Helsinki University of Technology, Networking Laboratory, N. Beijar
S-38.2121 Routing in Communication Networks

Model solutions for the exam 3.1.2007

Question 1

1. Kuvaa kiinteän hierarkkisen väylöityksen periaate ja väylöitysalgoritmi.
   Describe the principle and the algorithm of fixed hierarchical routing (FHR).

Model solution and grading

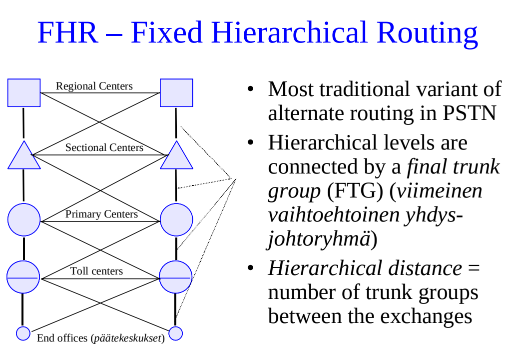
Principle and properties (3p of the following 4p)

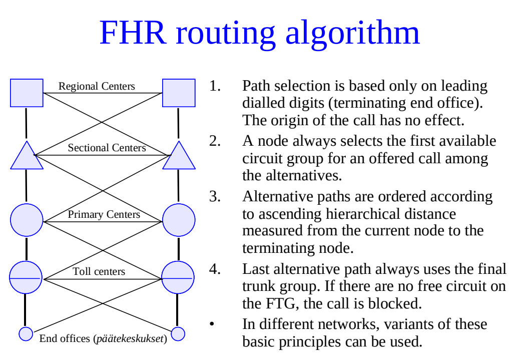
- static routing tables (1p)
- alternate routing (1p)
- hierarchy description (1p)
- loops are not possible (1p)

Routing algorithm (3p)

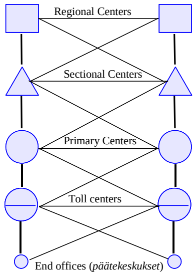
- path selection only based on leading digits
- the first available circuit groups among the alternatives is selected
- alternative paths are ordered according to ascending hierarchical distance
- the final trunk group is the last laternative path, call blocked if the final trunk group is not available

Related slides





Properties of Fixed Hierarchical Routing



- Sets minimal requirements for the nodes
- Loops (call circulating in a loop) are not possible.
- Divides nodes into *end offices* and *transit nodes*. From the point of view of digital exchange technology, transit capability is almost a subset of end office capability.
- Can be shown to rather far from optimal in terms of network resource usage.

Question 2

2. Milloin etäisyysvektoriprotokolla voi johtaa äärettömään laskemiseen? Mitä silmukoiden vastatoimia voidaan rakentaa etäisyysvektoriprotokollaan?
   When can counting to infinity occur in distance vector protocols? What countermeasures for routing loops can be built into distance vector protocols?

Model solution and grading

Counting to infinity occurs if both of these happen:

- Network has become partitioned. (if a link breaks without the network becoming partitioned, the counting does not go toward infinity but some finite distance!) (1½p)
- The refresh timers trigger in the incorrect order (sending old information) OR the message containing the distance vector is lost (1p for one, 1½p for both reasons)

Countermeasures: (1½p for one, 2½p for two, 3p for three countermeasures)

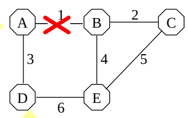
- Since the counting stops when infinity is reached, infinity has to be defined as a low value
- Split horizon (with poisonous reverse)
- Triggered updates

Related slides

Counting to infinity occurs when failures break the network into isolated islands (1)

- Link 1 is broken, and the network has recovered.
- All link costs = 1

A to	Link	Distance
D	3	1
A	-	0
B	3	3
E	3	2
C	3	3

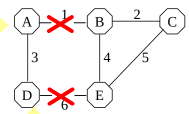


D to	Link	Distance
D	-	0
A	3	1
B	6	2
E	6	1
C	6	2

Counting to infinity occurs when failures break the network into isolated islands (2)

- Also link 6 breaks.
- D updates its routing table but has not yet sent its distance vector.

A to	Link	Distance
D	3	1
A	-	0
B	3	3
E	3	2
C	3	3

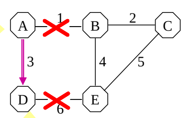


D to	Link	Distance
D	-	0
A	3	1
B	6	Inf.
E	6	Inf.
C	6	Inf.

Counting to infinity occurs when failures break the network into isolated islands (3)

- A sends its distance vector first:
  A=0,B=3,D=1,C=3,E=2
- D adds the information sent by A into its routing table.

A to	Link	Distance
D	3	1
A	-	0
B	3	3
E	3	2
C	3	3

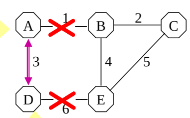


D to	Link	Distance
D	-	0
A	3	1
B	3	4
E	3	3
C	3	4

Counting to infinity occurs when failures break the network into isolated islands (4)

- The result is a loop. Costs are incremented by 2 on each round.
- We need to define infinity as a cost greater than any normal route cost.

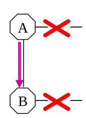
A to	Link	Distance
D	3	1
A	-	0
B	3	5
E	3	4
C	3	5



D to	Link	Distance
D	-	0
A	3	1
B	3	4
E	3	3
C	3	4

The first method to avoid loops is to send less information

The split horizon rule:
If node A sends to node X through node B, it does not make sense for B to try to reach X through A
⇒ A should not advertise to B its short distance to X

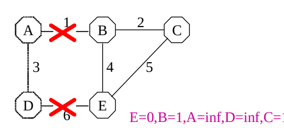


Implementation choices:

1. Split horizon
   - A does not advertise its distance to X towards B at all
   - ⇒ the loop of previous example can not occur
2. Split horizon with poisonous reverse
   - A advertises to B: X=inf.
   - ⇒ two node loops are killed immediately

Three-node loops are still possible (2)

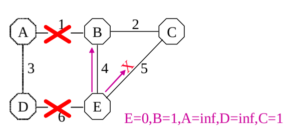
- Also link 6 fails.
- E sends its distance vector to B and C
  E=0,B=1,A=inf,D=inf,C=1



x to D	Link from x	Distance
B→D	4	2
C→D	5	2
E→D	6	Inf.

Three-node loops are still possible (3)

- Also link 6 fails.
- E sends its distance vector to B and C
  E=0,B=1,A=inf,D=inf,C=1
- ... But the DV sent to C is lost



x to D	Link from x	Distance
B→D	4	Inf.
C→D	5	2
E→D	6	Inf.

The second method to avoid loops is to use triggered updates

- A triggered update happens when an entry in the routing table is modified (e.g. when a link breaks)
- Triggered updates reduce the probability of loops
- Triggered updates also speed up counting to infinity
- RIP advertises
  - when the refresh timer expires, and
  - when a change occurs in an entry
- Loops are still possible, e.g. because of packet loss

Common problems

- In this question, the reasons were asked, not an example. For an example to be a satisfactory answer, it must clearly show why counting to infinity occurs, otherwise it may give reduced points.

Question 3

3. Miten linkkien tilaan perustuvassa reitityksessä selvitään osittuneen verkon jälleenyhdistymisestä?
   How is a fractioned network re-united in link-state routing?

Model solution and grading

The link state database must be identical in all nodes. While the network is fractioned the link state databases **change independently** in both parts. (1p)

The LS protocol must **synchronize** the databases of the different parts when they are re-united (1p)

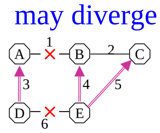
The **sequence numbers** are used in synchronizing to compare which record is the newest (1p)

The whole link table does not need to be transferred, instead the **headers are compared** (1p). This is done by the **exchange protocol** with **description** and **request** packets (1p)

Finally, the **rest of the network must be updated** with the synchronized information. This is done with the flooding protocol (1p)

Related slides

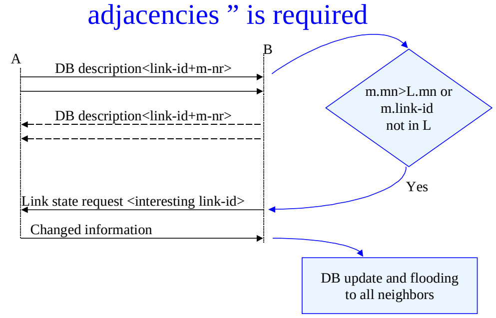
If network splits into islands, DBs in islands may diverge

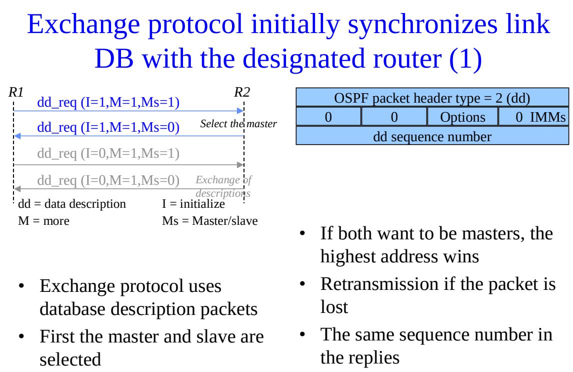


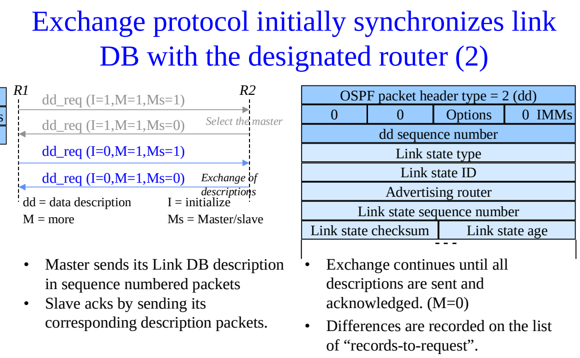
From	To	Link	Cost	Seq.num
A	B	1	inf	2
A	D	3	1	1
B	A	1	inf	2
B	C	2	1	1
B	E	4	1	1
C	B	2	1	1
C	E	5	1	1
D	A	3	1	1
D	E	6	inf	2
E	B	4	1	1
E	C	5	1	1
E	D	6	1	1

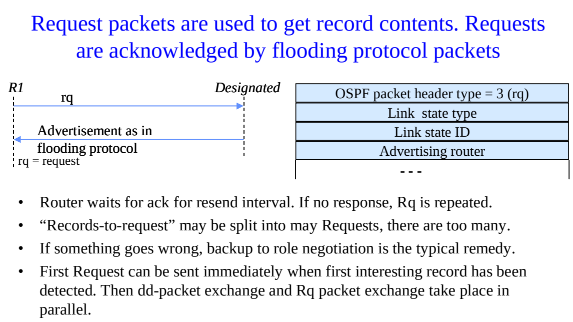
From	To	Link	Cost	Seq.num
A	B	1	inf	2
A	D	3	1	1
B	A	1	inf	2
B	C	2	1	1
B	E	4	1	1
C	B	2	1	1
C	E	5	1	1
D	A	3	1	1
D	E	6	1	1
E	B	4	1	1
E	C	5	1	1
E	D	6	inf	2

After reconnection of the islands "bringing up adjacencies " is required









Common problems

- Most understood the problem of different link state databases in different parts of the network, and the need to synchronize. However, quite few described how the synchronization actually is done.

Question 4

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

Model solution and grading

For each sub-protocol 2p (½p for the name, 1p for the task, ½p for the operational priciples)

Hello protocol (½p)

- Task: Checks if the link is working bidirectionally (½p), selects designated router and backup designated router (½p)
- Operational principle: Periodical sending of Hello messages on all links (½p)

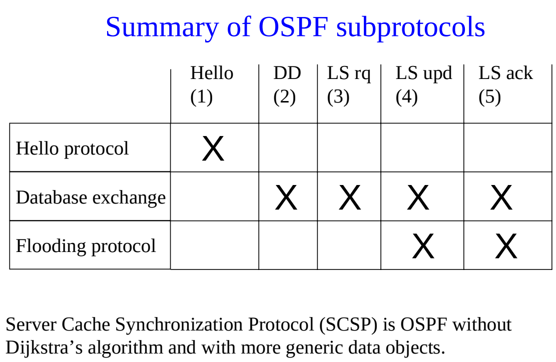
Database Exchange protocol (½p)

- Task: Syncronizes link databases when a link starts working (1p)
- Operational principle: Each end of the link describes its link database with database description packets, the other side of the link requests differing and new records (½p)

Flooding protocol (½p)

- Task: Updating the local LSAs to all routers in the area (1p)
- Operational principle: Periodical sending of Update messages on all links. The Update messages are distributed with flooding to all other routers in the area. (½p)

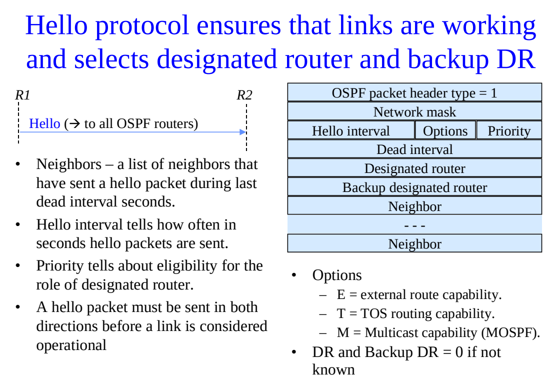
Related slides

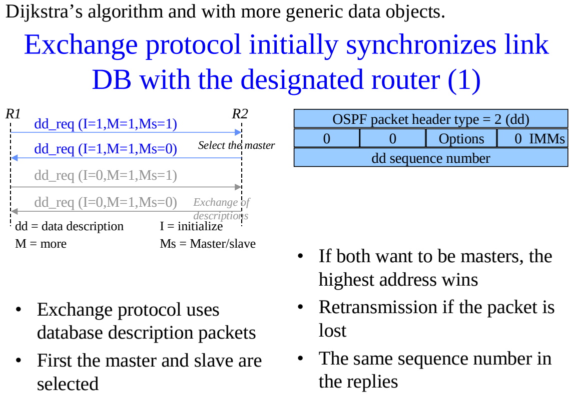


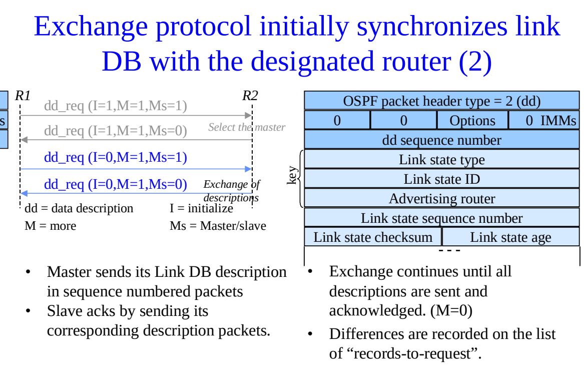
Summary of OSPF subprotocols

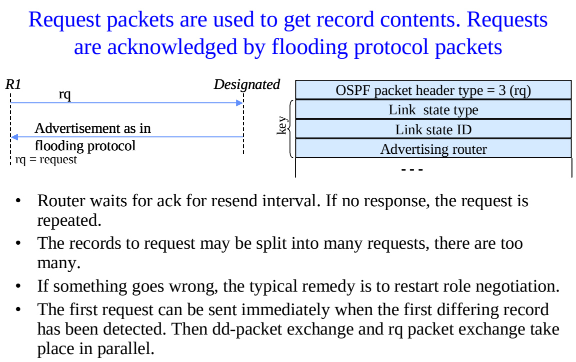
	Hello (1)	DD (2)	LS rq (3)	LS upd (4)	LS ack (5)
Hello protocol	X				
Database exchange		X	X	X	X
Flooding protocol				X	X

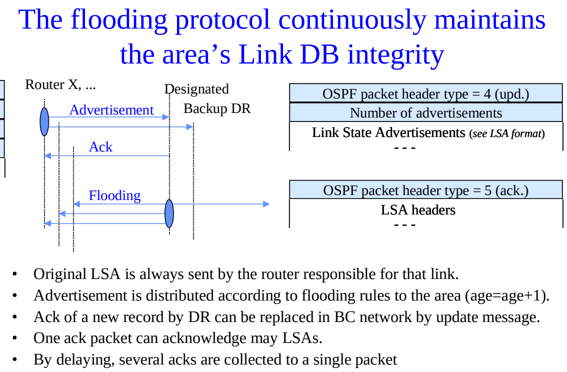
Server Cache Synchronization Protocol (SCSP) is OSPF without Dijkstra's algorithm and with more generic data objects.











Common problems

- This question went very well although it was focused on details. You did a good job!

Question 5

5. Vertaile keskuspohjaisen puun ja "tulvi ja karsi" algoritmien etuja ja haittoja.
   Compare the advantages and disadvantages of the center-based tree algorithm and the "flood and prune" algorithm.

Model solution and grading

Collect up to 6 points of the following:

Bandwidth: The flood-and-prune algorithm wastes bandwidth by periodically flooding the whole or part of the network with multicast packets. In the center-based tree algorithm, the multicast packets are only sent on branches leading to receivers. (1p) Because of this property, the flood-and-prune algorithm is feasible only when the number of multicast receivers is high compared to the number of nodes, i.e. in dense multicast groups. (1p)

Multicast routes: The flood-and-prune algorithm generates source-specific trees, meaning that every receiver has the shortest possible route to every source, i.e. a minimal delay (1p). Since there is a separate tree for every source, the traffic is more evenly distributed in the network (1p). The center-based tree algorithm generates a shared tree rooted in the center. Therefore the routes are not optimal.

Joining: In the flood-and-prune algorithm, the receiver has to wait for the following periodical flooding before it starts receiving packets. In the center-based tree algorithm, the receiver sends a join message to the center, and starts to receive multicast packets almost immediately. (1p)

Centralization: The center-based tree algorithm is centralized. The center may become a bottleneck (1p) and a single point of failure (1p). The flood-and-prune algorithm is decentralized.

Complexity: The flood-and-prune algorithm is simple, easy to implement, and requires less signalling. The center-based tree algorithm is more complex. (1p)

Other issues: The center-based tree algorithm provides better control over receivers, since every receiver has to join explicitly (1p). The flood-and-prune algorithm must deal with the possibility of several paths to a receiver, while there is only one path to a receiver in the center-based tree algorithm (1p). The performance of the center-based tree algorithm depends on how the center is selected (1p).

Question 6

6. Selitä tunneloinnin käyttö Mobile IP:ssä. Miten tunnelointi toteutetaan? Miksi täytyy joskus tunneloida kumpaankin suuntaan menevät paketit?
Explain the use of tunneling in Mobile IP. How is tunneling implemented? Why must the packets be tunneled in both directions sometimes?

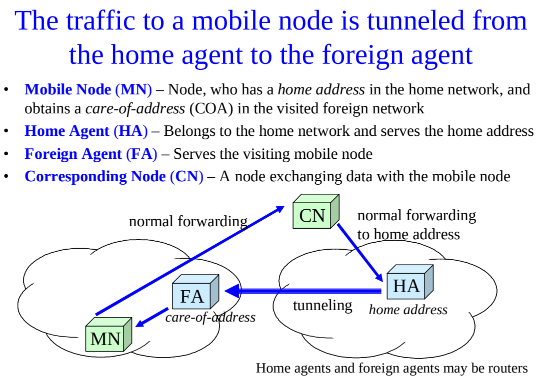
Model solution and grading

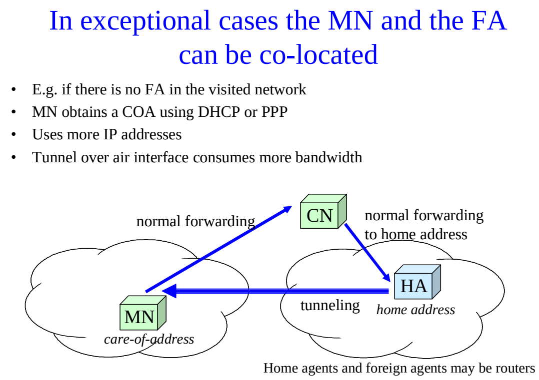
Use of tunneling: The Home Agent intercepts packets sent to the mobile host and tunnel them to the Foreign Agent (or directly to the mobile host if there is no foreign agent). (1½p)

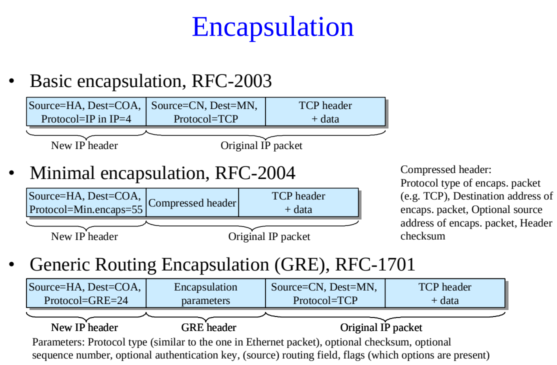
Implementation (3p of the following): Tunneling is usually implemented with IP-in-IP, i.e. transporting the original IP packet within another IP packet. (1p) The destination address of the inner packet is the Home Address. The destination address of the outer packet is the Care-of-Address. (1p) To save bandwidth in wireless networks, a compressed inner IP header is often used. (1p) Tunneling can also be implemented with GRE-encapsulation, e.g. if other protocols than IP should be tunneled. (1p) In principle, tunneling could even be implemented using source routing. (1p) If the mobile host wants to receive multicast and broadcast packets from the home network, these must be double-encapsulated. (1p)

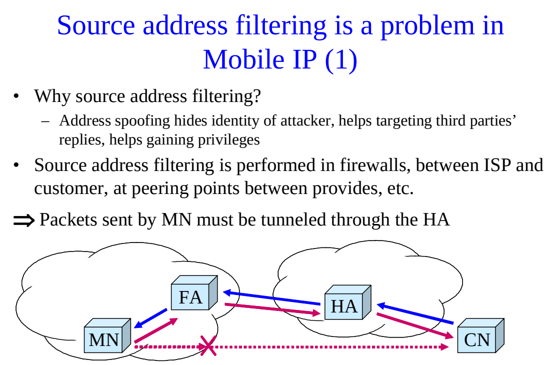
Reverse tunneling: If source address filtering is used, e.g. in firewalls, reverse tunneling is necessary. (1½p)

Related slides









General grading principles

Note 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 in details do not decrease the points. Serious errors showing misunderstanding decrease the points. Some extra information **related to the question** may give small extra points.