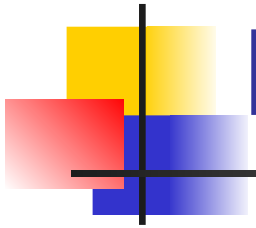
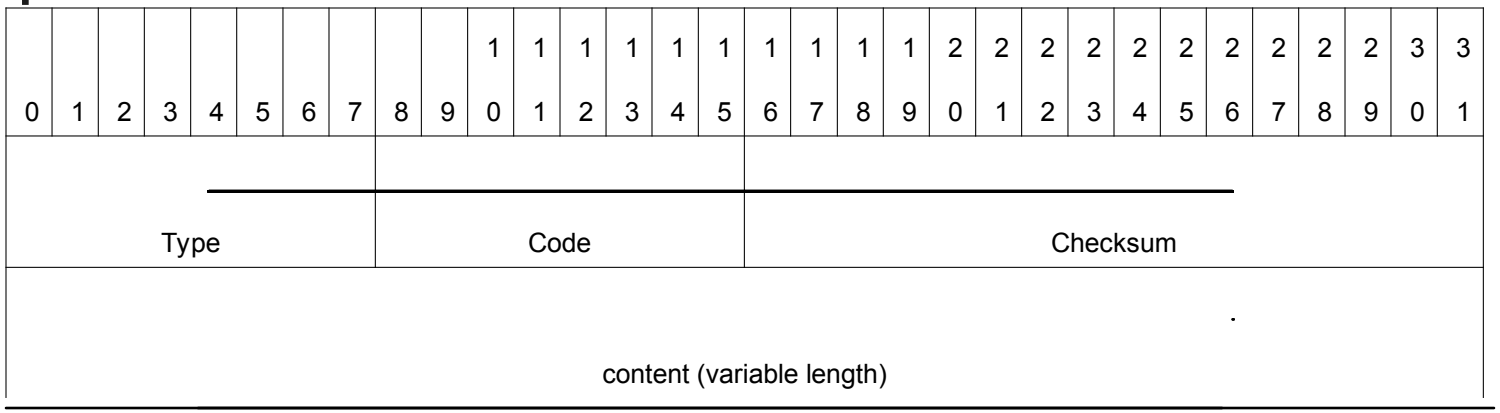
CSBridge – Net 7

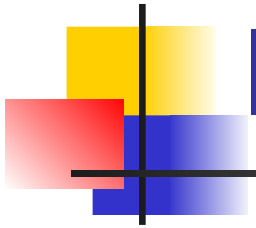
Internet Control Message Protocol (ICMP)



- Layer 3 protocol with works in conjunction with IP
- Used for passing informational messages
- Used for informing a station that an error has occurred in transmission

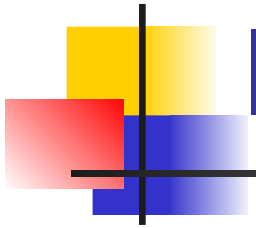
ICMP Header


0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Type
Code
Checksum
content (variable length)



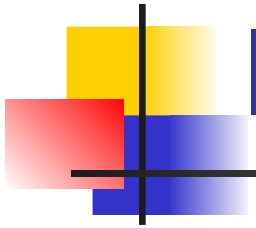
ICMP Rules

- An ICMP error message is never sent in response to an ICMP error message
- An ICMP error message will never be sent in response to a packet destined for a broadcast address
- An ICMP error message will never be sent in response to a fragment other than the first.



ICMP Types/codes

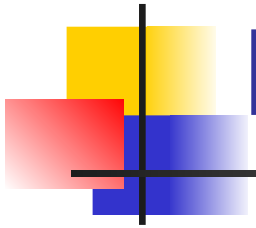
- 0/0 – Echo Reply
- 8/0 – Echo Request
- 3/0 – Network Unreachable
- 3/1 – Host unreachable
- 3/3 – Port Unreachable
- 3/4 – Fragmentation needed but DF set
- 3/9 – Destination Network prohibited
- 3/10 – Destination host prohibited



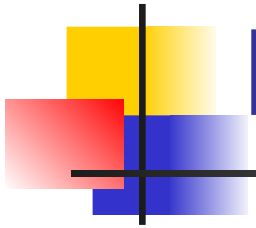
ICMP types/codes

- 4/0 – Source quench
- 5/0 – Redirect for network
- 5/1 - Redirect for host
- 11/0 – TTL Exceeded during transit
- 17/0 – Address Mask Request
- 18/0 – Address Mask Reply

Address Mask Request/Reply

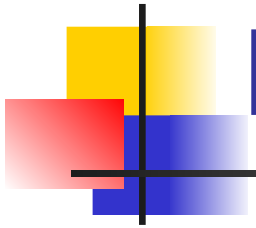


- Used for workstations that implement RARP for address assignment.
- The header is modified to include an 16-bit identifier, and 16-bit sequence number after the checksum.
- A packet is sent to the broadcast address and will be replied to by the address mask authority. The 32-bit address mask will follow the sequence number.



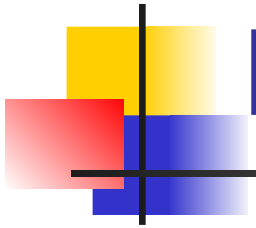
Ping

- Used (primarily) to determine if we have layer 3 connectivity to another device
- And ICMP type 8 code 0 message is sent to the destination with a variable amount of data
- The destination host replies with the same data in an ICMP type 0 code 0 packet.



Ping benefits

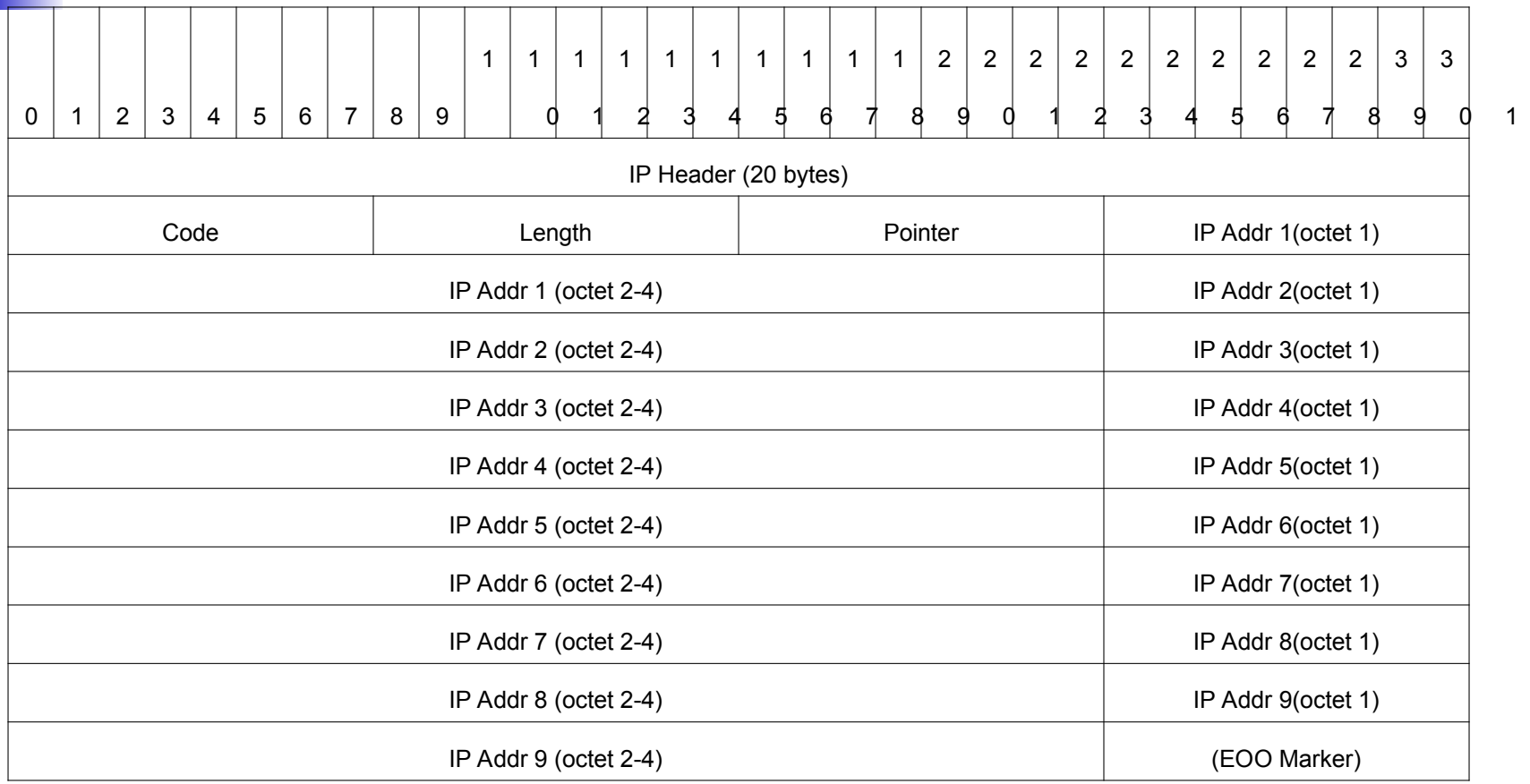
- Can be used to determine network connectivity
- Can be used to determine average speed of the network
- Can be used to determine the “distance” to the destination.
- Can be used to determine route path.
- Useful for finding “black holes”

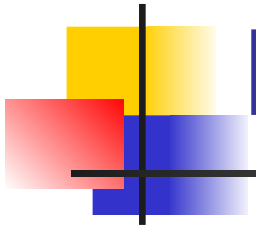


Ping disadvantages

- A positive response doesn’t always mean the destination is working properly
- A negative (NULL) response doesn’t always mean the destination isn’t working properly
- ICMP gets the lowest possibly processing priority so time measurements cannot always be trusted
- Has a very limited size for Recording route and timestamping

Record Route



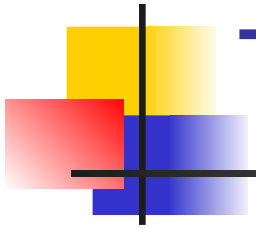


Record Route

- Code is set to 7, length is set to 39 and ptr is set to 4
- Each router places it’s IP address in the packet starting at offset ptr-1
- If PTR reaches 40 no more data can be placed in the packet
- The destination station sends the entire packet back
- This does not effect the operation of ICMP!

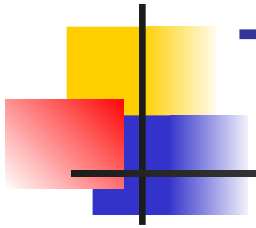
Ping In Actio

```
IP: ID = 0xB625; Proto = ICMP; Len: 100
  IP: Version = 4 (0x4)
  IP: Header Length = 60 (0x3C)
  IP: Precedence = Routine
  IP: Type of Service = Normal Service
  IP: Total Length = 100 (0x64)
  IP: Identification = 46629 (0xB625)
  IP: Flags Summary = 0 (0x0)
  IP: Fragment Offset = 0 (0x0) bytes
  IP: Time to Live = 246 (0xF6)
  IP: Protocol = ICMP - Internet Control Message
  IP: Checksum = 0x23F1
  IP: Source Address = 64.2.85.40
  IP: Destination Address = 128.238.35.133
 IP: Option Fields
  IP: Record Route Option
    IP: Option Type = Record Route
    IP: Option Length = 39 (0x27)
    IP: Next Slot Pointer = 40 (0x28)
   IP: Route Traveled
     IP: Gateway = 128.238.30.3
     IP: Gateway = 128.238.40.6
     IP: Gateway = 169.130.14.10
     IP: Gateway = 169.130.1.38
     IP: Gateway = 169.130.3.130
     IP: Gateway = 209.220.117.26
     IP: Gateway = 64.220.3.83
     IP: Gateway = 209.220.116.41
     IP: Gateway = 64.2.85.40
  IP: End of Options = 0 (0x0)
  IP: Data: Number of data bytes remaining = 40 (0x0028)
ICMP: Echo Reply: To 128.238.35.133 From 64.02.85.40
  ICMP: Packet Type = Echo Reply
  ICMP: Echo Code = 0 (0x0)
  ICMP: Checksum = 0x415C
  ICMP: Identifier = 512 (0x200)
  ICMP: Sequence Number = 4608 (0x1200)
  ICMP: Data: Number of data bytes remaining = 32 (0x0020)
```



Traceroute

- Very useful program to see the route which a packet follows in traveling from A to B.
- Uses either ICMP or UDP
- The concept can be used for any protocol which operates on IP
- Overcomes the 9 hop problem with IP RR



Traceroute operation

- A packet is sent to the destination with a TTL of 1
- When the first router receives the packet it decrements it to zero and an ICMP type 11 code 0 message is returned to the sender
- The TTL is incremented and the process continues
- We can stop when we receive the expected response from the destination