Surname Name:	Pimenov Gleb
ID:	1820243077
Chapter:	5
Date:	May 5, 2024

Computer Networks
Assignment Chapter №5

Task 1. *Explain the difference between routing, forwarding, and switching.*

Solution. Routing:
- Routing is the process of determining the path that data packets should take from the source to the destination across a network.
- It involves analyzing network topology, traffic conditions, and routing protocols to determine the best path for data transmission.
- Routers are the devices responsible for routing. They use routing tables and algorithms to make decisions about where to forward packets based on factors like destination IP addresses, network congestion, and available paths.
- Routing occurs at the network layer (Layer 3) of the OSI model.

Forwarding:
- Forwarding is the act of passing data packets from one network device to another along the path determined by the routing process.
- It involves inspecting the destination address of each incoming packet and then sending it out through the appropriate interface to reach its next hop or final destination.
- Forwarding is performed by devices like routers.
- Forwarding operates at the network layer (Layer 3) of the OSI model.

Switching:
- Switching is the process of forwarding data packets within a local area network (LAN) from one device to another based on the hardware address (MAC address) of the devices.
- It involves making decisions about how to efficiently deliver data packets to their intended recipients within the same network segment or VLAN.
- Switches are the primary devices responsible for switching.
- They maintain MAC address tables to determine the appropriate port to forward incoming packets based on their destination MAC addresses.
- Switching operates at the data link layer (Layer 2) of the OSI model.

□

Task 2. *For the network given in Fig. 5-1, give global distance–vector tables like Table 5-1 (where D is the distance, N is neighbor) when*
(a) Each node knows only the distances to its immediate neighbors.
(b) Each node has reported the information it had in the preceding step to its immediate neighbors.
(c) Step (b) happens a second time.

Solution. Using Distance Vector Algorithm that is same as Bellman-Ford algorithm. It means that we are building routes from every node (router) to every node (router).

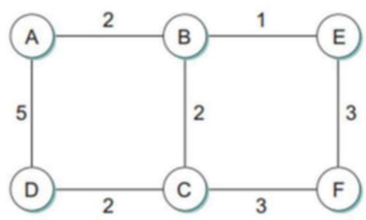

Fig. 5-1 A graph of a network (Task 2)

Table 5-1 Global Distance-Vector table (Task 2)

Node	Distances and neighbors to reach node											
	A		B		C		D		E		F	
	D	N	D	N	D	N	D	N	D	N	D	N
A												
B												
C												
D												
E												
F												

Table 5-1-1 Step 1 of building global distance-vector table (Task 2)

Node	Distances and neighbors to reach node											
	A		B		C		D		E		F	
	D	N	D	N	D	N	D	N	D	N	D	N
A	-	-	2	A	INF		5	A	INF		INF	
B	2	B	-	-	2	B	INF		1	B	INF	
C	INF		2	C	-	-	2	C	INF		3	C
D	5	D	INF		2	D	-	-	INF		INF	
E	INF		1	E	INF		INF		-	-	3	E
F	INF		INF		3	F	INF		3	F	-	-

Table 5-1-2 Step 2 of building global distance-vector table (Task 2)

Node	Distances and neighbors to reach node											
	A		B		C		D		E		F	
	D	N	D	N	D	N	D	N	D	N	D	N
A	-	-	2	A	4	B	5	A	INF		INF	
B	2	B	-	-	2	B	4	C	1	B	4	E
C	4	B	2	C	-	-	2	C	3	B	3	C
D	5	D	4	C	2	D	-	-	INF		5	C
E	3	B	1	E	3	B	INF		-	-	3	E
F	INF		4	E	3	F	5	C	3	F	-	-

Table 5-1-3 Step 3 (Solution) of building global distance-vector table (Task 2)

Node	Distances and neighbors to reach node											
	A		B		C		D		E		F	
	D	N	D	N	D	N	D	N	D	N	D	N
A	-	-	2	A	4	B	5	A	3	B	6	E
B	2	B	-	-	2	B	4	C	1	B	4	E
C	4	B	2	C	-	-	2	C	3	B	3	C
D	5	D	4	C	2	D	-	-	5	B	5	C
E	3	B	1	E	3	B	5	C	-	-	3	E
F	6	B	4	E	3	F	5	C	3	F	-	-

□

Task 3. *Suppose we have the forwarding tables shown in Table 5-2 for nodes A and F in a network where all links have cost 1. Give a diagram of the smallest network consistent with these tables.*

Table 5-2 Forwarding table (Task 3)

A

Node	Cost	Nexthop
B	1	B
C	2	B
D	1	D
E	2	B
F	3	D

F

Node	Cost	Nexthop
A	3	E
B	2	C
C	1	C
D	2	E
E	1	E

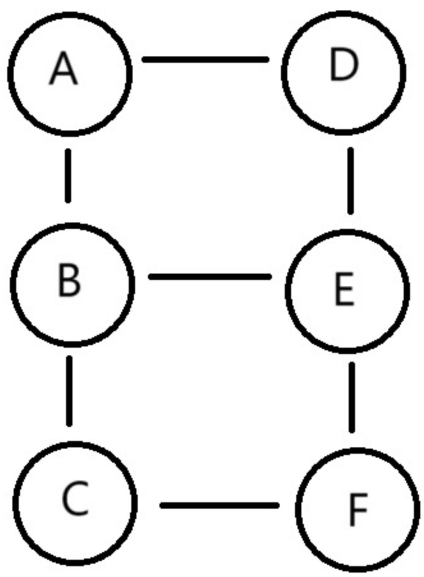

Fig. 5-1-4 Smallest network (Task 3)

Solution. □

Task 4. *An unfragmented IP packet, shown in Fig 5-2(a), has 1400 bytes of data and a 20-byte IP header. When the packet arrives at router RA, which has an MTU of 532 bytes, it has to be fragmented. The 3 fragmented packets are shown in Fig 5-2 (b). Suppose these fragments all pass through another router RB with an MTU of 380 bytes, not counting the link header.*
(a) Show the fragments the router RB produced.
(b) If the packet were originally fragmented for this MTU, how many fragments would be produced?

Solution. a) Given that after passing through router RA, the packet is fragmented into three fragments with sizes 512 bytes, 512 bytes, and 376 bytes respectively, we need to further fragment these packets to fit the

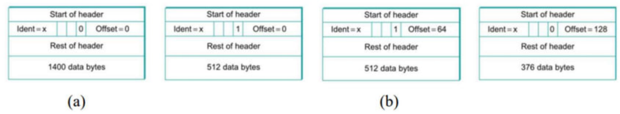

Fig. 5-2 (a) One unfragmented packet, (b) Three fragmented packets (Task 4)

MTU of router RB, which is 380 bytes.
To calculate the number and size of fragments for the second and third fragments after passing through router RB, we need to divide them into smaller fragments that fit the MTU of 380 bytes.
Let's perform the calculations:
For the first fragment (512 bytes):
It needs to be fragmented into smaller fragments to fit the MTU of router RB (380 bytes).
It can fragmented into 2 fragments with sizes 380 (360 of data + 20 of header) and 172 (152 of data + 20 of header) bytes.
First fragment has MF = 1 (more fragments), Fragment offset = 0
Second fragment has MF = 1, Fragment offset = 360/8 = 45
For the second fragment (512 bytes):
Similar to the first fragment, it needs to be fragmented into smaller fragments to fit the MTU of router RB (380 bytes).
It can fragmented into 2 fragments with sizes 380 (360 of data + 20 of header) and 172 (152 of data + 20 of header) bytes.
First fragment has MF = 1, Fragment offset = 512/8 = 64
Second fragment has MF = 1, Fragment offset = 872/8 = 109
For the third fragment (376 bytes):
It needs to be fragmented into smaller fragments to fit the MTU of router RB (380 bytes). Because 376 bytes of data + 20 bytes of header > 380
It can fragmented into 2 fragments with sizes 380 (360 of data + 20 of header) and 36 (16 of data + 20 of header) bytes.
First fragment has MF = 1, Fragment offset = 1024/8 = 128
Second fragment has MF = 0 (this fragment completes the data of original fragment), Fragment offset = 1384/8 = 173
Summary:
Fragment 1: 360 bytes data + 20 bytes header, MF=1, Offset=0
Fragment 2: 152 bytes data + 20 bytes header, MF=1, Offset=45
Fragment 3: 360 bytes data + 20 bytes header, MF=1, Offset=64
Fragment 4: 152 bytes data + 20 bytes header, MF=1, Offset=109
Fragment 5: 360 bytes data + 20 bytes header, MF=1, Offset=128
Fragment 6: 16 bytes data + 20 bytes header, MF=0, Offset=173

b) If the packet were originally fragmented for 380 bytes MTU we would have 4 fragments -> 1400 / (380 - 20) = 4 full fragments.
Fragment 1: 360 bytes data + 20 bytes header, MF=1, Offset=0
Fragment 2: 360 bytes data + 20 bytes header, MF=1, Offset=45
Fragment 3: 360 bytes data + 20 bytes header, MF=1, Offset=90
Fragment 4: 320 bytes data + 20 bytes header, MF=0, Offset=135

□

Task 5. *What is the maximum bandwidth at which an IP host can send 576-byte packets without having the Ident field wrap around within 60 seconds? Suppose that IP's maximum segment lifetime (MSL) is 60 seconds; that is, delayed packets can arrive up to 60 seconds late but no later. What might happen if this bandwidth were exceeded?*

Solution. To determine the maximum bandwidth at which an IP host can send 576-byte packets without having the Ident field wrap around within 60 seconds, we need to calculate how many packets can be sent before the Ident field (16 bits) wraps around.
Ident Field Size: The Ident field in the IP header is 16 bits, meaning it can represent values from 0 to 65535.
Number of Unique Ident Values: $2^16 = 65536$
Packet Size: Each packet is 576 bytes.
Time Period: 60 seconds.
We need to calculate the maximum number of packets that can be sent in 60 seconds without reusing an Ident value.
The Ident field can uniquely identify 65536 packets.
Maximum packet rate $= \frac{65536}{60} = 1092.2667$packets/second
Given each packet is 576 bytes:
Bandwidth = Packet Rate · Packet Size
Bandwidth $= 1092.2667 \cdot 576 = 629688$ bytes/second $= 629.688$ KB/s
The maximum bandwidth at which an IP host can send 576-byte packets without having the Ident field wrap around within 60 seconds is 629.688 KB/s.
If the bandwidth exceeds this limit, the Ident field will wrap around within the MSL (60 seconds). This can lead to several issues:
Packet Misidentification: Packets may be misidentified as duplicate or out-of-order if they share the same Ident value.
Data Corruption: Delayed packets might be incorrectly reassembled if they have the same Ident value as new packets.
Network Congestion: Increased packet collision and retransmission can cause network congestion and degrade overall network performance.
Security Risks: Potential for malicious users to exploit the wrap-around for replay attacks or other security vulnerabilities.

□

Task 6. *An organization has been assigned the prefix 200.1.1.0/24 and wants to form subnets for four departments, with hosts as follows:*
Department A 72 hosts,
Department B 35 hosts,
Department C 20 hosts,
Department 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)
Step 1: Calculate the Required Number of IP Addresses for Each Department
Department A: 72 hosts + 2 (network broadcast) = 74 addresses
Department B: 35 hosts + 2 (network broadcast) = 37 addresses
Department C: 20 hosts + 2 (network broadcast) = 22 addresses
Department D: 18 hosts + 2 (network broadcast) = 20 addresses
Step 2: Determine the Smallest Subnet Mask for Each Department

For Department A (74 addresses): The smallest subnet mask that can accommodate 74 addresses is /25 (128 addresses).
For Department B (37 addresses): The smallest subnet mask that can accommodate 37 addresses is /26 (64 addresses).
For Department C (22 addresses): The smallest subnet mask that can accommodate 22 addresses is /27 (32 addresses).
For Department D (20 addresses): The smallest subnet mask that can accommodate 20 addresses is /27 (32

addresses).
Step 3: Assign Subnets

Starting with the largest subnet:
Department A: 200.1.1.0/25 (128 addresses: 200.1.1.0 - 200.1.1.127)
Department B: 200.1.1.128/26 (64 addresses: 200.1.1.128 - 200.1.1.191)
Department C: 200.1.1.192/27 (32 addresses: 200.1.1.192 - 200.1.1.223)
Department D: 200.1.1.224/27 (32 addresses: 200.1.1.224 - 200.1.1.255)
This arrangement gives:
Department A: 200.1.1.0 - 200.1.1.127 (74 hosts, /25 subnet mask)
Department B: 200.1.1.128 - 200.1.1.191 (37 hosts, /26 subnet mask)
Department C: 200.1.1.192 - 200.1.1.223 (22 hosts, /27 subnet mask)
Department D: 200.1.1.224 - 200.1.1.255 (20 hosts, /27 subnet mask)
b)
If Department D grows to 34 hosts, the current /27 subnet (which supports only 30 hosts) will not be sufficient. We'll need to reallocate subnets to accommodate this change.
Reevaluate Subnet Requirements:
Department D needs at least $34 + 2 = 36$ addresses.
The smallest subnet mask that can accommodate 36 addresses is /26 (64 addresses).
Reassign Subnets:
To accommodate Department D's growth, we need to adjust the subnets:
Department A: 200.1.1.0/25 (unchanged, 128 addresses: 200.1.1.0 - 200.1.1.127)
Department B: 200.1.1.128/26 (unchanged, 64 addresses: 200.1.1.128 - 200.1.1.191)
Department D: 200.1.1.192/26 (new range, 64 addresses: 200.1.1.192 - 200.1.1.255)
Department C: We need to find a new range for Department C within the available address space.
Since we've allocated 200.1.1.192/26 for Department D, we need to move Department C to the next available range. We must split the range further:
New Department C: 200.1.1.192/27 (32 addresses: 200.1.1.192 - 200.1.1.223)
New Department D: 200.1.1.224/26 (64 addresses: 200.1.1.224 - 200.1.1.255)
Thus, the new subnet allocation will be:
Department A: 200.1.1.0 - 200.1.1.127 (74 hosts, /25 subnet mask)
Department B: 200.1.1.128 - 200.1.1.191 (37 hosts, /26 subnet mask)
Department C: 200.1.1.192 - 200.1.1.223 (22 hosts, /27 subnet mask)
Department D: 200.1.1.224 - 200.1.1.255 (34 hosts, /26 subnet mask)
In this new allocation, all departments will have enough IP addresses to accommodate their hosts, including the growth of Department D.

□

Task 7. *A router has just received the following new IP addresses: 57.6.96.0/21, 57.6.104.0/21, 57.6.112.0/21, and 57.6.120.0/21. If all of them use the same outgoing line, can they be aggregated? If so, to what? If not, why not?*

Solution. To determine if the given IP address blocks can be aggregated, we need to check if they share a common prefix that allows them to be summarized into a single, larger network.
First, let's convert these IP addresses and their subnet masks into binary form to find the common prefix.
57.6.96.0 = 00111001.00000110.01100000.00000000
Subnet Mask: /21 = 11111111.11111111.11111000.00000000

57.6.104.0 = 00111001.00000110.01101000.00000000
Subnet Mask: /21 = 11111111.11111111.11111000.00000000

57.6.112.0 = 00111001.00000110.01110000.00000000
Subnet Mask: /21 = 11111111.11111111.11111000.00000000

57.6.120.0 = 00111001.00000110.01111000.00000000
Subnet Mask: /21 = 11111111.11111111.11111000.00000000

Let's look at the binary forms and find the longest common prefix:
The common prefix here is 00111001.00000110.011, which is 19 bits long.
If all the networks can be aggregated, the resulting network must cover the entire range of the given IP addresses.
57.6.96.0 = 00111001.00000110.01100000.00000000
Subnet Mask: /19 = 11111111.11111111.11100000.00000000

In this case, the network 57.6.96.0/19 covers all the given IP address blocks:
57.6.96.0 - 57.6.127.255

Conclusion
Yes, the given IP address blocks can be aggregated. The aggregated address block is:
57.6.96.0/19

□

Task 8. *Given the network in Fig. 5-3, determine the routing table of R2 by aggregating the routes. The main entries of the routing table are shown in Table 5-3.*

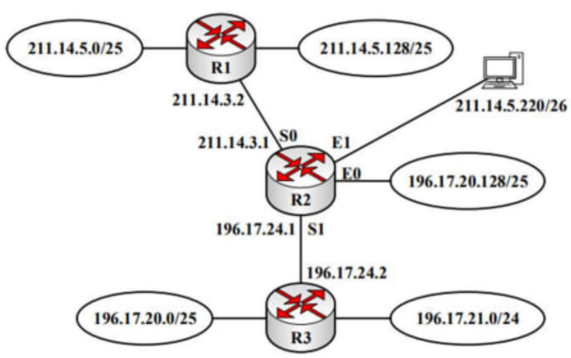

Fig. 5-3 A network (Task 8)

Table 5-3 Routing table (Task 8)

Destination	Mask	Next-hop	Interface	Metric

Solution. To determine the routing table of R2 by aggregating the routes given in Fig. 5-3, we need to identify the networks connected to each router and find common prefixes that can be aggregated.

Table 5-3-1 Routing table without aggregating (Task 8)

Destiantion	Mask	Next-hop	Interface	Metric
211.14.5.0	/25	211.14.3.2	S0	1
211.14.5.128	/25	211.14.3.2	S0	1
211.14.5.220	/26	Directly connected	E1	0
196.17.20.128	/25	Directly connected	E0	0
196.17.20.0	/25	196.17.24.2	S1	1
196.17.21.0	/24	196.17.24.2	S1	1

R1:
211.14.00000101.00000000/25
211.14.00000101.10000000/25

Result:
211.14.5.0/24
Verifying:
211.14.5.0-211.14.5.255
Aggregated subnet includes the entire range of IP addresses from the individual subnets.
R3:
196.17.00010100.00000000/25
196.17.00010101.00000000/24

Result:
196.17.20.0/23
Verifying:
196.17.20.0-196.17.21.255
Aggregated subnet includes the entire range of IP addresses from the individual subnets.

Table 5-3-2 Routing table with aggregating (Task 8)

Destiantion	Mask	Next-hop	Interface	Metric
211.14.5.0	/24	211.14.3.2	S0	1
211.14.5.220	/26	Directly connected	E1	0
196.17.20.128	/25	Directly connected	E0	0
196.17.20.0	/23	196.17.24.2	S1	1

□