Module 4
(Lecture – 4)

(Network Layer: Router architecture; Internet Protocol (IP) - Forwarding and Addressing in the Internet; Routing algorithms - Link-state routing, Distance vector routing, Hierarchical routing; Routing in the Internet - RIP, OSPF, BGP; Broadcast & multicast routing; ICMP; Next Generation IP - IPv6)

Dr. Nirnay Ghosh

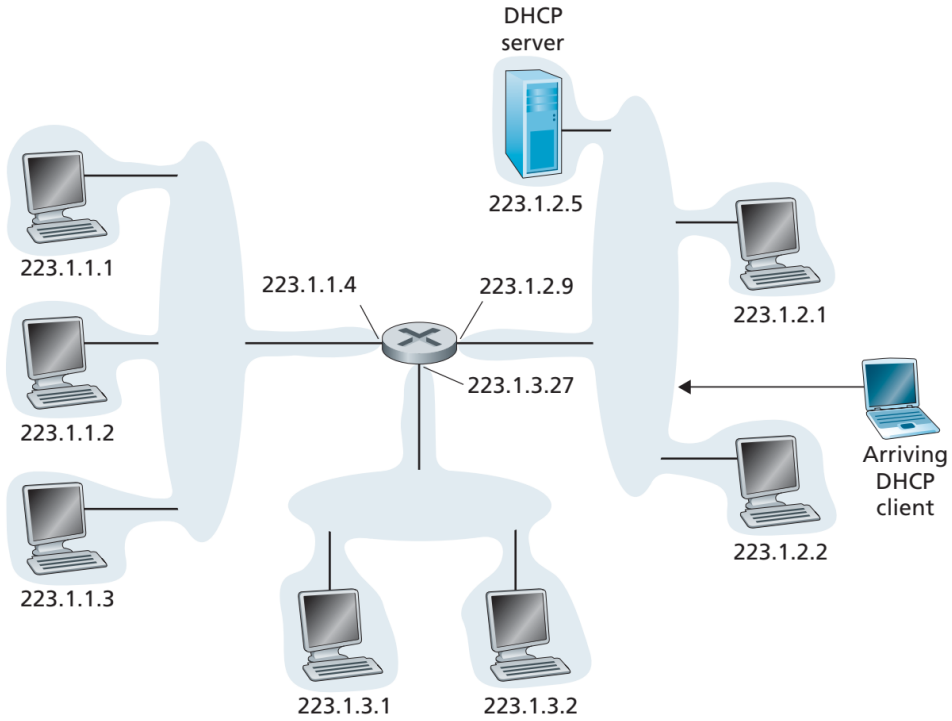
Assistant Professor

Department of Computer Science & Technology

IIEST, Shibpur

Dynamic Host Configuration Protocol (DHCP)

- Dynamic Host Configuration Protocol (DHCP)
  - Allows a host to obtain (be allocated) IP address automatically – removes overhead of manual configuration
  - DHCP server configured by the network administrator such that a host:
    - receives the same IP address every time it connects to the network
    - receives temporary IP address that will be different each time the host connects to the network
  - Additional information given to the host: subnet mask, the address of its first-hop router (often called the default gateway), and the address of its local DNS server
  - Ideal use-case: many users joining and leaving the network; addresses are needed for only a limited amount of time
- DHCP server: updates its list of available IP addresses as users join and leave
  - Host joining: arbitrary address from current pool of available addresses is allocated
  - Host leaving: address is returned to the pool

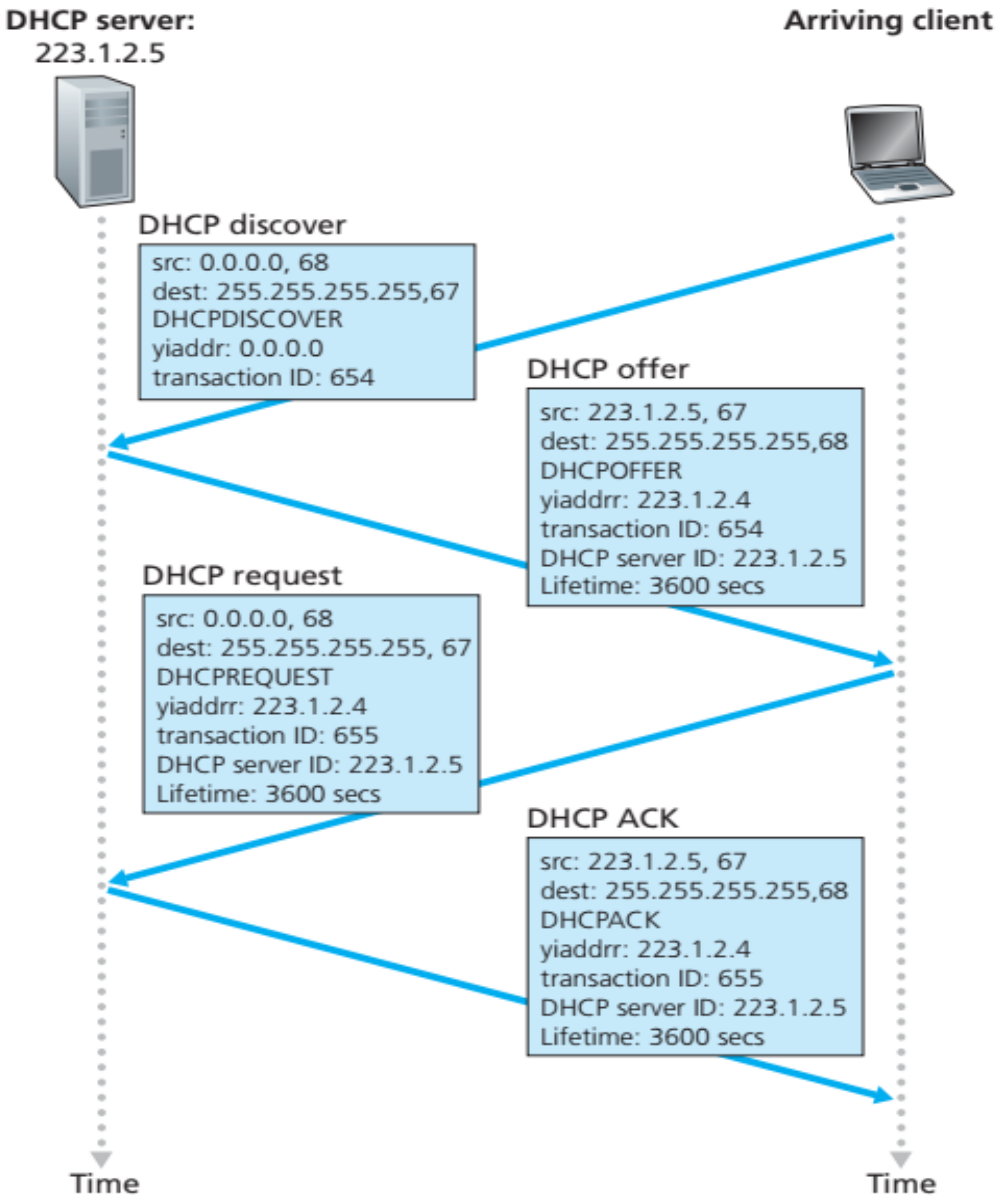


DHCP Client-Server Scenario

- Client-server protocol: arriving hosts act as clients
- DHCP server: typically configured for each subnet
- Otherwise - router relays the DHCP request to the remote DHCP server hosted in another subnet
- Example: DHCP configured for subnet 223.1.2.0/24; Router acts as relay for subnets 223.1.1.0/24 and 223.1.3.0/24 (no local DHCP server)

DHCP Protocol: 4 steps

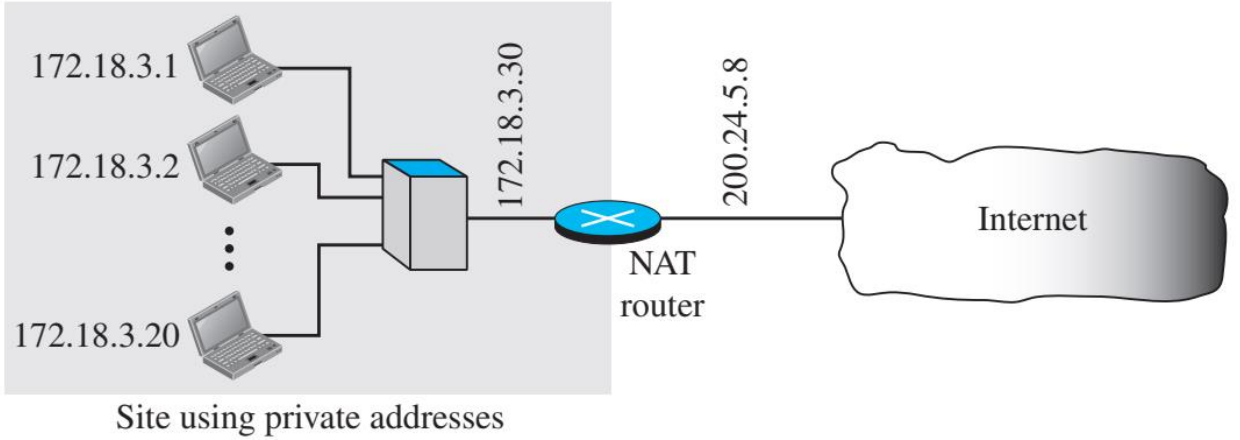
- DHCP discovery
  - Client needs to find a DHCP server (multiple DHCP servers may be present in a subnet)
  - It sends UDP packet to port 67 (port number for DHCP)
    - Destination IP address: 255.255.255.255 (broadcast address); source IP address: 0.0.0.0 (“this” host)
  - Passes the packet to the link layer - broadcasts the frame to all stations attached to the subnet
- DHCP Offer
  - Server broadcasts (using destination address: 255.255.255.255) its offer to all stations in the subnet
  - Contents of the message: transaction ID of the received discover message, the proposed IP address for the client, the network mask, and an IP address lease time
  - Lease time: several hours or days
- DHCP Request
  - Client chooses from among one or more server offers
  - Respond to its selected offer with a DHCP request message
  - Echoes back the configuration parameters
- DHCP ACK
  - Server responds to the DHCP Request message
  - Confirms the requested parameters



DHCP Client-Server Interaction

Network Address Translation (NAT)

- Emergence of hundreds of thousands of small office, home office subnets
- Possibility of address space collision if ISP continues allocating contiguous address blocks
- Observation: fraction of stations in a small network need Internet access simultaneously
  - Private block addresses can be used for internal communication
    - Four blocks of private addresses: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, and 169.254.0.0/16
  - Few universal/public addresses can be assigned by the ISP for accessing the global Internet
- Network Address Translation (NAT)
  - Supports mapping between private and universal addresses

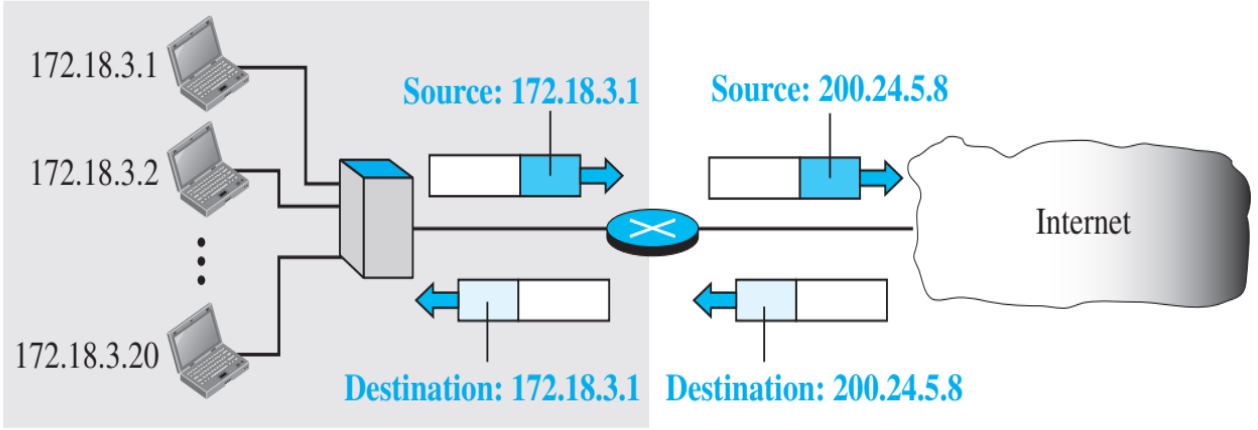


Network Address Translation

- NAT-enabled router: runs the NAT software; connects the networked hosts to the global Internet
- Private network: invisible to the rest of the Internet
- Only NAT-router (with universal/public address) is visible to the rest of the Internet

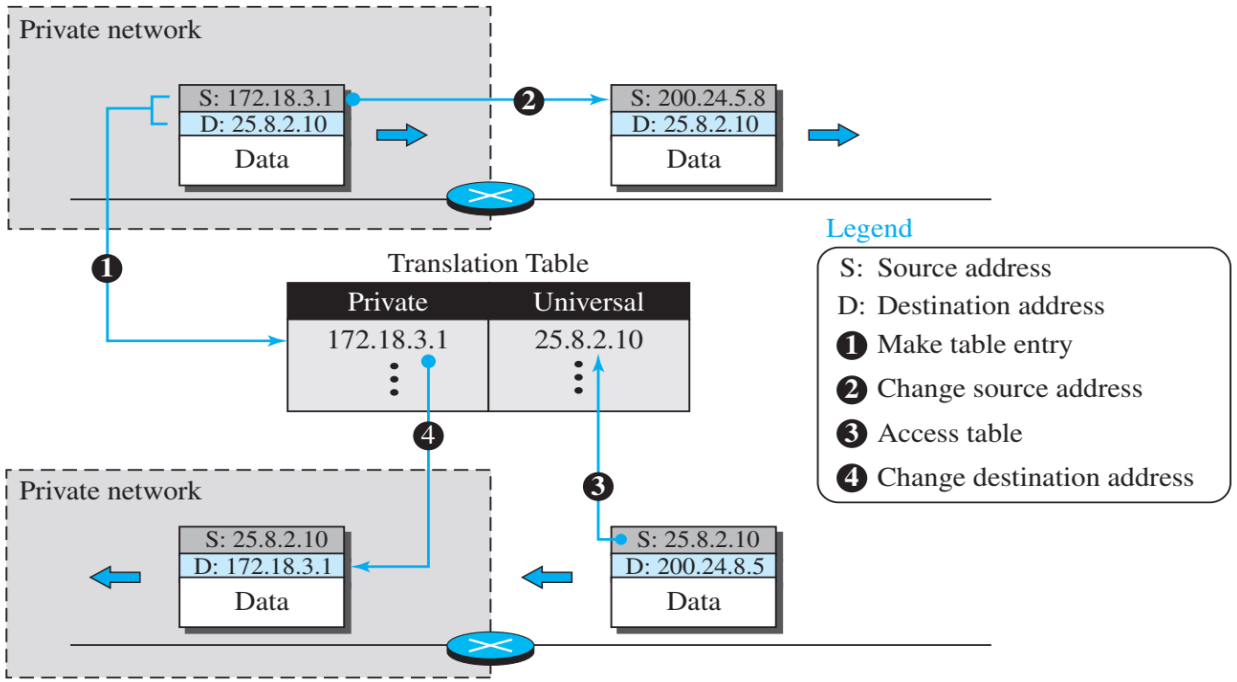
Network Address Translation (NAT)

- Address Translation at NAT-router
  - Outgoing packet: source address is replaced with the global NAT address
  - Incoming packet: global NAT address is replaced with appropriate private address
    - Tens or hundreds of private IP addresses – belonging to specific host – which one to be mapped?
    - Mapping done by translation table
- Using one global NAT address
  - Translation table: two columns – source (private) address & destination (external) address
  - Request packet from private network: router stores the address pair in the table during translation
  - Response packet to private network: router uses the source (external) address to find the destination (private) address
  - Communication – to be initiated by private network
  - Only one private-network host can access external server at a time (one-to-one connection)



Site using private addresses

Address Translation



Translation with One Global NAT Address

Network Address Translation (NAT)

- Using a pool of global NAT address
  - NAT-router uses multiple global addresses
  - Each address pair (global NAT address, external host address) defines a separate connection
  - Enables multiple private-network host to communicate with multiple external hosts at the same time
  - Drawbacks:
    - Connections to the same destination is limited by the number of global NAT addresses
    - No private-network host can access two external server programs (e.g., HTTP and TELNET) at the same time

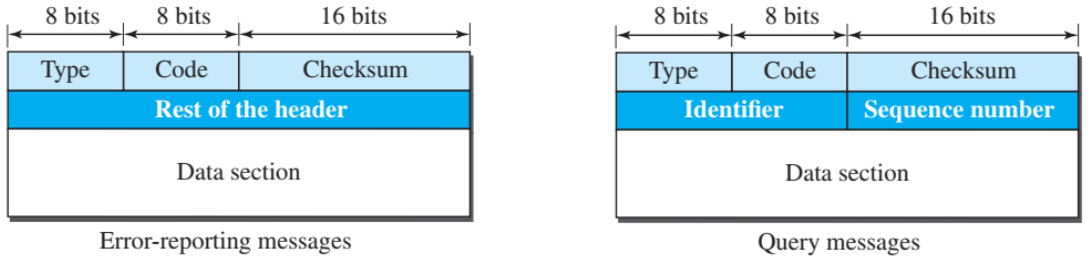
- Using both IP addresses and Port numbers
  - Allow a many-to-many relationship between private-network hosts and external server programs
  - Translation table has five columns: private address, private port, external address, external port, and protocol
  - Request packet from the private network: NAT router maps the combination of source (private) address and source (private) port to destination (external) address and destination (external) port
  - Response packet to the private network: NAT router uses the combination of source (external) address and destination (private) port
  - Determines the private-network host's address - eliminates ambiguity even if two hosts access the same external server program

Five Column Translation Table

Private address	*Private port*	*External address*	*External port*	*Transport protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
⋮	⋮	⋮	⋮	⋮

Internet Control Message Protocol (ICMP)

- IPv4 has no error-reporting or error-correction mechanism
- It also lacks a mechanism for host and management queries (e.g., if a host or router is alive)
- ICMP: used by hosts and routers to communicate network-layer information
- ICMP message – carried inside IP datagram (similar to TCP or UDP segments)
- Value of the protocol field in the IP datagram is set to 1
- Two broad categories:
  - Error-reporting massages: report problems that a router or a host (destination) may encounter when it processes an IP packet
  - Query messages: occurs in pairs – help a host or network manager to get specific information from another router or host
- 8-byte header and a variable size data section
  - Common fields: type, code, checksum



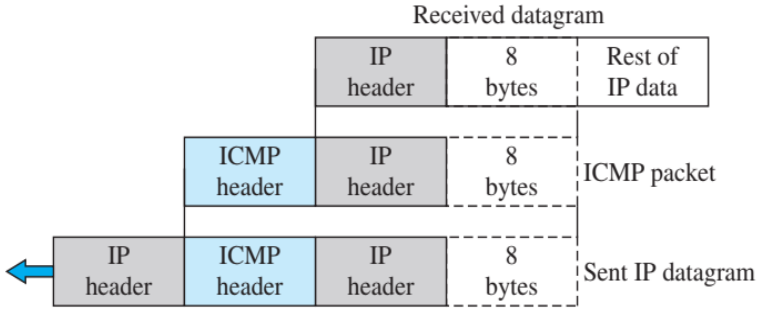
General Format of ICMP Message

ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

ICMP Message Type

ICMP: Error Reporting Messages

- ICMP reports errors that may occur during processing of the IP datagram
- Error messages: sent back to the source
- No ICMP error message for the following datagrams containing:
  - Multicast address
  - ICMP error message
  - Fragmented datagram that is not the first fragment
- Data section of ICMP message:
  - IP header
  - First 8 bytes of IP data: port numbers (UDP and TCP) and sequence number (TCP)
- ICMP forms the error packet which is then encapsulated in an IP datagram



Contents of Data Fields for the Error Messages

Type and code values

Error-reporting messages	Query messages
03: Destination unreachable (codes 0 to 15)	08 and 00: Echo request and reply (only code 0)
04: Source quench (only code 0)	13 and 14: Timestamp request and reply (only code 0)
05: Redirection (codes 0 to 3)	
11: Time exceeded (codes 0 and 1)	
12: Parameter problem (codes 0 and 1)	

- Types of ICMP error message
  - Destination Unreachable: most widely used error message – this may happen when we use the HTTP protocol to access a web page, but the server is down
  - Source Quench: performs congestion control – used by a congested router to a host to force it to reduce its transmission rate
  - Redirection Message: used when the source uses a wrong router to send out its message - router redirects the message to the appropriate router - informs the source the IP address of the default router
  - Parameter Problem Message: sent when either there is a problem in the header of a datagram or some options are missing or cannot be interpreted

ICMP: Query Messages

- Usages:
  - Used to probe or test the liveliness of hosts or routers in the Internet
  - Find the one-way or the round-trip time for an IP datagram between two devices.
- Comes in pairs: request and reply
- Used by debugging tools: *ping* and *traceroute*
- Ping program
  - Sends ICMP echo request (type 8, code 0) and receives ICMP echo reply (type 0, code 0) from the remote host
  - Ping server: most TCP/IP implementation support it directly in the Operating system
  - Client program needs to be able to instruct the OS to generate an ICMP message of type 8 code 0.
- Traceroute program
  - Traces a route from source to destination
  - Enables the source to learn the number and identities of intermediate routers and the RTT to the destination
  - Source sends a series of ordinary datagram to determine the names and addresses of the intermediate routers
  - Client program: instructs the OS to generate UDP segments with specific TTL values
    - The datagrams contain UDP segments with an unlikely port numbers - have increasing TTL values – source starts the timer for each datagram
  - When the n^{th} datagram arrives at the n^{th} router, the TTL of the datagram expires
    - The router discards the datagram and sends an ICMP warning message (type 11, code 0) to the source
    - The warning message includes the name and IP address of the router
    - Source obtains the RTT from the timer
  - OS notifies the client program about the arrival of the ICMP message
  - Source stops sending the UDP segments after it receives port unreachable ICMP message (type 3, code 3) from the destination