שאלה 1-4

1) What aspect of IP addresses makes it necessary to have one per network interface, rather than just one per host? In light of your answer, why does IP tolerate point-to-point interfaces that have non-unique addresses or no addresses?

The hierarchical aspect of the IP addresses: network-host parts of the address. This allows routers to ‘route’ network addresses only.

IP addresses are hierarchical, by which they are made up of several parts tat correspond to some sort of hierarchy on the internetwork: the network and host parts. The network part of in IP address identifies the network to which the host is attached. All host attached to the same network have the same network part of their IP address. The host part identifies that host uniquely on the network.

The routers are attached to 2 networks. They need to have an address on each network, one for each interface.

Point-to-point communication is done between routers and within a network directly to a host.

שאלה 2:

Why does the offset field in the IP header measure the offset in 8 byte units?

תשובה:

גודלה המקסימלי של חבילת IP הינו 65535 בייטים, כלומר, 2 בחזקת 16, אורך שדה ה OFFSET הינו 13
ביטים. חישוב פשוט מראה שניתן ליצג כל חבילה בעזרת שדה ה OFFSET רק אם נתייחס ליחידה בסיסית
של 8 בייטים (2 מחזקת 3).

שאלה 3:

Suppose that a TCP message that contains 2048 bytes of data and 20 bytes of TCP header is passed to IP for delivery across two networks of the internet, the first uses 14-bytes header and MTU of 1024, while the second uses 8 byte headers and MTU of 512 bytes

MTU = payload of data link layers, so ignore all information about the data link layer headers.
MTU = IP header + IP payload
IP payload = TCP header + TCP payload
Original IP payload = 20+2048 =2068 bytes
First network:
Maximum IP payload = 1004 bytes
So broken down into 2068/1004 = 3 IP datagrams:

ID	Offset	Bytes	Flag
1	0	1004	0
2	0	1004	0
3	0	60	0

Second network:
Maximum IP payload = 492 bytes
So the first two IP datagrams are broken down into 3 IP datagrams.

ID	Offset	Bytes	Flag
1	0	492	1
1	492	492	1
1	984	20	0
2	0	492	1
2	492	492	1
2	984	20	0
3	0	60	0

שאלה 4:

Suppose an IP packet is fragmented into 10 fragments, each with a 1% (independent) probability of loss. To a reasonable approximation, this means there is a 10% change of losing the whole packet due to loss of a fragment. What is the probability of net loss of the whole packet if the packet is transfer twice,

(a) Assuming all fragments received must have been part of the same transmission?
(b) Assuming any given fragment may have been part fo the either transmission?
(c) Explain how use of the ident field might be applicable here.

תשובה:

שאלה 5:

Suppose the fragments of Figure 4.5(b) all pass through another router onto a link with an MTU of 380 bytes, not counting the link header. Show the fragments produced. If the packet were originally fragmented for this MTU, how many fragments would be produced?

M	offset	bytes data	source
1	0	360	1st original fragment
1	360	152	1st original fragment
1	512	360	2nd original fragment
1	872	152	2nd original fragment
1	1024	360	3rd original fragment
0	1384	16	3rd original fragment

אילו החלוקה היתה היתה ל 380 בייטים במקור, הרי היו רק 4 חבילות.

שאלה 6:

What is the maximum bandwidth at which an IP host can send 576-byte packets without having the ident warp around within 60 second? What would happen if this bandwidth were exceeded?

תשובה:

גודל שדה ה IDENT הינו 16 ביט, כלומר 65535 ערכים שונים. משמעות הדבר היא שבכל חלון זמן של 60 שניות, ניתן להעביר ברשת רק 65535 חבילות שונות! גודל כל חבילה הינו 576 בייטים נגרר מכך שרוחב הפס המקסימלי הינו 614.4Kbytes/sec. במקרה והרוחב פס יהיה גבוה יותר, הודעה בעלת X IDENT עלולה להתעקב כ 60 שניות ובמשך הזמן הזה הודעה אחרת בעלת אותו IDENT (עקב החזרה) תישלח, המטרה לא ידע איזה הודעה היא הנכונה.

שאלה 7:

ATM AAL 3/4 uses fields Btag/Etag, BASsize/Len, type, SEQ, MID, Length and CRC10 to implement fragments into cells. IPv4 uses Ident, Offset and the M bit in Flags, among others. What is the IP analog, if any, for each AAL 3.4 field?
Does each IP field listed here have an AAL 3/4 analog? How well do there fields correspond?

תשובה:

MID דומה ל ID ב IP.
Length דומה ל OFFSET.
Type דומה לביט M ב IP.
המידע בשאר השדות אינו מעובר ב IP, מידע זה כולל גודל החוצץ הדרוש, גירסת פרוטוקול ועוד.

שאלה 8:

Why do you think IPv4 has fragment reassembly done at the endpoint, rather than at the next router? Why do you think IPv6 abandoned fragmentation entirely?

תשובה:

חיבור עולה זיכרון וזמן. חיבור וחילוק של החבילות בכול נתב יעלו הרבה זיכרון לאותו נתב (לדאוג לחבר את כל ההודעות שנכנסות אליו, לא לשכוח את החוצץ של אותו נתב) וגם זמן יקר (כל נתב יחכה עד שכל ההודעה תגיע אליו, יחבר, יחלק (אם צריך) ורק אז ישלח- ההודעות יתעקבו מאוד).
ב- IPv6 הוחלט לותר על חילוק כיוון ששכבת החיבור הפיסי (לעומת החיבור ה לוגי של IP) תעשה את זה הרבה יותר טוב, ללא צורך לבצע חישובים על ה header של חבילת ה IP.

שאלה 9:

Having ARP table entries time out after 10-15 minutes is an attempt at a reasonable compromise. Describe the problems that can occur if the timeout value is too small or too large.

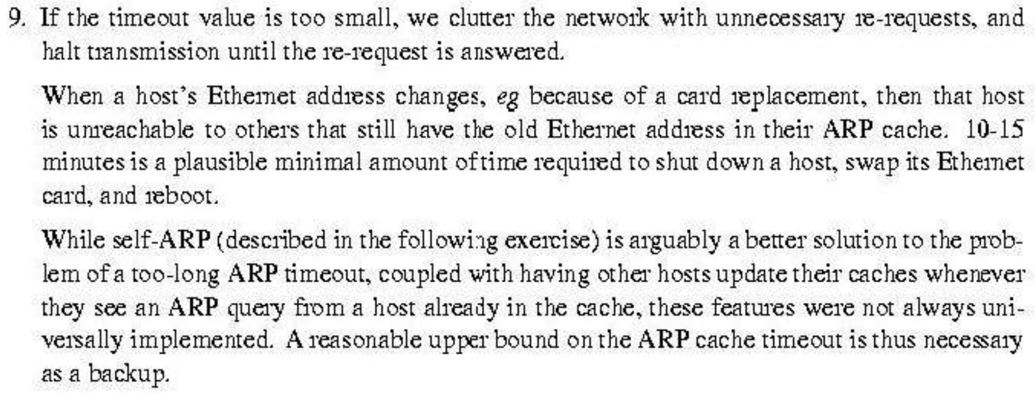
תשובה:

ערך נמוך מידי (נניח חצי דקה) יגרום לכך שכמעט כל תיקשורת בין שני מחשבים בתת-הרשת תיגרום לבקשת ARP. סביר להניח שמחשב שעבד לפני חצי דקה, יעבוד גם כעת ולכן בקשת ARP תאיט את פעולת התקשורת.

ערך גבוהה מידי (נניח שעה) יגרום לכך שההנחה שמחשב מסוים עדיין עובד, אינה כול כך סבירה. הרבה יכול לקרות בשעה.

שאלה 9-4

Having ARP tables entries time out after 10 – 15 minutes is an attempt at a reasonable compromise. Describe the problems that can occur if the timeout value is too small or too large. (4/9)



9. If the timeout value is too small, we clutter the network with unnecessary re-requests, and halt transmission until the re-request is answered.

   When a host's Ethernet address changes, *eg* because of a card replacement, then that host is unreachable to others that still have the old Ethernet address in their ARP cache. 10-15 minutes is a plausible minimal amount of time required to shut down a host, swap its Ethernet card, and reboot.

   While self-ARP (described in the following exercise) is arguably a better solution to the problem of a too-long ARP timeout, coupled with having other hosts update their caches whenever they see an ARP query from a host already in the cache, these features were not always universally implemented. A reasonable upper bound on the ARP cache timeout is thus necessary as a backup.

שאלה 10-4

10) Suppose hosts A and B have been assigned the same IP address on the same Ethernet, on which ARP is used. B starts up after A. What will happen to A's existing connections? Explain how "self-ARP" (querying the network on start-up for one's own IP address) might help with this problem.

B starts up: Everyone still maps the IP address to the Ethernet address. B sends update to other hosts. So, all messages to that IP address go to B. A doesn't get anymore messages.

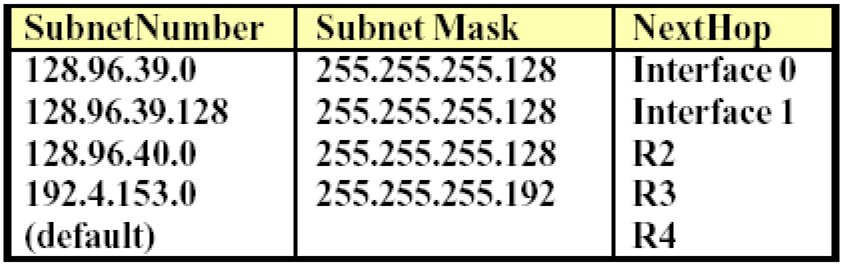
SelfARP

If someone has the same hardware address, you could request a different IP address for the IP\Link-layer address pair. But ARP doesn't assign addresses, so who do you have to ask for a different IP address

שאלה מספר 16-4

6) Suppose a router has built up the routing table shown below. The router can deliver packets directly over interfaces 0 and 1, or it can forward packets to routers R2, R3, R4. Describe what the router does with a packet addressed to each of the following destinations:
a) 128.96.39.10 b) 128.96.40.12 c) 128.96.40.151 d) 192.4.153.17 e) 192.4.153.90

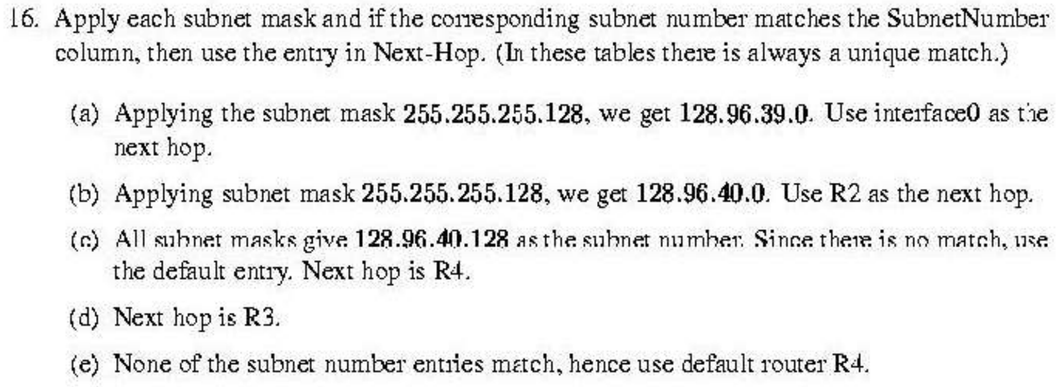
Subnet Number	Subnet Mask	Next Hop
128.96.39.0	255.255.255.128	Interface 0
128.96.39.128	255.255.255.128	Interface 1
128.96.40.0	255.255.255.128	R2
192.4.153.0	255.255.255.192	R3
(default)		R4



SubnetNumber	Subnet Mask	NextHop
128.96.39.0	255.255.255.128	Interface 0
128.96.39.128	255.255.255.128	Interface 1
128.96.40.0	255.255.255.128	R2
192.4.153.0	255.255.255.192	R3
(default)		R4

Table 2

Solution:



16. Apply each subnet mask and if the corresponding subnet number matches the SubnetNumber column, then use the entry in Next-Hop. (In these tables there is always a unique match.)

(a) Applying the subnet mask **255.255.255.128**, we get **128.96.39.0**. Use interface**0** as the next hop.

(b) Applying subnet mask **255.255.255.128**, we get **128.96.40.0**. Use R2 as the next hop.

(c) All subnet masks give **128.96.40.128** as the subnet number. Since there is no match, use the default entry. Next hop is R4.

(d) Next hop is R3.

(e) None of the subnet number entries match, hence use default router R4.

שאלה מס' 38-4

9) The following table is a routing table using CIDR. Address bytes are in hexadecimal. The notation “/12” in C4.50.0.0/12 denotes a netmask with 12 leading 1 bits, that is FF.F0.0.0. Note that the last three entries cover every address and thus serve in lieu of a default route. State to what next hop the following will be delivered:

a)C4.5E.13.87 b)C4.5E.22.09 c) C3.41.80.02
d)5E.43.91.12 e) C4.6D.31.2E f) C4.6B.31.2E

Routing Table:

Net/MaskLength	Next Hop
C4.50.0.0/12	A
C4.5E.10.0/20	B
C4.60.0.0/12	C
C4.68.0.0/14	D
80.0.0.0/1	E
40.0.0.0/2	F
00.0.0.0/2	G

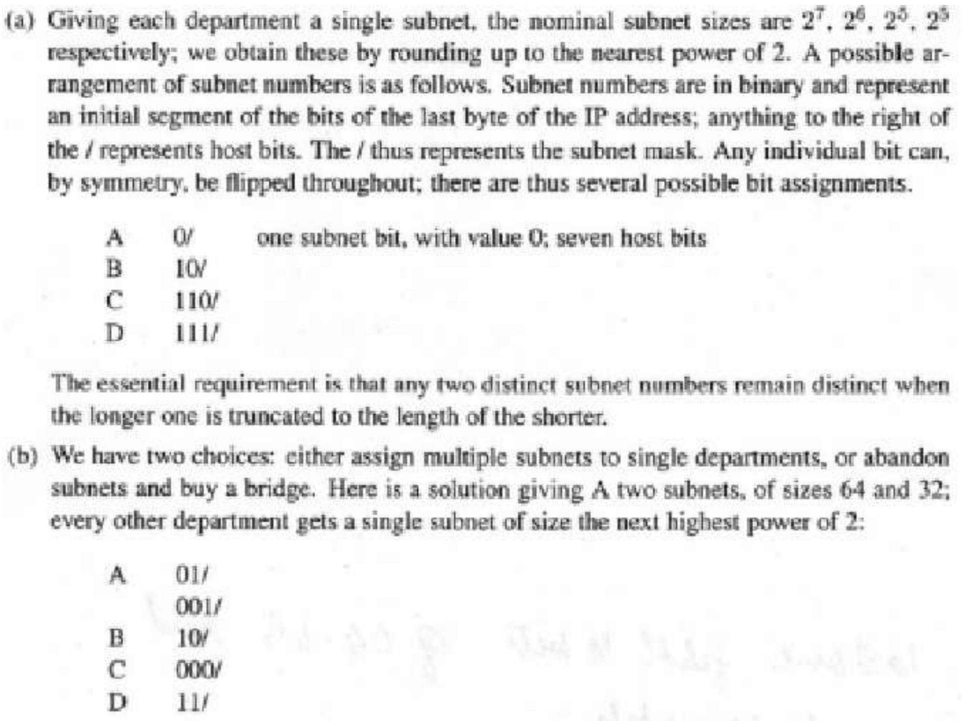
Solution:

a) B
b) A

c) E
d) F
e) C
f) D

שאלה 33-4

8) An organization has a class C network 200.1.1 and wants to form subnets for four departments with hosts as follows:
A 72 hosts, B 35 hosts, C 20 hosts, D 18 hosts
There are 145 hosts in all.
a) Give a possible arrangement of subnet masks to make this possible
b) Suggest what the organization might do if department D grows to 34 hosts.
Solution:



(a) Giving each department a single subnet, the nominal subnet sizes are 2^7, 2^6, 2^5, 2^5 respectively; we obtain these by rounding up to the nearest power of 2. A possible arrangement of subnet numbers is as follows. Subnet numbers are in binary and represent an initial segment of the bits of the last byte of the IP address; anything to the right of the / represents host bits. The / thus represents the subnet mask. Any individual bit can, by symmetry, be flipped throughout; there are thus several possible bit assignments.

A	0/	one subnet bit, with value 0; seven host bits
B	10/	
C	110/	
D	111/	

The essential requirement is that any two distinct subnet numbers remain distinct when the longer one is truncated to the length of the shorter.

(b) We have two choices: either assign multiple subnets to single departments, or abandon subnets and buy a bridge. Here is a solution giving A two subnets, of sizes 64 and 32; every other department gets a single subnet of size the next highest power of 2:

A	01/
	001/
B	10/
C	000/
D	11/

שאלה 21-4

21. Consider the network in Figure 3, using a link-state router. Suppose the B – F link fails, and the following events occur in sequence:
a. Node H is added to the network connected to G
b. Node D is added to the network connected to C
c. A new link D – A is added
d. The failed B – F link is now restored.
Describe what link-state packets will pass back and forth. Assume that the initial sequence number at all nodes is 1, and that no packets time out, and that both ends of a link use the same sequence number in their LSP for that link.

21. There is some confusion in the last paragraph of this exercise. OSPF routers send out *one* LSP, with one sequence number, that describes all the router's connections; however, the language "both ends of a link use the same sequence number in their LSP for that link" incorrectly suggests that routers send out a different LSP (or at least different LSA) for each link, each with its own sequence number. While it is certainly possible for link-state routing to take this approach, it is not how OSPF works and it is not what the text describes. We will use OSPF-style numbering here. We will also assume that each node increments its sequence number only when there is some change in the state of its local links, not for timer expirations ("no packets time out").

The central *point* of this exercise was intended to be an illustration of the "bringing-up-adjacencies" process: in restoring the connection between the left- and righthand networks, it is not sufficient simply to flood the information about the restored link. The two halves have evolved separately, and full information must be exchanged.

Given that each node increments its sequence number whenever it detects a change in its links to its neighbors, at the instant before the B—F link is restored the LSP data for each node is as follows:

node	seq#	connects to
A	2	B,C,D
B	2	A,C
C	2	A,B,D
D	2	A,C
F	2	G
G	2	F,H
H	1	G

When the B–F link is restored, OSPF has B and F exchange their full databases of all the LSPs they have seen with each other. Each then floods the other side's LSPs throughout its side of the now-rejoined network. These LSPs are as in the rows of the table above, except that B and F now each have sequence numbers of 3. (Had we assigned separate sequence numbers to each individual link, every sequence number would be 1 except for link B—F.)

The initial sequence number of an OSPF node is actually $-2^{31} + 1$.

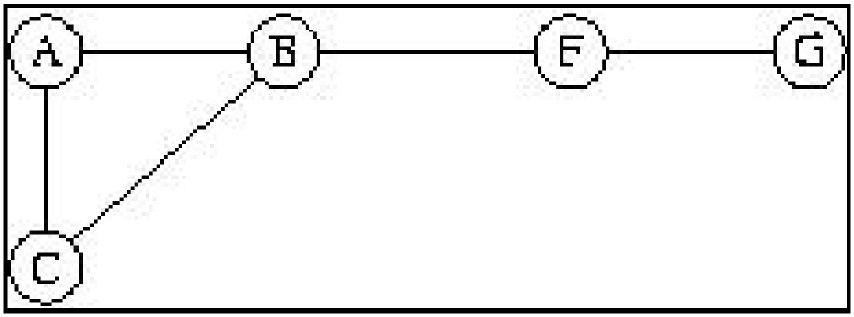


Figure 3

שאלה 13-4

13. For the network given in Figure 2, show how the link-state algorithm builds the routing table for node D.

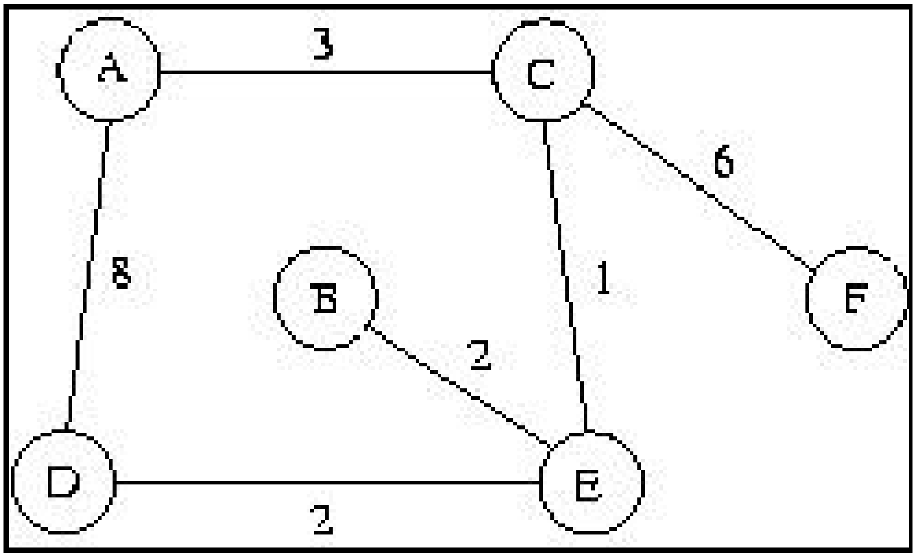
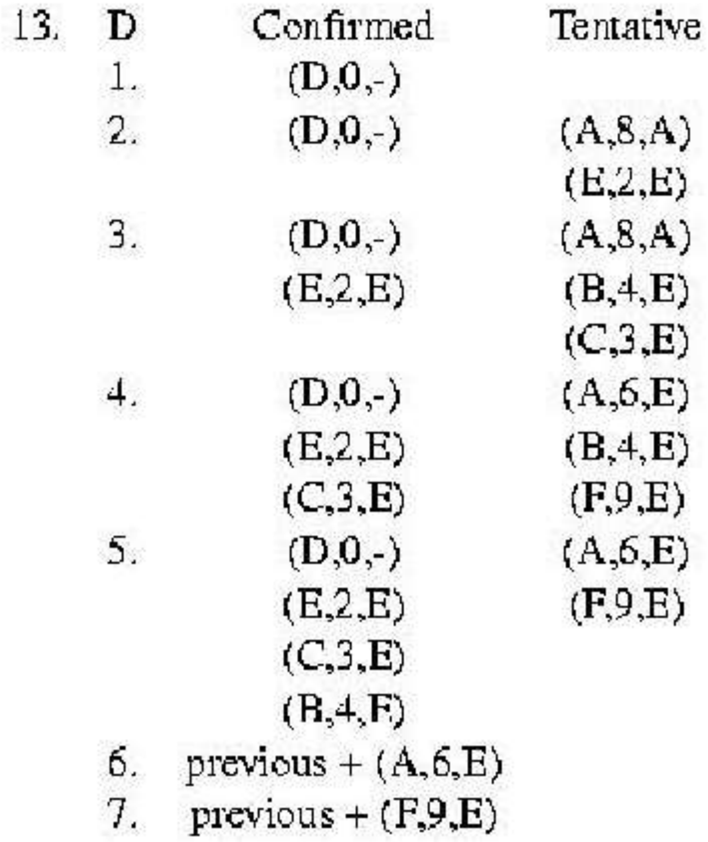


Figure 2

	NODE A				NODE F	
node	cost	nexthop		node	cost	nexthop
B	1	B		A	3	E
C	2	B		B	2	C
D	1	D		C	1	C
E	2	B		D	2	E
F	3	D		E	1	E

Table 1



13.

D	Confirmed	Tentative
1.	(D,0,-)	
2.	(D,0,-)	(A,8,A) (E,2,E)
3.	(D,0,-) (E,2,E)	(A,8,A) (B,4,E) (C,3,E)
4.	(D,0,-) (E,2,E) (C,3,E)	(A,6,E) (B,4,E) (F,9,E)
5.	(D,0,-) (E,2,E) (C,3,E) (B,4,E)	(A,6,E) (F,9,E)
6.	previous + (A,6,E)	
7.	previous + (F,9,E)	

שאלה 17-4

8. Consider the simple network in Figure 3, in which A and B exchanges distance-vector routing
information. All links have cost 1. Suppose the A-E link fails.
(a) Give a sequence of routing table updates that leads to a loop between A and B.
(b) Estimate the probability of the scenario in (a), assuming A and B send out routing updates
at random times, each at the same average rate.
(c) Estimate the probability of a loop forming if A broadcasts an updated report within 1 second of discovering the A-E failure, and B broadcasts every 60 seconds uniformly.

8.
(a) A necessary and sufficient condition for the routing loop to form is that B reports to A the networks B believes it can currently reach, after A discovers the problem with A-E link, but before A has communicated to B that A no longer can reach E.
(b) At the instant that A discovers A-E failure, there is a 50% chance the next report will be B's and a 50% chance that the netxt report will be A's. If it is A's, the loop will not form; if it is B's, the loop will form.
(c) At the instant A discovers the A-E failure, let t be the time until B's next broadcast, t is equally likely to occur anywhere in the interval [0,60]. The event of a

loop forming is the same as the event that B broadcast first, which is the event that t< 1.0 sec; the probability of this is 1/60.

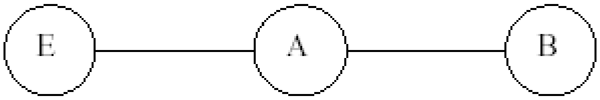


Figure 3

שאלה 19-4

5. Suppose a set of routers all use the split-horizon technique; we consider here under what circumstances it makes a difference if they use poison reverse in addition.

(a) Show that poison reverse makes no difference in the evolution of the routing loop in the two examples described in Section 4.2.2 of your textbook, given that the hosts involved using split horizon.

(b) Suppose split-horizon routers A and B somehow reach a state in which they forward traffic for a given destination X toward each other. Describe how this situation will evolve with and without the use of poison reverse.

(c) Give a sequence of events that leads A and B to a looped state in (b), even if poison reverse is used. Hint: Suppose B and A connect through a very slow link. They each reach X through a third node, C, and simultaneously advertise their routes to each other.

5.

(c) Without poison reverse, A and B would send each other updates that simply did not mention X, this would mean that the false routes to X would sit there until they eventually aged out. With the poison reverse, such a loop would go away on the first table update exchange.

(d) 1. B and A each send out announcements of their route to X via C to each other.

2. C announces to A and B that it can no longer reach X; the announcements of step1 have not yet arrived.

3. B and A receive each others announcements from step 1, and adopt them.

שאלה 20-4

6. Hold down is another distance-vector loop-avoidance technique, whereby hosts ignore updates for a period of time until link failure news has had a chance to propagate. Consider the networks in figure 2, where all links have cost 1 except E-D with cost 10. Suppose that E-A link breaks and B reports its loop forming E route to A immediately afterwards (this is the false route, via A). Specify the details of a hold-down interpretation, and use this to describe the

evolution of the routing loop in both networks. To what extent can hold down prevent the loop
in the EAB network without delaying the discovery of the alternative route in the EABD network?

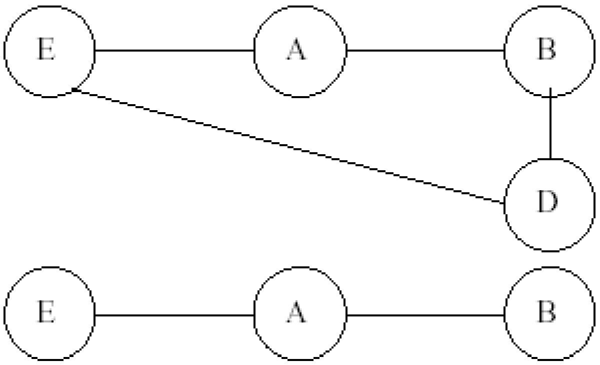
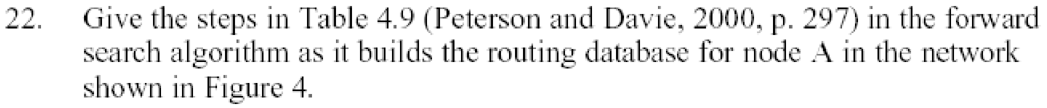


Figure 2

6.
We will implement hold-down as follows: When an update record arrives that indicates a destination is unreachable, all subsequent updates within some given interval are ignored and discarded.
Given this, then in the EAB network A ignores B’s reachability news for one time interval, during which time A presumably reaches B with the correct unreachability information.
Unfortunately, in the EABD case, this also means A ignores the valid B-D-E path. Suppose, in fact, that A reports its failure to B, D report its valid path to B, and then B reports to A, all in rapid succession. This new route will be ignored.
One way to avoid delaying discovery of the B-D-E path is to keep the hold-down time interval as short as possible, relying on triggered updates to spread the unreachability news quickly.
Another approach to minimizing delay for new valid paths is to retain route information receiving during the hold-down period, but not to use it. At the expiration of the holddown
period, the sources of such information might be interrogated to determine whether
it remains valid. Otherwise we might have to wait not only the hold-down interval but also until the next regular update in order to receive the new route news.

שאלה 22-4



22. Give the steps in Table 4.9 (Peterson and Davie, 2000, p. 297) in the forward search algorithm as it builds the routing database for node A in the network shown in Figure 4.

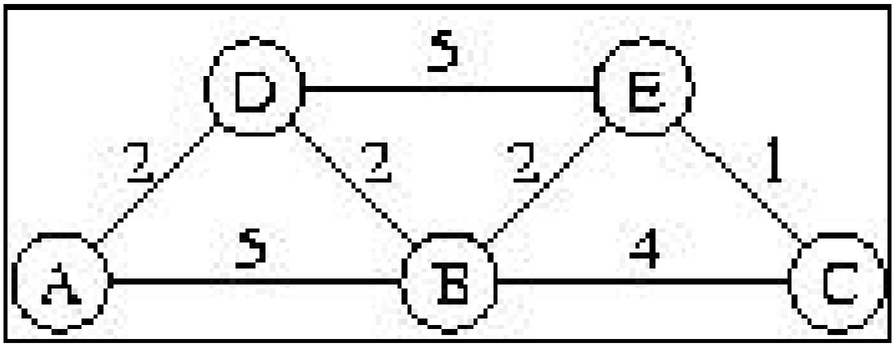
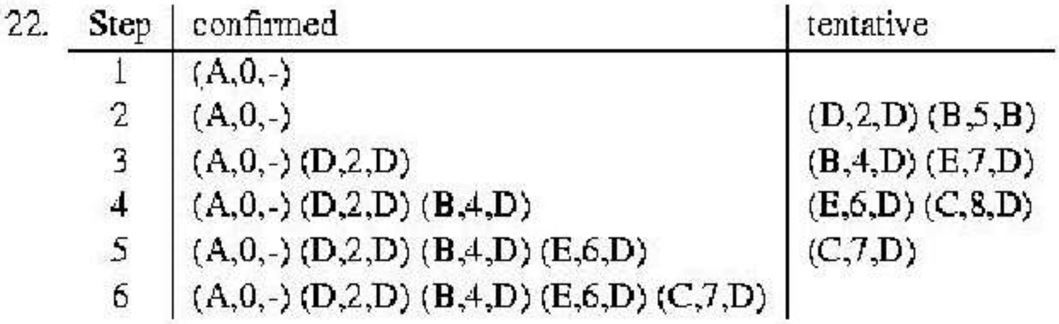


Figure 4

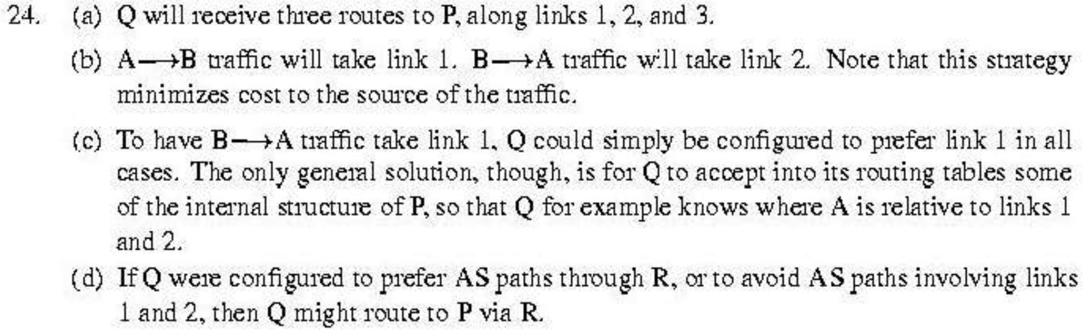


22.

Step	confirmed	tentative
1	(A,0,-)	
2	(A,0,-)	(D,2,D) (B,5,B)
3	(A,0,-) (D,2,D)	(B,4,D) (E,7,D)
4	(A,0,-) (D,2,D) (B,4,D)	(E,6,D) (C,8,D)
5	(A,0,-) (D,2,D) (B,4,D) (E,6,D)	(C,7,D)
6	(A,0,-) (D,2,D) (B,4,D) (E,6,D) (C,7,D)	

שאלה 24-4

Consider the network shown in Figure 1, in which horizontal lines represent transit providers and numbered vertical lines are interprovider links.
(i) How many routes to P could provider Q's BGP speakers receive?
(ii) Suppose Q and P adopt he policy that outbound traffic is routed to the closest link to the destination's provider, thus minimising their own cost. What path will traffic from Host A to Host B and from Host B to Host A take?
(iii) What could Q do to have the B to A traffic use the closer link 1?
(iv) What could Q do to have the B to A traffic pass through R?



24. (a) Q will receive three routes to P, along links 1, 2, and 3.

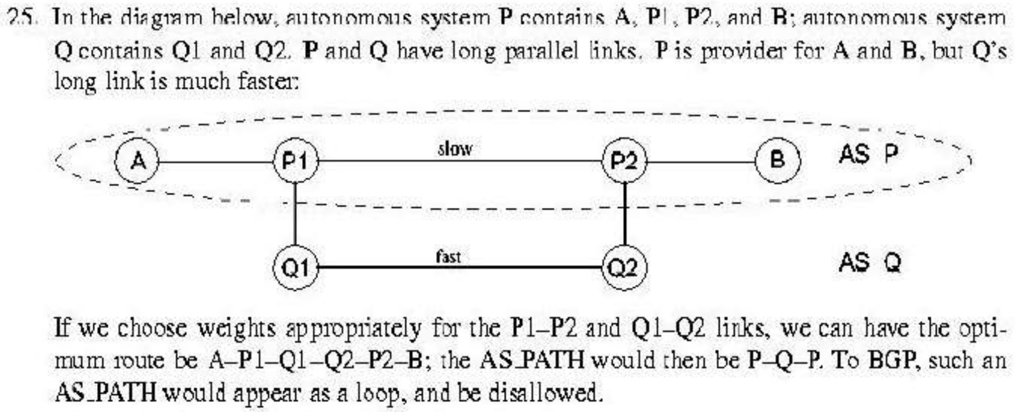
(b) A⟶B traffic will take link 1. B⟶A traffic will take link 2. Note that this strategy minimizes cost to the source of the traffic.

(c) To have B⟶A traffic take link 1, Q could simply be configured to prefer link 1 in all cases. The only general solution, though, is for Q to accept into its routing tables some of the internal structure of P, so that Q for example knows where A is relative to links 1 and 2.

(d) If Q were configured to prefer AS paths through R, or to avoid AS paths involving links 1 and 2, then Q might route to P via R.

שאלה 25-4

Give an example of an arrangement of routers grouped into autonomous systems so that the path with the fewest hops from a point A to another point B crosses the same AS twice. Explain what BGP would do with this situation. (4/25)



25. In the diagram below, autonomous system P contains A, P1, P2, and B; autonomous system Q contains Q1 and Q2. P and Q have long parallel links. P is provider for A and B, but Q's long link is much faster:

A
P1
slow
P2
B
AS P
Q1
fast
Q2
AS Q

If we choose weights appropriately for the P1–P2 and Q1–Q2 links, we can have the optimum route be A–P1–Q1–Q2–P2–B; the AS_PATH would then be P–Q–P. To BGP, such an AS_PATH would appear as a loop, and be disallowed.

שאלה 26-4

7. Let A be the number of autonomous systems on the Internet, and let D (for diameter) be the

maximum AS path length.

(a) Give the connectivity model for which D is of order log A and another for which D is of

order *A* .

(b) Assuming each AS number is 2 bytes and each network number is 4 bytes, give an estimate

for the amount of data a BGP speaker must receive to keep track of the AS path to every network. Express your answer in terms of A, D, and the number of networks N.

7.

(a) The diameter D of a network organized as a binary tree, with root node as "backbone", would be of order logA. The diameter of a planar rectangular grid of connections would be of order

(b) For each AS S, the BGP node needs to maintain a record of AS_PATH to S, requiring 2*actual_path_length bytes. It also needs a list of all the networks within S, requiring 4*number_of_networks bytes. Summing these up for all autonomous systems, we get 2AD+4N, or 2AClogA+4N and 2AC +4N for the models from part (a), where C is a constant.

שאלה 28-4

28) IP hosts that are not designated routers are *required* to drop packets misaddressed to them, even if they would otherwise be able to forward them correctly. In the absence of this requirement, what would happen if a packet addressed to IP address A were inadvertently broadcast at the link layer? What other justifications for this requirement can you think of?

Network would be flooded with packets to A.

If the same host part of the address arrived at a misaddressed network address, it would be forwarded to the wrong host.

Increase latency.

Security issue?

שאלה 39-4

39) Suppose P,Q, and R are network service providers, with respective CIDR address allocations (*using the notation: "/12 in C4.50.0.0/12 denotes a netmask with 12 leading 1 bits, that is FF.F0.0.0*) C1.0.0.0/8, C2.0.0.0/8, and C3.0.0.0/8. Each provider's customers initially receive address allocations that are a subset of the provider's.

P has the following customers:

PA, with allocation C1.A3.0.0/16 and
PB, with allocation C1.B0.0.0/12.

Q has the following customers:

QA, with allocation C2.0A.10.0/20 and
QB, with allocation C2.0B.0.0/16.

Assume there are no other providers or customers.

(a) (a) Give routing tables for P, Q, and R assuming each provider connects to both of the others

P's routing table

Address	Next Hop
C2.0.0.0/8	Q
C3.0.0.0/8	R
C1.A3.0.0/16	PA
C1.B0.0.0/12.	PB

Q's routing table

Address	Next Hop
C3.0.0.0/8	R
C1.0.0.0/8	P
C2.0A.10.0/20	QA
C2.0B.0.0/16	QB

R's routing table

Address	Next Hop
C2.0.0.0/8	Q
C1.0.0.0/8	P

(b) (b) Now assume P is connected to Q and Q is connected to R , but P and R are not directly connected. Give tables for P and R.

P's routing table

Address	Next Hop
C2.0.0.0/8	Q

Q's routing table

Address	Next Hop
C3.0.0.0/8	R

R's routing table

Address	Next Hop
C2.0.0.0/8	Q

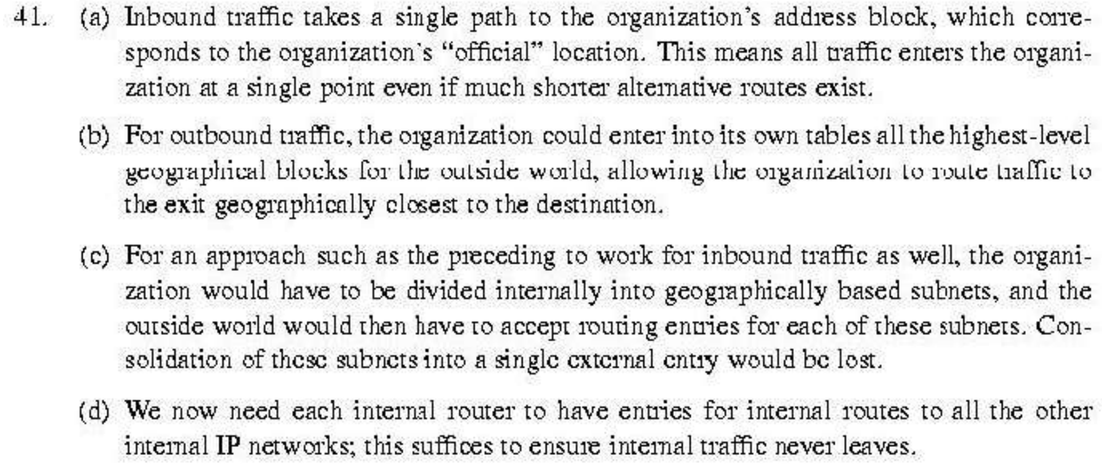
C1.B0.0.0/12.	PB	C1.0.0.0/8	P
C1.A3.0.0/16	PA	C2.0A.10.0/20	QA
		C2.0B.0.0/16	QB

(c) **(c) Suppose customer PA acquires a direct link to Q and QA acquires a direct link to P, in addition to existing links. Give tables for P and Q, ignoring R.**

P's routing table		Q's routing table		R's routing table	
Address	Next Hop	Address	Next Hop	Address	Next Hop
C2.0.0.0/8	Q	C3.0.0.0/8	R	C2.0.0.0/8	Q
~~C3.0.0.0/8~~	~~R~~	C1.0.0.0/8	P	~~C1.0.0.0/8~~	~~P~~
C1.A3.0.0/16	PA	C2.0A.10.0/20	QA		
C1.B0.0.0/12.	PB	C2.0B.0.0/16	QB		
C2.0A.10.0/20	QA	C1.A3.0.0/16	PA		

שאלה 41-4

Suppose most of the Internet used some form of geographical addressing, but that a large international organisation has a single IP network address and routes its internal traffic over its own links.
(i) Explain the routing inefficiency for the organisation's inbound traffic inherent in this situation.
(ii) Explain how the organisation might solve the problem for outbound traffic.
(iii) For your method above to work for inbound traffic, what would have to happen?
(iv) Suppose the large organisation now changes its addressing to separate geographical addresses for each office. What will its internal routing structure have to look like if internal traffic is still to be routed internally?
(4/41)



41. (a) Inbound traffic takes a single path to the organization's address block, which corresponds to the organization's "official" location. This means all traffic enters the organization at a single point even if much shorter alternative routes exist.

(b) For outbound traffic, the organization could enter into its own tables all the highest-level geographical blocks for the outside world, allowing the organization to route traffic to the exit geographically closest to the destination.

(c) For an approach such as the preceding to work for inbound traffic as well, the organization would have to be divided internally into geographically based subnets, and the outside world would then have to accept routing entries for each of these subnets. Consolidation of these subnets into a single external entry would be lost.

(d) We now need each internal router to have entries for internal routes to all the other internal IP networks; this suffices to ensure internal traffic never leaves.

שאלה 42-4

42) The telephone system uses geographical addressing. Why do you think the Internet didn't adopt this as a matter of course?

Mobility of products was foreseeable.

The logistics of the networks they were addressing lent better to parochial networks rather than parochial geography.

-Heterogenity

שאלה 4-45

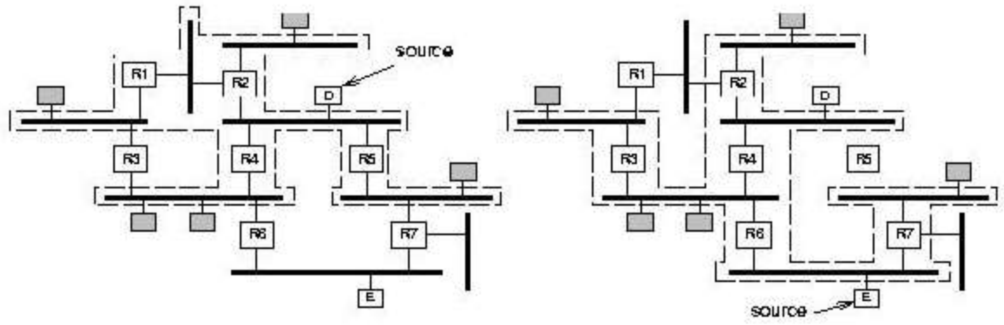
45) Suppose a network N within a larger organization A acquires its own direct connection to an Internet service provider, in addition to an existing connection via A. Let R1 be the router connecting N to its own provider, and let R3 be the router connecting N to the rest of A.

- **(a) (a) Assuming N remains a subnet of A, how should R1 and R2 be configured? What limitations would still exist with N's use of its separate connection? Would A be prevented from using N's connection? Specify your configuration in terms of what R1 and R2 should advertise, and with what paths. Assume BGP-like mechanism is available.**
- **(b) (b) Now suppose N gets it won network number; how does this change your answer in (a)?**
- **(c) (c) Describe a router configuration that would allow A to use N's link when its own link is down.**

שאלה 46-4

Consider the example internet in which sources d and e send packets to multicast group g, whose members are shaded in gray. Show the shortest path multicast trees for each sources

46.


R1
R2
source
D
R3
R4
R5
R6
R7
E
R1
R2
D
R3
R4
R5
R6
R7
source
E