1. Describe the dynamic alternative routing system.

   Dynamic Alternative Routing is a form of randomised routing used in telephone networks.

   Initially, a direct route (*i.e.* of path length 1) is offered. If this is unavailable, then the algorithm will offer a randomly selected path of length 2. If this path is full, then then router will randomly choose another path. This is a provably optimal way of routing using randomness allowing maximal utilisation of circuits.

2. Compare and contrast intra-domain routing with inter-domain routing. Explain why distance vector routing is used for inter-domain routing and link state routing is used for intra-domain. Why can't they be used the other way around?

   Definition 1 (Autonomous System)**.** A subgraph of the network which has been assigned its own Autonomous System Number and can set its own network policy. These are usually controlled by one organisation.

   Definition 2 (Policy Based Routing)**.** Routing where the goal is to *find a good route* which conforms with arbitrary and complicated *business relations* rather than necessarily the best possible route

   Definition 3 (Information Hiding)**.** A situation where parties on the network are not willing to share all their information with each other because *i.e.* they are in competition or do not want to reveal details about their internal infrastructure *etc.*

Intra-domain routing	Inter-domain routing
routing within a single AS	routing between ASs
full information	information hiding
"best path" routing	policy-based routing
smaller network	internet scale network
shared distance metric	many distance metrics

Table 1: Comparison of intra-domain and inter-domain routing

Link State routing is used for intra-domain routing because:

- it allows the networks to get the best routes globally – rather than just some approximation
- routers can use arbitrarily complicated routing distance metrics
- fast recovery

Distance Vector routing is used for inter-domain routing because:

- it allows the aggregation of ASs into a single node on the network
- it supports information hiding
- it (mostly…) allows routing to respect business relations
- it scales well

Link State routing shouldn't be used for inter-domain routing because:

- it scales poorly: nodes have to flood the network and this doesn't work if "the network" is the whole internet!
- it does not support information hiding
- the whole internet would have to agree on a single unified routing metric to avoid looping: this is impossible at internet-scale

- does not easily support policy-based routing

Distance Vector routing shouldn't be used for intra-domain routing:

- it has long convergence times
- it can only use additive routing metrics
- slow recovery *c.f.* count-to-infinity problem

3. Describe how reverse path forwarding works in multicast. Explain how it ensures you find the shortest path.

   Reverse path forwarding is a method of flooding a network used in multicast routing. The overall goal is for every node to receive a message and to minimise the number of messages sent on the network.

   When router C receives a message from router A via router B: if B is on the shortest path from A to C, then C will forward the message on all interfaces (except the interface to B). Otherwise, C will not forward the message. This means that every node will receive exactly one copy of the message – and it will be from the shortest path from the sender.

4. Explain what is meant by pruning.

   Pruning is a way to reduce the number of messages which are sent across a network in multicast routing. When pruning, children tell their parents when they have no child that is in a particular group. This means that the parent no longer forwards messages for that group. The result is that messages for a particular group are no longer sent to all LANs on the AS: just to those which have members in the group.

5. Briefly describe 3 more multicast routing protocols.

   - Distance Vector Multicast Routing Protocol (DVMRP)

     DVMRP is a distance-vector based protocol which implements multicast routing. It uses reverse-path-flooding with pruning. This is very similar to DVMRP.

   - Multicast Open Shortest Path First (MOSPF)

     This is a multicast extension to OSPF. Rather than flooding group information separately, it adds information to link state updates. Multicast-capable routers then compute a forwarding table for each group. Using IGMP, routers know whether there are any nodes to which they are connected which are in the group. This information is put into the messages. Thus we get the same effect of pruning for free. However, this adds a lot of state to the rest of the network.

   - Protocol Independent Multicast (PIM)

     PIM is an efficient method of multicast. It has two modes:

     – Dense Mode PIM

       This is a reverse path forwarding with pruning protocol. This is acceptable when a high proportion of nodes in the network are in the group.

     – Sparse Mode PIM

       This is a Centre-based multicast routing algorithm. Each group has a dedicated Rendezvous Point (RP). This is an arbitrarily chosen router in the network. Any sender will send the RP any messages they want to forward. All routers who have receivers in the group will send messages to the RP saying as much. Thus the RP keeps track of all the nodes in the group and will forward any messages it receives for the group to them all.

6. What does it mean to say that fibbing introduces fake nodes into the control plane? How does that help?

   Fibbing is a way of augmenting a link-state routing protocol which allows centralised control and allows efficient implementation of *i.e.* backup links, load balancing, differentiated services *etc.* In fibbing, there is a set of centralised controllers. Each of these listen to the network, and find augmentations to the topology which would cause packets to take preferable routes. They then "fib" and advertise fake link costs from virtual nodes which encourage the network to use preferable routes which cannot easily be expressed in a distance metric. These fibs can either be local (only seen by one node) or global (seen by every node on the network). Any set of forwarding DAGs can be enforced by fibbing.

   All other nodes in the network use "normal" link-state routing to decide where to send packets. Introducing virtual nodes into the network has the effect of encouraging them to send ways which are not usually optimal. This allows the controller to force arbitrary forwarding on their network. This allows networks to have arbitrary forwarding policies which cannot be expressed in a distance metric that could be used for link state routing *i.e.* messages to these datacenters should go via the high capacity link even if it's slower; *even though* messages to the interactive server physically close to it should go the same route. Fibbing can implement either fail-open or fail-closed semantics.

   Definition 4 (Fail-Open Semantics)**.** On the failure of the central coordinator, the network should continue working; in this case it should revert back to link-state routing

   Definition 5 (Fail-Closed Semantics)**.** On the failure of the central coordinator, the network should stop completely.

```
# rib is the routing information base
rib = None
# requirements are set in some arbitary way
requirements = ...

while True:
    # event manager
    new_rib = listen_to_network()

    if new_rib != rib:
        forwarding_dags = compile_requirements(requirements)
        topology = compute_augmented_topology(forwarding_dags, rib)
        topology = optimize_topology(topology)

        for fib in extract_fibs(topology):
            if fib.type == local:
                send(fib.dest, fib)
            else: # fib.type == global
                broadcast(fib)

    # refresh fibs before they expire
    if validity_timer_running_out():
        resend_fibs()
```