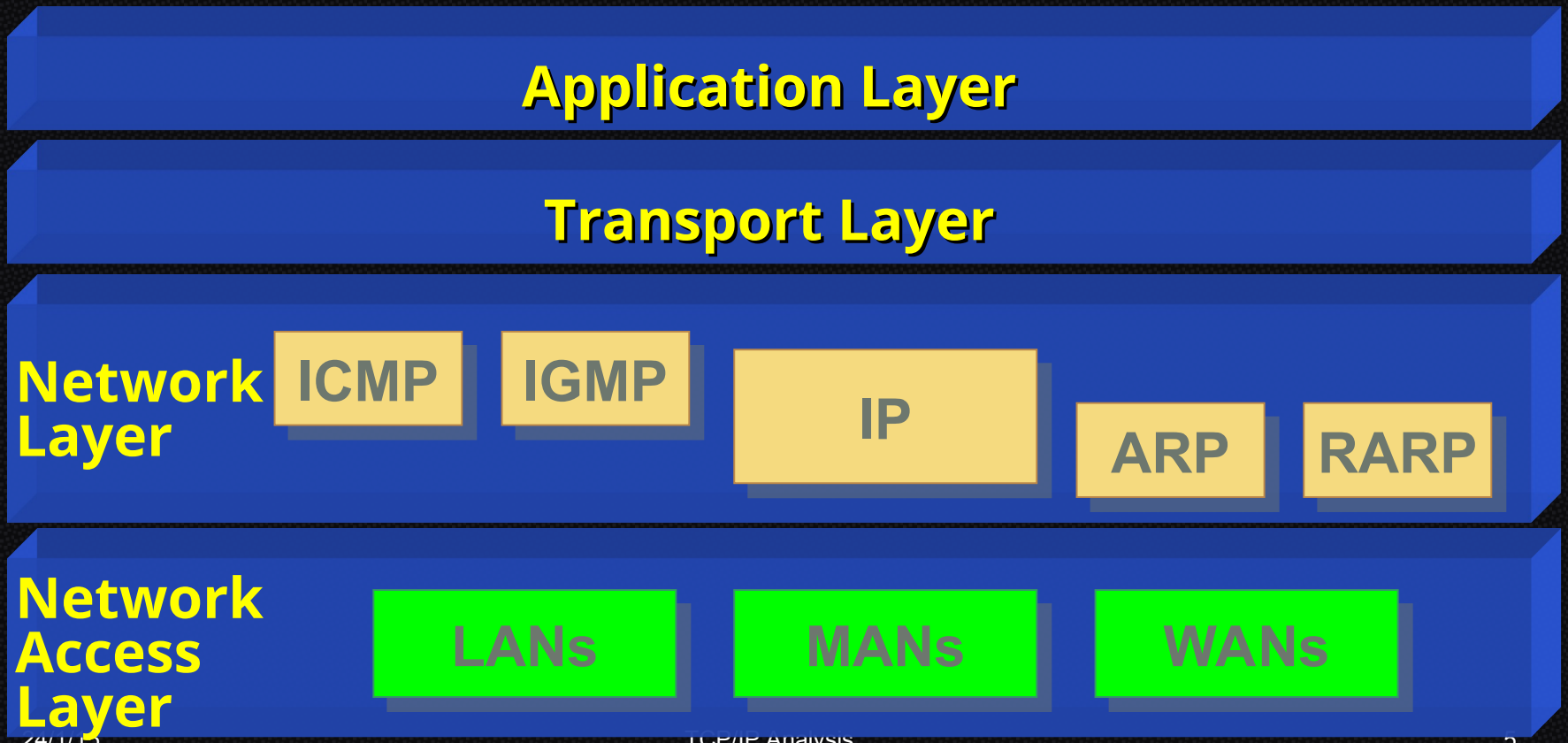
Error Reporting VS Error Correction

- IP 传输过程中出现差错是不可避免的
  - IP 分组传输出现差错时，会产生相应的 ICMP 报文
  - 通过 ICMP 报文提供**差错报告**
- ICMP 差错报告只能送给 IP 分组的**源站**，协议只提供**差错处理建议**
  - 原因：
    - IP 数据报中只记录了 IP 源和目的地址，而没有记录完整路由
    - 检查到错误的路由器无法了解分组经过了哪些中间路由器
    - 差错纠正由上层协议负责

源站可能无法确定差错源，
需要与网络管理员一起协作处理

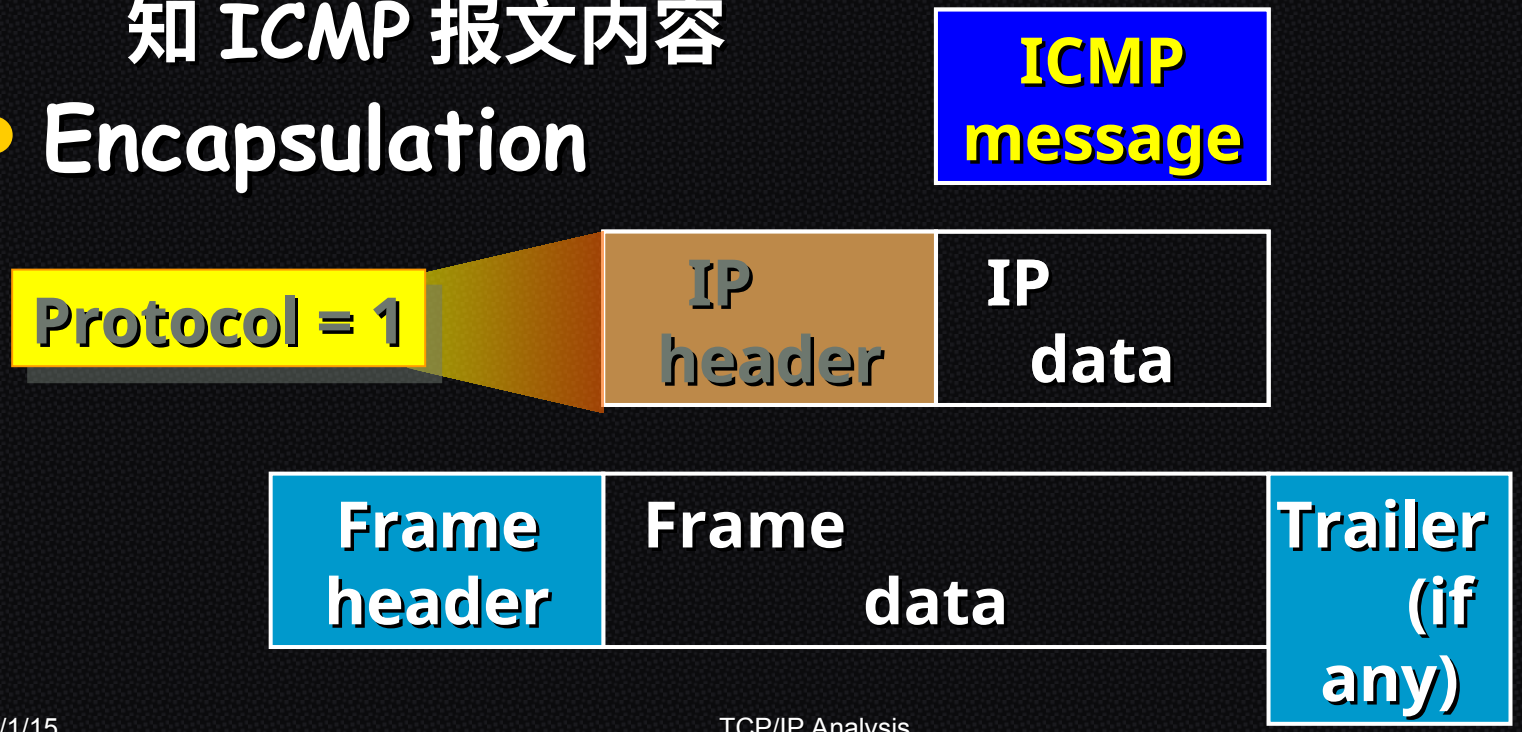
Internet Control Message Protocol

- RFC792 : Internet Control Message Protocol , 1981
- RFC1256 : ICMP Router Discovery Messages , 1991



Message delivery and Encapsulation

- ICMP 在 IP 之上实现，逻辑上与 IP 同在网络层
  - Connectionless communication
  - 直接送达目的站点，沿途的转发路由器不能获知 ICMP 报文内容
- Encapsulation



Chapter 8 ICMP

- Overview
- Types of messages
- Message format
- Error reporting
- Query
- Checksum
- ICMP package

Types of Messages

ICMP messages

Error-reporting 差错报告

To report problems that a router or a destination host may encounter when it processes an IP packet

Query 测试查询

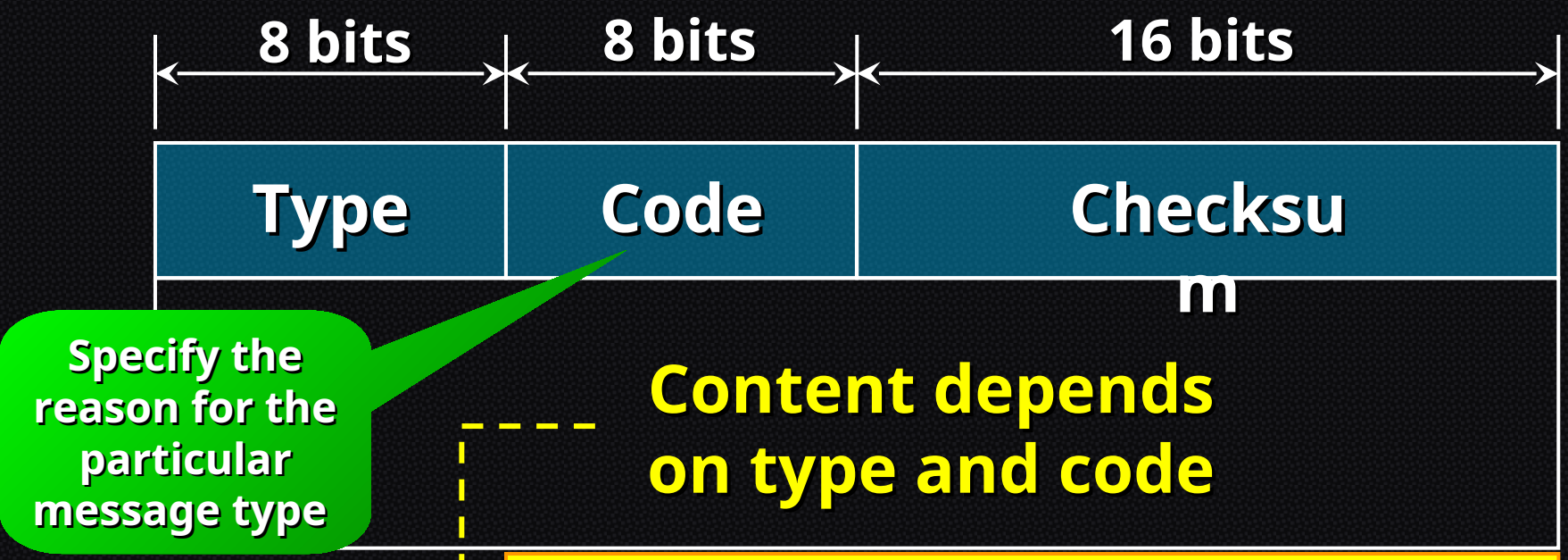
To help a host or a network manager get specific information from a router or another host

过时:
15 Information request
16 Information response

Types

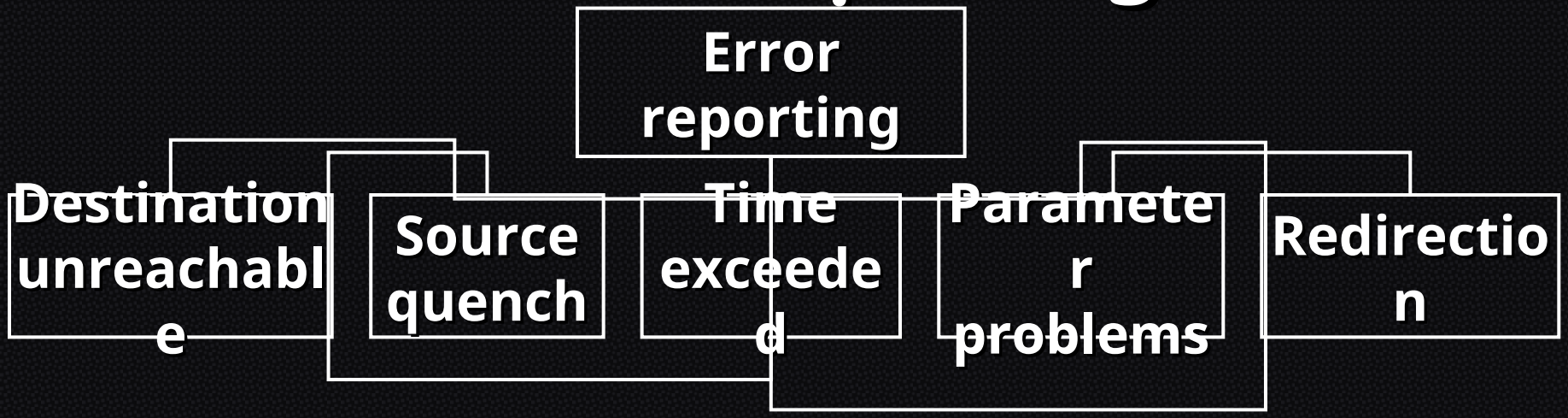
Category	Type	Message	Reason
Error-reporting messages	3	Destination unreachable	Unreachable
	4	Source quench	Congestion
	11	Time exceeded	Too long route
	12	Parameter problem	Format error
	5	Redirection	Route changed
Query messages	8 or 0	Echo request or reply	Reachability
	13 or 14	Timestamp request or reply	Synchronization
	17 or 18	Address mask request or reply	Mask maintenance
	10 or 9	Router solicitation or advertisement	Coincidence between routers

Message Format



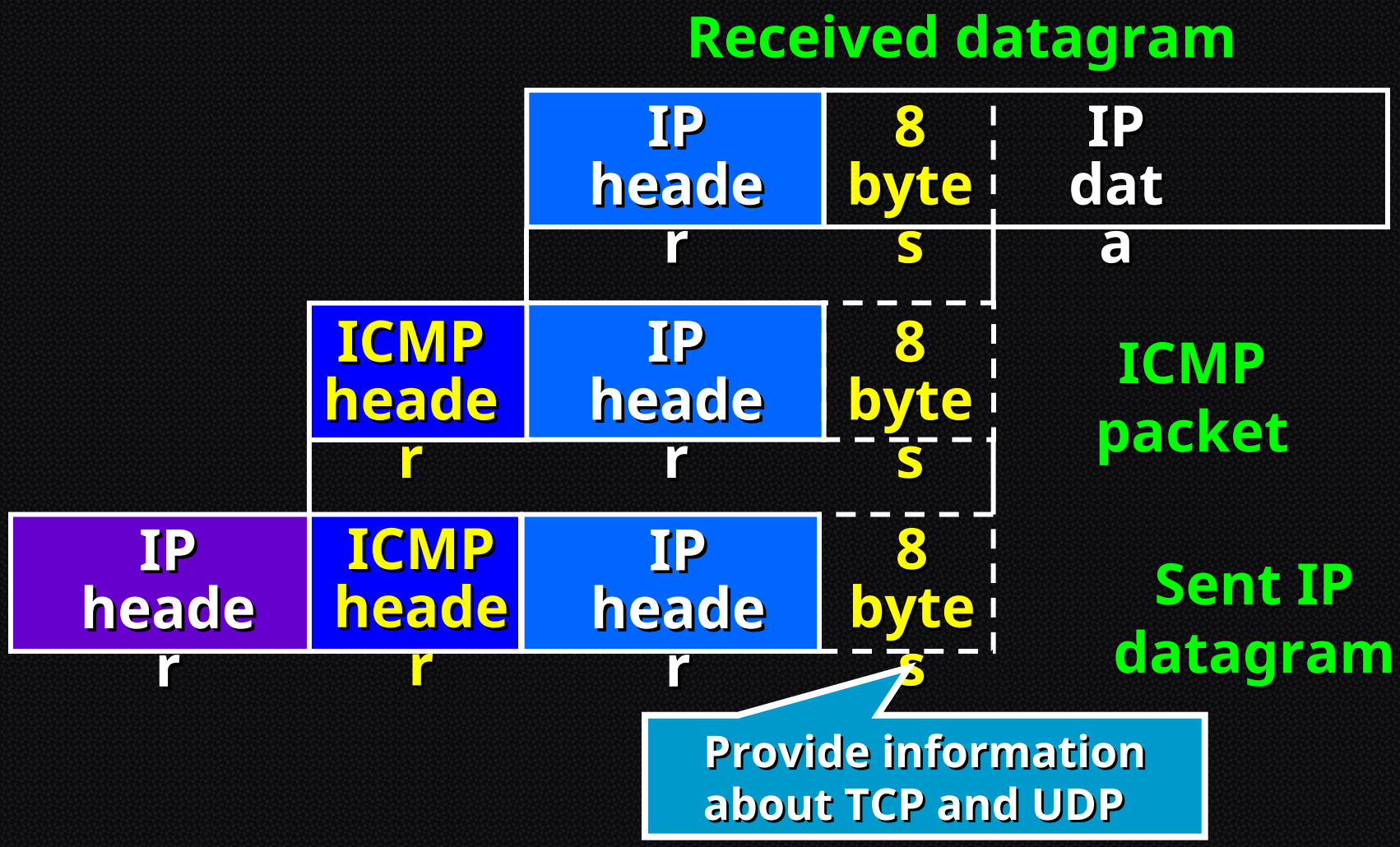
- 差错报文：引起差错的原始数据报的一部分（首部 + 数据部分的前 8 个字节）
- 查询报文：基于查询类型的额外信息

Error Reporting



- ICMP just simply report errors → not correct
- ICMP always reports error messages to the original source
- ICMP error message will NOT be generated for:
  - A datagram carrying an ICMP error message
  - A fragmented datagram that is NOT the first fragment
  - A datagram having a multicast address
  - A datagram having a special address such as 127.0.0.0 or 0.0.0.0

Contents of Data Field for Error Messages



Destination Unreachable

- When a *router* cannot route a datagram or a *host* cannot deliver a datagram
  - The datagram is discarded
  - The router or the host sends a destination unreachable message back to the source

不可达的原因

Type = 3	Code = 0~12	Checksum
0x00000000		
IP header + 8 bytes IP data		

A router cannot detect all problems that prevent the delivery of a packet

供源站分析错误

Destination Unreachable Codes

Code	Description	Code	Description
0	网络不可达	7	目的主机未知
1	主机不可达	8	源主机被隔离
2	协议不可达	9	与目的网络的通信被禁止
3	端口不可达	10	与目的主机的通信被禁止
4	需要分片，但 DF=1	11	对指定 TOS，网络不可达
5	源路由失败	12	对指定 TOS，主机不可达

哪些目的不可达报文只能由目的主机产生？

哪些目的不可达报文只能由路由器产生？

Source Quench （源点抑止）

- The lack of flow control in IP → congestion
  - 拥塞：路由器中队列溢出
  - 源站点，中继节点（Router），目的站点间没有关于流量信息的通信
    - 主机产生的数据量可能比网络快
    - 不适当的路由使流量过分集中，超过信道容量
    - 路由器的转发性能低
- 路由器或主机因拥塞丢弃 IP 分组时，向源站发送 ICMP 源抑制报文，通知源站
  - The datagram has been discarded
  - There is a congestion somewhere in the path and the source should slow down the sending process ——quench

Source Quench （源点抑止）

- Congested router or destination sends one source-quench ICMP for each discarded datagram to the source
- There is no mechanism to tell the source that the congestion has been relieve

Type = 4	Code = 0	Checksum
0x00000000		
IP header + 8 bytes IP data		

The Solution of the Congestion

- 发送队列缓冲：缓解短暂的突发数据
- 丢弃报文，产生源抑制 ICMP 报文给源站
  - 丢弃算法 — QoS
  - 源站减缓发送速率
  - 源站没有收到源抑制报文后逐步提高发送速率
- 源抑制报文的拥塞控制能力
  - 只能解决因某个特定主机问题造成的拥塞
  - 对因路由或路由器问题造成的拥塞不起作用

Time Exceeded

- 若数据报的 TTL ＝ 0 ，路由器丢弃分组，并向源站发送 ICMP 超时报文
  - 路由器对每一个被处理数据报的 TTL 值自动减 1
- 目的主机为需要重组的数据报启动定时器，如果重组无法在定时内完成，丢弃分组，并向源站发送 ICMP 超时报文

Code = 0 —— 路由器检测到分组的 TTL 值为 0

Code = 1 —— 目的站在规定时间内没有收到所有分片

Type = 11	Code = 0,1	Checksum
0x00000000		
IP header + 8 bytes IP data		

Parameter Problem

- 路由器或主机因首部字段格式或取值错误而丢弃报文时，向源站发送 ICMP 参数问

Code = 0 —— 首部字段错误，指针字段指向错误字节
Code = 1 —— 缺少所需的选项部分，指针字段无效

Type = 12	Code = 0,1	Checksum
Pointer	0x00000000	
IP header + 8 bytes IP data		

Redirection

- 重定向（改变路由）：主机配置最少的路由信息，可以从路由器了解新的路由

Net 1	直接交付
Net 2	R2
0.0.0.0/0	R1

A want to send datagrams to B, but it doesn't know R2 is the better choice. What will it do?

IP packet

Redirection message

Format

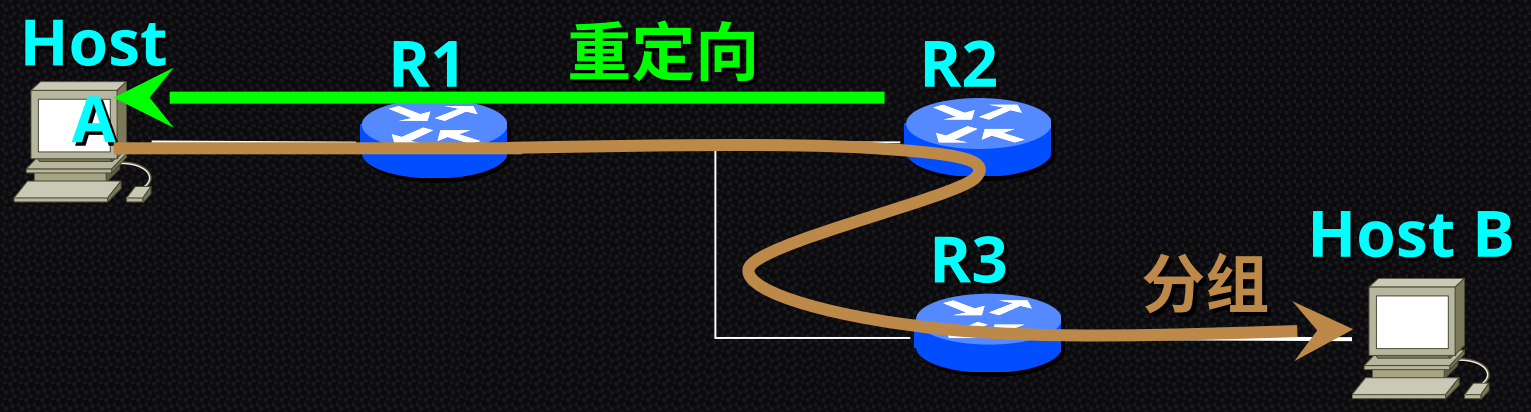
Type = 5	Code = 0~3	Checksum
IP address of the target router		
IP header + 8 bytes IP data		

Code	Description
0	Network specific
1	Host specific
2	Network specific (specified service)
3	Host specific (specified service)

缩小路由改变的范围

思考

- 在以下情况中，重定向报文是否有用?

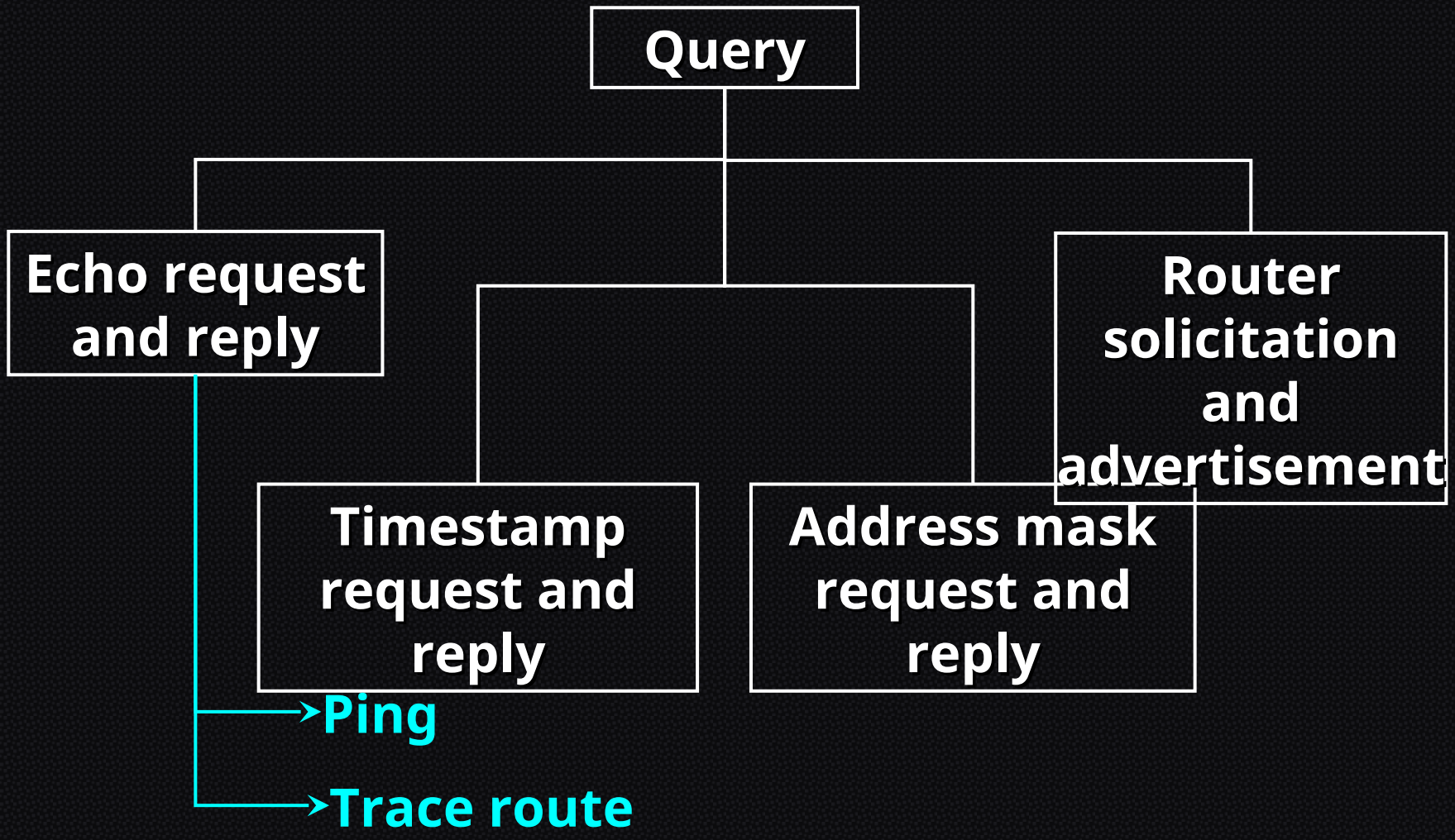


R2 发出的重定向报文应该送给谁？

Query

- 功能：
  - 帮助主机从某个路由器或主机处得到特定的信息
- 这种类型的 ICMP 报文的通信特点：**成对出现**
  - 一个节点产生请求 ICMP
  - 目的节点用特定的 ICMP 报文应答

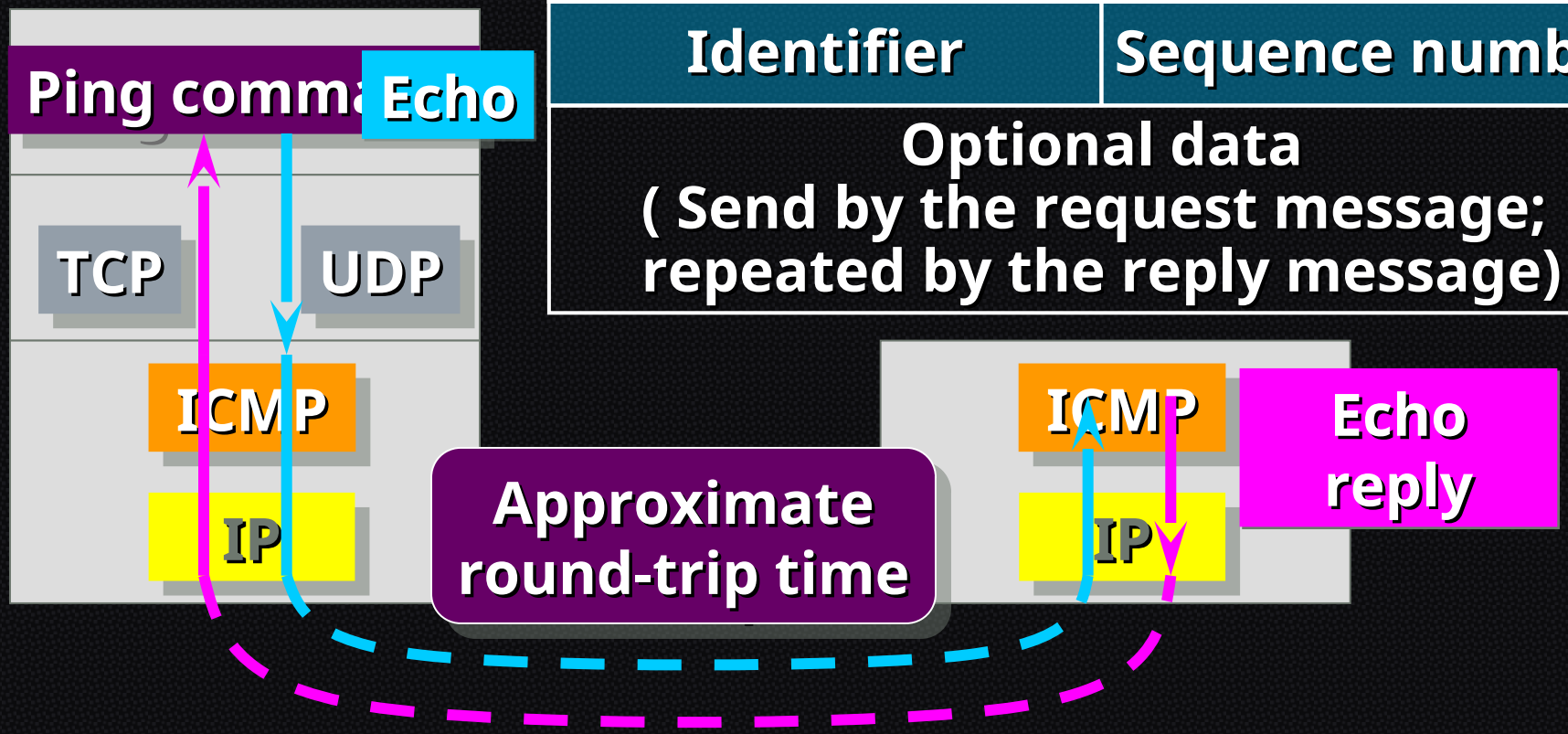
Query


Query
Echo request and reply
Timestamp request and reply
Address mask request and reply
Router solicitation and advertisement
Ping
Trace route

Echo Request and Reply

- For diagnostic purposes： whether two systems can communicate with each other —— 确定 IP 层能否通信

Type = 8,0	Code = 0	Checksum
Identifier		Sequence number
Optional data (Send by the request message; repeated by the reply message)		

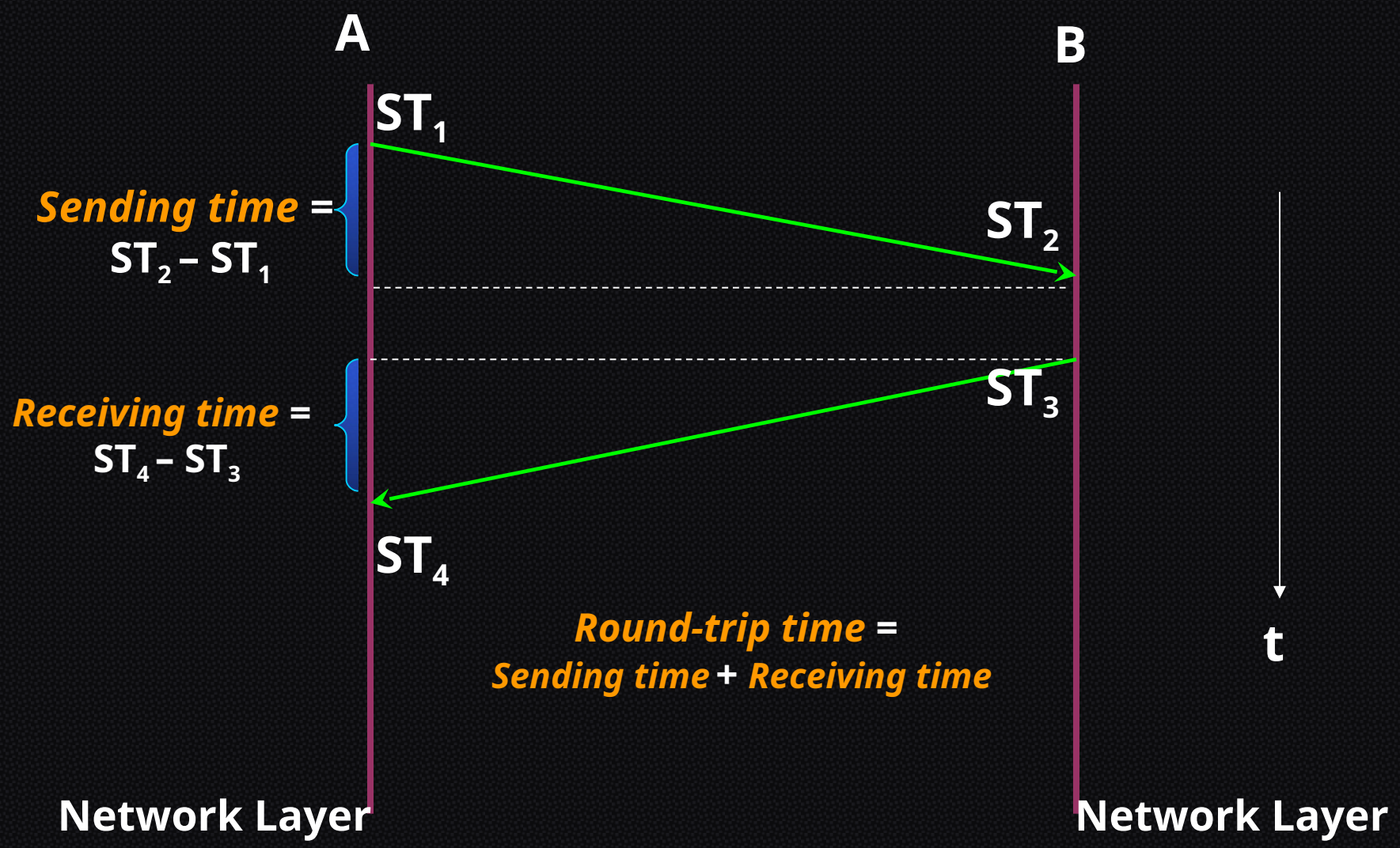


Timestamp Request and Reply

Type = 13, 14	Code = 0	Checksum
Identifier		Sequence number
Original timestamp (filled by source)		
Receive timestamp (filled by destination)		
Transmit timestamp (filled by destination)		

- Used to calculate the round-trip time （ms）
  - 发时间 = 收时戳 - 初始时戳，收时间 = 返回时间 - 发时戳
  - 往返时间 = 发时间 + 收时间
- Used to synchronize two clocks in two machines
- 由于路径、传输，难以得到非常精确的时间

Calculate the time



Mask Request and Reply

Type = 17, 18	Code = 0	Checksum
Identifier		Sequence number
Mask		

- 应用
  - 供 IP 协议软件使用
  - 主机知道路由器地址时，可以向路由器发送请求
  - 不知道路由器时，可广播发送，路由器作应答

Route Solicitation and Advertisement

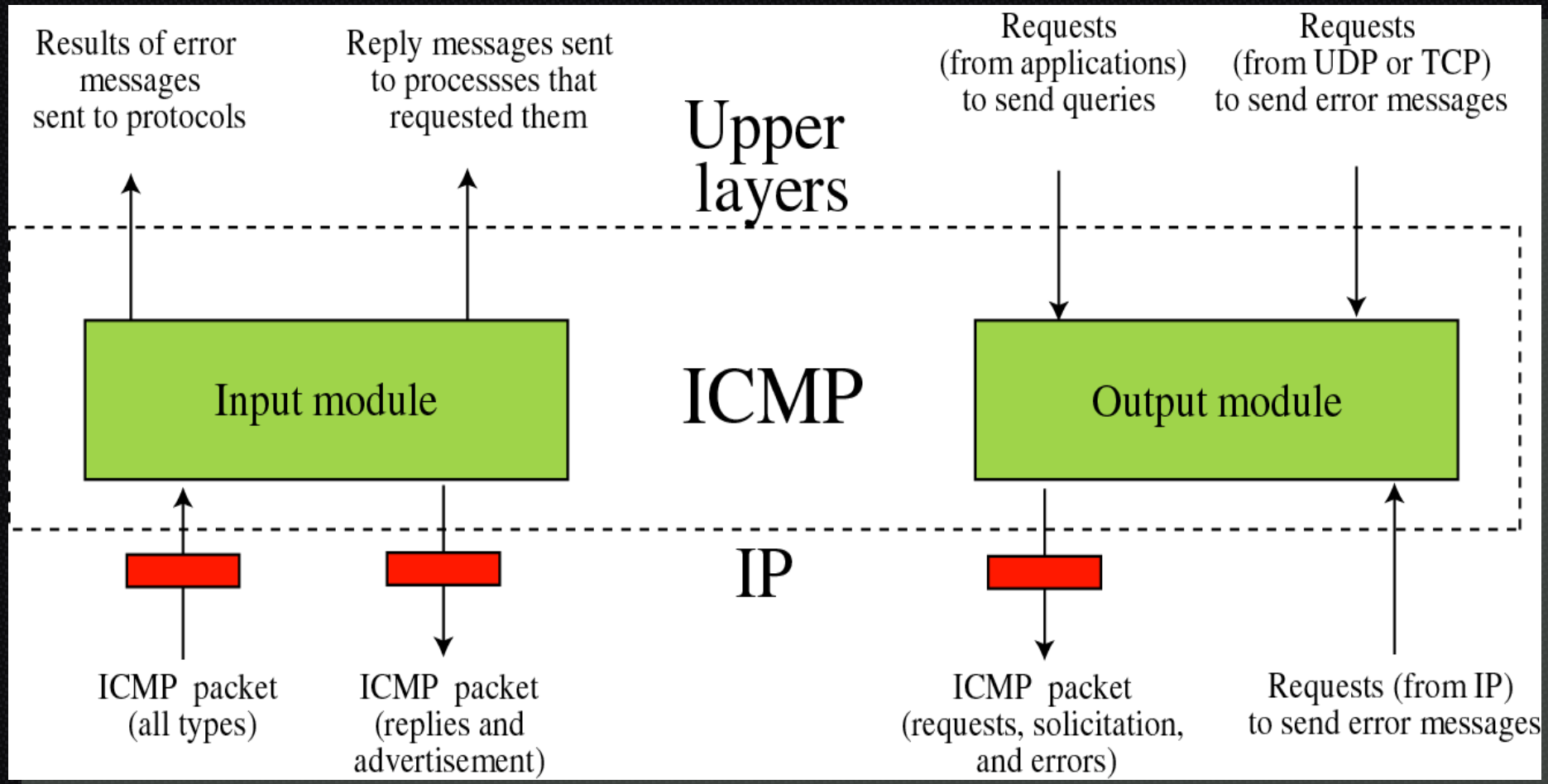
- 主机发送路由器询问报文，查询本网中的路由器

Type = 10	Code = 0	Checksum
Identifier		Sequence number

- 路由器发送路由器通告报文，通告自己以及所知的本网中其他路由器的存在

Type = 10	Code = 0	Checksum
Identifier		Sequence number
Router address 1		
Address preference 1		
Router address 2		
Address preference 2		
……		

ICMP Package



Summary

- ICMP
  - 作用、通信方式
- ICMP 报文
  - 封装：直接封装在 IP 分组中
  - 类型：差错报告（传输特点）、测试查询
  - 作用、特点