Broadcast Propagation and Packet forwarding process:

- Broadcast propagation: When broadcast are transmitted to all host within the source of host subnet by another host basically packets

- Device checks if packet destination is part of local subnet.
    - If packet destination/end point is part of local subnet then the will go to network switch where it will be propagated around the local subnet
    - If not then → operating system will evaluate the subnet mask using and + or operations to find to the official destination network address
    - The packet will be sent to router:
- **Routers:**
    - Located in each subnet and are referred to as the default gateway they are responsible for forwarding traffic outside local subnet or forward packets from one network to another
    - The packet is sent to the router in its local subnet
    - The router will decide where to propagate packet based on destination IP address
    - One Router interfaces (ports) must belong to different IP subnet since the whole point of router is to send packets outside the network ***Refer to Tutorial for sense

Principals/Process of routing packeting between networks:

- Router/Devices make decision alone based on its own routing table
- If One router has info in its routing table doesn't mean others router will have the same info in its *routing table*
- The Routing info about a path from one network to another does not provide the info about the reverse, or return path

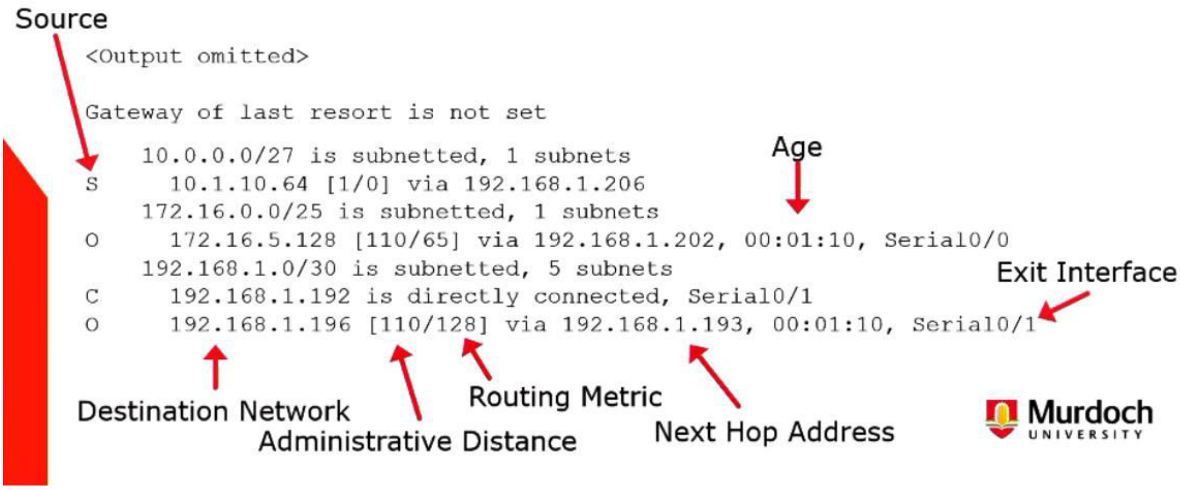
Routing Table:

- Every device that operates at layer 3 will have some sort of routing table
- Maps of known possible destination networks (or Ip network that devices knows about)

- When Packets that have multiple routes matches for destination IP address, the route with the longest number of bits that match is selected ****LOOK UP LECTURE FOR MORE INFO ON HOW TO MATCH**

- When Packets that doesn't have any matches on the routing table is sent to default gateway or is dropped (if no default gateway or destination IP)

Attributes of Routing Table:



- **Source:** how it is routed: Static route = s Connected route = c o: ospf
- **Destination Network:** Ip where we know how to reach or where the packet will end up
- **Next hop address:** how we are going to route the packet/Path packets takes
- **Age:** last confirmation
- **Exit interface:** which router interface we are going to send packet from
- **Metrics:**
  - Used by various routing protocols to determine the best route and works out the cost
    - Includes- hop count, bandwidth, delay, load
- **Administrative Distance:** each source is given an administrative distance and usually the lower number the higher priority.

When a router first boots up it only have the routing info about directly connected networks.

So in order to **acquire route info of remote networks use two techniques:**

Static Routing:

- The process where the static routes is easily manually configured by network engineers
- Static Routing is ideal for small networks with limited redundancy
- Contains **default route** and this route tells where packets should be propagated when no specific route is configured (default gate way may be one)
  - IF no default route then packets dropped

Configuration/components of static routes: (might not be in exam)

- Destination network
- Subnet mask (of destination network)
- Next hop ip address
- Exit interface (only when using point to point links)

Advantages

- Gives maximum control over how packets will be routed or the overhead of routing protocols are to be avoided
- If there is only one path to the destination the static route will use optimum path
- Simple to implement

There are many advantages of static routes over a dynamic routing protocol. One of the reasons is that it is good for security and maximum control because of how packets gets propagated around a network. But if more devices and routes needs to be implemented than static routes are not advised. For small organisations such as an office a static routing is more than enough and it has the benefits of routers not sharing static routes with each other therefore making cpu overhead less and saving bandwidth.

Disadvantages

- Poor scalability labour intensive as network grows since you have to manually config
- Difficult to predict consequences of installing new route like packet speed or traffic
- Not adaptable to changes in the network since routes must be manually updated

Dynamic Routing:

- Dynamic routing is when **dynamic routing protocols** are used to propagate routing information throughout network and update routing tables
  - Makes routers aware of all networks directly connected too. (static) Not tell router the specific networks it needs to reach
- Determines best path to a given destination w/o human intervention

Steps/Process/How it works for Dynamic Routing:

- Discover remote networks
- Update the routing information
- Find the best path to destination networks and install this info in the routing table
- Find out alternative paths to destination networks if link failure occurs
- They don't make forwarding decisions they look at routing table (opposite to static)

Structure (Remember before going deep end to put in context)

Dynamic routing Protocols:

Interior Gateway Protocols:

- Distance Vector Routing Protocol:
    - Routing Information protocol (RIP):
    - Enhanced Interior gateway routing protocol (EIGRP)
- Link state routing protocol:
    - Open Shortest Path First (OSPF)

Exterior Gateway Protocols

- Border Gateway Protocol (BGP)

Types of **dynamic routing *protocols*** used to propagate routing info throughout network

Interior Gateway protocol: are used to route within an administrative domain (think inside single organisation/Autonomous system not between two) **Classes-**

- **Distance Vector Routing Protocol:**
  - Entire Routing table is *periodically* broadcasted to all neighbours (think send info to router one after another like Chinese whispers)
  - Each router has limited or incomplete view of network
    - Therefore low memory (As router just advertise their routing table)
  - What it does is router learns about routing table based on what they receive from neighbours

  - **Uses:** Bellman ford algorithm that determines the lowest cost (in terms of hops not money) of routes from router to router (Year 12 shortest path of nodes/routers)
    - **If** router links are down then distances table will change and if it comes back up distance table will change

  - **Examples** of Distance Vector Routing Protocols:
    - **Routing information protocol (RIP):**
      - Simple routing protocol that uses hop count as metric (think less hop counts the better)
      - Updates distance table periodically every 30 seconds, but includes support for triggered updates
      - Uses split horizon and poison reverse to prevent loops
    - **Enhanced interior gateway protocol (EIGRP)**
      - Dual algorithm
      - Includes enhancements usually associated by link state protocols (removal of periodic updates)

- **Link state Routing Protocol:**

  - Establish relationship with all other routers. (think each router knows about every router in network)
  - Routers will therefore have a complete view of the network, knowledge of entire topology
    - Therefore, uses high memory (to remember network)
  - Each router works out shortest path to destination therefore to make cost efficient
  - Uses Link state advertisement to propagate information by creating a database of information of all routers

  - **Uses:** Dijkstra algorithm

  - **Examples** of Link state routing Protocols: OSPF (next Review)

Exterior Gateway protocol:

- are used for routing packets systems between **autonomous systems** *(think Between two or more organisations/Autonomous system)*
- Routers involved in external routing will usually be owned by different organisations
- Have knowledge of whole internet routing table

Autonomous system:

- AS is a group of routers that share similar routing policies and operate within a single administrative domain
- Only large organisation would have own AS- ISP, university, government
- Every Autonomous system is assigned a unique number

	Distance Vector	Link-State
Message complexity	Exchange entire routing table between neighbours	Flood link-state advertisements throughout network
Robustness / Accuracy of path cost	Errors by one router can propagate throughout network	Each router computes its own table
Resource requirements	Low (just use advertised routing tables)	High memory and CPU requirements (compute own routing table)
Convergence	Slow (unless triggered updates available	Fast

Routing protocol terminology:

- **Convergence:** describes a state where the routing table for all routers are consistent
- **Metrics:** are used by routing protocols to determine the best route (think how good a path is) eg
  - Hop count
  - Bandwidth