TEKNILLINEN KORKEAKOULU
Tietoverkkolaboratorio
S-38.121 Reititys tietoliikenneverkoissa
Nicklas Beijar

Examination 4.11.2002
Model solutions and grading

Vastaa lyhyesti viiteen (5) kysymykseen.
*Give brief and concise answers to five (5) questions.*

**Question 1**

Mihin vaikutusgraafia tarvitaan? Anna käyttöesimerkki.
*For what is an influence graph needed? Give an example of the use of the influence graph.*

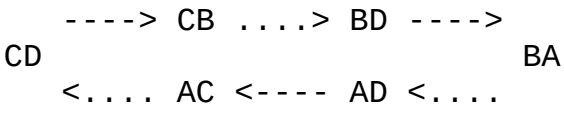
**Answer 1**

The influence graph is mainly used to check for cycles in routing. In SOC routing, the routing decisions are only based on the state of the links adjacent to the node that the call has reached. Thus, generally there exists a possibility that the routing will enter a cycle. The influence graph provides a systematic way to detect cycles. Standard methods of graph theory can detect the cycles in the influence graph. (2p)

The influence graph can also detect mutual overflow, where one link i receives calls from another link j, which in turn receives calls from link i (from another traffic stream). (1p)

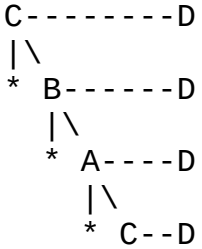
The influence graphs are also a basis for discussing the notation of order in a network, and for numerical algorithms for certain types of networks. (extra ½p, not required)

Example influence graph with loop:




(2p for a correct influence graph. the graph or the attached description should show how loops are visible)

Generated from the route tree:



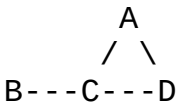
(1p for the corresponding route tree. although not asked, this is required, since otherwise it is not possible to check which network the influence graph describes)

**Question 2**

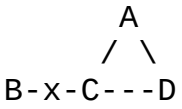
Näytä esimerkin avulla tilanne, jossa RIP joutuu laskemaan äärettömään.
*Show an example situation where RIP must count to infinity.*

**Answer 2**

Assume the network:




The link B-C breaks. The problem happens only if the network is split into two parts. (1p)




Node C updates its distance C→B to infinity. RIP uses poisoned distance vectors. Node C then generates its distance vector and sends it to B and A. The situation stabilizes if A and D correctly receive the distance vector. However, if the message sent to D is lost, only A receives the distance vector. Then D sends its poisoned distance vector and A updates its distance A→B to 3. When D sends its poisoned distance vectors, C updates its distance C→B to 4, and a three-node loop has been generated. Packets send to B will loop between C, A and D. (2p)

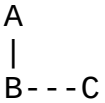
The problem happens if a message is lost or because of timing problems (2p).

On the following update, D updates its distance D→B to 5. Then A updates A→B to 6, and so on. Thus, on each round of updates, the distance increases by 3. This is repeated until the distance reaches the maximum value, that is infinity (=16). (1p)

Alternative

The following example is only correct if poisoned distance vectors are **not** used. Although RIP uses poisoned vectors, points have also been given for a solution without poisoned distance vectors.

Assume the network:




The link B-C breaks. The problem happens because the network is split into two parts. (1p)

A
|
B-x-C

B updates its distance B→C to infinity. The situation stabilizes if B sends its distance vector to A before A sends its distance vector to B. But if A sends its distance vector (A→C distance 2) first, then B updates that its distance to C is 3 through node A. A loop has been created. Packets send to C will loop between A and B. (2p)

The problem happens because of the timing or if a message is lost. (2p)

When B sends its distance vector to A, node A updates that its distance to C is 4 through node B. Then, when A sends its distance vector to B, node B updates that its distance to C is 5 through node A. Thus, on each round of updates, the distance increases by 2. This is repeated until the distance reaches the maximum value, that is infinity (=16). (1p)

(Grading: 6p for a working example, where RIP starts counting to infinity: 2p for the general description of the example, 2p for mentioning timing or packet loss as the cause of the problem. 1p for mentioning that the network must be split into parts, 1p for describing what happens when counting to infinity. Only some few noticed that RIP uses poisoned distance vectors – no points are removed for not observing this)

**Question 3**

Kuvaa OSPF:n osa-protokollat. Selitä naapuruuskäsite OSPF:ssä.
*Describe the subprotocols of OSPF. Explain the concept of neighborhood in OSPF.*

**Answer 3**

OSPF has three sub-protocols
1. Hello protocol
   - Ensures that the link is operating (1p)
   - Selects the designated router and backup designated router (1p)
2. Exchange protocol (1p)
   - Synchronizes the databases using database description. When a node receives information about an entry that is newer than its own corresponding, it requests the new entry.
3. Flooding protocol (1p)
   - Sends incremental updates when topology changes and refreshes entries from timing out

(Grading: lower points are given if only protocol names are given without description or with too simple description. 1/2 p minus for every wrong name (some variation in Finnish translations accepted). Extra ½p if the messages are included (not required))

In the hello message, a node lists the neighbors that have sent hello messages during the last dead interval seconds. The hello message is sent over one hop. A link is considered operating (bi-directional) if the node **sees its own address** in the hello message send by the neighbor. (1½ p)
In a broadcast network, the nodes are only neighbors with the designated router. (1/2 p)

**Question 4**

Selitä topologian aggregoinnin periaate PNNI:n loogisen solmun avulla.
*Explain how topology can be aggregated in PNNI using the concept of a logical node.*

**Answer 4**

Using aggregation, the topological information can be reduced, so that the protocol scales to large networks (even including all ATM nodes in the world). The topology is accurately described for the surrounding nodes, and the accuracy decreases for nodes farther away. (Extra 1p for describing the purpose of aggregation)

PNNI builds up the topology of the network recursively from the bottom to the top. The nodes with a common address prefix form a peer group. The peer group is seen as a logical node at the higher hierarchical level. At the lowest level, the nodes are physical nodes (switches). (2 p) (This may be described using a drawing)

In each peer group (except at the top level), a node is selected as the peer group leader (PGL), which represents the group at the following level. (1 p). The PGL collects the topology of its peer group, aggregates it and distributes it in the upper-level peer group. Is also distributes topology information from higher levels within its peer group. (1 p)

The peer group is described as a logical node using the complex node representation. The inside of the peer group is modeled as a nucleus. Spokes represent link connections from the nucleus to other logical nodes. An exceptional connection between two neighboring logical nodes can be modeled as a bypass. (2 p) (This may be described using a drawing)

**Question 5**

Kuvaa PIM-SM:n ja PIM-DM:n toimintaperiaatteet. Missä tilanteessa käyttäisit PIM-SM:ä ja missä tilanteessa PIM-DM:ä? Miksi?
*Describe the operating principles of PIM-SM and PIM-DM. In which situation would you use PIM-SM and in which situation PIM-DM? Why?*

**Answer 5**

PIM-SM uses the center-based algorithm. The receiver sends a join message to the rendezvous point (RP). Senders send packets to the RP, which distributes the packets along the shared multicast tree. (2p)

PIM-DM uses the Reverse Path Forwarding (RPF) (or “flood and prune”) algorithm. The first packets are flooded to the whole network. Branches without members are pruned. When the prune state times out, the packet is flooded again. (2p)

PIM-SM (sparse mode) is suited for sparse multicast groups (= few members per area), PIM-DM (dense mode) is suited for dense multicast groups (= many members per area) (1p)

PIM-DM floods the whole network regularly with packets, and the routers must keep state for all groups and senders. This is good if most of the routers have receivers, but it does not scale in large

networks where the distance between members is long. On the other hand, PIM-SM uses a central RP. The traffic is contained to the multicast tree. In large dense networks, it is often difficult to place the RP to obtain maximum performance. The RP may also be congested in groups with many joining sources. (1p)

## Question 6

Miten ennakoivat (proaktiiviset) ja reagoivat (reaktiiviset) reititysmenetelmät eroavat toisistaan? Kuvaa, miten reagoiva reititysprotokolla muodostaa reitin. Nimeä kaksi reagoivaa reititysprotokollaa, ja selitä lyhyesti miten pakettien lähetys tapahtuu niissä.
*How do proactive and reactive routing methods differ? Describe how a reactive routing protocol creates a route. Name two reactive routing protocols, and describe briefly how packets are sent in them.*

## Answer 6

In proactive routing, the routing tables are generated before the packets can be sent. A routing protocol generates and maintains routes to all hosts in the network. In reactive routing, the route is generated when it is needed. Routes are generated and maintained only between active senders and receivers. (2p)

Reactive routing protocols flood the network with a route request packet. The destination or an intermediate node with a route to the destination replies. The reply travels the reverse path to the requesting node. Gererally the whole network is flooded, but if expanding ring search is used, a reply can be gerenated when the destination is reached or if some node has a valid route to the destination. (2p)

Dynamic Source Routing (DSR). The data packets contain the source route. The packet travels through all nodes in the source route. No state needs to be maintained by intermediate nodes. (1p)

Ad-hoc On-Demand Distance Vector (AODV). The intermediate nodes store the next hop information (distance vectors) for the routes that goes through them. (1p)

(Grading: 1/2p for a name of a reactive protocol and 1/2p for the description of it. ZRP is accepted as an example protocol if there is a description that is is only partially reactive. ZRP however gives maximum 1/2p since it is not a pure reactive protocol)

## General grading principles:

Node that this document only describes the grading principles. The model solutions describe the main points that were expected to be included in the answer. It is not a strict requirement list. A good answer must clearly show that the subject is understood.

Generally small errors do not decrease the points. Serious errors decrease the points. Some extra information **related to the question** may give small extra points.