TEKNILLINEN KORKEAKOULU
Tietoverkkolaboratorio
S-38.121 Reititys tietoliikenneverkoissa
Nicklas Beijar

Tenttikysymykset 3.11.2003
Examination

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

Question 1

1. Solmut A, B, C ja D muodostavat täydellisesti silmukoidun verkon; solmu E liittyy A:han ja C:hen. Kuvaa käyttäjän kannalta optimaalinen reititys B:stä D:hen täydenneteyllä väylöistyspuulla.
   The nodes A, B, C and D form a completely connected network; node E connects to A and C. Describe, from the user's point of view, the optimal routing from B to D using an augmented routing tree.

From the user's point of view, the routing is optimal when loss is minimal and quality is maximal. To reduce loss, all possible routes should be included. To increase quality (e.g. delay), the shortest routes should be preferred.

Further, to reduce loss, cranckback should be used (only a loss node from the originating node). (-1p if loss nodes from other nodes)

The resulting augmented routing tree is:

```
    E  (1p)  B------D   (5p)
   / \       |\\
  A---C      *| C--D
  |\ /|       | |\
  | X |       | | A--D
  |/ \|       | |
  B---D       | E--A--D
              |
              A--D
              |\
              | C--D
              |
              E--C--D
```

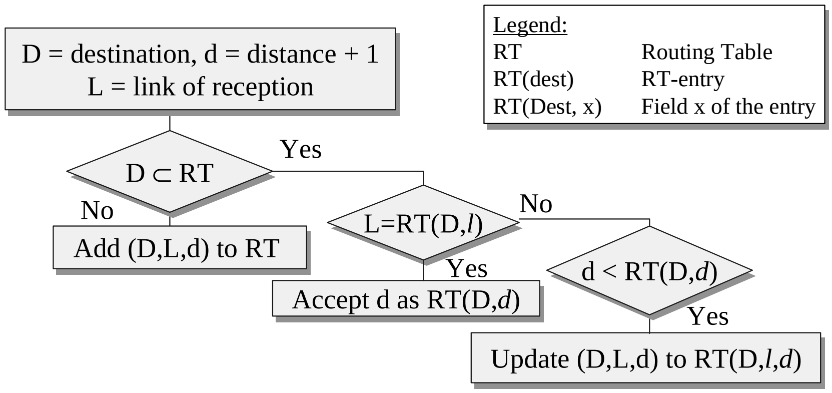
-2p if not augmented (loss node missing)

-1/2p per missing/impossible route alternative if only a few

Question 2

2. Kuvaa etäisyysvektoriprotokollan vastaanottoalgoritmi. Kuvaa etäisyysvektoriprotokollan toimintaperiaate pienen esimerkkiverkon avulla (verkossa ei ole vikoja ja kaikkien linkkien painot ovat 1).
   Describe the reception algorithm of a distance vector protocol (3p). Describe the operational principles behind the distance vector protocol using a small example network (there are no faults in the network and the weight of every link is 1) (3p).

Processing of Received Distance Vectors



Note: this is simplified, shows only the principle!

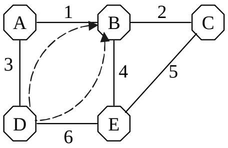
NB: The routing table is also updated if the node receives a distance vector with higher distance than the previous entry, if it is received on the same link as the previous entry. One minus point (–1p) given if this is not mentioned.

NB: The cost of the link is added to the distance in the received vector. One minus point (–1p) given if this is not mentioned.

Question 3

3. Mitkä ovat pakettiliikenteen vaihtoehtoisille poluille jakamisen edut ja haitat tai hankaluudet? Mitä useiden etäisyysmittojen (viive, kapasiteetti, jne) käyttö edellyttää?
   What are the benefits and drawbacks or difficulties of using alternative routes for packet traffic? (3p) What is required for using several metrics (delay, capacity, etc)? (3p)

Spreading load to alternative equidistant paths improves network efficiency



+ Queues in nodes become shorter

+ Average delay is decreased

+ End-to-end jitter decreases

+ Less traffic to reroute under failure conditions

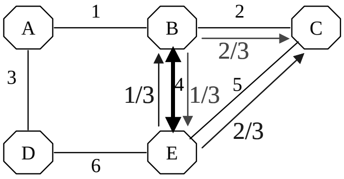
- May change packet order because paths may have different delay (queue lengths in nodes)

- Existing traffic can not be pinned down to primary path so that only overload would take the alternative path ⇒ stability is a problem

? When are paths equidistant enough?

When are paths equidistant enough?

- What happens if the traffic to C is divided between two alternative paths?



⇒ The packet to X can be sent through Y is Y is closer to the destination than the local node

- Rule A→Y...→X, if distance(Y→X) < distance(A→X) accepts only monotonic alternative routes

Using several metrics (1)

Using several metrics requires:

- Metrics must be stored for each link (***L.cost1***, ***L.cost2*** ...)
- The protocol must carry all metrics
- Computing separate routing tables for each metric (***P***(***cost1***), ***P***(***cost2***) ...)
- User packets must be marked with the required metric.

Required for a):

- improved network efficiency / load distribution (1p)

- lower delay / jitter / shorter queues (1p)

- less traffic to reroute on failure / error resistence / alternative paths (1p)

Required for b):

- separate routing tables for each metric / all metrics must be configured for each link and protocol carries all metrics / protocol must support metrics (e.g. OSPF) (1p)

- packets market with used metric, otherwise loops can occur (2p)

Question 4

4. Luettele OSPF:n osa-protokollat. Kuvaa lyhyesti jokaisen osa-protokollan tehtävät ja toimintaperiaatet.
   List the sub-protocols of OSPF. Describe shortly the tasks and operational principles of each sub-protocol.

2p for each correctly named, and described sub-protocol (½p for the name, ½p for the task, 1p for the description)

Hello protocol (½p) is constantly running

- ensures links are working (½+p) bidirectionally
- selects designated router (½p) and backup dr (+)

Database exchange protocol (½p) runs when a new link is activated

- syncronizes link databases (½p)
- master-slave selection, database description packets (½p)
- differing records requested (½p)

Flooding protocol (½p) constantly refreshes the information

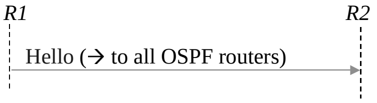
- floods updates to the whole network (1p)
- every node forward LS updates on every link (½p)

Summary of OSPF subprotocols

	Hello (1)	DD (2)	LS rq (3)	LS upd (4)	LS ack (5)
Hello protocol	X				
Database exchange		X	X	X	X
Flooding protocol				X	X

Server Cache Synchronization Protocol (SCSP) is OSPF without Dijkstra’s algorithm and with more generic data objects.

Hello protocol ensures that links are working and selects designated router and backup DR

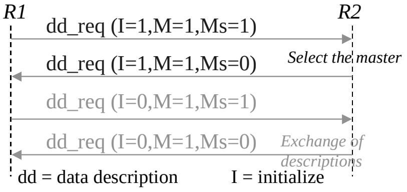


OSPF packet header type = 1		
Network mask		
Hello interval	Options	Priority
Dead interval		
Designated router		
Backup designated router		
Neighbor		
- - -		
Neighbor		

- Neighbors – a list of neighbors that have sent a hello packet during last dead interval seconds.
- Hello interval tells how often in seconds hello packets are sent.
- Priority tells about eligibility for the role of designated router.
- A hello packet must be sent in both directions before a link is considered operational

- Options
  - E = external route capability.
  - T = TOS routing capability.
  - M = Multicast capability (MOSPF).
- DR and Backup DR = 0 if not known

Exchange protocol initially synchronizes link DB with the designated router (1)



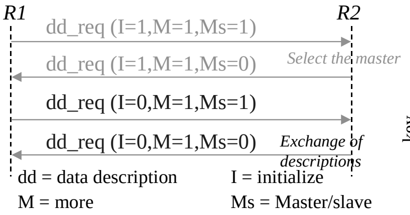
dd = data description
M = more
I = initialize
Ms = Master/slave

OSPF packet header type = 2 (dd)			
0	0	Options	0 IMMs
dd sequence number			

- Exchange protocol uses database description packets
- First the master and slave are selected

- If both want to be masters, the highest address wins
- Retransmission if the packet is lost
- The same sequence number in the replies

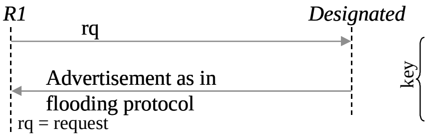
Exchange protocol initially synchronizes link DB with the designated router (2)



	OSPF packet header type = 2 (dd)			
	0	0	Options	0 IMMs
	dd sequence number			
key	Link state type			
	Link state ID			
	Advertising router			
	Link state sequence number			
	Link state checksum		Link state age	
	- - -			

- Master sends its Link DB description in sequence numbered packets
- Slave acks by sending its corresponding description packets.
- Exchange continues until all descriptions are sent and acknowledged. (M=0)
- Differences are recorded on the list of “records-to-request”.

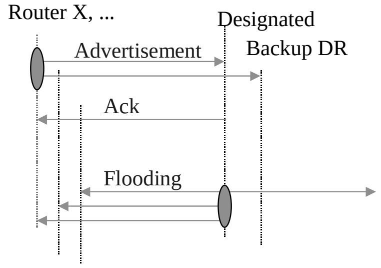
Request packets are used to get record contents. Requests are acknowledged by flooding protocol packets



	OSPF packet header type = 3 (rq)
key	Link state type
	Link state ID
	Advertising router
	- - -

- Router waits for ack for resend interval. If no response, the request is repeated.
- The records to request may be split into many requests, there are too many.
- If something goes wrong, the typical remedy is to restart role negotiation.
- The first request can be sent immediately when the first differing record has been detected. Then dd-packet exchange and rq packet exchange take place in parallel.

The flooding protocol continuously maintains the area’s Link DB integrity



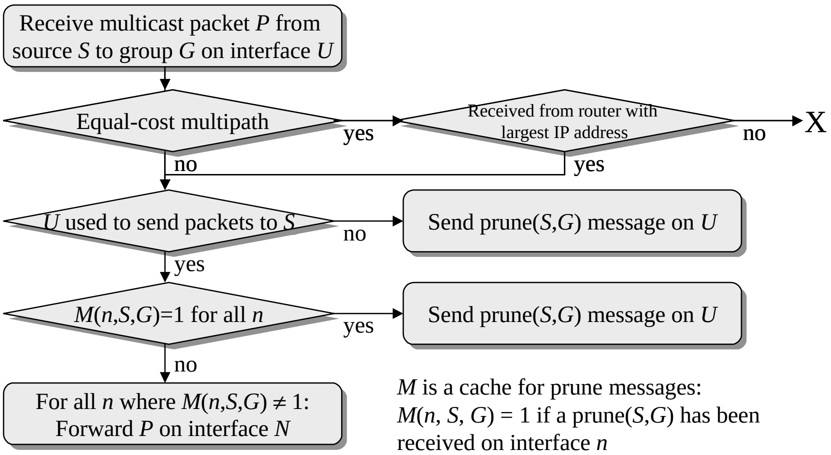
OSPF packet header type = 4 (upd.)
Number of advertisements
Link State Advertisements (*see LSA format*)
- - -

OSPF packet header type = 5 (ack.)
LSA headers
- - -

- Original LSA is always sent by the router responsible for that link.
- Advertisement is distributed according to flooding rules to the area (age=age+1).
- Ack of a new record by DR can be replaced in BC network by update message.
- One ack packet can acknowledge may LSAs.
- By delaying, several acks are collected to a single packet

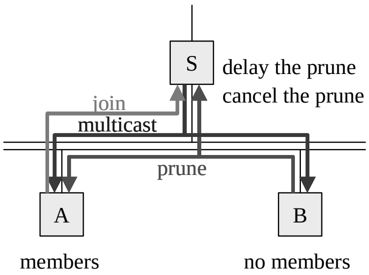
Question 5

5. Esitä PIM-DM monilähetyksen periaate. Miten PIM-DM tukee yleislähetysverkkoja?
   Present the principles of PIM-DM multicasting (3p). How does PIM-DM support broadcast networks? (1½p + 1½p)

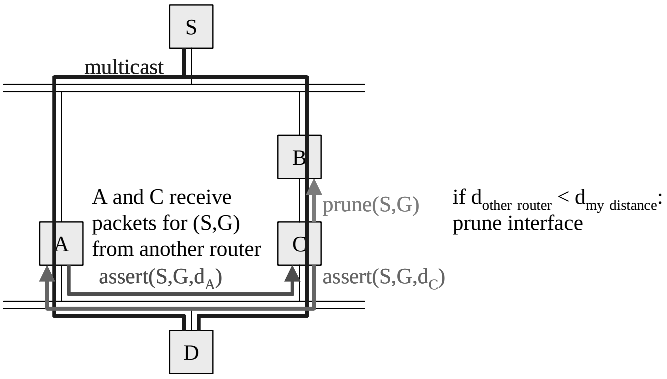

Receive multicast packet *P* from source *S* to group *G* on interface *U*
Equal-cost multipath
yes
Received from router with largest IP address
no
X
no
yes
U used to send packets to *S*
no
Send prune(*S*,*G*) message on *U*
yes
M(*n*,*S*,*G*)=1 for all *n*
yes
Send prune(*S*,*G*) message on *U*
no
For all *n* where *M*(*n*,*S*,*G*) ≠ 1: Forward *P* on interface *N*

M is a cache for prune messages:
M(*n*, *S*, *G*) = 1 if a prune(*S*,*G*) has been received on interface *n*
Least recently used entries may be dropped

PIM-DM – Pruning on broadcast networks



PIM-DM – Resolving multicasts received on multiple path


S
multicast
B
A and C receive packets for (S,G) from another router
prune(S,G)
if $d_{\text{other router}} < d_{\text{my distance}}$: prune interface
A
C
assert(S,G,d_A)
assert(S,G,d_C)
D

Question 6

6. Miten ennakoivat (proaktiiviset) ja reagoivat (reaktiiviset) reititysmenetelmät eroavat toisistaan? Kuvaa reitin muodostus ja ylläpito reagoivassa reititysprotokollassa.
   How do proactive and reactive routing methods differ (3p)? Illustrate the generation (2p) and maintenance (1p) of a route in a reactive routing protocol.

Traditional routing is proactive

- In proactive routing (table-driven routing), the routing tables are created before packets are sent
  - Link-state (e.g. OSPF)
  - Distance-vector (e.g. RIP)
- Each node knows the routes to all other nodes in the network
- Problems in Ad-Hoc networks
  - Maintenance of routing tables requires much bandwidth
  - Dynamic topology ⇒ much of the routing information is never used
    ⇒Waste of capacity
  - Flat topology
    ⇒No aggregation

Reactive routing

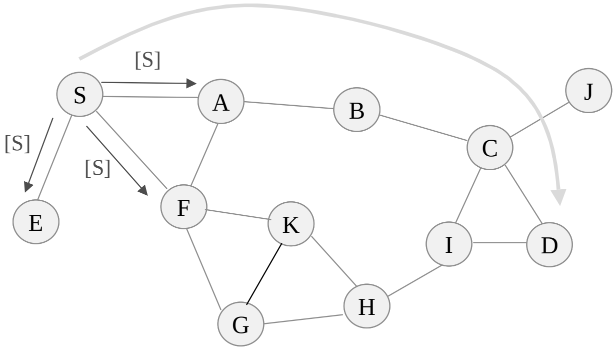
- In reactive routing the routes are created when needed
  - Before a packet is sent, a *route discovery* is performed
  - The results are stored in a cache
  - When intermediate nodes move, a *route repair* is required
- Advantages
  - Only required routes are maintained
- Disadvantages
  - Delay before the first packet can be sent
  - Route discovery usually involves flooding

Reactive routing – route request

- Also called ”on demand”
- The source must discover a route to the destination
  - The source broadcasts a *route request* message
  - Each node re-broadcasts the route request (flooding), and adds its own address to the path
  - When the destination receives the route request, it generates a *route reply*, which traverses the reverse path back to the source
- Route discovery effectively floods the network with the route request packet

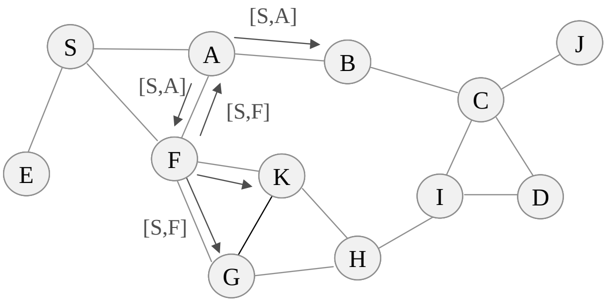
DSR – Dynamic Source Routing Example

Source node S floods a Route Request (RREQ)



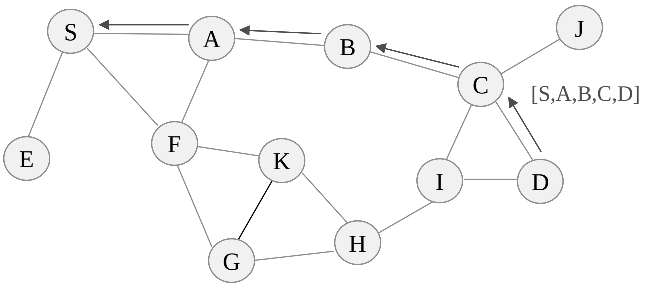
DSR – Dynamic Source Routing Example

Nodes receiving the Route Request forward it to their neighbors



DSR – Dynamic Source Routing Example

The destination generates a Route Reply (RREP), which is forwarded back to the source along the reversed path.



Reactive routing – route maintenance

- The source and the intermediate nodes must maintain the route when it is used.
- If the topology changes, the route must be *repaired*
  - The source sends a new route request to the destination
  - Improvement: Intermediate nodes can discover broken links and automatically repair the connection
- Intermediate nodes can remember successful paths
  - If a route request to the destination is received from another node, the intermediate node can answer on behalf of the destination

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.