Routing Protocols = Distance Vector, Link State

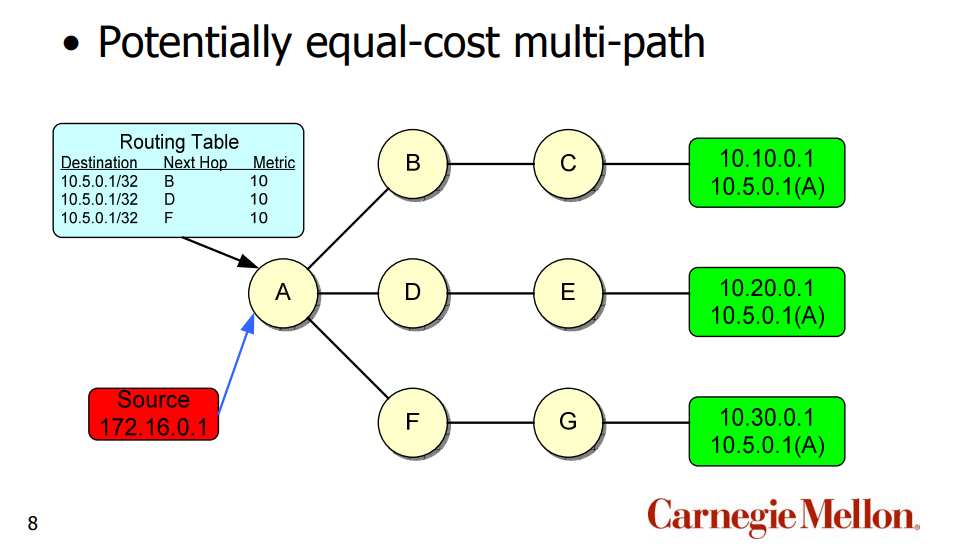
* Distance Vector-
  + Distributed Bellman-Ford
  + Approximated with shortest paths for efficiency and fairness
  + Slow convergence with many exchanges
  + Excellent storage and computation time
* Nodes know only the cost to their neighbors, not the topology
* Nodes can talk only to their neighbors using messages
* All nodes run the same algorithm concurrently
* Nodes and links may fail, messages may be lost
  + Initialize vectors with 0 cost to self, infinity to other destinations
  + Periodically send vectors to neighbors
  + Update vector for each destination by selecting the shortest distance heard, after adding cost of neighbor link
    - Use best neighbor for forwarding
* Link-State Routing-Trades computation for better dynamics
  + Replicated Dijkstra
  + Approximated shortest paths for efficiency and fairness
  + Fast- Flood and compute
  + Moderate storage and computation
* Each node computers their forwarding table in the same distributed setting as distance vectors
  + Node knows only the cost to its neighbors, not the topology
  + Node can talk only to its neighbors using messages
  + Nodes run the same algorithm concurrently
  + Nodes/links may fail, messages may be lost
* Two phases:
  + Nodes flood topology in the form of link state packets
    - Each node learns full topology
  + Each node computers has its own forwarding table
    - By running Dijkstra
* Link failure:
  + Both nodes notice, send updated LSPs
  + Link is removed from topology
* Node failure:
  + All neighbors notice a link has failed
  + Failed node can’t update its own LSP
  + All links to node removed

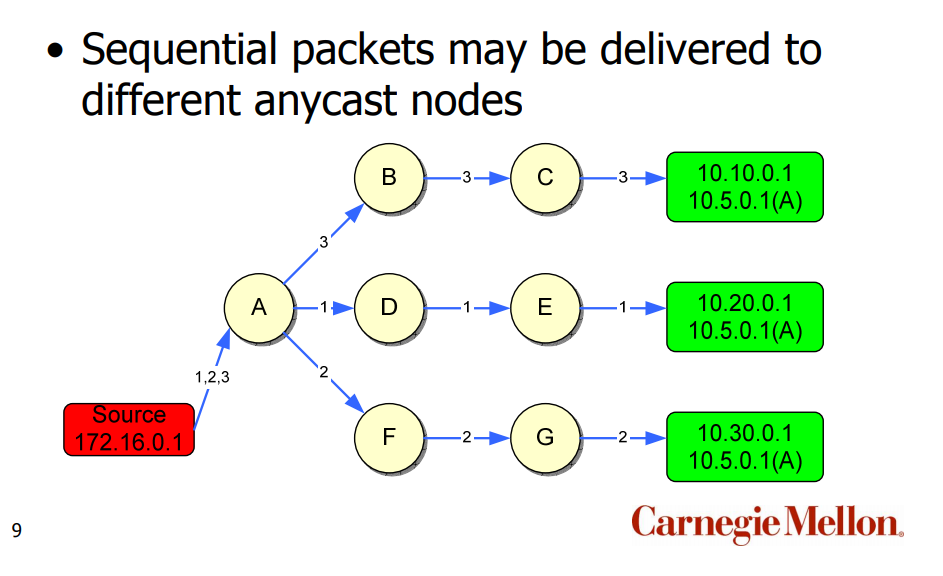
OSPF = default route, route priority, LSA, LSU, LSP, Use of IP Multicast, loop back or Administrative address

* OSPF-Open Shortest Path First
* Default Route-A router generates a default route to indicate itself as the next hop for an external network. This route is injected into the router area.
* Router priority-Determined by the highest router ID. Chooses the most powerful or most idle router so that OSPF converges as fast as possible un der maximum network load conditions
* Link State Announcement (LSA)-Describes the state and cost of the router’s links to the area
  + Flooded throughout the particular area and no more
  + All of the router’s links in an area must be described in a single LSA
* Link State Advertisements (LSA)-OSPF advertises the status of directly connected links
  + OSPF sends updates when there is a change to open of its links and will only send the change in the update
* Link-State Update (LSU)- It communicates the router's local routing topology to all other local routers in the same OSPF area. OSPF is designed for scalability, so some LSAs are not flooded out on all interfaces, but only on those that belong to the appropriate area. In this way detailed information can be kept localized, while summary information is flooded to the rest of the network
* Link State Packet (LSP)- Information generated by a router that lists the router’s neighbors. Determines the names and cost to any neighboring router and associated networks. Used to determine what the new neighbor is.
* IP Multicast-Members of a group will share a group IP Address. Any packet sent to the group IP Address gets forwarded to every router holding the group IP Address.
  + UDP based only. TCP requires a 3-way handshake
  + May lead to out of order delivery
  + Lack of TCP functions means no congestion avoidance
  + May lead to generate of duplicate packets
* Loopback interface-When advertised in OSPF, it will be advertised as a specific host route (with a mask). This forces OSPF to advertise the address with a proper subnet mask
  + If there isn’t a known route, OSPF routers will default to this route
* Administrative Address (Loopback address 127.0.0.1)-Uses the largest matching address
  + Special IP address used for testing network cards.
  + Used to identify the device in a network
  + 3 address 10.10.10.1, 10.10.20.1, 10.10.30.1
    - 10.10.30.1 is the administrative address. If it dies, then 10.10.20.1 is used

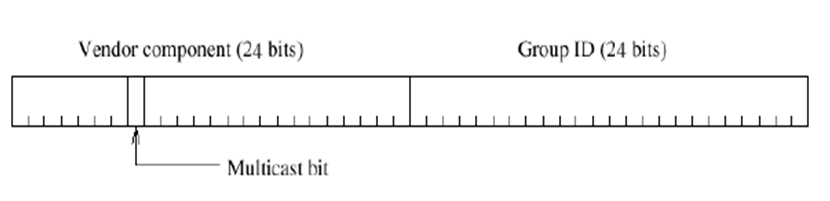
IP Addressing = Unicast, Broadcast, Anycast, IP Multicast, Ethernet Multicast

* Anycast-Multiple nodes are configured to accept traffic on a single IP address
  + Multiple machines share the same IP address
  + The sender uses a routing algorithm to send a packet to the topologically closest node to the sender
  + Anycast addresses usually designed as loopbacks
  + Must maintain a unique management address on each host





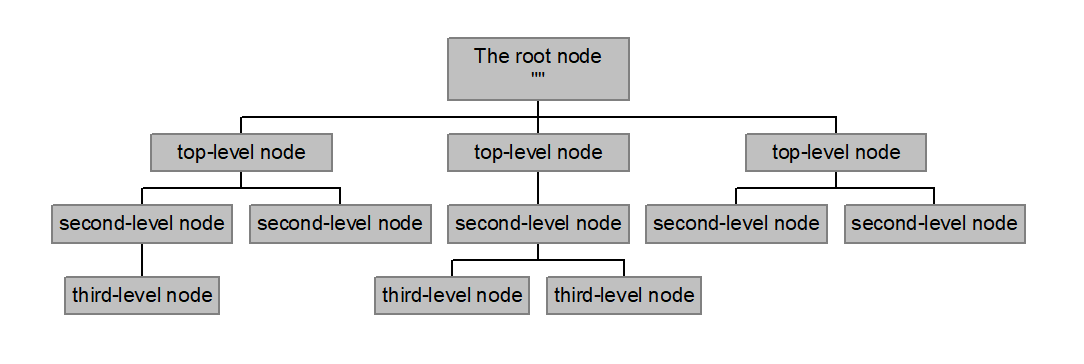
* IP Multicast-A form of One-To-Many communication service between a source IP host and several destinations hosts under a group
  + One sends host communicates with a group of specific hosts
  + Uses class D reserved address spaces
  + Uses IGMP for receive clients to send messages requesting to join a group
* Ethernet Multicast-Unicast packets are delivered to a specific recipient on an Ethernet setting a specific layer-2 MAC address on the Ethernet packet address
  + Broadcast: FF:FF:FF:FF:FF
* Multicast destination IP Address is directly mapped to an Ethernet multicast address
* Because receivers have group IP addresses, they also have a corresponding MAC addresses
* ARP can’t be used for Ethernet multicast, switches work only for unicast
* 48-bit long Ethernet address consists of
  + 24-bit vendor component
  + 234-bit group identifier
  + A multicast bit set if the address is an Ethernet multicast address
* Because switches don’t understand Ethernet multicast addresses, it will flood the frame to all ports
* The system’s Network card (NIC) or operating system has to filter the frames sent on Layer-2 to multicast groups they are not subscribed to
* Use switches that listen to IGMP traffic and maintain a state table that informs which network systems are subscribed to a given multicast group
* This is called IGMP snooping



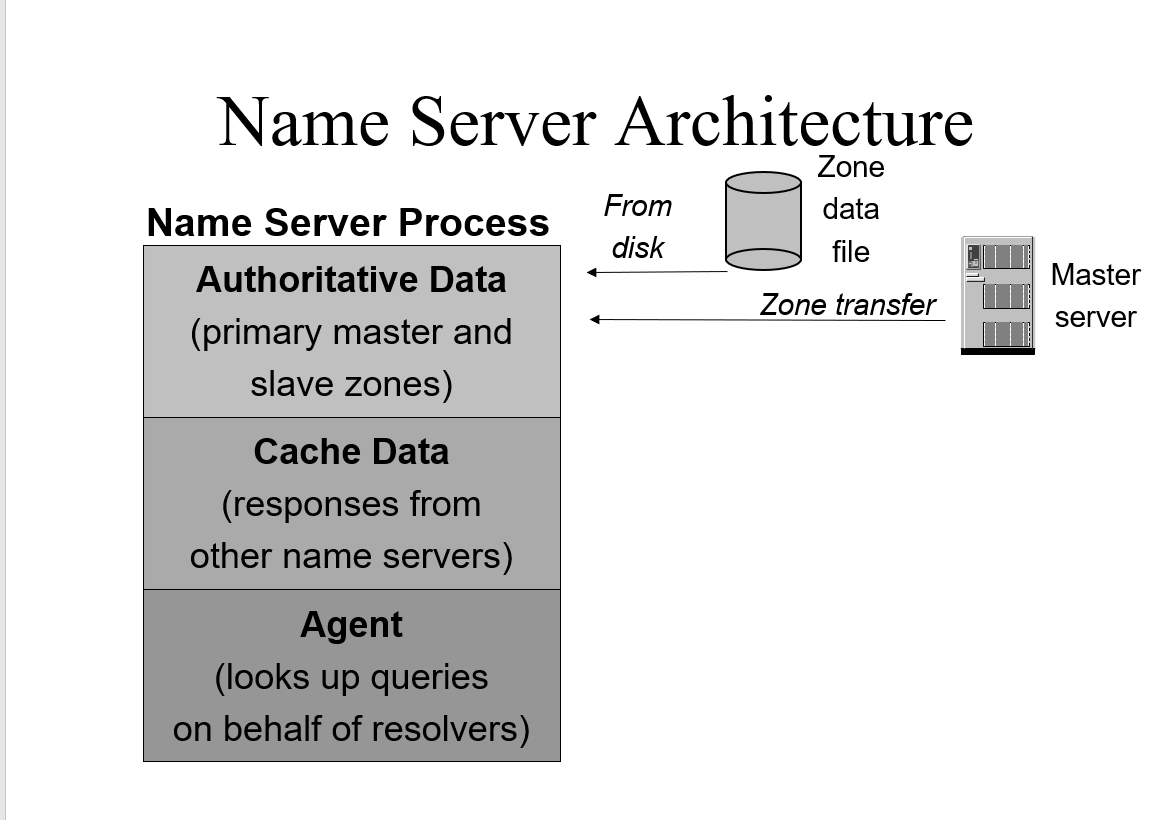
IP Multicast – Dense vs. Sparce mode, DVMRP, PIM, address range

* Protocol Independent Multicast (PIM) – Protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other protocols
  + Not dependent on a specific unicast routing protocol
  + Can use any unicast routing protocols in use on the network
* PIM has 4 multicast distribution scenarios
  + Dense mode-Multicast group members are densely located; that is, many or most of the routers in the area need to be involved in routing multicast datagrams
  + Sparse mode-The number of routers with attached group members is small with respect to the total number of routers; points to set up the multicast distribution tree
  + Bidirectional
  + Source specific multicast
* DVMRP-Distance-Vector Multicast Routing Protocol (DVMRP) – Implements source-based trees with reverse path forwarding and pruning
* Address Range-Multicast uses only class D address ranges
  + Cannot use subnets
  + 224.0.0.0 – 239.255.255.255
  + IP Address has 32 bits, but the first 4 bits are the same (1110)
  + Each multicast IP Address has 28 unique bits

DNS - Name space, Domain Names, domains, subdomains, zones, authoritative servers, reverse lookup

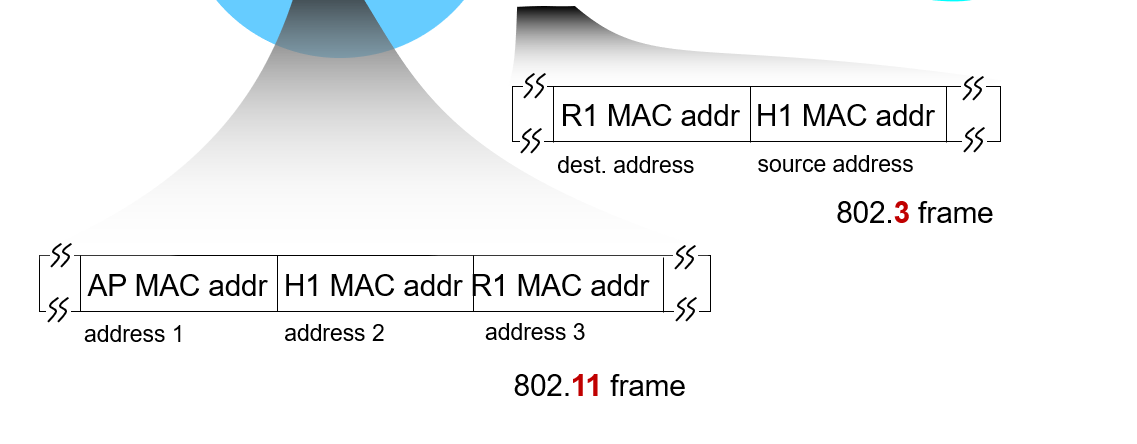


* Name Space-Structure of the DNS database
  + Inverted tree with the root node on top
  + Each node has a label
  + Each label has to be a string of up to 63 bytes
    - A-Z, 0-9, and “- “only with a-z and A-Z treated as the same
  + Sibling nodes must have unique labels
* Domain name-Sequence of labels from a node to the root, separated by dots “.”, read left to right
  + - Maximum depth of 127 levels
    - Domain names are limited to 255 characters
* A node’s domain name identifies its position in the name space
* Subdomains – One domain is a subdomain of another if its domain name ends in the other’s domain name
  + Sales.nominum.com is a subdomain of
    - Nominum.com & com
  + Nominum.com is a subdomain of com
* Zones-Each time an administrator delegates a subdomain, a new unit of administration is created
  + The subdomain and its parent domain can now be administered independently
  + These units are called zones
  + The boundary between zones is a point of delegation in the name space
* Authoritative servers-Servers that maintains data
  + Master – Data is edited
  + Slave-Data is replicated to
  + Caching-stores data obtained from an authoritative server
* Servers are a part of
  + Database server – Answers queries about the parts of the name space it knows about
    - Authoritative data-Primary master and slave zones
  + Cache-Temporarily storing data it learns from other name servers. Responses from other name servers
  + Agent-Helps resolvers and other name servers find data. Looks up queries on behalf of resolvers



* Reverse Lookup-
* Lookup types (NS, A, AAAA)

Wireless/802.11– 802.11 vs 802.3, RTS, CTS, Access Point



* 802.3 frames
  + Uses only Source Address and Destination Address in a layer 2 header
  + Collision detection
* 802.11 frames
  + Collision avoidance
  + Four address fields in the MAC header
  + Uses MAC Addressing
* RTS (Request to send) packets-To avoid collisions, senders will reserve channels rather than random access of data frames. Senders transmit RTS packets to BS using CSMA
  + BS broadcasts clear-to-send CTS packets to respond to the RTS
  + These small reservation packets avoid data frame collisions
* CTS (Clear-to-Send) packets-Sent by the BS broadcasts as a response to the RTS
  + Head by all nodes
  + Sender transmits data frames
  + Other stations defer transmissions
* Access Points-A Base station that a wireless host communicates with

ATM/MPLS – Virtual Circuits vs packet routing, RSVP, RSVP-TE, 1+1 & 1+m backups, label

switching vs routing, LER, LSR, SVC, PVC, circuit setup

* OSPF uses Network-Network Interfaces (NNI)
  + Connects two switches
* User-Network interface (UNI)-Connects ATM end-point to a switch
* ATM Supports QoS guarantees
  + Traffic contract: Intended data flow
  + Traffic Shaping-Constrain data bursts
    - Takes the data burst from the user and smooths it out
  + Traffic policing-The Switch measures the actual traffic and compares it to the contract
    - Notifies other switches that the package can be dropped in periods of congestion
* Virtual Circuits-A means of transporting packet-switched networks in a way that it looks as though there is a physical link between the source and destination
  + Combination of packet and circuit switching
  + Logical circuit between source and destination
  + Every virtual circuit is identified by a VC ID
  + Source set-up will establish the path for the VC
  + Switch will then map the VC to an outgoing link
  + Packet will have a fixed length label in the header
* IP Routing-Path to destination is determined by destination address alone
* Packet Switching:
  + Data is divided into packets
  + Each packet contains its own header
  + Destination reconstructs the message
* Circuit Switching
  + Source first establishes a connection to the destination
  + Source sends data over the connection
  + Source tears down the connection when done
* Resource Reservation Protocol (RSVP)-An end-to-end protocol that allows a host in a network to reserve resources to get a guaranteed quality of service
  + Reservation to set up a circuit
* Resource Reservation Protocol with Traffic Engineering (RSVP-TE)-Used to reserve bandwidth across the network and reserve resources
  + Looks for the shortest path with enough available bandwidth to carry a particular LSP
  + If available, the LSP is signaled across a set of links
  + The LSP bandwidth is removed from the available bandwidth pool
  + Future LSPs may be denied if there is insufficient bandwidth
  + Will be routed to another path even if latency is higher
* 1+1 – For every circuit set up, there will be a backup set up
* 1+m- - Sharing multiple routes under the assumption that there is always a backup prepared
* Label switching vs. routing
  + Label Switching:
    - Traditionally, label switching is when two phone lines were plugged into a circuit to directly connect to each other
    - IP datagrams use destination IP address
    - VCs must signal along the path
    - Routers in VCs also know about connections
* Why is label switching more efficient?
  + Reduce overhead for router lookups
  + Support virtual circuits
  + Better network consolidation
  + IP routing has to perform an IP lookhop for every network hop in order to find the next network destination
  + Label switching precomputes backup routes in case of link failure
  + Label switching has the first hop detect the final destination first before applying a label for that route so that future routers know where to forward a packet to in the future
  + This reduces the overhead of discovering the next router

IP Multicast and Ethernet Multicast are not different

What does MPLS provide that OSPF doesn’t

* OSPF runs on IP routing protocols where the path to destination is determined by destination address alone
  + Uses labels to direct data from one network element to another
  + MPLS uses network packets to switch traffic
  + Establishes a dedicated path
  + IP Datagrams use destination IP address
  + VCs must signal along the path
  + Routers in VC know about the connection
  + First device in the routing lookup detects the final router in the path rather than the next hop
  + Uses labels to inform future routers to apply this label to route the traffic
  + Removes the need to do any additional IP lookups
  + Precomputes backup routes in case of link failure
* MPLS routing is based on source and destination address
  + Runs on top of IP
  + Traffic is based on destination IP Address alone
  + MPLS can be paired with Traffic Engineering
    - MPLS forwarding decisions will use routing that flows to the same destination different
    - Take the uncongested path even if the latency could be higher rather than congest the shortest path on one link while leaving available bandwidth unused on another link
    - Using RSVP-TE to reserve bandwidth across a network for guaranteed service
  + Fast rerouting protocol where a backup path is used if a failure occurs
  + MPLS is used for consistency and guarantee of service
    - Mostly used by TV stations that want guaranteed bandwidth to support their service
    - Has to be paid for upfront
* Traffic Engineering
  + Starts with routers establishing local links
  + Requires hardware support
  + MPLS with no tunnel gives no guarantees
  + With traffic engineering gives guarantees
  + An MPLS traffic engineering sets up a tunnel where the service is guaranteed to work
  + To reduce congestion, takes burst of packets and smooths out the distribution