University of Toronto
ECE361
Computer Networks

Dynamic Host Configuration Protocol (DHCP)

IP addresses: how to get one?

Q: How does a *host* get IP address?

- Option 1: hard-coded by system admin in a file
  - Windows: control-panel->network->configuration
  - UNIX: /rc.config
- Option 2: DHCP: Dynamic Host Configuration Protocol: Dynamically get an IP address from as server.
  - "plug-and-play"

2

DHCP: Overview

- When a new computer is attached to a LAN, the computer broadcasts a message asking a server "give me a network address."
- Server maintains a pool of free IPs and assigns one to this computer with a specified time-to-live (e.g. one hour).
- The computer can then start using the standard Internet applications.
- As the time-to-live becomes close to zero, computer asks the server for an extension (which is normally granted).
- If connection is terminated then the IP is returned to the pool of free IPs.

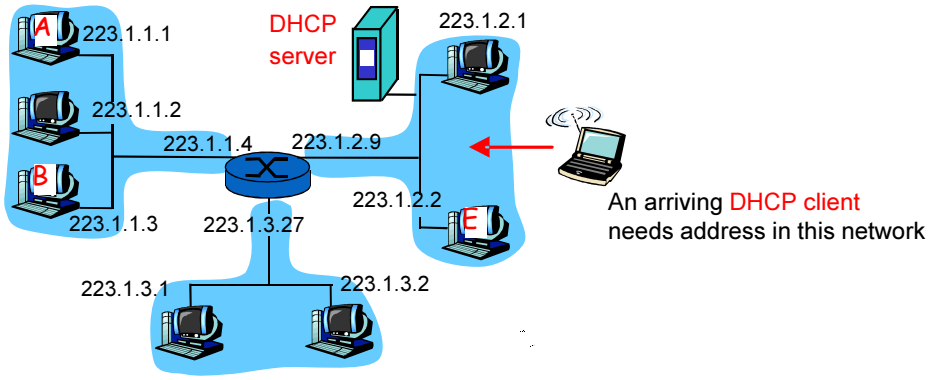
3

DHCP: Dynamic Host Configuration Protocol

- Dynamic assignment of IP addresses is desirable for several reasons:
  - Avoid manual IP configuration.
  - IP addresses are assigned on-demand.
  - Support mobility of laptops.
  - Allows reusing of the IP Addresses
  - Supports temporary allocation ("leases") of IP addresses.
  - Is the preferred mechanism for dynamic assignment of IP addresses.

4

DHCP client-server scenario



5

DHCP overview:

- DHCP discover: Client broadcasts in order to find out available DHCP servers.
- DHCP offer: Response from a server to a DHCPDISCOVER and offering IP address and other parameters.
- DHCP request: Message from a client to servers that does one of the following:
  - Requests the parameters offered by one of the servers and declines all other offers.
  - Verifies a previously allocated address after a system or network change (a reboot for example).
  - Requests the extension of a lease on a particular address.
- DHCP ack: Acknowledgement from server to client with parameters, including IP address.

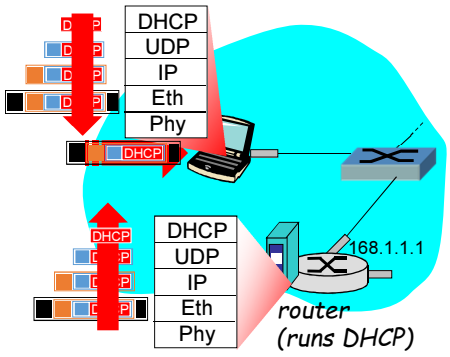
6

DHCP: more than IP address

- DHCP can return more than just allocated IP address on subnet:
  - address of first-hop router for client
  - name and IP address of DNS server
  - network mask (indicating network versus host portion of address)

7

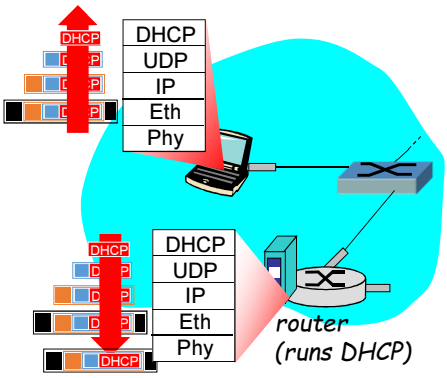
DHCP: Example



- Connecting laptop needs its IP address, addr of first-hop router, addr of DNS server: use DHCP
- DHCP request encapsulated in UDP, encapsulated in IP, encapsulated in 802.1 Ethernet
- Ethernet frame broadcast (dest: FFFFFFFFFFFF) on LAN, received at router running DHCP server
- Message is demultiplexed.

8

DHCP: Example

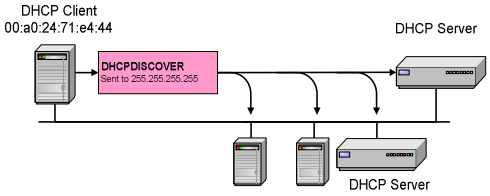


- DHCP server formulates ACK containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server
- Encapsulation of DHCP server, frame forwarded to client
- Client now knows its IP address, name and IP address of DNS server, IP address of its first-hop router

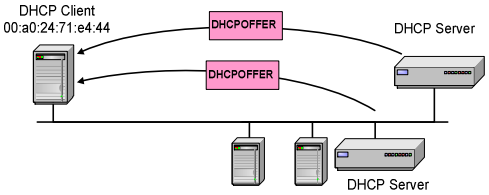
9

DHCP Operation

DCHP DISCOVER



DCHP OFFER

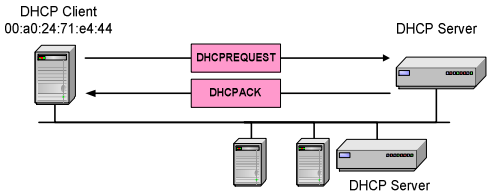


10

DHCP Operation

DCHP Request / DHCP ACK

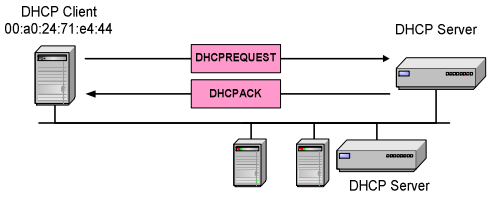
After receiving ACK, the DHCP client can start to use the IP address



Renewing a Lease

(sent when 50% of lease has expired)

If DHCP server sends DHCPNACK, then address is released.



11

Broadcast or Unicast

- It is possible to use broadcast for the complete assignment process (DISCOVERY, OFFER, REQUEST, ACK), but unicast is frequently used:
  - When DHCP client knows address of DHCP server, it may use unicast in all its messages.

12

Notes

- An issue that arises with automatic assignment of IP addresses from a pool is for how long an IP address should be allocated. If a host leaves the network and does not return its IP address to the DHCP server, that address will be permanently lost.
  - After a period of time, many addresses may be lost.
  - To prevent that from happening, IP address may be assigned for a fixed period of time, this technique is called leasing.
  - Then before the lease expires, the host must ask for a DHCP renewal.
  - If client does not receive an ACK message after its lease has expired, then client is automatically forced to stop its current TCP configuration.
  - Client may then return to the initial state, issuing a DISCOVER broadcast to try and obtain any valid address.

13

University of Toronto
ECE361
Computer Networks

Network Address Translation

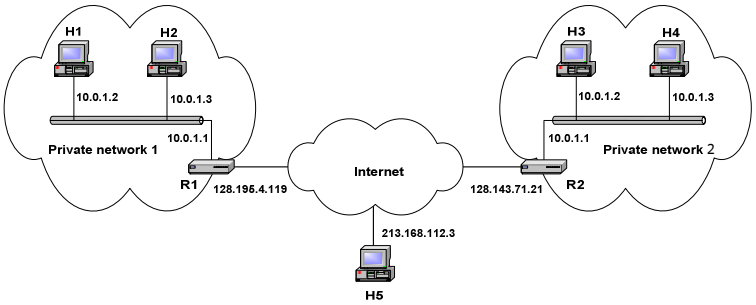
(NAT)

Private Network

- A *Private IP* network is an IP network that is not directly connected to the Internet.
- IP addresses in a private network can be assigned arbitrarily.
  - Not registered and not guaranteed to be globally unique.
- Private networks can use addresses from the following experimental address ranges:
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255

15

Private Addresses



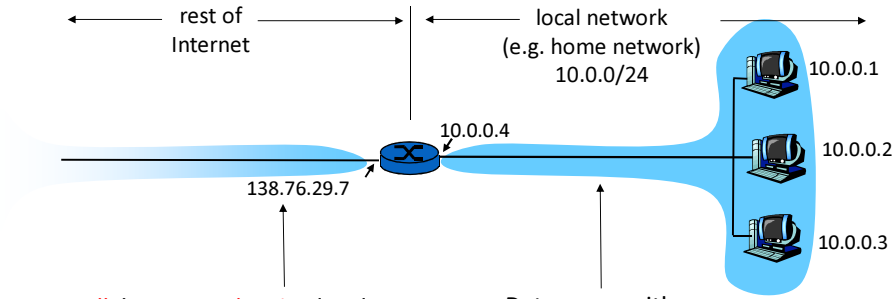
16

Network Address Translation (NAT)

- Is a method that enables hosts on private networks to communicate with hosts on the Internet.
- Runs on routers that connect private networks to the public Internet, to replace the IP address-port pair of an IP packet with another IP address-port pair.

17

NAT: Network Address Translation

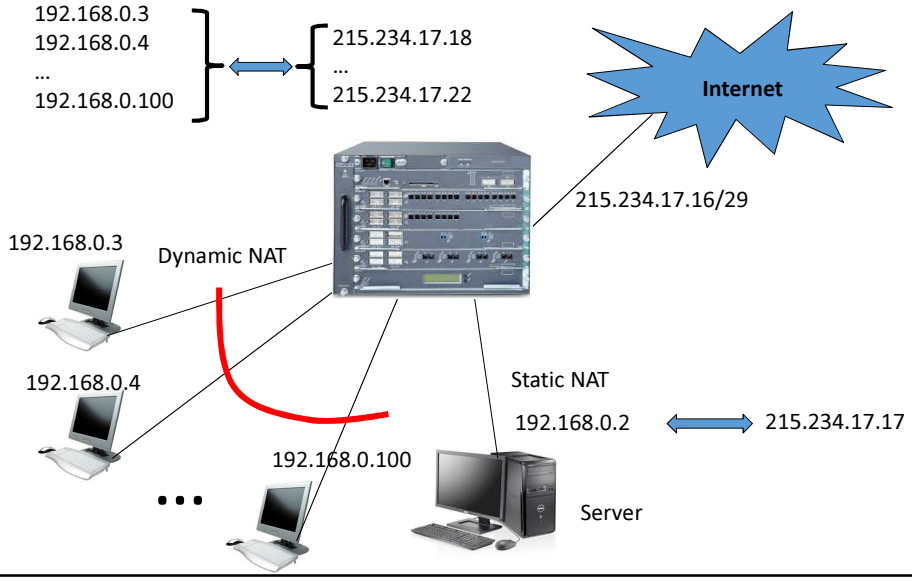


All datagrams *leaving* local network have same single source NAT IP address: 138.76.29.7, different source port numbers

Datagrams with source or destination in this network have 10.0.0.0/24 address

18

Address Translation



19

Static/Dynamic NAT

Static NAT – Mapping an unregistered IP address to a registered IP address on a one-to-one basis. Particularly useful when a device needs to be accessible from outside the network.
Example: In previous example, the computer with the IP address of 192.168.0.2 will always translate to 215.234.17.17

Dynamic NAT – Maps an unregistered IP address to a registered IP address from a group of registered IP addresses.
Example: In previous example, the computer with the IP address of 192.168.0.3 will translate to the first available address in the range from 215.234.17.17 to 215.234.17.22

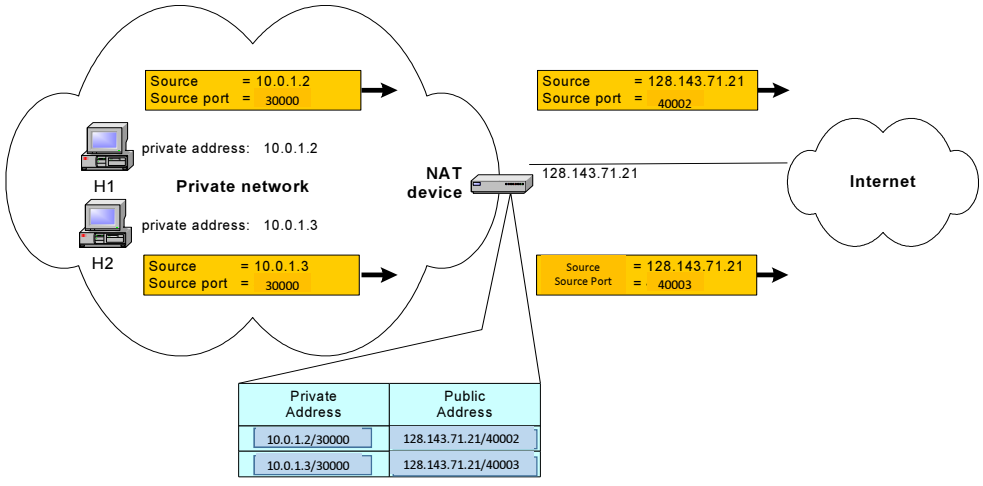
20

IP Overloading

- NAT maps single public IP address to multiple unregistered IP addresses (private network addresses) by using different port numbers.
  - Called PAT (Port Address Translation), single address NAT, port-level multiplexed NAT, or NAPT (Network Address and Port Translation).
  - NAPT operates at the Transport Layer.
  - NAPT translation Table contains 4-tuples of source and destination protocol port numbers and IP addresses.
- **Example:** Each computer on the private network is translated to the same IP address (215.234.17.17) but with a different port number assignment**.**

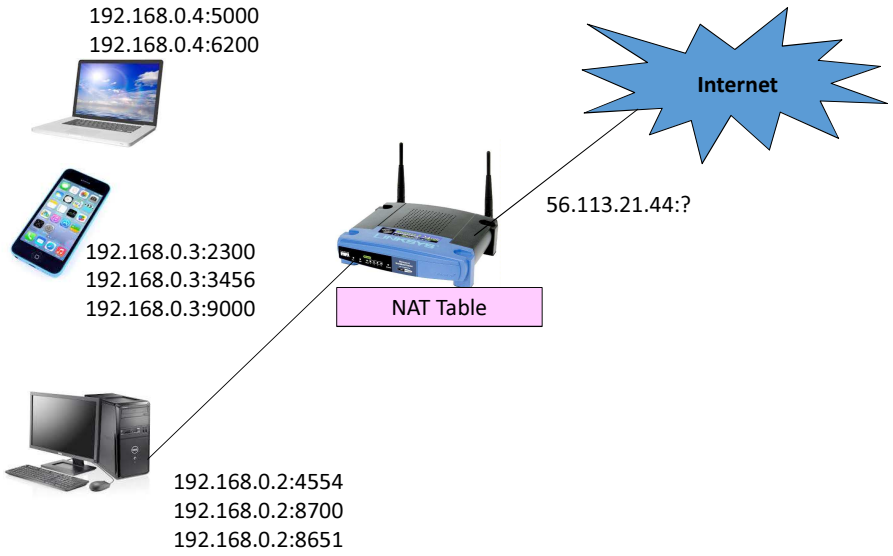
21

IP Overloading



22

Port Translation



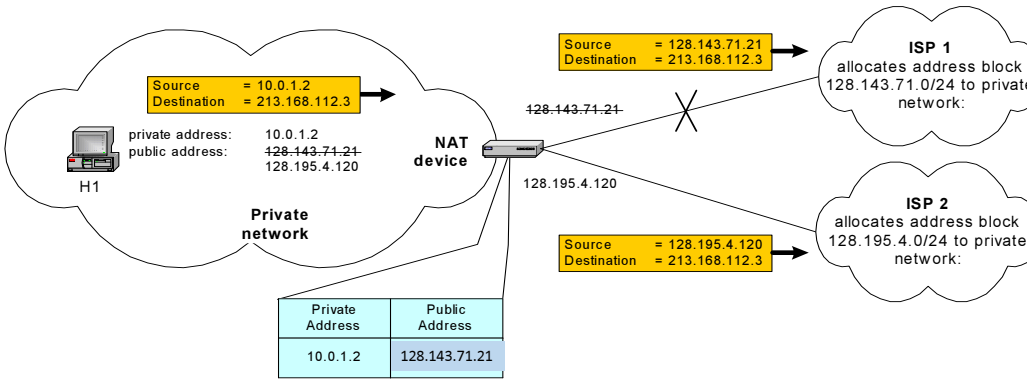
23

Supporting migration between ISPs

- **Scenario:** IP addresses in a corporate network are obtained from the service provider. Changing the service provider requires changing all IP addresses in the network.
- **NAT solution:**
  - The corporate network is assigned private addresses to its hosts.
  - NAT device has static address translation entries that can bind the private addresses of hosts to the public addresses.
  - Migration to a new network service provider merely requires an update of the NAT device. The migration is not noticeable to the hosts on the network.

24

Supporting migration between network ISPs



25

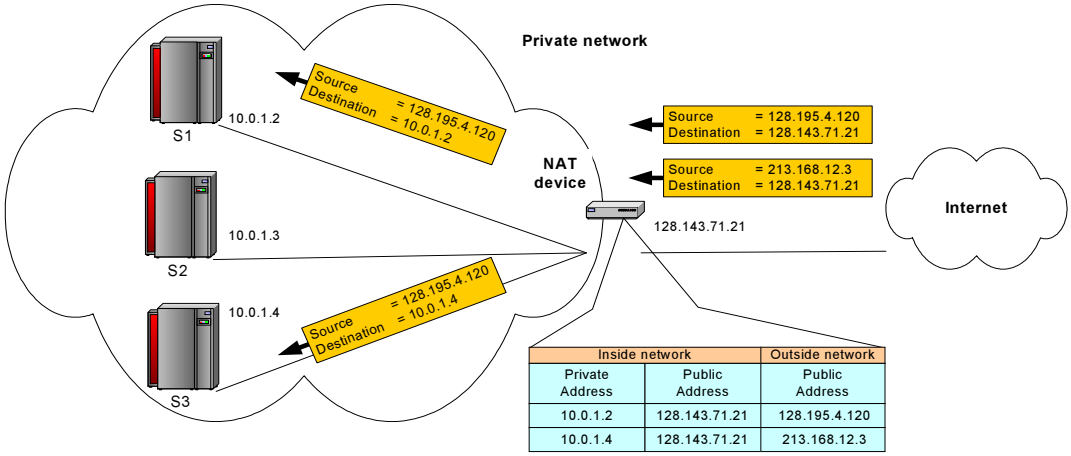
Load balancing of servers

- **Scenario:** Balance the load on a set of identical servers, which are accessible from a single IP address.

- **NAT solution:**
  - Servers are assigned private addresses.
  - NAT device acts as a proxy for requests to the server from the public network.
  - NAT device changes the destination IP address of arriving packets to one of the private addresses for a server.
  - Then can evenly distribute the load.

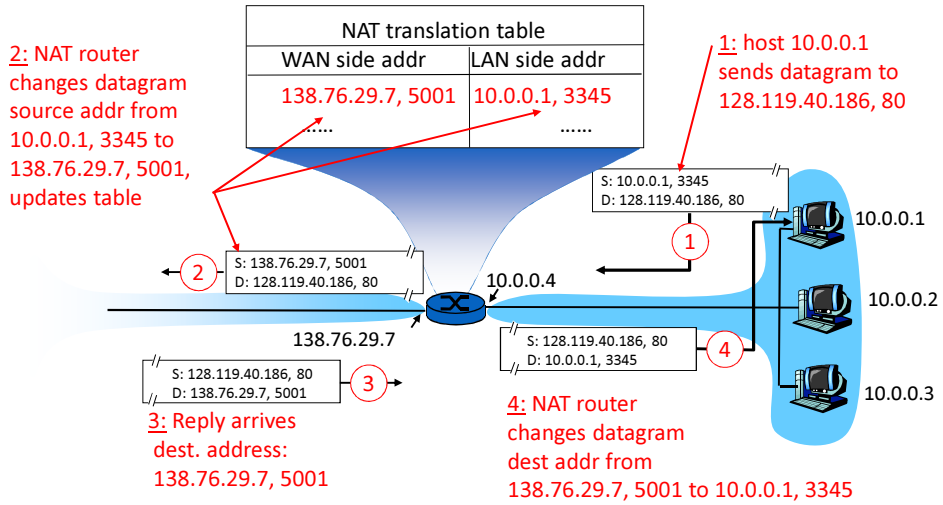
26

Load balancing of servers



27

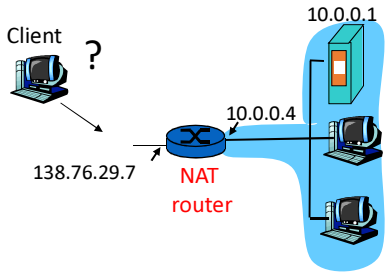
NAT: Network Address Translation



28

NAT traversal problem

- client wants to connect to server with address 10.0.0.1
  - server address 10.0.0.1 local to LAN (client cannot use it as destination address)
  - only one externally visible NATted address: 138.76.29.7
- solution: statically configure NAT to forward incoming connection requests at a given port to server
  - e.g. (123.76.29.7, port 2500) always forwarded to 10.0.0.1 port 25000



29

NAT Advantages

- Can use only one IP address (could be more) for all the devices in the network.
- Can change addresses of devices in local network without notifying outside world.
- Devices inside local net not explicitly addressable, visible by outside world (a security plus).
- Can perform load balancing of servers.
- Reduces the cost associated with purchasing host numbers.
- Makes transition from one ISP to another easy.

30

NAT Disadvantages

- **Intensive computation:**
  - NAT requires intensive computation such to modify IP addresses, port numbers, and recalculate checksums.
- **End-to-end connectivity:**
  - NAT destroys universal end-to-end reachability of hosts on the Internet.
  - If any end-to-end security protocol is implemented then NAT may not work since NAT changes the IP header and this is considered as a security violation.
  - A host in the public Internet often cannot initiate communication to a host in a private network.
  - Routers should only process up to layer 3
- **Better approach:** IP address shortage should instead be solved by IPv6.

31

University of Toronto
ECE361
Computer Networks

Internet Control Message Protocol

(ICMP)

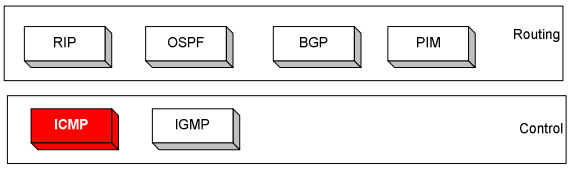
Chapter 4: Network Layer

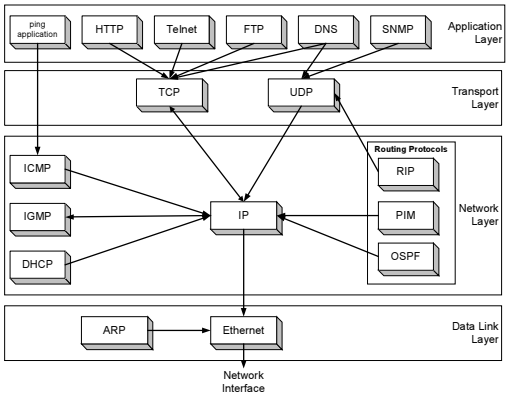
- 4. 1 Introduction
- 4.2 Virtual circuit and datagram networks
- 4.3 What's inside a router
- 4.4 IP: Internet Protocol
  - Datagram format
  - IPv4 addressing
  - ICMP
  - IPv6
- 4.5 Routing algorithms
  - Link state
  - Distance Vector
  - Hierarchical routing
- 4.6 Routing in the Internet
  - RIP
  - OSPF
  - BGP
- 4.7 Broadcast and multicast routing

33

Overview

- The IP (Internet Protocol) relies on several other protocols to perform necessary control and routing functions:
  - Control functions (ICMP)
  - Multicast signaling (IGMP)
  - Setting up routing tables
    (RIP, OSPF, BGP, PIM, …)





34

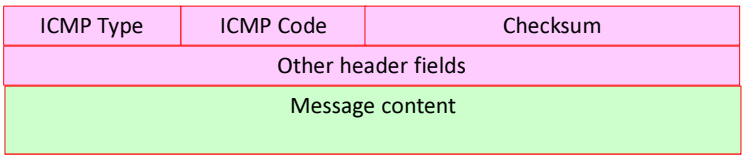
ICMP: Internet Control Message Protocol

- Used by hosts and routers to communicate network-level information
  - Error reporting: unreachable host, network, port, protocol
  - Echo request/reply (used by ping)
  - Simple queries
- Resides at the Network-layer "above" IP:
  - ICMP messages are carried in IP datagrams
- ICMP messages are encapsulated as IP datagrams:
  - Protocol field in the IP header is set to: 0x01

35

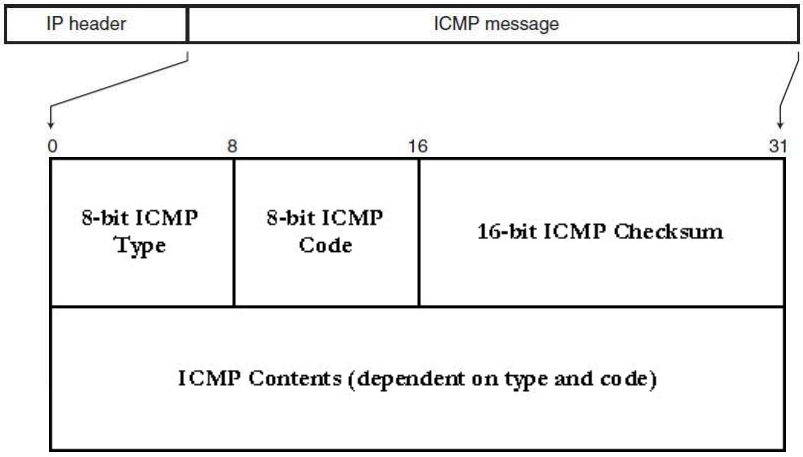
ICMP Header

- All ICMP packets will have an 8-byte header and variable-sized data section:
  - The first byte is for the ICMP type.
  - The second byte is for the ICMP code.
  - The third and fourth bytes are a checksum of the entire ICMP message.
  - The contents of the remaining 4 bytes of the header will vary based on the ICMP type and code. If there is no additional data, then these 4 bytes are set to zero.



36

ICMP Message



37

ICMP: Internet Control Message Protocol

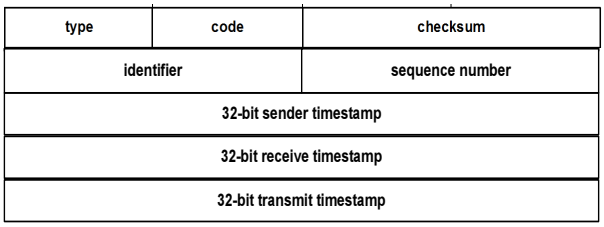
- ICMP message: type, code plus first 8 bytes of IP datagram causing error

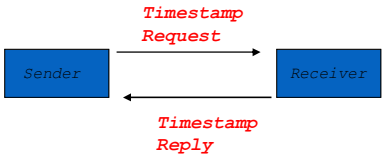
Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

38

Example of a Query: ICMP Timestamp

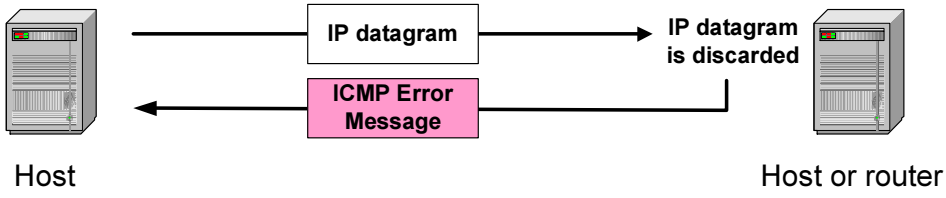
- A system (host or router) asks another system for the current time.
- Time is measured in milliseconds after midnight UTC (Universal Coordinated Time) of the current day
- Sender sends a request, receiver responds with reply





39

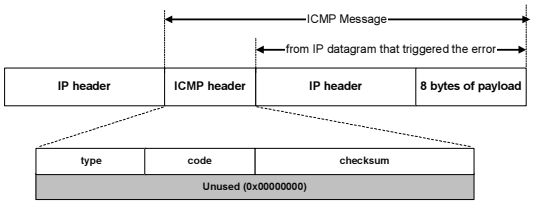
ICMP Error message



- ICMP error messages report error conditions
- Typically sent when a datagram is discarded
- Error message is often passed from ICMP to the application program

40

ICMP Error message



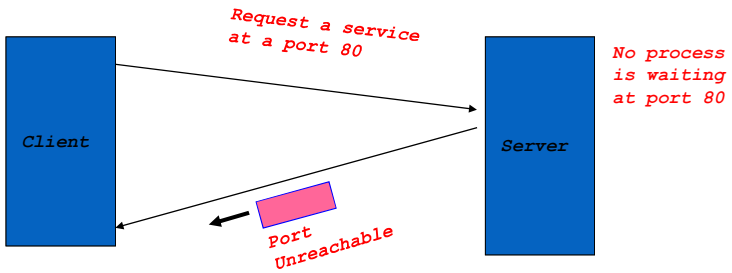
20-byte IP header (protocol = 1—ICMP)		
Type = 11	Code	Checksum
unused		
IP header + first 8 payload bytes of packet that caused ICMP to be generated		

- ICMP error messages include the complete IP header and the first 8 bytes of the payload (typically: UDP, TCP) of the packet that triggered the error condition

41

Example: ICMP Port Unreachable

- RFC 792:
  - If, in the destination host, the IP module cannot deliver the datagram because the indicated protocol module or process port is not active, the destination host may send a destination unreachable message to the source host.
- Scenario:
  - We request to non-existing web server



42

Traceroute

- Is implemented by ICMP
- Allows to determine the names and addresses of the routers from source to destination.
- Sends a series of UDP datagrams with TTL 1, 2, 3, …, n
  - Potentially with no Port Number.
- Starts a timer for each datagram.
- As a datagram arrives at a router and eventually the TTL expires:
  - Router sends back an unreachable ICMP message (type 11, code 0)
  - Router drops the datagram.
  - The ICMP message has both name and the IP address of the router.

43

Traceroute

- When ICMP message arrives at the source then source calculates RTT.
- Traceroute sends sets of 3 packets with the same TTL.

Stopping criterion

- UDP segment eventually arrives at the destination host
- Destination returns ICMP "host unreachable" packet (type 3, code 3)
- When source gets this ICMP, stops.

44