Chapter 4 Advanced Internetworking

• Routing Areas
  o Motivation: Use hierarchical routing within an AS to improve scalability of routing
  o In link-state routing, a routing domain can be partitioned into subdomains called areas.
    ▪ An area is a set of routers that are administratively configured to exchange link-state information with each other
    ▪ One special area is the backbone area (area 0), whose job is to route traffic between other areas in the domain.
    ▪ A router that is a member of both the backbone area and a nonbackbone area is an area border router (ABR).
  o Routing within a single area
    ▪ All the routers in the same area send link-state advertisements to each other and develop a complete, consistent map of the area
      • A router does not know the detailed topology of other areas other than its own
    ▪ This makes the flooding and route calculation processes more scalable
  o How does a router in one area determine the right next hop for a packet destined to a network in another area?
    ▪ ABRs in area k (k≠0) determine the cost of reaching any network in area k and send this information into area 0.
      • This enables all the area 0 routers to learn the cost to reach all networks in area k.
- ABRs in area 0 then advertise the costs of reaching the networks in area k into other nonbackbone areas.
  - This enables all routers not in area k learn how to reach all networks in area k
- The tradeoff between scalability and optimality
  - When hierarchy is introduced, information is hidden from some nodes in the network
  - Information hiding saves all nodes from having global knowledge. This leads to scalability.
  - However, information hiding hiders the nodes’ ability to make perfectly optimal decisions
  - In large networks scalability is more important than optimality
- IP Version 6 (IPv6)
  - Motivation: deal with exhaustion of the IPv4 address space
  - Changes from IPv4 to IPv6
    - IP address size is increased from 32 bits to 128 bits
      - $2^{128} = 340$ trillion trillion trillion: IPv6 provides over 1500 addresses per square foot of the Earth’s surface (based on the most pessimistic estimates of address assignment efficiency)
    - Header format simplification
      - Some IPv4 header fields have been dropped or made optional to reduce the common-case processing cost of packet handling
    - Improved support for extensions and options
    - Flow labeling capability
    - Authentication and privacy capabilities
- Address notation
  - Standard representation: x:x:x:x:x:x:x:x (x is a hexadecimal representation of a 16-bit piece of the address)
  - Contiguous 0s are compressed, e.g., 47CD::C356:1624 represents 47CD:0000:0000:0000:0000:0000:C356:1624
- Unicast address allocation
  - IPv6 unicast addresses are being allocated from the block that begins with 001
  - The Internet Assigned Numbers Authority (IANA) assigns large address blocks (/23 up to /12) to five Regional Internet Registries (RIRs), which allocate address blocks to Internet service providers
  - As with CIDR, the key idea is to use an address prefix to aggregate reachability information to a large number of networks
    - An RIP assigns an address prefix (e.g., a /32 block) to a provider
    - Then the provider assigns longer prefixes (e.g., /48 blocks) that begin with that prefix to its subscribers
  - Aggregation at the national or continental level
    - E.g., if all addresses in Europe had a common prefix, then most routers in other continents only need one routing table entry for all networks with the Europe prefix

<table>
<thead>
<tr>
<th>001</th>
<th>RegistryID</th>
<th>ProviderID</th>
<th>SubscriberID</th>
<th>SubnetID</th>
<th>InterfaceID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>An IPv6 unicast address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IPv6 Packet format

- 40-byte fixed-length header, simpler than IPv4
- TrafficClass: used to identify and distinguish between different classes or priorities of IPv6 packets
- FlowLabel: used by a source to label sequences of packets for which it requests special handling by the IPv6 routers, such as real-time service
- PayloadLen: number of bytes in the IPv6 datagram flowing the 40-byte header

- The NextHeader field cleverly replaces the Options and the Protocol fields of IPv4
  - An Options field is no longer a part of the standard IP header. This results in a fixed-length, 40-byte header
  - Extension headers may follow the fixed-length header
  - Each extension header contains a NextHeader field identifying the type of the next extension header
  - NextHeader field in the last extension header identifies the higher-level protocol running over IP; it serves the same purpose as the IPv4 Protocol field

- HopLimit: same as TTL in IPv4
- Fragmentation related fields are gone!
  - Fragmentation is handled by an extension header
  - Only source can fragment an IPv6 datagram
• If a router receives a IPv6 datagram that is too big to be forwarded over the outgoing link, the router simply drops the datagram and sends an ICMP error message back to the source
• Removing fragmentation functionality from the routers speeds up IP forwarding
  ▪ Header checksum is gone!
  • IPv4 header checksum needs to be recomputed at every router; removing the header checksum results in faster processing of IP packets
  ▪ Types of extension headers (should appear in following order)
    • Hop-by-Hop Options header
      o Carries optional info that must be examined by every node along a packet’s delivery path
    • Destination Options header (for options to be processed by all nodes whose address appears in the destination address field and in the Routing header)
    • Routing header
      o Used by an source to list one or more intermediate nodes to be visited on the way to a packet’s destination
    • Fragment header
    • Authentication header
    • Encapsulating Security Payload header
    • Destination Options header (for options to be processed by the final destination of the packet)
Advanced routing capabilities

- The routing header contains a list of IPv6 addresses that represent nodes or topological areas (e.g., backbone networks) that the packet should visit en route to its destination
- IPv6 defines an *anycast* address to provide the ability to specify topological entities
  - An anycast address is assigned to a set of interfaces
  - A packet sent to an anycast address is delivered to the “nearest” interface in the set.
- E.g., all routers of a backbone provider could be assigned a single anycast address, which would be used in the routing header

Transition from IPv4 to IPv6

- Dual-stack operation
  - IPv6 nodes run both IPv6 and IPv4 and use the Version field to decide which stack should process an arriving packet
  - The IPv6 address could be unrelated to the IPv4 address, or be the IPv4-mapped IPv6 address (e.g., ::FFFF:128.96.33.81)
- Tunneling
  - Used to send an IPv6 packet over a piece of the network that only understands IPv4
  - Sender and receiver of the IPv6 packet implement dual-stack
  - The IPv6 packet is encapsulated within an IPv4 header