- Two versions of IP in use today
  - IPv4
    - IPv4 addressing — Each IP address is 32-bits long (4 bytes) — Typically written in dotted decimal notation
    - IPv6 addressing — Expanded addressing capabilities — Each IP address is 128-bits long
  - IPv6
    - IPv6 — Backward compatible with IPv4 and IPv6 — Can be used by a company to communicated securely in the non-secure public Internet
    - Transitioning from IPv4 to IPv6
      - Dual-stack approach
        - IPv4-capable nodes also have a complete IPv6 implementation
        - If either the sender or the receiver is only IPv4 capable, an IPv4 datagram must be used

Figure 4.32 • A dual-stack approach

New node

Figure 4.33 • Tunneling

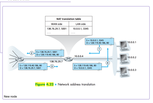
New node

    - Tunneling
      - 3BN-SBT

- The Internet's network layer has three major components
  - The IP protocol
  - The routing component — Determines the path a datagram follows from source to destination.
  - The Internet's network-layer error- and information-reporting protocol: the Internet Control Message Protocol (ICMP)
    - Used by routers and hosts to communicate network-layer information to each other
    - Carried inside IP datagrams, i.e. as IP payload
    - When a host receives and IP datagram with ICMP specified as its upper-layer protocol, it delivers the datagram's contents to ICMP, just as it would distribute a datagram's contents to TCP or UDP
    - Fields
      - Type
      - Code
    - Contain the header and the first 8 bytes of the IP datagram that caused the ICMP message to be generated in the first place
    - Transmitted in implemented using ICMP messages, p. 380

- Datagram format
  - IPv4 datagram format
    - Version number
    - Header length — Needed to determine where in the IP datagram the data actually begins
    - Type of service (TOS)
    - Datagram length — Total length of the IP datagram (header plus data)
    - Time-to-live (TTL)
      - Ensures that that datagram does not circulate forever
      - Decremented each time the datagram is processed by a router
      - If the TTL field reaches 0, the datagram must be dropped
    - Protocol
      - Only used when the datagram reaches its final destination
      - Indicates the specific transport-layer protocol to which the data portion of the IP datagram should be passed
      - The glue that binds the network and transport layers together, corresponding to the glue that ties the first two layers of the protocol stack together
    - Header checksum
      - Aids a router in detecting bit errors in a received IP datagram
      - A router computes the header checksum for each received IP datagram and detects an error condition if the checksum in the datagram header does not equal the computed checksum
        - Note that only the IP header is checksummed at the IP layer, because TCP and UDP also perform checksums over the entire TCP/UDP segment
      - Routers typically discard datagrams for which an error has been detected
      - Must be recomputed and stored again at each router, as the TTL field, and possibly the options field as well, may change
    - Source and destination IP addresses
    - Options
    - Data (payload)
  - IPv6 datagram format
    - Version
    - Traffic class — Similar to IPv4 "TOS" field
    - Flow label — Used to identify a flow of datagrams
    - Payload length — The number of bytes following the fixed length, 40 byte datagram header
    - Next header — Similar to IPv4 "protocol" field, i.e this field identifies the protocol to which the content (data field) will be delivered
    - Hop limit — Similar to IPv4 TTL field
    - Source and destination addresses
    - Data — The payload portion of the IPv4 datagram

The Internet Protocol (IP): Forwarding and Addressing in the Internet

- IP datagram fragmentation — Not all link-layer protocols can carry network-layer packets of the same size
  - Maximum transmission unit (MTU) — The maximum amount of data that a link-layer frame can carry is called the maximum transmission unit (MTU). Because each IP datagram is encapsulated within the link-layer frame for transport from one router to the next router, the MTU limits the IP datagram to have a length of no more than the MTU of the link-layer protocol
    - If a router receives a datagram that is too large to be forwarded over a link because the MTU of that outgoing link is too small, it fragments the data in IP datagram into two or more smaller IP datagrams, encapsulates each of these smaller IP datagrams in a separate link-layer frame, and sends these fragments over the outgoing link. Each of these smaller datagrams is referred to as a fragment
      - Fragments need to be reassembled before they reach the transport layer at the destination host (p 380-383)
      - Fragment reassembly is done at the receiving host
  - If the outgoing link has an MTU that is smaller than the length of the IP datagram
  - IPv6 does not allow for fragmentation and reassembly at intermediate routers; these operations can be performed only at the source and destination.
- Interface
  - The boundary between the host and the physical link.
  - The boundary between the router and any one of its links
  - IP requires each host and router interface to have its own IP address. — Thus, an IP address is technically associated with an interface, rather than with the host or router containing that interface
- Subnet
  - A network interconnecting interfaces
  - Subnet mask
- IP addressing
  - Each interface on every host and router in the global Internet must have an IP address that is globally unique (except for interfaces behind NATs).
    - Internet address assignment
      - Classless Interdomain Routing (CIDR)
        - The 32-bit IP address is divided into two parts and again has the dotted-decimal form a.b.c.d/x, where x indicates the number of bits in the first part of the address.
        - Prefix
          - The x most significant bits of an address of the form a.b.c.d/x define the network address; the other 32-x bits are used to distinguish hosts on the public-IP network portion of the address
        - Hierarchical aggregation (or route summarization), p. 389
          - Using a single prefix to advertise multiple networks.
      - Classful addressing (replaced by CIDR), p. 370
    - Obtaining a host address — Dynamic Host Configuration Protocol (DHCP)
      - Allows a host to be allocated an IP address automatically.
      - Plug-and-play protocol
      - Ideal for situations where many users are coming and going, and addresses are needed for only a limited amount of time.
      - DHCP server
        - Contains a list of available IP addresses on the subnet and IP gw
        - Each time a host joins, the DHCP server allocates an address from its address pool. Each time a host departs, address, each time a host leaves, the address is returned to the pool
        - If no DHCP server is present on the subnet, a DHCP relay agent is required to obtain an address via DHCP server on the main network or neighbor
      - DHCP relay agent
      - For a newly arriving host, the DHCP protocol is a four-step process
        - DHCP server discovery
        - DHCP server offer(s)
          - A DHCP server receiving a DHCP discover message responds to the client with a DHCP offer message that is broadcast to all nodes on the subnet
            - The transaction ID of the received discover message
            - Each DHCP offer message contains
              - The proposed IP address for the client
              - An IP address lease time, the amount of time for which the IP address is valid
        - DHCP request
          - An arriving DHCP client (will choose from among one or more server offers and respond to its selected offer with a DHCP request message, echoing back the configuration parameters.
        - DHCP ACK
          - The server responds to the DHCP request message with a DHCP ACK message, confirming the requested parameters.
      - Once a client receives the DHCP ACK for a request, the client can use the DHCP allocated IP address for the lease duration.
      - Since a new IP address is obtained from DHCP each time a node connects to a new subnet, a TCP connection to a mobile application cannot be maintained as a mobile node moves between subnets
    - A portion of an interface's IP address will be determined by the subnet to which it is connected
      -
      - **Figure 4.17** • Interfaces
    - IP addressing assigns an address to a subnet, (e.g 223.1.1.0/24).
      - On the subnet mask, indicated that the leftmost 24 bits of the 32-bit quantity define the subnet address.
  - IP broadcast address (255.255.255.255)
    - When a host wants to datagram with destination address 255.255.255.255, the message is delivered to all hosts on the same subnet.
  - Network Address Translation (NAT)
    - Realm
      - A realm with private addresses refers to a network whose addresses only have meaning to devices within that network.
    - NAT-enabled router
      - Does not look like a router to the outside world. Instead the NAT router behaves to the outside world as a single device with a single IP address.
      - Hides the details of the home network from the outside world
      - Uses its address from the ISP's DHCP server
      - Runs a DHCP server to provide addresses to computers within the NAT-DHCP-router-controlled home network's address space.
      - How does the router know the Internal host to which it should forward a given datagram?
        - NAT translation table — View both port numbers and IP addresses in the table entries
          - 
            NAT translation table
WAN side
LAN side
138.76.29.7, 5001
10.0.0.1, 3345
138.76.29.7, 5001
10.0.0.4, 3345
138.76.29.7, 5001
10.0.0.3, 3345
138.76.29.7, 5001
10.0.0.2, 3345
10.0.0.1
10.0.0.2
10.0.0.3
10.0.0.4
138.76.29.7
138.76.29.7
138.76.29.7