

ТЕСТОВЕ ПО КОМПЮТЪРНИ МРЕЖИ (отговори)

Този файл е предназначен за студенти, изучаващи курса „Компютърни мрежи“ при Факултета по Математика и Информатика на СУ.

Включва 10 теста с отговори и секция с Блиц-въпроси.

Поради известни причини, които няма да бъдат опоменати тук, авторът пожела да остане анонимен!

Успешно преписване!

20. 12. 2013 г.

ТЕСТ 1

Въпрос 1:

100 BASE-FX реализира Етернет (Ethernet) стандарта при скорост на предаване 100 Mbps ...

Изберете едно:

- a. по тънък коаксиален кабел.
- b. по оптичен кабел. ✓
- c. по дебел коаксиален кабел.
- d. по кабел тип „усукана двойка“ (UTP).

Въпрос 2:

От време на време наблюдавате задръстване на локалната мрежа. Какви може да са причините?

Изберете едно или повече:

- a. Сегментиране на мрежата
- b. Broadcast storms (бури) ✓
- c. Работа в Full duplex (пълен дуплекс)
- d. Broadcast domain с твърде много хостове ✓
- e. Multicasting
- f. Ниска скорост на линиите ✓

Въпрос 3:

На рутер е въведена следната команда:

IP nat pool nat-тест 192.168.6.10 192.168.6.20 net-маска 255.255.255.0

Какъв тип NAT имаме?

Изберете едно:

- a. Статичен NAT
- b. Dynamic NAT with overload
- c. Port Address Translation
- d. Dynamic NAT ✓

Въпрос 4:

Кое от полетата на IPv4 header не е идентично с поле в IPv6 header?

Изберете едно:

- a. TTL ✓
- b. Version
- c. ToS
- d. Checksum

Въпрос 5:

Кой от посочените адреси е адрес на мрежа от клас C?

Изберете едно:

- a. 255.255.255.0
- b. 223.254.254.0
- c. 224.100.0.0
- d. 195.255.256.0 ✓

Въпрос 6:

На кой слой от OSI модела се определя оптималния път до дестинацията в мрежата?

Изберете едно:

- a. Физически
- b. Представителен
- c. Транспортен
- d. Сесиен
- e. Канален
- f. Мрежов ✓

Въпрос 7:

В полуудуплекс (half-duplex) Ethernet LAN, два хоста се опитват едновременно да изпратят данни, което предизвиква колизия (колизия). Какво следва да направят двата хоста?

Изберете едно:

- a. Destination хост изпраща „молба“ до източника за повторно предаване на фрейма.
- b. Електрически импулс показва, че колизията е изчистена.
- c. Рутерът, който е на сегмента, ще сигнализира, че колизията е изчистена.
- d. Сигналът „jam“ показва, че колизията е изчистена.
- e. И двата хоста ще опитат повторно предаване след произволен интервал от време. ✓
- f. Хостовете нищо няма да правят, тъй като по-горните слоеве са отговорни за корекция на грешки и повторно предаване.

Въпрос 8:

Коя от следните разновидности на NAT реализира политиката множество портове и частни IP адреси да излизат с един единствен публичен IP адрес?

Изберете едно:

- a. Port Loading
- b. Статичен NAT
- c. Dynamic NAT
- d. Port Address Translation ✓

Въпрос 9:

Конфигурирате PPP на интерфейс на рутер. Какви методи на аутентикация можете да изберете?

Изберете едно или повече:

- a. VNP
- b. SSL
- c. PAP ✓
- d. LAPB
- e. SLIP
- f. CHAP ✓

Въпрос 10:

Какво ще стане, ако IPv6 рутер, на който има 6to4, трябва да предава пакет към отдалечена дестинация, а следващият възел (хоп) е с адрес 2002::/16?

Изберете едно:

- a. На IPv6 пакета му се маха header-а и се заменя с IPv4 header.
- b. IPv6 пакет се опакова в IPv4 пакет, използвайки IPv4 protocol type 41. ✓
- c. Пакетът се тагва с IPv6 header и IPv6 префикс включително.
- d. IPv6 пакетът се изхвърля, защото тази дестинация не може да маршрутизира IPv6 пакети.

Въпрос 11:

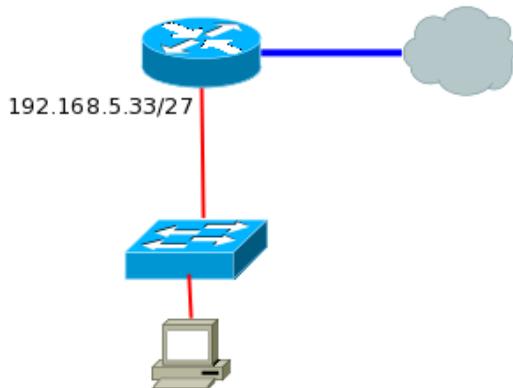
Имате class B мрежа с маска 255.255.255.0. Кое е вярно за тази мрежа?

Изберете едно или повече:

- a. 254 хоста на подмрежа ✓
- b. 24 хоста на подмрежа
- c. 256 подмрежи ✓
- d. 256 хоста на подмрежа
- e. 50 подмрежи

Въпрос 12:

На долната схема е показана клоновата мрежа Texas:



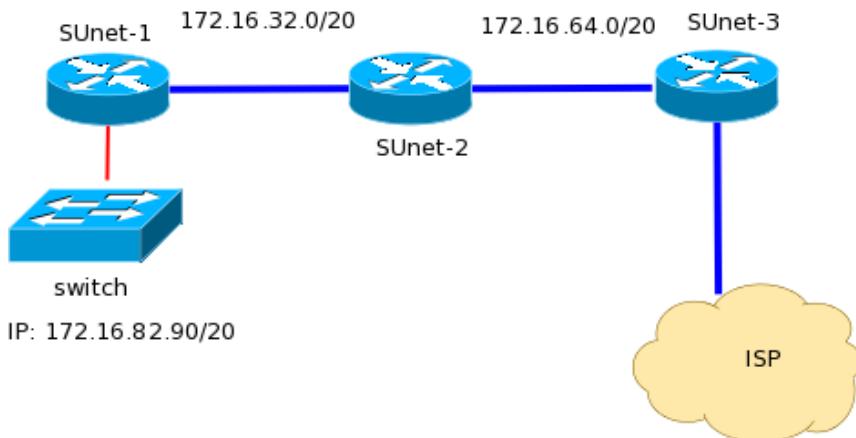
Кой IP ще бъде присвоен на PC-то?

Изберете едно:

- a. 192.168.5.5
- b. 192.168.5.63
- c. 192.168.5.75
- d. 192.168.5.40 ✓
- e. 192.168.5.32

Въпрос 13:

Дадена е мрежата:



Кои от долните IP адреси са broadcast адреси на горните префикси?

Изберете едно или повече:

- a. 172.16.32.255
- b. 172.16.64.255
- c. 172.16.47.255 ✓
- d. 172.16.95.255 ✓
- e. 172.16.79.255 ✓
- f. 172.16.82.255

Въпрос 14:

С кое от следните устройства администраторът може да сегментира локалната си мрежа?

Изберете едно или повече:

- a. медиа конвертори (FO-UTP)
- b. комутатори (суичове) ✓
- c. хъбове
- d. рипитери
- e. Маршрутизатори (рутери) ✓
- f. мостове (Bridges) ✓

Въпрос 15:

Кой от следните IP адреси е използваем (usable) за конфигуриране на мрежово устройство в мрежата 150.25.0.0 с маска 255.255.224.0?

Изберете едно или повече:

- a. 150.25.224.30
- b. 150.25.30.23 ✓
- c. 150.25.40.24
- d. 150.25.0.27 ✓

Въпрос 16:

Кое от следните твърдения за IPv6 е вярно?

Изберете едно:

- a. Имаме в наличност 2.7 милиоарда адреси.
- b. Broadcast-и няма, заменени са с мултикасти (multicasts). ✓
- c. Адресите не са йерархични и се присвояват произволно.
- d. Интерфейсът може да се конфигурира само с един IPv6 адрес.

Въпрос 17:



В софтуерна компания се изгражда локална мрежа. На фигуранта е посочен броят на компютрите във всеки отдел на компанията, които трябва да бъдат свързани в мрежата. Поставено е изискване компютрите от всеки отдел да бъдат в различни подмрежки на една клас „C” мрежа. Коя мрежова маска ще използвате?

Изберете едно:

- a. 255.255.255.192
- b. 255.255.255.224
- c. 255.255.255.240
- d. 255.255.255.128 ✓

Въпрос 18:

Изберете валидните IPv6 адреси.

Изберете едно или повече:

- a. 2001:3452:4952:2837:: ✓
- b. :: ✓
- c. 2000::
- d. ::192:168:0:1 ✓
- e. 2003:dead:beef:4dad:23:46:bb:101 ✓
- f. 2002:c0a8:101::42 ✓

Въпрос 19:

```
RA(config)#interface fastethernet 0/1
RA(config-if)#no shutdown
RA(config-if)#interface fastethernet 0/1.1
RA(config-subif)#encapsulation dot1q 1
RA(config-subif)#ip address 192.168.1.17 255.255.255.240
RA(config-if)#interface fastethernet 0/1.2
RA(config-subif)#encapsulation dot1q 2
RA(config-subif)#ip address 192.168.1.33 255.255.255.240
RA(config-if)#interface fastethernet 0/1.3
RA(config-subif)#encapsulation dot1q 3
RA(config-subif)#ip address 192.168.1.49 255.255.255.240
RA(config-subif)#end
```

Към виртуална локална мрежа (VLAN) 1 трябва да се добави ново мрежово устройство. Маршрутизаторът (router) RA е конфигуриран както е указано по-горе. Кой от посочените по-долу IP адреси трябва да получи новото мрежово устройство?

Изберете едно:

- a. 192.168.1.11/28
- b. 192.168.1.1/26
- c. 192.168.1.33/28
- d. 192.168.1.22/28 ✓

Въпрос 20:

Инсталирали сте FTP сървър, достъпен от Internet. По отношение на OSI модела, Кой е най-високият слой, по който стават FTP сесиите?

Изберете едно:

- a. Приложен ✓
- b. Транспортен
- c. Представителен
- d. Канален
- e. Сесиен
- f. Интернет

Въпрос 21:

Как изглежда в двоичен вид шеснайсетично число 78F3?

Изберете едно:

- a. 1010101101010100
- b. 1101010110011010
- c. 0010101111001101
- d. 0111100011110011 ✓
- e. 1010000011001101
- f. 1111010011001001

Въпрос 22:

Имате class C мрежа и трябва да я разделите така, че да имате поне 5 подмрежки с по минимум 18 хоста. Коя маска ще приложите?

Изберете едно:

- a. 225.225.224.0
- b. 225.225.255.240
- c. 255.255.255.224 ✓
- d. 225.225.240.0
- e. 225.225.255.0

Въпрос 23:

```
R#(config) #interface fastethernet 0/1
R#(config-if) #no shutdown
R#(config-if) #interface fastethernet 0/1.1
R#(config-subif) #encapsulation dot1q 10
R#(config-subif) #ip address 192.168.1.49 255.255.255.240
R#(config-if) #interface fastethernet 0/1.2
R#(config-subif) #encapsulation dot1q 60
R#(config-subif) #ip address 192.168.1.65 255.255.255.192
R#(config-if) #interface fastethernet 0/1.3
R#(config-subif) #encapsulation dot1q 120
R#(config-subif) #ip address 192.168.1.193 255.255.255.224
R#(config-subif) #end
```

Маршрутизатор (рутер) е конфигуриран да се свързва с магистрална (trunk) линия както е показано на диаграмата по-горе. На физическия FastEthernet 0/1 интерфейс е получен пакет от виртуална локална мрежа (VLAN) 10. Адресът на крайната точка (получател) за този пакет е 192.168.1.120. Какво ще направи маршрутизатора (рутер) с този пакет?

Изберете едно:

- a. Няма да направи нищо, защото адресите на подателя и получателя са от една и съща под-мрежа.
- b. Ще го върне обратно през под-интерфейс FastEthernet 0/1.2 към виртуална локална мрежа (VLAN) 60. ✓
- c. Ще го върне обратно през под-интерфейс FastEthernet 0/1.1 към виртуална локална мрежа (VLAN) 10.
- d. Ще го върне обратно през под-интерфейс FastEthernet 0/1.3 към виртуална локална мрежа (VLAN) 60.

Въпрос 24:

На мрежата SUnet е дадена Class C мрежа 199.166.131.0. Администраторът прилага маска 255.255.255.224. Колко хоста ще има на всяка подмрежка?

Изберете едно:

- a. 64
- b. 14
- c. 32
- d. 62
- e. 16
- f. 30 ✓

Въпрос 25:

Коя от следните характеристики е вярна по отношение на приложение на хъбове и комутатори?

Изберете едно:

- a. Комутаторите увеличават броя на колизионните домейни в мрежата. ✓
- b. Хъбовете са ефективни по отношение на оползотворяване на пропускателя спосоност.
- c. Портовете на хъбовете могат да се конфигурират с VLAN-и.
- d. Комутаторите не прехвърлят broadcasts.
- e. Комутаторите са по-ефективни от хъбовете при обработване на фреймове.

ТЕСТ 2

Въпрос 1:

Мрежта Alabala се състои от 5 отдела:

- Директорска администрация – 7 компютъра;
- Отдел „Поддръжка“ – 15 компютъра;
- Отдел „Финансов“ – 13 компютъра;
- Отдел „Търговски“ – 7 компютъра;
- Отдел „Иновации“ – 16 компютъра.

Каква маска ще приложите?

Изберете едно:

- a. 255.255.255.128
- b. 255.255.255.192
- c. 255.255.255.252
- d. 255.255.255.240
- e. 255.255.255.224 ✓
- f. 255.255.255.248

Въпрос 2:

Какъв е максимални брой IP адреси, които могат да бъдат присвоен в подмрежа с маска 255.255.255.224?

Изберете едно:

- a. 31
- b. 30 ✓
- c. 15
- d. 14
- e. 16
- f. 32

Въпрос 3:

PC в мрежов сегмент изпраща данни до друго PC на друг сегмент. Кой от следните отговори правилно описва точния ред на опаковане (encapsulation) на данните?

Изберете едно:

- a. Данни, Frame, сегмент, пакет, Bit
- b. Данни, пакет, Frame, сегмент, Bit
- c. Данни, сегмент, пакет, Frame, Bit ✓
- d. Данни, сегмент, Frame, пакет, Bit
- e. Данни, Frame, пакет, сегмент, Bit
- f. Данни, пакет, сегмент, Frame, Bit

Въпрос 4:

Кой е адреса на подмрежата за следния IP адрес на хост 172.16.210.0/22?

Изберете едно:

- a. 172.16.208.0 ✓
- b. 172.16.252.0
- c. 172.16.42.0
- d. 172.16.254.0
- e. 172.16.107.0

Въпрос 5:

Кое твърдение е вярно за комуникацията на мрежови устройства, разпределени във виртуални локални мрежи (VLAN)?

Изберете едно:

- a. Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на маршрутизатор (рутер). ✓
- b. Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на протокола VTP.
- c. Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта намагистрална (trunk) линия между комутаторите (комутатори).
- d. Устройства от една виртуална локална мрежа (VLAN) комуникират с помощта на маршрутизатор.

Въпрос 6:

Кой от следните IP адреси е частен IP адрес?

Изберете едно:

- a. 172.20.14.36
- b. 172.33.194.30
- c. 192.168.42.34 ✓
- d. 12.0.0.1
- e. 168.172.19.39

Въпрос 7:

Кое от следните ще уговори LCP (1-а фаза на PPP) при установяване на PPP връзка?

Изберете едно или повече:

- a. IPCP ✓
- b. Multilink
- c. Callback
- d. CHAP ✓
- e. Q.931

Въпрос 8:

Един маршрутизатор (рутер) има два серийни и два „FastEthernet“ интерфейси. Той трябва да свърже към Интернет основният офис и четири виртуални локални мрежи (VLANs) от мрежата на компанията. Как най-ефективно може да стане това?

Изберете едно:

- a. Чрез използване на преходници (transceivers) от серийни към FastEthernet интерфейси за свързване на две от виртуалните локални мрежи (VLANs) към маршрутизатора, и свързване на останалите две виртуални локални мрежи (VLANs) директно към FastEthernet портовете на маршрутизатора.
- b. Чрез добавяне на два допълнителни FastEthernet интерфейса за свързване на виртуалните локални мрежи (VLANs).
- c. Чрез магистрална (trunk) линия между FastEthernet интерфейсите на комутатора (комутатор) и маршрутизатора (рутер) и създаване на логически под-интерфейси (subinterfaces) за всяка виртуална локална мрежа (VLAN). ✓
- d. Чрез хъб (hub) за свързване на четирите виртуални локални мрежи (VLANs) с FastEthernet интерфейса на маршрутизатора (рутер).

Въпрос 9:

В мрежи, поддържащи VLSM, кой префикс ще използвате за връзки „точка-точка“, така че да не хабите IP адреси?

Изберете едно:

- a. /27
- b. /30 ✓
- c. /26
- d. /24
- e. /32

Въпрос 10:

Какъв вид съобщение издава PING, изпратен да тества свързаност?

Изберете едно:

- a. Няма верен отговор
- b. Information Interrupt Request
- c. Source Quench
- d. Timestamp Reply
- e. ICMP Echo Request ✓

Въпрос 11:

Свързвате PC към порт на комутатор, но PC-то няма достъп до ресурси на LAN-а.

Какъв е на-вероятният проблем, след като другите PC-та не го изпитват?

Изберете едно:

- a. В маршрутната таблица на рутера ням запис за новия хост.
- b. Комутаторът няма твърдо закодиран MAC адрес в MAC адрес таблицата.
- c. MAC адресът на хоста е неправилно конфигуриран.
- d. Портът на комутатора, към който е свързан хоста, не е присвоен към точния VLAN. ✓
- e. STP топологията (instance) с новия хост не е инициализирана.

Въпрос 12:

С коя команда можем да видим информация за всички мрежови интерфейси под Linux?

Изберете едно или повече:

- a. ifconfig -a ✓
- b. ifconfig /all
- c. ipconfig |A
- d. ifconfig |A
- e. ipconfig /all
- f. ipconfig
- g. ip -a ✓
- h. ifconfig

Въпрос 13:

Кой адрес за получател използва един DHCP клиент, когато се опитва да получи IP адрес?

Изберете едно:

- a. 0.0.0.255
- b. 255.255.255.255 ✓
- c. 0.0.0.0
- d. 127.0.0.1

Въпрос 14:

Кое от следните не се поддържа от IPv6?

Изберете едно:

- a. Unicast
- b. Anycast
- c. Broadcast ✓
- d. Multicast

Въпрос 15:

За да има коректна адресация, всеки един MAC адрес следва да е ...

Изберете едно:

- a. уникален за всички мрежи в организацията.
- b. уникален за Интернет (всички мрежи, до които имаме свързаност) освен ако не е мултикастен.
- c. уникален за Интернет (всички мрежи, до които имаме свързаност).
- d. уникален за локалния сегмент на мрежата.
- e. уникален за всички мрежи в организацията освен ако не е мултикастен.
- f. уникален за локалния сегмент на мрежата освен ако не е мултикастен. ✓

Въпрос 16:

На кой OSI слой заглавната част съдържа адрес на хост, който е дестинация и се намира в отдалечена мрежа?

Изберете едно:

- a. Приложен
- b. Сесиен
- c. Представителен
- d. Мрежов ✓
- e. Транспортен
- f. Физически
- g. Канален

Въпрос 17:

Кой IEEE стандарт дефинира Wi-Fi?

Изберете едно:

- a. IEEE 802.11 ✓
- b. IEEE 802.3
- c. IEEE 802.11c
- d. IEEE 802.5
- e. IEEE 802.11h

Въпрос 18:

Кои от долу изброените протоколи оперират на Интернет слоя на TCP/IP модела?

Изберете едно или повече:

- a. IPsec ✓
- b. DNS
- c. SONET/SDH
- d. HDLC
- e. RARP ✓
- f. SNMP
- g. DHCP
- h. BOOTP

Въпрос 19:

Мрежата 213.115.77.0 е разделена на подмрежки с префикс /28. Колко подмрежки и с по колко хоста ще се получат?

Изберете едно:

- a. 16 мрежи с 16 хоста
- b. 2 мрежи с 62 хоста
- c. 6 мрежи с 30 хоста
- d. 62 мрежи с 2 хоста
- e. 14 мрежи с 14 хоста ✓

Въпрос 20:

Вашият Cisco маршрутизатор има един WANинтерфейс към Интернет и два интерфейса, свързани към два сегмента на вашата LAN:

- IP адрес на интерфейс 1 – 195.196.197.1/25
- IP адрес на интерфейс 2 – 195.196.197.254/25

За известно време искате да прехвърлите само пощенския сървър с IP адрес 195.196.197.10 в другия сегмент, и то без да му променяте IP адреса. Коя команда ще трябва да изпълните на маршрутизатора, за да укажете новия път за достъп до този пощенски сървър?

Изберете едно:

- a. IP маршрут 195.196.197.10 255.255.255.255 195.196.197.254 ✓
- b. IP маршрут 195.196.197.10 255.255.255.128 195.196.197.254
- c. IP маршрут 195.196.197.10 255.255.255.255 195.196.197.1
- d. IP маршрут 195.196.197.10 255.255.255.128 195.196.197.1

Въпрос 21:

Кои са двете характеристики а “store and forward” switching (комутиране)?

Изберете едно или повече:

- a. Комутаторът получава целият кадър (фрейм), преди да започне да го прехвърля към изходен порт. ✓
- b. Закъснението през комутатора варира според дължината на фрейма. ✓
- c. Флуктуации в закъснението независещи от размера на фрейма.
- d. Комутаторът проверява адреса на дестинацията при получаван на заглавната част на фрейма (header).

Въпрос 22:

PC-то ви има IP адрес 172.16.209.10/22. Към коя подмрежка принадлежи?

Изберете едно:

- a. 172.16.42.0
- b. 172.16.107.0
- c. 172.16.254.0
- d. 172.16.208.0 ✓
- e. 172.16.252.0

Въпрос 23:

Кое от следните мрежови устройства работи на 2 слой?

Изберете едно или повече:

- a. повторител (Repeater)
- b. рутер
- c. хъб (Hub)
- d. комутатор ✓
- e. мост (Bridge) ✓

Въпрос 24:

Как би изглеждал IPv6 адреса 2001:67c:20d0:ffff::bac в разгърнат вид?

Изберете едно:

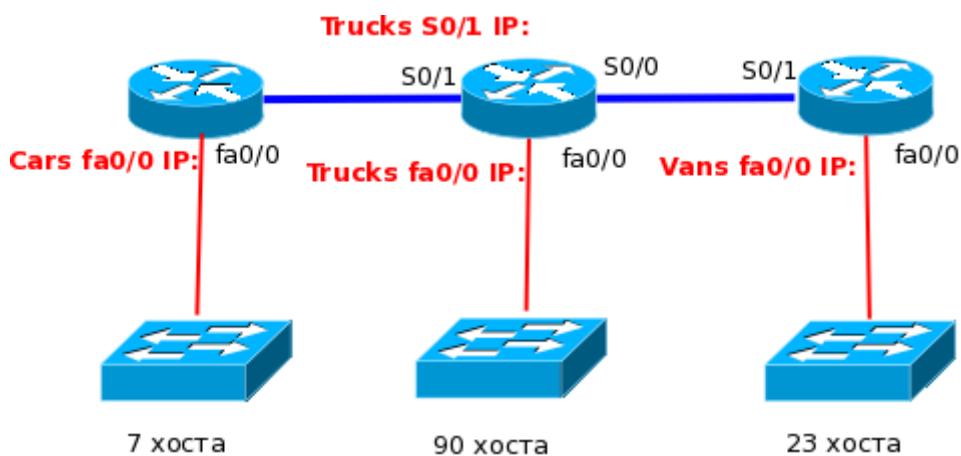
- a. 2001:67c:20d0:ffff:0000:ffff:0bac
- b. 0000:ffff:2001:67c:20d0:ffff:bac
- c. 2001:67c:20d0:ffff:0:bac
- d. 2001:067c:20d0:ffff:0000:0000:0000:0bac ✓

Въпрос 25:

Мрежата АВТОнет е получила префикс 192.168.55.0/24. Администраторите са приложили необходимите подмрежкови маски. При тази постановка са ви дадени следните IP адреси:

192.168.55.57/27
192.168.55.29/28
192.168.55.1/30
192.168.55.132/25
192.168.55.0/30
192.168.55.127/26

На кои интерфейси ще ги присвоите според посочената схема?



Cars fa0/0 IP: 192.168.55.29 /28

Trucks s0/1 IP: 192.168.55.1 /30

Trucks fa0/0 IP: 192.168.55.132 /25

Vans fa0/0 IP: 192.168.55.57 /27

ТЕСТ 3

Въпрос 1:

Стандартът IEEE 802.3 е за ...

Изберете едно:

- a. Token-Ring технология.
- b. ATM технология.
- c. Ethernet технология. ✓
- d. FDDI технология.

Въпрос 2:

Кой от следните слоеве на OSI модела принадлежи и на TCP/IP модела?

Изберете едно или повече:

- a. Приложен ✓
- b. Канален
- c. Мрежов
- d. Транспортен ✓
- e. Физически
- f. Сесиен

Въпрос 3:

Какъв е типа на информацията относно VLAN, която се вмъква в заглавната част на кадъра (фрейма)?

Изберете едно:

- a. VTP
- b. 802.1Q ✓
- c. CDP
- d. ISL
- e. LLC

Въпрос 4:

Имате мрежа, която поддържа VL2M и искате да приложите оптимален префикс за връзка „точка-точка“ (point to point). Кой ще е той?

Изберете едно:

- a. /18
- b. /23
- c. /30 ✓
- d. /38
- e. /27

Въпрос 5:

Кой обхват от IP адреси в двоичен формат съответства на първи октет от клас B адреси?

Изберете едно:

- a. 11100000-11101111
- b. 00000111-10001111
- c. 10000000-10111111 ✓
- d. 11000000-11011111
- e. 00000011-10011111

Въпрос 6:

Имате 2 комутатори във FMI LAN, нямате рутери. Портове 1, 2 и 3 са присвоени на VLAN 1 в комутатори 1 и 2, а портове 4, 5 и 6 са присвоени на VLAN 2 в двета комутатора. Тези два комутатора са свързани чрез trunk канал.

С кои от долните действия ще докажете, че trunk и VLAN са правилно зададени?

Изберете едно или повече:

- a. Хост 1 на VLAN 1 може да ping хост 2 на VLAN 1. ✓
- b. Хост 4 on VLAN 2 може да ping хост 2 on VLAN 2. ✓
- c. Хост 4 on VLAN 2 не може да ping хост 1 на VLAN 1. ✓
- d. Хост 1 на VLAN 1 може да ping хост 4 на VLAN 2.
- e. Хост 1 on VLAN 1 не може да ping хост 2 на VLAN 1.

Въпрос 7:

Колко подмрежки и хостове към всяка от тях ще имате, ако приложите префикс /28 маска на мрежа 210.10.2.0?

Изберете едно:

- a. 32 подмрежки и 18 хоста
- b. 6 подмрежки и 30 хоста
- c. 8 подмрежки и 32 хоста
- d. 16 подмрежки и 14 хоста ✓
- e. 30 подмрежки и 6 хоста

Въпрос 8:

Сравнявайки мостове (bridge-ове) и комутатори, кои от следните твърдения са верни?

Изберете едно или повече:

- a. Bridge-ове и комутатори увеличават размера на колизионния домейн.
- b. Комутаторът е многопортов bridge. ✓
- c. Bridge-овете и комутаторите научават MAC адреси чрез анализ на полето „source MAC адрес“ в заглавието на получния фрейм. ✓
- d. Bridge-ът прехвърля broadcast, но комутаторът не го прави.
- e. Bridge-овете са по-бързи от комутаторите защото имат по-малко портове.

Въпрос 9:

TCP/IP моделът се различава от OSI модела. Кой от слоевете принадлежи на TCP/IP модела?

Изберете едно или повече:

- a. Канален
- b. Сесиен
- c. Транспортен ✓
- d. Мрежов
- e. Приложен ✓
- f. Интернет ✓
- g. Физически

Въпрос 10:

Кое е вярно за Ethernet технологията?

Изберете едно:

- a. Хостовете са в логическа шинна топология. ✓
- b. Хостовете са в логическа кръгова топология.
- c. Хостовете са директно свързани към концентратор, наречен MSAU.
- d. Хостовете трябва да чакат електронен сигнал, за да предават данни.

Въпрос 11:

Кой е мултикаст адреса за all-router multicast access?

Изберете едно:

- a. FF02::1
- b. FF02::4
- c. FF02::3
- d. FF02::2 ✓

Въпрос 12:

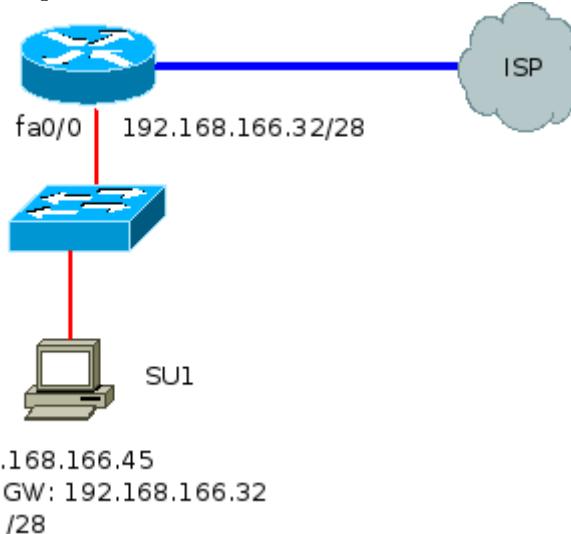
След смяна на NIC карта на PC в LAN мрежа комутаторът показва нов MAC адрес, присъединен към неговия port. Кои от следните отговори правилно описват MAC адреса?

Изберете едно или повече:

- a. Глобалн уникален 48 bit адрес. ✓
- b. Осигурен е от производителя на NIC картата. ✓
- c. Използван е като част от IPX/SPX конфигурация.
- d. Публичен IP адрес.
- e. Това е логически адрес

Въпрос 13:

Нова LAN е реализиран в мрежата SUNet:



Хостът SU1 няма достъп до никакви ресурси в мрежата. Какъв е проблемът?

Изберете едно:

- a. Default gateway е мрежовият адрес. ✓
- b. Маската на хоста е несъвместима с маската, която е на интерфейса на рутера.
- c. IP адресът на хоста принадлежи на друга подмрежка.
- d. Default gateway принадлежи на друга подмрежка, различна от тази на хоста.

Въпрос 14:

На IPv6 корпоративна (enterprise) мрежа се препоръчва да се присвои следния префикс:

Изберете едно:

- a. /8
- b. /48 ✓
- c. /16
- d. /3

Въпрос 15:

LAN мрежа с комутатори е зададена чрез следния списък, като за всеки комутатор е показано с кои други е свързан:

SWI-1 (SWI-2, SWI-4)	SWI-4 (SWI-1, SWI-5)
SWI-2 (SWI-1, SWI-3, SWI-6)	SWI-5 (SWI-4, SWI-6)
SWI-3 (SWI-2, SWI-6)	SWI-6 (SWI-2, SWI-3, SWI-5)

Така зададената топология съдържа цикли. Какъв тип зациклияне се предизвиква и кой е протокола, който предпазва то да не стане проблем?

Изберете едно:

- a. Маршрутно зациклияне, STP
- b. Маршрутно зациклияне (routing loops), hold down таймери
- c. Маршрутно зациклияне, split horizon
- d. Комутиращи цикли (switching loops), STP ✓
- e. Комутиращи цикли (switching loops), split horizon
- f. Комутиращи цикли, VTP

Въпрос 16:

Какво означава NAT?

Изберете едно:

- a. Network Address Table
- b. Network Architecture Translation
- c. National Anthem of Toronto
- d. Network Address Translation ✓

Въпрос 17:

Кое поле от фрейма разглежда схемата за разпознаване на грешки за да изпълни своята функция?

Изберете едно:

- a. ERR
- b. PDU
- c. Flag
- d. MTU
- e. MAC
- f. FCS ✓

Въпрос 18:

Кои от следните твърдения са предимства на VLAN-ите?

Изберете едно или повече:

- a. Опостяват администраторския контрол на комутатора. ✓
- b. Подобряват сигурността на мрежата.
- c. Увеличават размера на колизионните домейни.
- d. Увеличават рамера на broadcast домейните, като същевременно намаляват броя им.
- e. Увеличават броя на broadcast домейните, като същевременно намаляват размера им. ✓
- f. Позволяват логическо групиране на потребителите по функции. ✓

Въпрос 19:

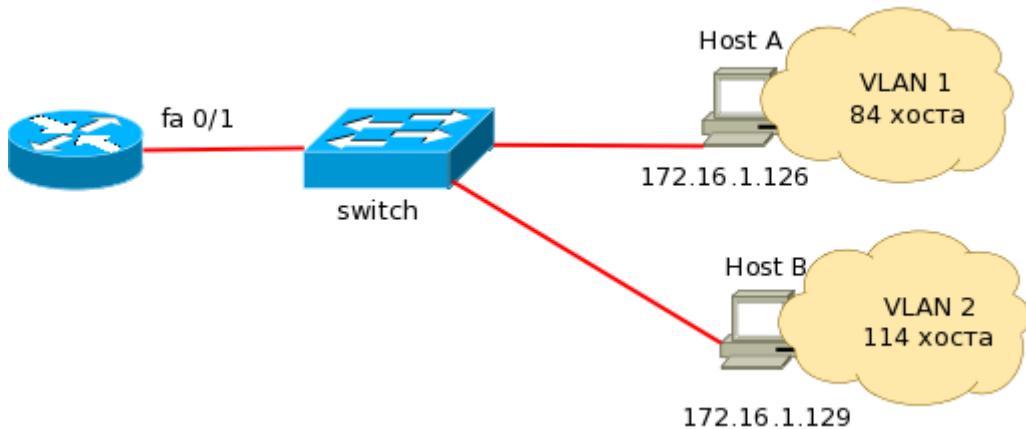
По отношение на мостове (bridge-ове) и комутатори, кое от следните твърдения е вярно?

Изберете едно или повече:

- a. И bridge-ове, и комутатори вземат решения за направляване на трафика на базата на адреси на 2 слой. ✓
- b. Bridge-овете са по-бързи от комутаторите.
- c. И bridge-ове, и комутатори направляват на 2 слой broadcast-ите. ✓
- d. Bridge-те дефинират broadcast домейн, докато комутаторите дефинират колизионни домейни.
- e. Комутаторите имат повече портове от bridge-овете. ✓
- f. Комутаторите са предимно софтуерно базирани bridge-ове.

Въпрос 20:

Дадена е мрежа на отдалечен офис:



Кое от долните твърдения описват правилната адресната схема в горната мрежа?

Изберете едно или повече:

- a. IP адресът 172.16.1.205 може да се присвои на хост във VLAN1.
- b. IP адресът 172.16.1.25 може да се присвои на хост във VLAN1. ✓
- c. Префиксът е 255.255.255.128 ✓
- d. LAN интерфейсът на рутера е конфигуриран с един IP адрес.
- e. LAN интерфейсът на рутера е конфигуриран с множество IP адреси. ✓
- f. Префиксът е 255.255.255.192

Въпрос 21:

Във всяка NAT конфигурация кой е вътрешният глобален (Inside Global) IP адрес?

Изберете едно:

- a. Публичен адрес, който представя вътрешен хост пред външната мрежа. ✓
- b. Уникален IP адрес, който се използва във вътрешната мрежа.
- c. Сумаризираният (summarized) адрес на всички вътрешни подмрежкови адреси.
- d. Частен IP адрес присвоени на хост във вътрешната мрежа.

Въпрос 22:

Адресът 172.0.0.1 е ...

Изберете едно:

- a. резервиран от IANA адрес.
- b. частен адрес.
- c. публичен адрес. ✓
- d. резервиран адрес за тестване (loopback адрес).

Въпрос 23:

Кои от следните съкращения са коректни за IPv6 адреса
2001:0d02:0000:0000:0014:0000:0000:0095?

Изберете едно или повече:

- a. 2001:d02::14:0:0:95 ✓
- b. 2001:d02::14::95
- c. 2001:0d02::0014::0095
- d. 2001:d02:0:0:14::95 ✓

Въпрос 24:

Кой от следните процеси се използва за откриване на hardware (MAC)адрес на LAN контролер?

Изберете едно:

- a. Proxy ARP
- b. Inverse ARP
- c. ARP ✓
- d. Reverse ARP

Въпрос 25:

Транспортният слой изпълнява следните функции:

Изберете едно:

- a. транслиране на данни, конвертиране, криптиране, декриптиране, компресия, декомпресия.
- b. кодиране на сигнали.
- c. контролиране на комуникацията от край до край между процеси, изпълнявани на различни хостове. ✓
- d. контролиране на достъпа до преносната среда, приемане и изпращане на кадри (frames).

ТЕСТ 4

Въпрос 1:

Кои са типични характеристики на VLAN?

Изберете едно или повече:

- a. Trunk каналите носят трафика на множество VLAN-и. ✓
- b. VLAN-ите логически разделят комутатора на множество независими суичове на слой 2. ✓
- c. VLAN-ите увеличават броя на необходимите комутатори.
- d. VLAN се разпростира през множество комутатори. ✓
- e. VLAN-ите намаляват броя на необходимите комутатори.
- f. VLAN значително увеличава трафика заради добавената trunking информация.

Въпрос 2:

Какви ползи ще извлече от VLAN технологията една голяма корпорация?

Изберете едно или повече:

- a. VLAN-ите повишават сигурността чрез филтриране на пакети.
- b. VLAN-ите дефинират сегментирани broadcast domain-и в мрежи с комутатори. ✓
- c. VLAN-ите осигуряват метод за комуникации между IP адреси в големи мрежи.
- d. VLAN-ите значително улесняват добавяне, преместване или промяна на хостове в мрежата. ✓
- e. VLAN-ите осигуряват комуникации с ниско закъснение и висока пропускателна способност.
- f. VLAN-ите позволяват мрежовите услуги да се организират по отдели, а не по физическо разположение. ✓

Въпрос 3:

Хост е конфигуриран със статичен IP адрес, но default gateway е некоректен. Кой слой на модела OSI ще бъде засегнат първи от тази конфигурационна грешка?

Изберете едно:

- a. слой 5
- b. слой 4
- c. слой 3 ✓
- d. слой 1
- e. слой 2

Въпрос 4:

Докато се опитвате да откриете със свързаността на дадено PC, получавате следната информация:

Local PC IP адрес: 190.0.3.35/24

Default Gateway: 190.0.3.1

Remote Server: 190.0.5.250/24

След това провеждате следните от PC-то:

Ping 127.0.0.1 - Unsuccessful

Ping 190.0.3.35 - Successful

Ping 190.0.3.1 - Unsuccessful

Ping 190.0.5.250 - Unsuccessful

Каква е причината, предизвикала този проблем?

Изберете едно:

- a. TCP/IP не е инсталиран ✓
- b. Отдалечен проблем във физическия слой
- c. Мрежовият контролер (NIC) не работи
- d. Локален проблем във физическия слой

Въпрос 5:

Кои са трите адресни обхвата, принадлежащи на частните адреси според RFC 1918 и използвани в NAT?

Изберете едно или повече:

- a. 172.16.0.0 to 172.31.255.255 ✓
- b. 10.0.0.0 to 10.255.255.255 ✓
- c. 224.0.0.0 to 239.255.255.255
- d. 0.0.0.0 to 255.255.255
- e. 127.0.0.0 to 127.255.255.255
- f. 192.168.0.0 to 192.168.255.255 ✓
- g. 172.16.0.0 to 172.16.255.255

Въпрос 6:

Кой е префиксът на хост с IP адрес 201.100.5.68/28?

Изберете едно:

- a. 201.100.5.31
- b. 201.100.5.0
- c. 201.100.5.64 ✓
- d. 201.100.5.65
- e. 201.100.5.32
- f. 201.100.5.1

Въпрос 7:

На кой слой от OSI модела оперират TTL филтрите използвани от някои интернет доставчици?

Изберете едно:

- a. Сесиен
- b. Приложен
- c. Мрежов ✓
- d. Транспортен
- e. Презентационен

Въпрос 8:

Кои от следните IP адреси от мрежата 27.35.16.32/28 могат да бъдат присвоени на хостове?

Изберете едно или повече:

- a. 27.35.16.33 ✓
- b. 27.35.16.48
- c. 27.35.16.47
- d. 27.35.16.44 ✓
- e. 27.35.16.45 ✓
- f. 27.35.16.32

Въпрос 9:

Каква е целта на алгоритъма spanning-tree в комутираната LAN?

Изберете едно:

- a. Осигурява механизъм за следене на мрежи в среди с комутатори.
- b. Да сегментира мрежата на множество колизия домейни.
- c. Да управлява VLAN-и през множество комутатори.
- d. Да предпазва от зациклияне на 2 слой (switching loops) в мрежи с резервирани пътища между комутаторите. ✓
- e. Да предпазва от зациклияне на маршрути routing loops) в мрежите.

Въпрос 10:

Кои от следните предизвикват задръстване в LAN трафика?

Изберете едно или повече:

- a. Full duplex операции
- b. Сегментиране
- c. Твърде много хостове в broadcast domain ✓
- d. Broadcast storms (бури) ✓
- e. Multicasting ✓
- f. Тясна честотна лента (bandwidth), т.е ниска скорост ✓

Въпрос 11:

Две станции в LAN започват да предават в един и същи момент, което води до колизия. Какво става в мрежата при това положение?

Изберете едно или повече:

- a. След възстановяване на предаването устройствата, участвали в колизията, имат приоритет пред останалите.
- b. Всяко устройство на Ethernet сегмента спира да предава кратък период от време.
- c. Устройството, въвлечено в колизията, спира да предава за кратък период от време. ✓
- d. Сигнал „jam“ информира всички устройства, че е настъпила колизия. ✓
- e. Колизията стартира „random back-off algorithm“ (енратор на случайно число, след което предаването ще се повтори). ✓

Въпрос 12:

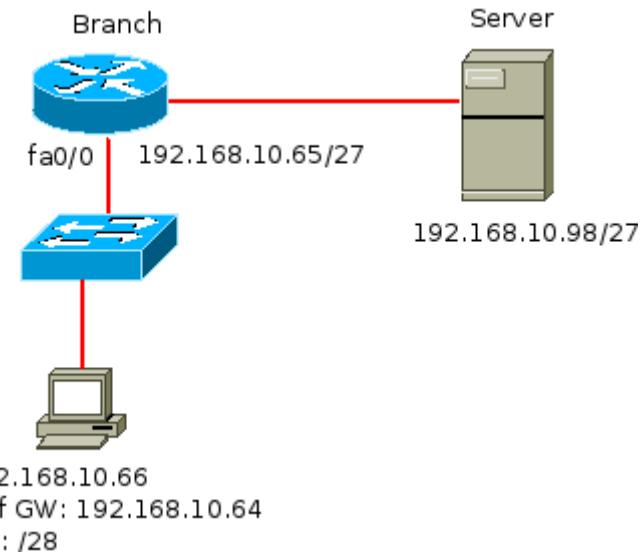
Кой от следните адреси може да се присвои на хост, ако се използва маска 255.255.254.0?

Изберете едно или повече:

- a. 113.10.4.0
- b. 26.35.3.255
- c. 152.135.7.0 ✓
- d. 175.33.4.255 ✓
- e. 17.35.36.0
- f. 186.54.3.0 ✓

Въпрос 13:

Дадена е следната схема:



В LAN-а на Branch рутера е инсталирано ново PC. PC-то не може да се свърже със сървъра.

Какъв е проблемът?

Изберете едно:

- a. IP адресът на рутера е неточен.
- b. Маската на PC-то е зададена неточно.
- c. Сървърът има невалиден IP адрес.
- d. Default gateway на PC-то е зададен неточно. ✓
- e. IP адресът на PC-то е невалиден.

Въпрос 14:

Вие сте системен администратор на БУЛДОГ ООД. Мрежата ви се състои от две подмрежки. Всички клиентски компютри са разположени в едната подмрежка. Всички сървъри и маршрутизатори се намират в център за данни и използват другата подмрежка и следните адреси:

рутер1	Маршрутизатор	10.1.1.1
рутер2	Маршрутизатор	10.1.1.2
рутер3	Маршрутизатор	10.1.255.1
DNS1	DNS Сървър	10.1.10.1
DNS2	DNS Сървър	10.1.10.2
Buldog1	Сървър за данни	10.1.11.1
Buldog2	Сървър за данни	10.1.11.2

Вие добавяте нов сървър за електронна поща в центъра за данни. Сървърът се казва Bulldog3.

По време на инсталацията вие настройвате TCP/IP по следния начин:

IP адрес	10.1.1.3
Subnet маска	255.255.255.0
Default gateway	10.1.1.2

След инсталацията вие откривате, че Bulldog3 не може да комуникира с никой от другите сървъри. Тествате мрежовата свързаност с командата PING и получавате следното съобщение за грешка: "Destination host unreachable".

За да функционира Bulldog3 трябва да може да комуникира с останалите сървъри. Коя от изброените промени ще отстрани проблема?

Изберете едно:

- a. Да се смени IP адреса на BULLDOG3 на 10.1.11.3
- b. Да се смени default gateway на BULLDOG3 на 10.1.1.1
- c. Да се смени маската на подмрежата на BULLDOG3 на 255.255.0.0 ✓
- d. Да се смени IP адреса на BULLDOG3 на 10.1.10.3

Въпрос 15:

RARP е протокол за ...

Изберете едно:

- a. динамично конфигуриране на IP адреса на хост, на базата на неговия MAC. Методът не изискава сървър.
- b. динамично намиране на IP адреса на хост, чиито MAC ни е известен. Методът не изискава сървър.
- c. динамично конфигуриране на IP адреса на хост, на базата на неговия MAC. Методът изискава сървър. ✓
- d. динамично намиране на MAC адреса на хост, чието IP ни е известно. Методът не изискава сървър.
- e. динамично намиране на IP адреса на хост, чиито MAC ни е известен. Методът изискава сървър.
- f. динамично намиране на MAC адреса на хост, чието IP ни е известно. Методът изискава сървър.

Въпрос 16:

Хой от следните IP адреси попада в CIDR блок 115.54.4.0/22?

Изберете едно или повече:

- a. 115.54.7.64 ✓
- b. 115.54.3.32
- c. 115.54.12.128
- d. 115.54.5.128 ✓
- e. 115.54.8.32
- f. 115.54.6.255 ✓

Въпрос 17:

Мрежата 201.145.32.0 е разделена на подмрежки с префикс /26. Колко подмрежки и с по колко хоста ще се получат?

Изберете едно:

- a. 2 мрежи с 62 хоста ✓
- b. 4 мрежи с 64 хоста
- c. 64 мрежи с 4 хоста
- d. 6 мрежи с 30 хоста
- e. 62 мрежи с 2 хоста

Въпрос 18:

В IPv6 адреса колко бита са включени във всяко поле, разделено със знака „::“?

Изберете едно:

- a. 24
- b. 4
- c. 16 ✓
- d. 3

Въпрос 19:

Имате двоичното число 10011101. Преобразувайте го в 16-ен формат.

Изберете едно:

- a. 157
- b. 0x9D ✓
- c. 158
- d. 0x19
- e. 0x9F
- f. 156

Въпрос 20:

Какъв е EUI-64 формата на идентификатора на интерфейса. ако MAC адресът е 00-0C-27-A2-13-1B?

Изберете едно:

- a. FEFE:C:27A2:131B
- b. 020C:27FF:FEA2:131B ✓
- c. C:27A2:131B
- d. 000C:27A2:131B:0000:0000

Въпрос 21:

Кои видове достъп до интернет могат да се осъществят в Етернет среда?

Изберете едно или повече:

- a. ISDN
- b. ADSL
- c. Dial-up
- d. PPPoE ✓
- e. DSL
- f. LAN ✓

Въпрос 22:

Кой метод на комутиране осигурява най-високо ниво на интегритет и безпогрешно транспортиране на трафика за сметка на по-голямо закъснение?

Изберете едно:

- a. 802.1q Forwarding
- b. Cut-through
- c. Fragment-free
- d. Store-and-forward ✓
- e. Frame-filtering
- f. VTP Transparent Mode

Въпрос 23:

Колизиите при мрежите от тип CSMA/CD възникват, когато ...

Изберете едно:

- a. две мрежови устройства не откриват сигнал по мрежата, след което започват да предават данни едновременно. ✓
- b. едно мрежово устройство „слуша” и не открива сигнал по мрежата.
- c. едно мрежово устройство получи съобщение по мрежата.
- d. едно мрежово устройство не функционира.

Въпрос 24:

Кое от следните полета се съдържа в заглавната част на IEEE Ethernet фрейма?

Изберете едно:

- a. Source и Destination MAC адрес. ✓
- b. Source мрежов адрес и Destination MAC адрес.
- c. Source и Destination MAC адрес и Source и Destination мрежов адрес.
- d. Source и Destination мрежов адрес.
- e. Source MAC адрес и Destination мрежов адрес.

Въпрос 25:

Как би изглеждал IPv6 адреса 2001:4b58:acad:252::2e в разгърнат вид?

Изберете едно:

- a. 2001:4b58:acad:252:ffff:2e
- b. 2001:4b58:acad:252:0000:2e
- c. 2001:4b58:acad:0252:0000:0000:0000:002e ✓
- d. 2001:4b58:acad:252:0000:ffff:002e

ТЕСТ 5

Въпрос 1:

Изберете валидните IPv6 адреси.

Изберете едно или повече:

- a. 2002:c0a8:101::42 ✓
- b. 2001:3452:4952:2837:: ✓
- c. 2000::
- d. 2003:dead:beef:4dad:23:46:bb:101 ✓
- e. ::192:168:0:1 ✓
- f. :: ✓

Въпрос 2:

Кои от следните твърдения са верни за IPv6 Unicast адресите?

Изберете едно или повече:

- a. Има само един loopback адрес, който е ::1 ✓
- b. Link-local адресите започват с FF00::/10
- c. Link-local адресите започват с FE00::/12
- d. Глобалните адресите започват с 2000::/3 ✓

Въпрос 3:

Кое е най-близко до машинен език (език на процесора)?

Изберете едно:

- a. Decimal
- b. Hexadecimal
- c. Binary ✓
- d. Octal

Въпрос 4:

Относно VLSM, кое от следните твърдения най-добре описва концепцията „маршрут aggregation“?

Изберете едно:

- a. Изтриване на неизползваните адреси при създаване на много подмрежки.
- b. Връщане на неизползваните адреси чрез промяна на мрежовите префикси.
- c. Изчисляване на наличните хост адреси в AS.
- d. Комбинира в един ред (супермрежа) маршрутите до множество мрежи. ✓

Въпрос 5:

Коя е максималната скорост, определена от IEEE 802.11B стандарта за безжични LAN?

Изберете едно:

- a. 100 Mbps
- b. 54 Mbps
- c. 10 Mbps
- d. 11 Mbps ✓

Въпрос 6:

IP мрежата 210.106.14.0 е разделена на подмрежки с префикс /24. Колко мрежи и с по колко хостове ще се получат?

Изберете едно:

- a. 6 мрежи с 64 хоста
- b. 4 мрежи с 128 хоста
- c. 2 мрежи с 24 хоста
- d. 8 мрежи с 36 хоста
- e. 1 мрежа с 254 хоста ✓

Въпрос 7:

Искате да сегментирате LAN-а на множество broadcast domain-и. Коя технология ще приложите?

Изберете едно:

- a. Transparent bridging (прозрачен мост)
- b. Cut-through switching
- c. Fragment-free switching (комутиране)
- d. Store-and-forward switching
- e. Virtual LANs ✓

Въпрос 8:

Каква информация се добавя към всеки фрейм при действието „frame tagging” в един комутатор (комутатор), за да може да се осъществи преноса на този фрейм по една магистрална (switched trunk) линия?

Изберете едно:

- a. Хардуерния (MAC) адрес на комутатора. (комутатор)
- b. Идентификатора на виртуалната локална мрежа (VLAN ID). ✓
- c. Хардуерния (MAC) адрес на крайното устройство, до което се изпраща фреймът.
- d. Специфичен идентификатор на крайния порт (the BID).

Въпрос 9:

Кой протокол автоматизира всички тези TCP/IP функции: конфигуриране на IP адреси, мрежови маски, default gateways и DNS сървър на хостове в мрежата?

Изберете едно:

- a. SMTP
- b. DARP
- c. DHCP ✓
- d. CDP
- e. SNMP

Въпрос 10:

Кой от долните три протоколи принадлежат на приложния слой?

Изберете едно или повече:

- a. SMTP ✓
- b. ARP
- c. TFTP ✓
- d. CDP
- e. ICMP
- f. HTTPS ✓

Въпрос 11:

Провайдерът ви предоставил една цяла клас В мрежа. Трябва да я разделите на най-малко 300 подмрежки, които да поддържат най-малко по 50 хоста. Кои от долните префикси удовлетворяват тези изисквания?

Изберете едно или повече:

- a. 255.255.255.0
- b. 255.255.248.0
- c. 255.255.255.128 ✓
- d. 255.255.255.192 ✓
- e. 255.255.255.224
- f. 255.255.252.0

Въпрос 12:

Кой протокол преобразува логическите адреси от мрежовия слой в локални хардуерни адреси?

Изберете едно:

- a. RARP
- b. BOOTP
- c. ARP ✓
- d. DHCP

Въпрос 13:

Кой от долните протоколи работи на слой 2 на OSI модела и служи за предпазване от зацикляне (loop-free мрежа)?

Изберете едно:

- a. IGRP
- b. STP ✓
- c. VTP
- d. CDP
- e. RIP

Въпрос 14:

Ако хост в мрежа има адрес 172.16.45.14/30, какъв ще е префиксът, към който принадлежи хостът?

Изберете едно:

- a. 172.16.45.4
- b. 172.16.45.0
- c. 172.16.45.8
- d. 172.16.45.12 ✓
- e. 172.16.45.18

Въпрос 15:

Кой е префиксът за IPv6 Multicast?

Изберете едно:

- a. F000::/16
- b. FF00::/8 ✓
- c. 0::/8
- d. 4000::/8

Въпрос 16:

Корпоративната LAN е един „плосък“ Ethernet сегмент. Искате да я разделите на 2 сегмента с помощта на рутер. Какво ще постигнете с това?

Изберете едно:

- a. Бродкастите от сегмент 1 няма да се пренасят в сегмент 2. ✓
- b. Ще се намали броя на broadcast домейните.
- c. Бродкастването на трафика между сегментите ще е по-ефективно.
- d. Ще се увеличи броят на колизиите.

Въпрос 17:

Кои от следните протоколи работят на Приложния слой на OSI модела?

Изберете едно или повече:

- a. Няма верен отговор
- b. Telnet ✓
- c. ARP
- d. FTP ✓
- e. IP
- f. TCP

Въпрос 18:

Кои от следните IP хост адреси са валидни за префикс /27?

Изберете едно или повече:

- a. 201.45.116.159
- b. 217.63.12.192
- c. 15.234.118.63
- d. 83.121.178.93 ✓
- e. 192.168.19.37 ✓
- f. 134.178.18.56 ✓

Въпрос 19:

ARP изпраща заявки, които са ...

Изберете едно:

- a. broadcast на 2-ри слой от OSI модела и broadcast на 3-ти.
- b. broadcast на 2-ри слой от OSI модела и unicast на 3-ти. ✓
- c. multicast на 2-ри слой от OSI модела и multicast на 3-ти.
- d. broadcast на 2-ри слой от OSI модела и multicast на 3-ти.
- e. multicast на 2-ри слой от OSI модела и broadcast на 3-ти.

Въпрос 20:

Към коя виртуална локална мрежа (VLAN) по поддабиране принадлежи една магистрална (trunked) линия?

Изберете едно:

- a. Към всички дефинирани виртуални локални мрежи (VLAN). ✓
- b. Към дефинирана виртуална локална мрежа (VLAN) с най-малък номер.
- c. Последната дефинирана виртуална локална мрежа (VLAN).
- d. Първата дефинирана виртуална локална мрежа (VLAN).

Въпрос 21:

На СУнет е предоставен class C IP префикс 189.66.1.0. Ако приложите маската 255.255.255.224, колко хоста ще има на всяка подмрежа?

Изберете едно:

- a. 32
- b. 16
- c. 64
- d. 14
- e. 62
- f. 30 ✓

Въпрос 22:

Кои от посочените са предимства на оптичните кабели при изграждане на мрежи?

Изберете едно или повече:

- a. По-висока скорост от UTP.
- b. Нисък шанс за поразяване от мълния. ✓
- c. Устойчивост към електромагнитни смущения. ✓
- d. Позволява информационен пренос на големи разстояния. ✓
- e. По-евтини мрежови карти (адаптори) отколкото за медни кабели.
- f. По-гъвкав от медните еквиваленти.

Въпрос 23:

Имате Class C мрежа и ви трябват 10 подмрежки. Каква маска ще изберете, за да имате оптимален брой хост адреси?

Изберете едно:

- a. 255.255.255.240 ✓
- b. 255.255.255.192
- c. 255.255.255.248
- d. 255.255.255.224

Въпрос 24:

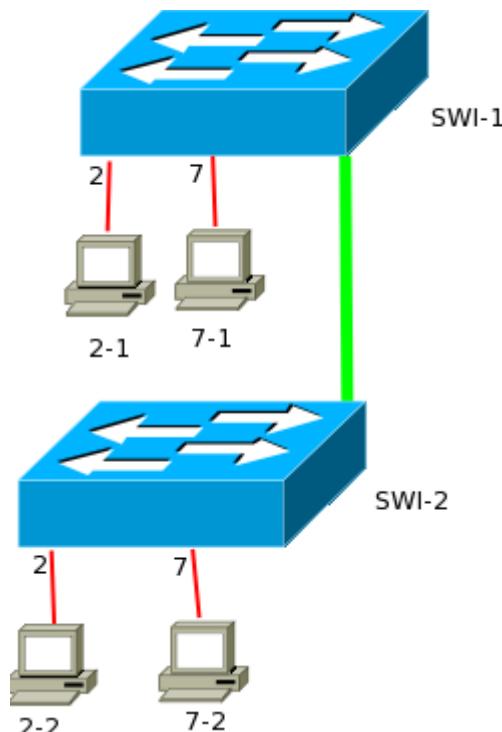
С коя команда се присвоява последния използваем IP адрес от префикса 192.168.32.128/28 на интерфейса на рутера?

Изберете едно:

- a. SUA(config-if)# ip адрес 192.168.32.158 255.255.255.240
- b. SUA(config-if)# ip адрес 192.168.32.158 255.255.255.240
- c. SUA(config-if)# ip адрес 192.168.32.142 255.255.255.240 ✓
- d. SUA(config-if)# ip адрес 192.168.32.144 255.255.255.240
- e. SUA(config-if)# ip адрес 192.168.32.143 255.255.255.240

Въпрос 25:

Разгледайте локалната мрежа с 2 FMI комутатора:



Мрежата съдържа два VLAN-а.

- ports 1 - 4 на всеки комутатор принадлежат на VLAN1
- ports 5 - 8 на всеки комутатор принадлежат на VLAN2.
- 802.1q trunk свързва двета two комутатора.

Въз основа на горното, кое е вярно?

Изберете едно или повече:

- a. хост 2-1 не може да ping хост 2-2
- b. хост 7-1 не може да ping хост 2-2 ✓
- c. хост 7-1 може да ping хост 7-2 ✓
- d. хост 2-1 може да ping хост 7-2
- e. хост 2-1 може да ping хост 2-2 ✓

ТЕСТ 6

Въпрос 1:

Колко хост IP адреса има в една Class C мрежа?

Изберете едно:

- a. 510
- b. 128
- c. 254 ✓
- d. 192
- e. 256

Въпрос 2:

На кой слой в OSI модела работи WAN мрежата?

Изберете едно или повече:

- a. Физически
- b. Канален ✓
- c. Представителен
- d. Приложен
- e. Сесиен
- f. Мрежов ✓
- g. Транспортен

Въпрос 3:

На мрежата SUNet е даден префикс 165.100.27.0/24. Колко подмрежки с по колко хоста поддържа този префикс?

Изберете едно:

- a. 65534 мрежи с по 255 хоста.
- b. 30 мрежи с по 64 хоста.
- c. 254 мрежи с по 254 хоста.
- d. Една мрежа с 254 хоста. ✓
- e. 254 мрежи с по 65,534 хоста.

Въпрос 4:

Имате MAC адрес на интерфейс wlan0 = 00:0e:2e:d1:ab:15. Какъв ще бъде Host ID на IPv6 link local адреса на интерфейс wlan0? (Имайте предвид, че MAC адресът се маркира в този случай като локално администриран)

Изберете едно:

- a. ff 00:0e2e:d1ab:1500
- b. 20e:2eff:ffd1:ab15
- c. 20e:2eff:fed1:ab15 ✓
- d. 0:e2e:d1ab:15ff
- e. e:2ed1:ab15

Въпрос 5:

Вие прилагате маската 255.255.255.224. Кои от долните IP можете да присвоите на хостове?

Изберете едно или повече:

- a. 134.178.18.56 ✓
- b. 87.45.16.159
- c. 217.168.166.192
- d. 192.168.16.87 ✓
- e. 16.23.118.63
- f. 92.11.178.93 ✓

Въпрос 6:

SUnet има клас C мрежа и иска на 5 департамента да се присвои отделна подмрежа.

Всяка подмрежа трябва да поеме най-малко 24 хоста.

Каква ще е маската?

Изберете едно:

- a. 255.255.255.252
- b. 255.255.255.224 ✓
- c. 255.255.255.254
- d. 255.255.255.248
- e. 255.255.255.240
- f. 255.255.255.192

Въпрос 7:

Колко голям е основния (basic) IPv6 header (без extension headers)?

Изберете едно:

- a. 512 bits
- b. 128 bits
- c. 320 bits
- d. 20 bytes ✓

Въпрос 8:

Комутаторите Cisco Catalyst прилагат технология за идентифициране и предпазване от топологично зацикляване, както и гарантиране на точно определен път на потоците от данни. Коя е тази технология?

Изберете едно:

- a. STP ✓
- b. 802.1Q
- c. ISL
- d. VTP

Въпрос 9:

Кой протокол автоматизира всичките тези функции за хостовете в мрежата: IP конфигурация, IP адреси, мрежови маски, default gateways и информация за DNS сървър(и)?

Изберете едно:

- a. DNS
- b. DHCP ✓
- c. ARP
- d. CDP
- e. SNMP

Въпрос 10:

Кое не е слой от OSI модела?

Изберете едно:

- a. Представителен
- b. Сесиен
- c. Канален
- d. Транслиращ ✓

Въпрос 11:

Кой OSI слой е обвързан със следното: потвърждение на предаването, последователност и управление на потока през мрежата?

Изберете едно:

- a. слой 5
- b. слой 2
- c. слой 4 ✓
- d. слой 3
- e. слой 6

Въпрос 12:

Кои от следните адреси е пример за валиден Unicast адрес?

Изберете едно:

- a. 172.31.128.255/18 ✓
- b. 255.255.255.255
- c. 224.0.0.5
- d. FFFF.FFFF.FFFF
- e. 192.168.24.59/30

Въпрос 13:

Кой метод на комутиране осигурява най-високо ниво на интегритет и безпогрешно транспортиране на трафика за сметка на по-голямо закъснение?

Изберете едно:

- a. VTP transparent mode
- b. Store-and-forward ✓
- c. Cut-through
- d. Frame-filtering
- e. Fragment-free
- f. 802.1q Forwarding

Въпрос 14:

Кой от следните е валиден хост unicast IPv6 адрес?

Изберете едно:

- a. 2001:0:240E::0AC0:3428:121C ✓
- b. 2001::240E::0AC0:3428:121C
- c. 2001::0000::240E::0000::0AC0::3428::121C
- d. 2001:240E::0AC0:3428::

Въпрос 15:

Какви са предимствата на сегментирането на мрежата с рутер?

Изберете едно или повече:

- a. Елиминират се бродкастите.
- b. Рутерът не прехвърля бродкастите от един сегмент в друг. ✓
- c. Добавянето на рутер в мрежата намалява закъсненията.
- d. Можете да приложите филтриране по слой 3 адреси. ✓
- e. Рутерите са по-ефективни от суичовете и по-бързо ще обработват данните.

Въпрос 16:

Кой слой на OSI модела в процеса на енкапсулиране не добавя хедър информация към пакета данни?

Изберете едно:

- a. Физически ✓
- b. Мрежов
- c. Транспортен
- d. Канален

Въпрос 17:

За какво се използва IPv6 адреса FF02::2?

Изберете едно:

- a. За всички рутери в локалния сегмент. ✓
- b. За всички хостове в конкретна Multicast група.
- c. За всички рутери в автономна система.
- d. За всички хостове в локалния сегмент.

Въпрос 18:

Какви компоненти са необходими за директно свързване на две PC-та, така че да се получи една приста peer-to-peer мрежа?

Изберете едно или повече:

- a. Рутер
- b. Кръстосан (Crossover) кабел ✓
- c. Съвместими мрежови интерфейси ✓
- d. Прав (Straight-through) кабел
- e. Хъб
- f. Мрежов протокол ✓

Въпрос 19:

Кои от по-долните твърдения за OSI модела са верни:

Изберете едно или повече:

- a. Всеки слой се характеризира с определено представяне на информацията. ✓
- b. Описва метода за предаване на информация между мрежови устройства.
- c. Представлява отворен стандарт. ✓
- d. Преминаването на информацията между слоевете е само възходящо.
- e. Състои се от четири слоя.
- f. Преминаването на информацията между слоевете е само низходящо.

Въпрос 20:

Имате адресен блок от обхвата на class B IP. Аква маска ще приложите, за да имате 100 подмрежки с по 500 хост адреса всяка?

Изберете едно:

- a. 255.255.254.0 ✓
- b. 255.255.255.224
- c. 255.255.255.0
- d. 255.255.224.0
- e. 255.255.0.0

Въпрос 21:

Имате Class C IP мрежа (префикс) и връзка „точка-точка“ (point-to-point). Искате да приложите VLSM. Кой префикс е най-ефективен?

Изберете едно:

- a. 255.255.255.248
- b. 255.255.255.240
- c. 255.255.255.0
- d. 255.255.255.254
- e. 255.255.255.252 ✓

Въпрос 22:

Кои от долните твърдения са верни за IPv6 адресите?

Изберете едно или повече:

- a. Всеки IPv6 интерфейс съдържа пне един loopback адрес. ✓
- b. Водещите нули в 16-bit шестнадесетичното поле на IPv6 адресите се изписва задължително.
- c. На един интерфейс може да се присвоят множество IPv6 адреси от различен тип. ✓
- d. Първите 64 бита са динамично създадения интерфейс ID.

Въпрос 23:

Кой от долните протоколи работи на слой 2 на OSI модела и служи за предпазване от зациклияне (loop-free мрежа)?

Изберете едно:

- a. RIP
- b. STP ✓
- c. CDP
- d. VTP

Въпрос 24:

С коя команда верифицирате свързаността между два хоста чрез изпращане и получаване на ICMP echo съобщения?

Изберете едно:

- a. tracert
- b. ping ✓
- c. show ip route
- d. netstat
- e. traceroute
- f. show cdp neighbors detail

Въпрос 25:

Кой от следните слоеве на TCP/IP модела най-добре съответства на мрежовия слой на OSI модела?

Изберете едно:

- a. Транспортен
- b. Интернет ✓
- c. Канален
- d. Приложен
- e. Мрежов

ТЕСТ 7

Въпрос 1:

Коя от следните стойности взема предвид STP, когато избира корен на дървото (root bridge)?

Изберете едно:

- a. Spanning-tree update number.
- b. BPDU version number.
- c. Номера на VLAN-а.
- d. Bridge ID. ✓
- e. Настройките на bridge-а в слоя за достъп.
- f. Приоритета на bridge-а.

Въпрос 2:

Кой е адреса на подмрежата за следния IP адрес на хост 201.100.5.68/28?

Изберете едно:

- a. 201.100.5.32
- b. 201.100.5.64 ✓
- c. 201.100.5.65
- d. 201.100.5.0
- e. 201.100.5.31
- f. 201.100.5.1

Въпрос 3:

Даден ви е префикс 115.64.4.0/22. Кои от долните IP адреси могат да се присвоят на хостове?

Изберете едно или повече:

- a. 115.64.3.255
- b. 115.64.12.128
- c. 115.64.5.128 ✓
- d. 115.64.6.255 ✓
- e. 115.64.8.32
- f. 115.64.7.64 ✓

Въпрос 4:

Какви са характеристиките на портовете на комутатор и мост (bridge) в напълно конвергирала spanning-tree мрежа на 2 слой?

Изберете едно:

- a. Всички портове на комутатор и bridge са в състояние stand-by.
- b. Всички портове на комутатор и bridge са присвоени или като root, или като designated портове.
- c. Всички портове на комутатор или bridge са в състояние forwarding или blocking. ✓
- d. Всички комутатори и bridge-ове са или блокирани, или в зациклияне.
- e. Всички портове на комутатор и bridges са в състояние forwarding.

Въпрос 5:

Вашият ISP ви е присвоил следната подмрежа и маска:

IP адрес: 199.141.27.0
Subnet маска: 255.255.255.240

Кои от следните адреси може да присвоите на хостове?

Изберете едно или повече:

- a. 199.141.27.2 ✓
- b. 199.141.27.112
- c. 199.141.27.175
- d. 199.141.27.208
- e. 199.141.27.13 ✓
- f. 199.141.27.11 ✓

Въпрос 6:

Колко дълъг е IPv6 адреса?

Изберете едно:

- a. 32 десетични числа
- b. 128 bits ✓
- c. 16 шестнадесетични числа
- d. 32 bits

Въпрос 7:

NIC (мрежова карта) има MAC адрес 00-0F-66-81-19-A3 и открива маршрутизиращ префикс 2001:0:1:5:/64. Кой IPv6 адрес ще се присвой на картата?

Изберете едно:

- a. FE80::20F:66FF:FE81:19A3
- b. FF02::1
- c. ::1
- d. 2001::1:5:20F:66FF:FE81:19A3 ✓

Въпрос 8:

Опаковане на IPv6 пакет в IPv4 пакет. Каква е тази технология?

Изберете едно:

- a. Routing
- b. Tunneling ✓
- c. Hashing
- d. NAT

Въпрос 9:

Каква е максималната препоръчана дължина на 10BaseT кабел?

Изберете едно:

- a. 100 feet
- b. 100 yards
- c. 100 meters ✓
- d. 200 meters

Въпрос 10:

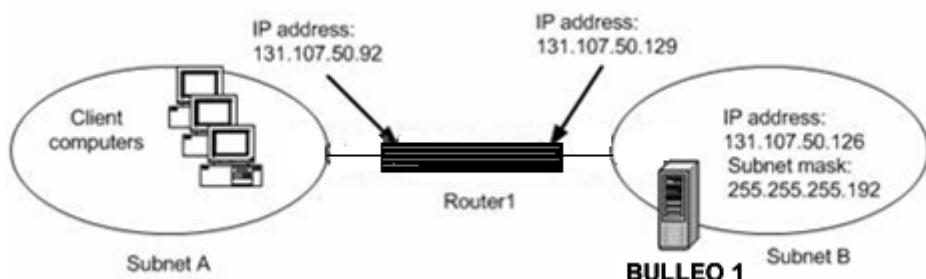
Кое от следните е вярно по отношение на мрежа (префикс) с маска 255.255.248.0?

Изберете едно или повече:

- a. Номерата на подмрежите са кратни на 8. ✓
- b. Отнася се към Class B адрес с взети назем 4 бита.
- c. С тази маска може да се създадат 16 подмрежи.
- d. Мрежовият адрес на последната подмрежа ще има 248 в 3-тиоктет. ✓
- e. Първите (старшите) 21 бита са хост частта на адреса.
- f. Отнася се към Class A адрес с взети назем 13 бита. ✓

Въпрос 11:

Вие сте мрежов администратор на BULLEO. Мрежата ви се състои от две подмрежи, както на показаната схема по-долу:



Подмрежата Subnet A съдържа 25 клиентски компютъра, които получават TCP/IP настройки от DHCP сървър. Обхватът на подмрежата Subnet A е от адрес 131.107.50.64 до адрес 131.107.50.95.

Подмрежа Subnet B съдържа единствено пощенски сървър с име BULLEO1.

Потребителите от подмрежа Subnet A съобщават, че не могат да се свържат с BULLEO1.

Стартирайки команда ping 131.107.50.126 от клиентски компютър от подмрежа Subnet A, Вие получавате следното съобщение за грешка: "Request timed out".

Трябва да осигурите свързаност на компютрите от подмрежа Subnet A до сървъра BULLEO1.

Какво трябва да направите?

Изберете едно:

- a. Ще промените IP адреса на интерфейса на Router1 към подмрежа Subnet A на 131.107.50.65.
- b. Ще промените маската на подмрежата на BULLEO1 на 255.255.255.224.
- c. Ще промените маската на подмрежата на клиентските компютри от подмрежа Subnet A на 255.255.255.224.
- d. Ще промените IP адреса на BULLEO1 на 131.107.50.130. ✓

Въпрос 12:

Как комуникират мрежови устройства разпределени във виртуални локални мрежи (VLAN)?

Изберете едно:

- a. Устройства от една виртуална локална мрежа (VLAN) комуникират с помощта на маршрутизатор.

- b. Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на магистрална (trunk) линия между комутаторите.
- c. Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на маршрутизатор. ✓
- d. Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на протокола VTP.

Въпрос 13:

Кои от следните твърдения са верни за VLAN?

Изберете едно или повече:

- a. Подобряват сигурността в мрежата. ✓
- b. Позволяват логическо групиране на потребителите по функции. ✓
- c. Увеличават размера на колизия домейни
- d. Увеличават размера на broadcast domain, същевременно намаляват броя на колизия домейни.
- e. Улесняват администрирането на съича (комутатора).
- f. Увеличават броя на broadcast домейни, като същевременно намаляват размера им. ✓

Въпрос 14:

Какво е backoff алгоритъм?

Изберете едно:

- a. Алгоритъм за определяне продължителността на изчакването преди следващ опит за предаване след настъпване на колизия при Етернет мрежа. ✓
- b. Алгоритъм за пресмятане на прага на допустимите грешки при FDDI.
- c. Алгоритъм за уведомяване за настъпила грешка в мрежата.
- d. Алгоритъм за определяне на най-добрия маршрут.

Въпрос 15:

Кой слой на OSI модела отговаря за установяване на надеждно съединение от-край-до-край (end-to-end)?

Изберете едно:

- a. Транспортен ✓
- b. Мрежов
- c. Презентационен
- d. Сесиен
- e. Приложен

Въпрос 16:

Рутерът получава пакет на интерфейс 172.16.45.66/26. source IP на пакета е 172.16.45.127/26, а destination - 172.16.46.191/26.

Как рутерът ще обработи пакета?

Изберете едно:

- a. Destination е хост на същата подмрежка, така че рутерът ще прехвърли пакета.
- b. Destination е broadcast адрес, така че рутерът няма да прехвърли пакета. ✓
- c. Destination е хост на друга подмрежка, така че рутерът няма да прехвърли пакета.
- d. Destination е мрежов адрес, така че рутерът ще прехвърли пакета.

Въпрос 17:

Кой от долните протоколи позволява на рутера да отговори на ARP запитване, отправено към отдалечен хост?

Изберете едно:

- a. Inverse ARP
- b. Reverse ARP
- c. Indirect ARP
- d. Gateway DP
- e. Proxy ARP ✓

Въпрос 18:

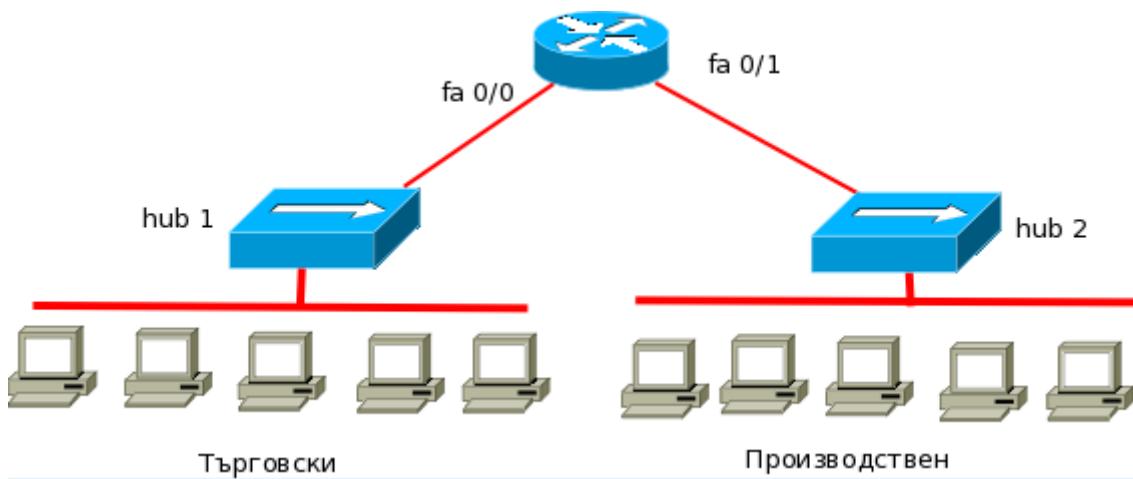
Кой от следните фактори по подразбиране, които определят стойността на пътя в spanning-tree?

Изберете едно:

- a. Това е стойността на отделна линия, изведена от закъснението.
- b. определя се динамично в зависимост от натоварването.
- c. Сумарният брой на хоповете.
- d. Това е сумата от стойностите на линиите по пътя, изведени от скоростите (bandwidth). ✓

Въпрос 19:

На долната схема е показана клонова мрежа:



Колко колизионни домейни има в тази мрежа?

Изберете едно:

- a. 2 ✓
- b. 3
- c. 14
- d. 4
- e. 1
- f. 5
- g. 6

Въпрос 20:

Опитвате се да откриете проблеми в локаната си мрежа. С кои от следните команди ще откриете проблеми с LAN свързаността?

Изберете едно или повече:

- a. show ip route ✓
- b. ipconfig
- c. winipcfg
- d. tracert
- e. ping ✓
- f. show interfaces ✓

Въпрос 21:

Имате задача да смените окабеляването в мрежата, така че да не бъде подвластно на електромагнитни смущения (EMI).

Какъв кабел ще изберете?

Изберете едно:

- a. Дебел коаксиален (Thicknet coaxial cable).
- b. Fiber optic кабел (оптически). ✓
- c. Category 5 UTP кабел.
- d. Category 5 STP кабел.
- e. Тънък коаксиален (Thinnet coaxial cable).

Въпрос 22:

Кое от двоичните числа представлява Class B адрес?

Изберете едно:

- a. 10xxxxxx ✓
- b. 110xxxxx
- c. 0xxxxxxxx
- d. 1110xxxx
- e. 11110xxx

Въпрос 23:

Когато станция изпрати съобщение до MAC адреса ff:ff:ff:ff:ff:ff, към кой вид съобщения може да бъде причислено то?

Изберете едно:

- a. Unicast
- b. Multicast
- c. Anycast
- d. Broadcast ✓

Въпрос 24:

За кой слой от OSI модела са характерни потвържденията (acknowledgements), последователното номериране (sequencing) и контрола на потока?

Изберете едно:

- a. слой 2
- b. слой 3
- c. слой 4 ✓
- d. слой 7

Въпрос 25:

На кой слой от OSI модела се извършва сегментирането на данните?

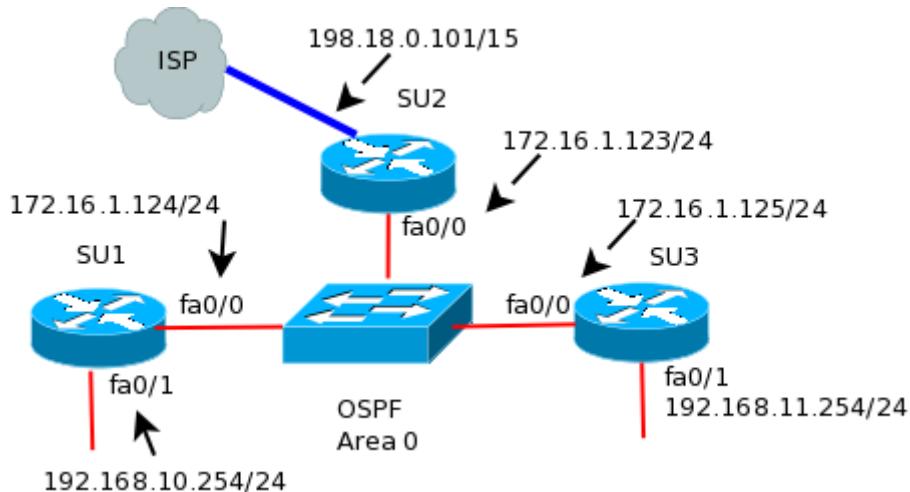
Изберете едно:

- a. Физически
- b. Канален
- c. Мрежов
- d. Транспортен ✓

ТЕСТ 8

Въпрос 1:

Три SUNet рутера са конфигурирани в OSPF област 0:



Искате рутер SU2 непременно да стане designated рутер (DR) за 172.16.1.0/24 LAN сегмента.

Какво трябва да направите?

Изберете едно или повече:

- a. Конфигурирайте loopback интерфейс на рутер SU2 с IP адрес, който да е по-голям от всички IP адреси на другите рутери. ✓
- b. Променете рутер id за рутер SU2, като му присвоите IP адреса 172.16.1.130/24 на Fa0/0 интерфейса на рутер SU2.
- c. Сложете приоритет = 0 на Fa0/0 интерфейса на рутер SU2.
- d. Не са необходими проемни в конфигурацията.
- e. Дайте на интерфейс Fa0/0 на рутер SU2 по-висока стойност отколкото на другите интерфейси на Ethernet мрежата. ✓
- f. Сложете приоритет = 0 на Fa0/0 интерфейсите на рутер SU1 и рутер SU3. ✓

Въпрос 2:

Каква е функцията на уеб-прокси (webproxy) сървърите?

Изберете едно:

- a. Да кешира посетените уеб страници (webpages) от различните клиенти. ✓
- b. Да преобразуват имената в IP адреси.
- c. Да поддържат локалния кеш на браузъра при всеки клиент.
- d. Да осигурява уеб интерфейс за всеки клиент към даден пощенски (mail) сървър.

Въпрос 3:

Кой от следните методи за предтвратяване на зацикляне се използва в протоколите с дистантен вектор?

Изберете едно или повече:

- a. Link-state advertisements (LSA)
- b. Hold-down timers ✓
- c. VRRP
- d. Shortest path first tree
- e. Split horizon ✓
- f. Spanning Tree Protocol

Въпрос 4:

RIP рутер има запис в таблицата с маршрути за конкретен префикс. След което получава „update“ за същия префикс, но с по-висока метрика (hop count) от съществуващата в таблицата с маршрути. Какво ще прави рутера?

Изберете едно:

- a. Ще добави update информацията в таблицата с маршрути.
- b. Ще игнорира update-а и нищо няма да прави. ✓
- c. Ще изтрие съществуващия запис в таблицата с маршрути и ще изпрати hello пакети, за да пренареди таблицата с маршрути.
- d. Ще замени съществуващия запис в таблицата с маршрути с обновената информация.

Въпрос 5:

Кои от термините са валидни за BGP?

Изберете едно или повече:

- a. Conglomerates
- b. Communities ✓
- c. Confederations ✓
- d. Corporations

Въпрос 6:

Какво означава iBGP?

Изберете едно:

- a. iBGP служи за маршрутизация в рамките на BGP Community.
- b. iBGP служи за gateway протокол в рамките на кампус мрежа.
- c. iBGP се отнася до internal BGP и се използва за маршрутизация между съседи в рамките на автономна система (AS). ✓
- d. iBGP служи за маршрутизация в рамките на BGP Confederation.

Въпрос 7:

Върху какъв протокол работи BGP?

Изберете едно:

- a. Директно върху IP
- b. UDP
- c. TCP ✓
- d. Няма верен отговор

Въпрос 8:

Кои от изброените протоколи са link-state?

Изберете едно или повече:

- a. RIP
- b. iBGP
- c. OSPF ✓
- d. IGRP
- e. EIGRP
- f. IS-IS ✓
- g. RIP v2
- h. BGP

Въпрос 9:

СУнет се състои от следните 5 IP мрежи:

- мрежа 1: 192.168.10.0/26
- мрежа 2: 192.168.10.64/27
- мрежа 3: 192.168.10.96/27
- мрежа 4: 192.168.10.128/30
- мрежа 5: 192.168.10.132/30

Кой от следните протоколи за маршрутизация поддържа горната IP адресна схема?.

Изберете едно или повече:

- a. RIP v2 ✓
- b. BGP
- c. RIP v1
- d. OSPF ✓
- e. IGRP

Въпрос 10:

Local preference е ...

Изберете едно:

- a. локална за отделна връзка между съседи.
- b. локална за отделен рутер.
- c. локална за отделна AS. ✓
- d. Няма верен отговор

Въпрос 11:

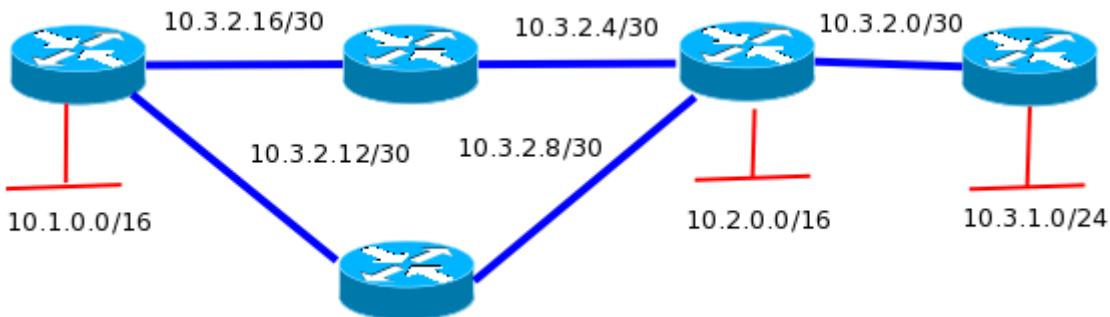
Какъв е максималния брой хопове (възли), след който OSPF смята даден префикс за недостижим?

Изберете едно:

- a. 16
- b. 15
- c. 255
- d. 99
- e. Неограничен ✓

Въпрос 12:

Дадена е диаграмата на СУнет:



Според горната схема кой протокол за маршрутизация ще се използва?.

Изберете едно или повече:

- a. OSPF ✓
- b. IGRP
- c. BGP
- d. RIP v2 ✓
- e. RIP v1

Въпрос 13:

Кои твърдения са верни по отношение на протоколите за беклассова маршрутизация (classless routing)?

Изберете едно или повече:

- a. RIP v1 е classless routing протокол.
- b. RIP v2 поддържа classless routing. ✓
- c. Прилагат маски с произволна дължина (variable length subnet mask). ✓
- d. IGRP поддържа classless routing.
- e. Не е възможно да се маршрутизират разпръснати подмрежки (discontiguous subnets).

Въпрос 14:

Кои от следните мрежки може да се използват в среда не поддържаща безкласово маршрутизиране?

Изберете едно или повече:

- a. 157.14.0.0/16 ✓
- b. 85.165.15.0/24
- c. 158.48.8.0/8
- d. 122.0.0.0/8 ✓
- e. 18.1.0.0/16
- f. 80.12.0.0/16
- g. 15.78.94.0/24
- h. 192.49.11.0/24 ✓

Въпрос 15:

При избор на най-добраия път BGP взима предвид информацията в следния ред:
Изберете едно:

- a. Path, origin type, local preference, multi-exit discriminator (MED).
- b. Path, origin type, multi-exit discriminator (MED), local preference.
- c. Local preference, path, origin type, multi-exit discriminator (MED). ✓
- d. Local preference, path, multi-exit discriminator (MED), origin type.

Въпрос 16:

RIPE Ви е присвоил обхвата от адреси 221.30.48.0 - 221.30.50.255, който е част от алокацията 221.30.48.0 - 221.30.63.255. Какъв префикс ще анонсирате по BGP:

Изберете едно:

- a. три /24-ки
- b. /23 и /24
- c. /22 ✓
- d. /19
- e. /20

Въпрос 17:

```
R#(config)#interface fastethernet 0/1
R#(config-if)#no shutdown
R#(config-if)#interface fastethernet 0/1.1
R#(config-subif)#encapsulation dot1q 10
R#(config-subif)#ip address 192.168.1.49 255.255.255.240
R#(config-if)#interface fastethernet 0/1.2
R#(config-subif)#encapsulation dot1q 60
R#(config-subif)#ip address 192.168.1.65 255.255.255.192
R#(config-if)#interface fastethernet 0/1.3
R#(config-subif)#encapsulation dot1q 120
R#(config-subif)#ip address 192.168.1.193 255.255.255.224
R#(config-subif)#end
```

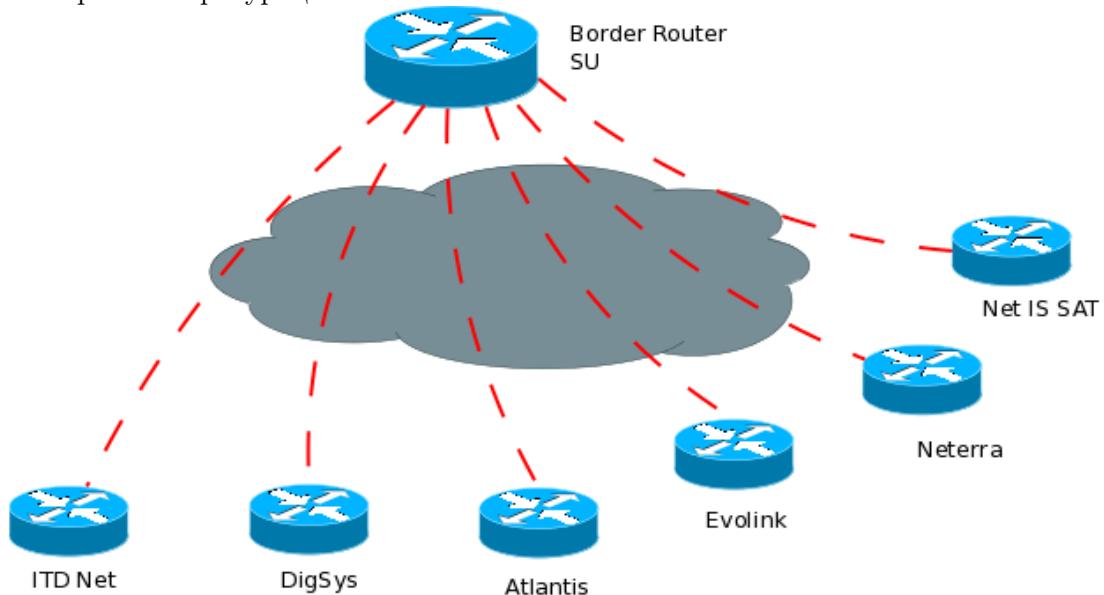
Маршрутизатор (рутер) е конфигуриран да се свързва с магистрална (trunk) линия, както е показано на диаграмата по-горе. На физическия FastEthernet 0/1 интерфейс е получен пакет от виртуална локална мрежа (VLAN) 10. Адресът на крайната точка (получател) за този пакет е 192.168.1.120. Какво ще направи маршрутизатора (рутер) с този пакет?

Изберете едно:

- a. Ще го препрати през под-интерфейс FastEthernet 0/1.3 към VLAN 120.
- b. Ще го препрати през под-интерфейс FastEthernet 0/1.2 към VLAN 10.
- c. Ще го препрати през под-интерфейс FastEthernet 0/1.1 към VLAN 60. ✓
- d. Няма да направи нищо, защото адресите на подателя и получателя са от една и съща под-мрежа.

Въпрос 18:

На долната схема Border Router SU има BGP сесии с рутерите ITD, Digsys и т.н., като на всички е наложена една и съща политика (Route Maps, Prefix Lists и т.н.). Как ще оптимизирате конфигурацията?



Изберете едно:

- a. Рутерите ITD, Digsys и т.н. се оформят като BGP Peer група. ✓
- b. Рутерите ITD, Digsys и т.н. трябва да са на общ Ethernet сегмент.
- c. Рутерите ITD, Digsys и т.н. се включват в BGP конфедерация.
- d. Рутерите ITD, Digsys и т.н. се включват в BGP Community List.

Въпрос 19:

Кой от следните протоколи отваря и UDP, и TCP портове за работа по транспортния слой?

Изберете едно:

- a. Telnet
- b. DNS ✓
- c. SMTP
- d. TFTP
- e. FTP

Въпрос 20:

Коя е версията на BGP, която поддържа CIDR?

Изберете едно:

- a. BGP version 1
- b. BGP version 2
- c. BGP version 5
- d. BGP version 4 ✓
- e. BGP version 3

ТЕСТ 9

Въпрос 1:

RIP version 2 се прилага за маршрутизация в СУнет. Кой механизъм в RIP version 2 предпазва от зацикляне (routing loops)?

Изберете едно или повече:

- a. Multicast routing updates
- b. Classless masking
- c. Path Vectoring
- d. Split horizon ✓
- e. CIDR
- f. Hold-down timers ✓
- g. Authentication

Въпрос 2:

Току що сте конфигурирали OSPF рутер с физически и логически интерфейси. Как ще се определи Router ID?

Изберете едно:

- a. Най-малкият IP адрес от всички физически интерфейси.
- b. Най-големият IP адрес от всички логически интерфейси.
- c. Най-малкият IP адрес от всички интерфейси.
- d. Най-големият IP адрес от всички физически интерфейси.
- e. Най-малкият IP адрес от всички логически интерфейси.
- f. Най-големият IP адрес от всички логически интерфейси. ✓
- g. Средният IP адрес от всички логически интерфейси.

Въпрос 3:

Кои от термините са валидни за BGP?

Изберете едно или повече:

- a. Confederations ✓
- b. Communities ✓
- c. Conglomerates
- d. Corporations

Въпрос 4:

Долните твърдения са сравнение между протоколите с дистантен вектор и тези със следене на състоянието на връзката. Кое от тях е вярно?

Изберете едно или повече:

- a. Дистантен вектор изпращат цялата таблица с маршрути до съседите, с които е директн свързан. ✓
- b. Следене на състоянието (link state) изпращат цялата таблица с маршрути до цялата мрежа.
- c. Следене на състоянието изпращат обновления (updates), отнасящи се до състоянията на техните връзки, до всички други рутери в мрежата. ✓
- d. Дистантен вектор изпращат обновления в маршрутите (updates) до всички мрежи, изброени в маршрутната таблица.

Въпрос 5:

Приемайки, че всеки OSPF рутер в дадена област е конфигуриран с един и същи приоритет, коя друга стойност ще се приеме за рутер ID, ако не е конфигуриран loopback интерфейс?

Изберете едно:

- a. Няма да има Router ID, докато не се конфигурира loopback интерфейс.
- b. Най-малкият IP адрес между активните интерфейси.
- c. IP адресът на конзолния интерфейс.
- d. IP адресът на първия Fast Ethernet интерфейс.
- e. Най-големият IP адрес между активните интерфейси. ✓

Въпрос 6:

При какъв тип мрежа OSPF рутер ще установи съседство с друг рутер, като не изпълнява избор на DR/BDR?

Изберете едно:

- a. Backbone area 0
- b. Broadcast
- c. Point-to-point ✓
- d. Non-broadcast multi-access

Въпрос 7:

Кое от долните е вярно за OSPF Hello протокол?

Изберете едно или повече:

- a. OSPF Hello протокол бродкаства (broadcast) hello пакети по мрежата, за да открие всички OSPF рутери.
- b. OSPF Hello протокол открива недостижими съседи през 90 секунди.
- c. OSPF Hello протокол помага за динамичн откриване на съседи. ✓
- d. OSPF Hello протокол с помощта на таймери избира рутера с най-бързи връзки за designated рутер.
- e. OSPF Hello протокол уговоря параметрите на интерфейсите между съседите.
- f. OSPF Hello протокол поддържа връзките със съседите. ✓

Въпрос 8:

ФМИнет има 25 компютъра, които трябва да бъдат свързани към Internet, но разполага само с 4 публични IP адреса. Какво трябва да бъде конфигурирано на рутера, така че всички компютри да имат достъп до Глобалната мрежа?

Изберете едно:

- a. Статичен NAT with ACLs
- b. Статичен NAT
- c. Global NAT
- d. Dynamic NAT
- e. Dynamic NAT with overload ✓

Въпрос 9:

Какво означава SNMP?

Изберете едно:

- a. Simple Network Mail Protocol
- b. Simple Network Management Protocol ✓
- c. Serial Network Management Protocol
- d. Serial Network Mail Protocol

Въпрос 10:

Кои от долните протоколи поддържат VLSM?

Изберете едно или повече:

- a. EIGRP ✓
- b. RIP v1
- c. RIP v2 ✓
- d. OSPF ✓
- e. IGRP

Въпрос 11:

Мъчейки се да откриете проблем с мрежовата свързаност, подозирате, че на рутера му липсва маршрут или че получава некоректна информация за маршрута до дестинацията.

Каква команда трябва да изпълните, за да видите какъв маршрут ще използва рутера, за да доведе пакета до дестинацията?

Изберете едно:

- a. show interface
- b. trace
- c. show cdp neighbors
- d. ping
- e. show ip route ✓

Въпрос 12:

Какво означава атрибутът LocPref?

Изберете едно:

- a. Една или повече 32-битови стойности, дефинирани от потребителя
- b. Помага да се избере път измежду няколко възможни, като атрибутът важи в рамките на AS. ✓
- c. Съдържа IP адреса на рутера, към който ще бъдат отправени пакетите за конкретна дестинация.
- d. Помага да се избере най-добрия път измежду многото до дадена AS.

Въпрос 13:

Кои от долните протоколи поддържа VLSM и „маршрут summarization“?

Изберете едно или повече:

- a. OSPF ✓
- b. CDP
- c. RIP v1
- d. RIP v2 ✓
- e. IGRP
- f. VTP

Въпрос 14:

По какво се различават IGPs (Interior Gateway Protocols) и EGPs (Exterior Gateway Protocols)?

Изберете едно:

- a. EGPs маршрутизират в рамките на един кампус.
- b. IGPs маршрутизират в рамките на една автономна система (AS), докато EGPs – между ASs. ✓
- c. IGPs маршрутизират в рамките на една сграда.

Въпрос 15:

В глобалната таблица с маршрути е възможно един и същи номер на автономна система (AS) да се появи повече от веднъж в даден път до дестинация. Как се нарича това и за какво служи?

Изберете едно или повече:

- a. предпазва от зацикляне
- b. заобикаля дадената AS
- c. AS prepend ✓
- d. изкуствено удължава пътя ✓
- e. променя LocPref

Въпрос 16:

На какви видове мрежи OSPF избира backup designated рутер?

Изберете едно:

- a. Point-to-multipoint и multi-access broadcasting
- b. Point-to-point и multi-access broadcasting
- c. Point-to-point и point-to-multipoint мрежи
- d. Nonbroadcast и broadcast multipoint multicasting
- e. Broadcast multiaccess ✓

Въпрос 17:

Командата “ip route 192.168.24.64 255.255.255.192 192.168.8.2” е конфигурирана на рутер SU1.

Изберете едно:

- a. Интерфейс с IP адрес 192.168.8.2 е на рутера SU1.
- b. Пакетите, насочени към хост 192.168.24.124 ще бъдат изпратени към 192.168.8.2. ✓
- c. Командата създава статичен маршрут за целия IP трафик със source 192.168.24.64.
- d. Тази команда дефинира „gateway of last resort“ за рутера SU1.

Въпрос 18:

На един хост с един IPадрес искате да инсталирате две отделни приложения за уеб сървър - ApacheWeb сървър само за стандартен http трафик, и втори webсървър, който ще осигурява само https. Какъв ще е резултатът от инсталациите на двете програми?

Изберете едно:

- a. Двата уеб сървъра не могат да работят едновременно на един и същ IP адрес, защото стандартно ще използват един и същи порт 80, а IP адреса е само един.
- b. Двата уеб сървъра ще работят успешно, понеже по подразбиране стандартния http трафик ще е на порт 80, а https трафика – на порт 8080.
- c. Двата уеб сървъра ще работят успешно, защото няма ограничение две различни приложения да работят върху един и същи порт на един и същи IP адрес.
- d. Двата уеб сървъра ще работят успешно, понеже по подразбиране стандартният http трафик ще е на порт 80, а https трафика – на порт 443. ✓

Въпрос 19:

Кои от следните OSPF команди ще приложите, за да влезе префикса 192.168.10.0/24 в OSPF area 0? (2 отговора)

Изберете едно или повече:

- a. router(config)#router ospf 0
- b. router(config)# router ospf 1 ✓
- c. router(config-router)# network 192.168.10.0 0.0.0.255 area 0 ✓
- d. router(config-router)# network 192.168.10.0 255.255.255.0 area 0
- e. router(config-router)#network 192.168.10.0 0.0.0.255 0

Въпрос 20:

Маршрутизатори A и B работят с OSPF протокол и са свързани помежду си едновременно с E1 (2 Mbps) и ADSL (2 Mbps). Каква цена ще сложите при конфигурирането на всеки от интерфейсите за свързване на маршрутизатор A с маршрутизатор B?

Изберете едно:

- a. cost (интерфейс E1) = cost (интерфейс ADSL)
- b. cost (интерфейс E1) < cost (интерфейс ADSL)
- c. cost (интерфейс E1) > cost (интерфейс ADSL) ✓
- d. cost (интерфейс E1) > = cost (интерфейс ADSL)

TECT 10

Въпрос 1:

Следната конфигурационна команда е въведена на рутера:
ip route 172.16.3.0 255.255.255.0 192.168.2.4

Какво представлява тя?

Изберете едно:

- a. С командата се декларира stub мрежа.
- b. С командата се конфигурират интерфейсите на рутера.
- c. Маската на source адрес е 255.255.255.0
- d. С командата се въвежда статичен маршрут. ✓

Въпрос 2:

От вас се иска да конфигурирате default маршрут. С кои команди ще го направите?

Изберете едно или повече:

- a. LTD(config)# ip route 0.0.0.0 192.168.15.36 255.255.255.255
- b. LTD(config)# ip route 0.0.0.0 255.255.255.255 S0
- c. LTD(config)# ip route 0.0.0.0 0.0.0.0 E0 ✓
- d. LTD(config-рутер)# ip route 255.255.255.255 0.0.0.0 192.168.15.36
- e. LTD# ip default-network 0.0.0.0 192.168.15.36 255.255.255.255
- f. LTD(config)# ip route 0.0.0.0 0.0.0.0 192.168.15.36 ✓

Въпрос 3:

Кой от долните протоколи използва TCP порт 443?

Изберете едно:

- a. HTML
- b. SMTP
- c. HTTPS ✓
- d. TFTP
- e. Telnet

Въпрос 4:

Маршрутизаторите изпълняват следните функции:

Изберете едно или повече:

- a. Филтриране на пакети ✓
- b. Разширяват broadcast домейна.
- c. Предпазват от колизии в LAN мрежи.
- d. Комуникация между различни мрежи ✓
- e. Пакетна комутация (packet switching) ✓
- f. Пренасочват broadcast.

Въпрос 5:

Кои от следните протоколи за маршрутизация са по-малк податливи на зацикляне и проблеми с „прекъснати“ (discontiguous) мрежи?

Изберете едно или повече:

- a. OSPF ✓
- b. CDP
- c. RIP v2 ✓
- d. IGRP
- e. RIP v1

Въпрос 6:

Кои от следните твърдения описват характеристиките на протоколите със следене на състоянието на връзките (link state routing)?

Изберете едно или повече:

- a. Всеки рутер в OSPF област има представа за пълната топология на мрежата. ✓
- b. Всички рутери си обменят таблици с маршрути в многоточкова мрежа.
- c. Само designated рутер в OSPF област има представа за пълната топология на мрежата.
- d. Обменът на реклами на маршрути се задейства при промяна в мрежата. ✓
- e. Пакетите се маршрутизират на базата на най-късия път до дестинацията. ✓
- f. Пътищата се избират в зависимост стойността „фактор на ефективността“.

Въпрос 7:

Non-contiguous мрежи (подмрежки от един префикс, които са отдалечени едни от други) предизвикват проблем с достъжимостта при определени обстоятелства. Кои от следните маршрутни (routing) протоколи могат да ограничат този риск?

Изберете едно или повече:

- a. IGRP
- b. OSPF ✓
- c. RIP v2 ✓
- d. ICMP
- e. RIP v1
- f. EIGRP ✓

Въпрос 8:

Относно OSPF маршрутизацията, кои са характеристики на OSPF областта?

Изберете едно или повече:

- a. Всяка OSPF област изисква да се конфигурира loopback интерфейс.
- b. На областите може да се присвояват произволно число в интервала от 0 до 65535.
- c. Област 0 се нарича backbone (опорна) област. ✓
- d. Йерархичните OSPF мрежи не изискват множество области.
- e. Другите OSPF области трябва да са свързани към област 0. ✓
- f. OSPF мрежи с една област трябва да се конфигурират в област 1.

Въпрос 9:

Кои полета са включени в заглавната част на TCP (header)?

Изберете едно или повече:

- a. Request Number
- b. Acknowledgement Number ✓
- c. Data
- d. Destination Address
- e. Source port ✓
- f. Window ✓

Въпрос 10:

Кой от следните протоколи се опира на TCP?

Изберете едно или повече:

- a. TFTP
- b. NTP
- c. NNTP ✓
- d. SMTP ✓
- e. HTTPS ✓
- f. SNMP

Въпрос 11:

Кой от следните протоколи използва UDP като транспортен механизъм на слой 4?

Изберете едно или повече:

- a. TACACS
- b. SNMP ✓
- c. TFTP ✓
- d. SMTP
- e. Telnet
- f. HTTP

Въпрос 12:

Кой от долните протоколи използва TCP на транспортен слой?

Изберете едно или повече:

- a. SMTP ✓
- b. HTTPS ✓
- c. HTTP ✓
- d. FTP ✓
- e. TFTP
- f. SNMP

Въпрос 13:

Коя от следните команди ще изпълните за да конфигурирате default маршрут до произволна дестинация, която не е в маршрутната таблица на рутера SU1?

Изберете едно:

- a. SU1(config)# ip route any any e0
- b. SU1(config)# ip route 0.0.0.0 255.255.255.255 s0
- c. SU1(config)# ip default-route 0.0.0.0 255.255.255.255 s0
- d. SU1(config)# ip route 0.0.0.0 0.0.0.0 s0 ✓
- e. SU1(config)# ip default-route 0.0.0.0 s0

Въпрос 14:

Кое от следните твърдения най-добре описва правилото „split horizon“?

Изберете едно:

- a. Само рутерите могат да разделят (split) границите (horizons) мрежите на отделни автономни системи (AS).
- b. Информацията за маршрут никога е трябва да бъде изпращана обратно по линията (интерфейса), по която е била получена. ✓
- c. След като един маршрут е получен на интерфейс, той се рекламира ка недостижим (unreachable) обратно по същия интерфейс.
- d. Всяка AS трябва да поддържа маршрутната таблица конвергирала, за да не пропуска маршрути към несъществуващи префикси да преминават границите й.

Въпрос 15:

TCP сегментите се различават от UDP дейтаграмите, но мат общи полета. Кои са те?

Изберете едно или повече:

- a. Options
- b. Source адрес
- c. Checksum ✓
- d. Sources
- e. Destination порт ✓
- f. Sequence number

Въпрос 16:

На серийния интерфейс на рутера е приложен филтър на входящия трафик, който забранява трафик от UDP и TCP портове 21, 23 и 25. Всякакъв друг трафик се пропуска.

Тогава, какъв тип трафик ще бъде пропуснат през този интерфейс?

Изберете едно или повече:

- a. DNS ✓
- b. Telnet
- c. SMTP
- d. POP3 ✓
- e. HTTP ✓
- f. FTP

Въпрос 17:

Кой от следните протоколи използва и TCP, и UDP портове?

Изберете едно:

- a. DNS ✓
- b. FTP
- c. Telnet
- d. SMTP

Въпрос 18:

Кои от следните твърдения са верни относно routed протоколи и routing протоколи?

Изберете едно или повече:

- a. routed протокол update-ва таблицата с маршрутите (таблица с маршрути) на рутера.
- b. routing протокол определя пътя на пакета през мрежата. ✓
- c. routed протокол определя пътя на пакета през мрежата.
- d. routing протокол работи на транспортния слой на OSI модела.
- e. routing протокол се присвоява на интерфейс и определя метода на доставяне на пакета до дестинацията.
- f. routed протокол се присвоява на интерфейс и определя метода на доставяне на пакета до дестинацията. ✓

Въпрос 19:

Каква е целта на управление на потока (flow control) в мрежа за данни?

Изберете едно:

- a. Реасемблира сегмента в правилния ред при устройството-получател.
- b. Регулира размера на сегмента.
- c. Осигурява механизъм, чрез който получателят да контролира скоростта на предаване. ✓
- d. Гарантира, че данните ще бъдат предадени повторно, ако не се получи потвърждение.

Въпрос 20:

Какъв вид пакети изпраща OSPF за да поддържа свързаността със съседните рутери?

Изберете едно:

- a. Keepalive пакети
- b. SPF пакети
- c. Dead Interval пакети
- d. LSU пакети
- e. Hello пакети ✓

БЛИЦ ВЪПРОСИ

1. Увод в TCP/IP:

Кой слой е отговорен за конвертирането на данните от каналния слой в електрически импулси?

Отговор: Физически

В кой слой е имплементирано маршрутизирането, позволяващо свързването и избирането на път за пренос на данни между две крайни системи?

Отговор: Мрежов

Кой слой определя как се форматират, представят, кодират и конвертират мрежовите данни?

Отговор: Презентационен

Кой слой е отговорен за създаването, управляването и прекратяването на сесии между приложения?

Отговор: Сесиен

Кой слой осигурява сигурното предаване на данни през физическата среда и отговаря основно за физическото адресиране, дисциплината на линията, мрежовата то-ология, нотификацията за грешки, преноса на рамки в правилен ред и контрола на потока?

Отговор: Канален

Кой слой се използва за надеждна комуникация между крайни хостове в мрежата и предоставя механизми за установяване, поддържане и прекратяване на виртуални вериги, откриване на и възстановяване от грешки, възникнали при транспорта на данни, и контрол на потока на информация?

Отговор: Транспортен

Кой слой предоставя логическо адресиране, което маршрутизаторите използват за установяване на маршрут за пренос на данни?

Отговор: Мрежов

Кой слой определя волтажа, скоростта и изводите (pinout) на проводника и предава битове между мрежови устройства?

Отговор: Физически

Кой слой комбинира битове в байтове и байтове в рамки, използва MAC адресиране и установява дали са възникнали грешки по време на преноса на данните във физическата среда?

Отговор: Канален

Кой слой е отговорен за разграничаването на данните от различните приложения (мултиплексиране) при мрежова комуникация?

Отговор: Транспортен

Продукт на кой слой са рамките?

Отговор: Канален

Продукт на кой слой са сегментите?

Отговор: Транспортен

Продукт на кой слой са пакетите?

Отговор: Мрежов

Продукт на кой слой са битовете?

Отговор: Физически

Поставете следните единици данни в ред на енкапсулация, започвайки от най-

вътрешната: Пакети, Рамки, Битове, Сегменти

Отговор: Битове, Рамки, Пакети, Сегменти

Кой слой сегментира и реасемблира данните?

Отговор: Транспортен

Кой слой се грижи за привеждането на данните във формат, удобен за предаване на физическо ниво и отговаря за нотификацията при възникване на грешки, мрежовата топология и контрола на потока?

Отговор: Канален

Кой слой управлява адресирането на устройствата, проследява положени- ето на устройства в мрежата и определя най-добрая път за пренос на данни?

Отговор: Мрежов

Каква е дължината в битове и в какъв вид се изразява MAC адресът?

Отговор: 48 бита, шестнайсетичен вид

Кой слой създава виртуална верига преди да започне да изпраща данни?

Отговор: Транспортен

Върху кои слоеве е дефиниран Ethernet?

Отговор: Канален и физически

В кой слой се използва логическото адресиране на хостовете в мрежата?

Отговор: Мрежови

В кой слой се дефинират хардуерните адреси на мрежовите интерфейси на хостовете?

Отговор: Канален

Маршрутизаторите оперират на слой № ..., LAN комутаторите оперират на слой № ..., LAN концентраторите оперират на слой № ..., текстообработката се извършва на слой №

Изберете едно:

- a. 3, 3, 1, 7
- b. 3, 2, 1, никой
- c. 3, 2, 1, 7 ✓
- d. 2, 3, 1, 7
- e. 3, 3, 2, никой

Коя е правилната последователност на енкапсулация на данните?

Изберете едно:

- a. Данни, рамка, пакет, сегмент, бит
- b. Сегмент, данни, пакет, рамка, бит
- c. Данни, сегмент, пакет, рамка, бит ✓
- d. Данни, сегмент, рамка, пакет, бит

Идентифицирайте слоя от DoD модела, към който принадлежи всеки един от следните протоколи:

- Internet Protocol (IP) - Интернет
- Telnet - Приложен
- FTP - Приложен
- SNMP - Приложен
- DNS - Приложен
- Address Resolution Protocol (ARP) - Интернет
- DHCP/BootP - Приложен
- Transmission Control Protocol (TCP) - Транспортен
- User Datagram Protocol (UDP) - Транспортен
- NFS - Приложен
- Internet Control Message Protocol (ICMP) - Интернет
- Reverse Address Resolution Protocol (RARP) - Интернет
- Proxy ARP - Интернет
- TFTP - Приложен
- SMTP - Приложен
- Ethernet - Канален

Кой от следните са слоеве на DoD модела?

Изберете едно или повече:

- a. Приложен ✓
- b. Сесиен
- c. Транспортен ✓
- d. Интернет ✓
- e. Физически

Кой слой от DoD модела е еквивалентен на мрежовия слой от OSI модела?

Изберете едно:

- a. Приложен
- b. Транспортен
- c. Интернет ✓
- d. Канален

2. IP Адресация

Имате клас В мрежа и се нуждаете от 29 подмрежи. Каква мрежова маска ще изберете?

Отговор: 255.255.248.0 или /21

Какъв е broadcast адресът на подмрежата, в която се намира хостът с адрес 192.168.192.10/29?

Отговор: 192.168.192.15

Колко адреса за хостове предлага подмрежа с маска /29?

Отговор: 6

Какъв е адресът на подмрежата на 10.16.3.65/23?

Отговор: 10.16.2.0

Какъв е максималният брой IP адреси, които могат да бъдат зачислени на хостове в локална подмрежа с маска 255.255.255.224?

Изберете едно:

- a. 14
- b. 15
- c. 16
- d. 30 ✓
- e. 31
- f. 62

Имате мрежа, която трябва да разделяте на 29 подмрежи, предлагащи възможно най-голям брой адреси на хостове. Колко бита трябва да заемете от полето на хоста, за да постигнете това?

Изберете едно:

- a. 2
- b. 3
- c. 4
- d. 5 ✓
- e. 6
- f. 7

Имате хост с IP адрес 200.10.5.68/28. Кой е адресът на подмрежата, от която е част този хост?

Изберете едно:

- a. 200.10.5.56
- b. 200.10.5.32
- c. 200.10.5.64 ✓
- d. 200.10.5.0

Колко подмрежи и колко адреса за хостове в подмрежа предоставя мрежовият адрес 172.16.0.0/19?

Изберете едно:

- a. 7 подмрежи, 30 хоста във всяка
- b. 7 подмрежи, 2046 хоста във всяка
- c. 7 подмрежи, 8190 хоста във всяка
- d. 8 подмрежи, 30 хоста във всяка
- e. 8 подмрежи, 2046 хоста във всяка
- f. 8 подмрежи, 8190 хоста във всяка ✓

Кои твърдения са верни за IP адреса 10.16.3.65/23?

Изберете едно или повече:

- a. Адресът на подмрежата му е 10.16.3.0/255.255.254.0.
- b. Най-ниският адрес на хост в подмрежата му е 10.16.2.1. ✓
- c. Последният валиден адрес на хост в подмрежата му е 10.16.2.254.
- d. Broadcast адресът на подмрежата му е 10.16.3.255. ✓
- e. Мрежата му не е разделена на подмрежи.

Ако хост в мрежа има адрес 172.16.45.14/30, какъв е адресът на подмрежата, към която принадлежи той?

Изберете едно:

- a. 172.16.45.0
- b. 172.16.45.4
- c. 172.16.45.8
- d. 172.16.45.12 ✓
- e. 172.16.45.16

Коя маска е най-практично да използваме при Point-to-point връзка за да намалим разхода на IP адреси?

Изберете едно:

- a. /8
- b. /16
- c. /24
- d. /30 ✓
- e. /31

Кой е адресът на подмрежата на хост с IP адрес 172.16.66.0/21?

Изберете едно:

- a. 172.16.36.0
- b. 172.16.48.0
- c. 172.16.64.0 ✓
- d. 172.16.0.0

На маршрутизатор имате интерфейс с IP адрес 192.168.192.10/29.

Колко хоста могат да имат адреси от локалната мрежа, свързана към интерфейса на маршрутизатора? (Маршрутизаторът се брои за хост в подмрежата.)

Изберете едно:

- a. 6 ✓
- b. 8
- c. 30
- d. 62
- e. 126

Имате нужда да конфигурирате мрежови интерфейс на сървър с IP адрес, който е част от подмрежата 192.168.19.24/29. На маршрутизатора в тази подмрежа е зачислен първият адрес от нея. Кой от следните адреси можете да зачислите на сървъра?

Изберете едно:

- a. 192.168.19.0/255.255.255.0
- b. 192.168.19.33/255.255.255.240
- c. 192.168.19.26/255.255.255.248 ✓
- d. 192.168.19.31/255.255.255.248
- e. 192.168.19.34/255.255.255.240

Имате маршрутизатор, свързан с локална мрежа, посредством мрежови интерфейс с адрес 192.168.192.19/29. Какъв е broadcast адресът, който хостовете в подмрежата ще използват?

Изберете едно:

- a. 192.168.192.15
- b. 192.168.192.23 ✓
- c. 192.168.192.63
- d. 192.168.192.127
- e. 192.168.192.255

Имате мрежа, която трябва да разделите на подмрежи, всяка от които да съдържа поне 16 хоста. Коя от следните маски бихте използвали, за да постигнете това?

Изберете едно:

- a. 255.255.255.192 ✓
- b. 255.255.255.224
- c. 255.255.255.240
- d. 255.255.255.248

Ако IP адресът 172.16.112.1/25 е зачислен на Ethernet порт на маршрутизатор, какъв ще бил адресът на подмрежата на този порт?

Изберете едно:

- a. 172.16.112.0 ✓
- b. 172.16.0.0
- c. 172.16.96.0
- d. 172.16.255.0
- e. 172.16.128.0

Имате мрежа с подмрежка 172.16.17.0/22. Кой от следните адреси е валиден адрес на хост от тази подмрежка?

Изберете едно:

- a. 172.16.17.1/255.255.255.252
- b. 172.16.0.1/255.255.240.0
- c. 172.16.20.1/255.255.255.254.0
- d. 172.16.16.1/255.255.255.240
- e. 172.16.18.255/255.255.252.0 ✓
- f. 172.16.0.1/255.255.255.0

Порт Ethernet0 на маршрутизатора Ви има адрес 172.16.2.1/23.

Кои от следните могат да бъдат валидни адреси на хостове, свързани с Ethernet0, посредством локална мрежа?

Изберете едно или повече:

- a. 172.16.0.5
- b. 172.16.1.100
- c. 172.16.1.192
- d. 172.16.2.255 ✓
- e. 172.16.3.0 ✓
- f. 172.16.3.255

За да тествате IP стека на локалния си хост, кой от следните адреси бихте подали като параметър на командата ping?

Изберете едно:

- a. 127.0.0.0
- b. 1.0.0.127
- c. 127.0.0.1
- d. 127.0.0.255 ✓
- e. 255.255.255.255

3. NAT (Network Address Translation)

Кои от следните са недостатъци на използването на NAT?

Изберете едно или повече:

- a. Спестява публично достъпни IP адреси.
- b. Причинява загуба на end-to-end проследимостта (traceability) на IP. ✓
- c. Увеличава гъвкавостта при свързване с Интернет.
- d. Някои приложения няма да функционират, когато мрежовите им връзки преминават през NAT. ✓
- e. Намалява случаите на припокриване на IP адреси.
- f. Отразява се негативно върху сигурността на мрежата.
- g. Намалява забавянето при обработка на мрежовия трафик от маршрутизатора.

Кои от следните са предимства на използването на NAT?

Изберете едно или повече:

- a. Спестява публично достъпни IP адреси. ✓
- b. Причинява загуба на end-to-end проследимостта на IP.
- c. Увеличава гъвкавостта при свързване с Интернет. ✓
- d. Някои приложения няма да функционират, когато мрежовите им връзки преминават през NAT.
- e. Намалява случаите на припокриване на IP адреси. ✓
- f. Отразява се негативно върху сигурността на мрежата.
- g. Намалява забавянето при обработка на мрежовия трафик от маршрутизатора.

Кои от следните са видове NAT?

Изберете едно или повече:

- a. Статичен NAT ✓
- b. IP NAT pool
- c. Двойно превеждане (NAT double-translation)
- d. PAT (Port Address Translation) ✓

Кои от следните са добри причини за използване на NAT?

Изберете едно или повече:

- a. Имате нужда да се свържете с Интернет, а хостовете Ви нямат глобално уникални IP адреси. ✓
- b. При избор на нов доставчик на Интернет възниква нужда за преномериране на цялата Ви мрежа. ✓
- c. Не искате никой хост да има връзка с Интернет.
- d. Искате две вътрешни мрежи с припокриващи се адресни пространства да се слеят. ✓

PAT (Port Address Translation) се нарича също ...

Изберете едно:

- a. Бърз (Fast) NAT.
- b. Статичен (Static) NAT.
- c. NAT Overload. ✓

4. Статична маршрутизация

Работите на хост с операционна система GNU/Linux 3.6.10. Напишете команда, с която ще въведете запис за мрежа 172.16.10.0/24 през маршрутизатор 172.16.20.1 в маршрутната таблица на хоста.

Отговор: route add -net 172.16.10.0/24 gw 172.16.20.1

Напишете команда, с която като маршрутизатор по подразбиране (default router) се задава хостът с адрес 172.16.40.1.

Отговор: ip route add default via 172.16.40.1

С коя команда се извежда маршрутната таблица?

Отговор: ip route show

Вярно или грешно: За да установите връзка с отдалечен хост (хост в отдалечена мрежа), трябва да знаете MAC адреса на този хост.

Отговор: Грешно

Вярно или грешно: За да установите връзка с отдалечен хост (хост в отдалечена мрежа), трябва да знаете IP адреса на този хост.

Отговор: Вярно

Намирате се в подходящата командна обвивка на софтуера за маршрутизация Quagga v. 0.99.21. С коя команда ще активирате RIP протокола на мрежовия интерфейс eth2?

Отговор: set protocols rip interface eth2

Имате маршрутизатор, който разчита на RIPv2 за автоматична конфигурация на записите в маршрутната си таблица. При прекъсване на мрежова връзка на маршрутизатора, кой механизъм за предотвратяване на маршрутни цикли своевременно ще изпрати информация, че пропадналите маршрути са на недостижимо разстояние 16?

Отговор: Route poisoning

Кой механизъм за предотвратяване на маршрутни цикли подтиска изпращането на маршрутна информация през интерфейс, по който тя е била получена?

Отговор: Split horizon

Компанията Eugene ЕАД използва маршрутизатора gw1, за връзка с доставчика си на Интернет услуги (ISP). IP адресът на маршрутизатора на доставчика е 206.143.5.2. Кои от следните команди ще позволят установяването на Интернет връзка на цялата мрежа на Eugene ЕАД?

Изберете едно или повече:

- a. # ifconfig eth0 206.154.5.2 netmask 255.255.255.252
- b. # route add -net 0.0.0.0 netmask 0.0.0.0 gw 206.143.5.2 ✓
- c. # ip route add default via 206.143.5.2 ✓
- d. # route add -net default gw 206.143.5.0

Кои от твърденията са верни за команда route add -net 172.16.4.0 netmask 255.255.255.0 gw 192.168.4.2?

Изберете едно или повече:

- a. Командата се използва за да се установи статичен маршрут. ✓
- b. Използва се метрика по подразбиране. ✓
- c. Командата се използва за създаване на маршрут по подразбиране.
- d. С тази команда се дефинира статичен маршрут към мрежа с адрес 192.168.4.2

Кое от следните е най-доброто описание на метода за предотвратяване на маршрутни цикли Split Horizon?

Изберете едно:

- a. Информацията за маршрут не трябва да бъде изпращана обратно в посоката, от която е дошла. ✓
- b. Разделя трафика, когато имаме голяма физическа мрежа.
- c. Задържа редовните обновявания от разпространение по пропаднала връзка.
- d. Не позволява редовните съобщения за обновяване на маршрутната таблица да създадат маршрут до недостъпна мрежа.

Нека маршрутизаторите Router A, Router B и Router C са свързани последователно.

Нека хостът Host A е свързан към Router A и хостът Host C е свързан към Router C. Кои от следните твърдения ще бъдат верни, ако Host A се опитва да комуникира с Host C докато интерфейсът между Router C и Host C е деактивиран?

Изберете едно или повече:

- a. Router C ще използва ICMP, за да информира Host A, че Host C не може да бъде достигнат. ✓
- b. Router C ще използва ICMP, за да информира Router B, че Host C не може да бъде достигнат.
- c. Router C ще използва ICMP, за да информира Host A, Router A и Router B че Host C не може да бъде достигнат.
- d. Router C ще изпрати съобщение от тип „Destination unreachable“. ✓
- e. Router C ще изпрати съобщение за избор на маршрутизатор.

Кое твърдение е вярно за безкласовите протоколи за маршрутизация (routing protocols)?

Изберете едно или повече:

- a. Не се допуска използването на недопирящи се мрежи.
- b. Позволено е използването на мрежови маски с променлива дължина (VLSM). ✓
- c. RIPv1 е безкласов протокол за маршрутизация.
- d. RIPv2 поддържа безкласова маршрутизация. ✓

1. Кой от следните е валиден хост unicast IPv6 адрес?
 - 2001:0:240E::0AC0:3428:121C
2. Кой от адресите е unicast?
 - 172.31.96.255/19
3. Кои от следните IP адреси от мрежата 27.35.16.32/28 могат да бъдат присвоени на хостове?
 - 27.35.16.33
 - 27.35.16.45
 - 27.35.16.44
4. В подкатегориите на резервните адреси в IPv6 има адрес, който се използва от хостовете да тестват самите себе си без да излизат от мрежата. Кой е този адрес?
 - Loopback
5. В случай на грешка „time exceeded”, когато пакетът е влязъл в рутер, стойността на полето „time to live” се:
 - декрементира се с 1
6. Как се нарича енкапсулирането (опаковане) на IPv6 пакети вътре в IPv4 пакети?
 - Тунелиране
7. Даден ви е префиксът 115.64.4.0/22. Кои от долните IP адреси могат да се присвоят на хостове?
 - 115.64.7.64
 - 115.64.6.255
 - 115.64.5.128
8. При IPv4 адресите класовото адресиране (classful addressing) е заменено с:
 - Безкласово
9. Какъв е максималният брой на IP адресите, които може да бъдат присвоени на хостове в подмрежа с маска 255.255.255.224?
 - 30
10. Кой адрес за получател използва един DHCP клиент, когато се опитва да получи IP адрес?
 - 255.255.255.255
11. IPv6 не използва следният тип адреси
 - Broadcast
12. Мрежата 213.155.77.0 е разделена на подмрежи с префикс /28. Колко подмрежи и с по колко хоста ще се получат?
 - 16 мрежи с 14 хоста
13. В LAN-а на Branch рутера е инсталирано ново PC. PC-то не може да се свърже със сървъра. Какъв е проблемът?
 - default gateway на PC-то е зададен неточно
14. Как се нарича физическият път, по който „пътува“ съобщението?
 - медия (комуникационна среда)
15. Мрежов администратор верифицира конфигурацията на новоинсталлиран хост, като установява FTP конекция към отдалечен сървър. Кой е най-високият слой в протоколния стек, използван в този случай?
 - Приложен
16. При конфигурирането на DHCP сървър за кои два IP адреса трябва да се има предвид, че не трябва да се раздават на хостове?
 - IP адресът на мрежата/подмрежата

- Бродкаст адресът на мрежата
17. Кои от следните протоколи работят на приложния слой на OSI модела?
- FTP
 - Telnet
18. Мрежата alabala се състои от 5 отдела: Директорска администрация – 7 компютъра; отдел „Поддръжка“ – 15 компютъра; отдел „Финансов“ – 13 компютъра; отдел „Търговски“ – 7 компютъра; Отдел „Иновации“ – 16 компютъра. Каква маска ще приложите?
- 255.255.255.224
19. Какви ползи ще извлече от VLAN технологията една голяма корпорация?
- VLAN-те дефинират сегментирани broadcast domain-и в мрежи с комутатори.
 - VLAN-те значително улесняват добавяне, преместване или промяна на хостове в мрежата.
 - VLAN-те позволяват мрежовите услуги да се организират по отдели, а не по физическо разположения
20. При класовото адресиране (classful addressing) голяма част от адресите се:
- Пропиливат
21. Как изглежда в двоичен вид шестнайсетично число 78F3?
- 0111100011110011
22. Броят на слоевете в TCP/IP протоколния стек е:
- 4
23. **При включване на захранването PC2 се опитва да се свърже с DCHP сървър. Как става това?**
- C Layer 3 broadcast съобщение
24. **Точният формат на пакета при преход на IPv6 мрежа (тунел) е: 1. IPv6 header, 2.Payload (поле за данни), 3. IPv4 header**
- 3-1-2
25. Кое е PDU-то в мрежовия слой?
- Пакет
26. Кой от долните протоколи работи на слой 2 на OSI модела и служи за предпазване от зациклияне(loop-free мрежа)?
- STP
27. Рутерът получава пакет на интерфейс 172.16.45.66/26, source IP на пакета е 172.16.45.127/26, a destination – 172.16.46.191/26. Как рутерът ще обработи пакета?
- destination е broadcast, така че рутерът няма да прехвърли пакета
28. Искате да сегментирате LAN-а на множество broadcast domain-и. Коя технология ще приложите?
- Virtual LANs
29. В полето за данни в IP пакета се записва следното:
- UDPдейтаграма
 - ICMP съобщение
 - TCPсегмент
30. Устройство, което направлява пакетите между различните мрежи, като обработва информацията на 3 слой в заглавните им части (header), се нарича:
- маршрутизатор (рутер)
31. link local адресите се използват в
- изолиран етернет сегмент
32. Bluetooth е пример на:

- Персонална мрежа
33. Колко хост IP адреса има в една Class C мрежа?
- 254
34. Кой е префикс за IPv6 мултиicast?
- FF00::/8
35. На кой OSI слой заглавната част съдържа адрес на хост, който е адрес на дестинация и се намира в отдалечена мрежа?
- Мрежов
36. Имате IP адрес 192.168.10.19/28
- 192.168.10.17
 - 192.168.10.29
37. Кой от следните адреси е broadcast адрес на клас В мрежа с маска по подразбиране?
- 172.16.255.255
38. Кои от посочените твърдения са верни за IPv6 unicast адресите?
- Глобалните адреси започват с 2000::/3
 - Има само един loopback адрес, който е ::1
39. Имате IP адрес 172.16.28.252 с маска 255.255.240.0. Към коя IP мрежа принадлежи този IP адрес?
- 172.16.16.0
40. ARP изпраща заявки, които са:
- Broadcast на втори слой от OSI модела и unicast на 3ти
41. Транспортният слой изпълнява следните функции:
- Контролиране на комуникацията от край до край между процеси, изпълнявани на различни хостове
42. Посочете две причини, заради които мрежовият администратор ще сегментира мрежата с помощта на Layer 2 сүич?
- Ограничава broadcast-те в отделните виртуални сегменти
 - Ще изолира трафика между сегментите
43. TCP/IP няма такъв слой, но OSI моделът го има. Кой е той?
- Сесиен
44. Рутер не може да маршрутизира (или хост да постави) пакет. Тогава пакетът се изхвърля и рутерът (или хостът) изпраща ICMP съобщение към възела – източник на пакета. Кое е то?
- Destination unreachable
45. Стандартите на IETF се наричат:
- RFC
46. Кое твърдение е вярно за IPv6?
- Мултиicastите изпълняват роля на бродкасти.
47. Колко дълъг е IPv6 адреса?
- 128 bits
48. 100BASE-FX реализира Етернет (Ethernet) стандарта при скорост на предаване 100Mbps
- По оптичен кабел
49. На мрежата ви е даден префикс 172.12.0.0 (class B). На всяка подмрежа трябва да има 515 хоста. Коя маска ще използвате
- 255.255.252.0
50. Скоростта на предаване в bit/s се определя от:

- Физическия слой
51. Кой от следните процеси се използва за откриване на hardware (MAC) адрес на LAN контролер?
- ARP
- ДРУГ ТЕСТ
1. Администраторът трябва да присвои статични IP адреси на сървърите в мрежата. За IP мрежа 192.168.20.24/29, на рутера е присвоен първият използваем (хост) адрес, а на сървър "Продажби" е даден последният използваем (хост) адрес. Кои от следните адреси ще бъдат въведени в "IP properties" полетата на сървър "Продажби"?
- c. IP address: 192.168.20.30
- Subnet Mask: 255.255.255.248
- Default Gateway: 192.168.20.25
2. Кой от следните IP адреси е частен IP адрес?
- c. 192.168.42.34
3. Кой слой осигурява директно услуги за потребителя?
- приложен Правилен отговор
4. Ако хост в мрежа има адрес 172.16.45.17/30, какъв ще е префикс, към който принадлежи хоста?
- 172.16.45.16 Правилен отговор
5. Кой от долните три протоколи принадлежат на приложния слой?
- TFTP
 - SMTP
 - HTTPS
6. Каква е целта на алгоритъма spanning-tree в комутираната LAN?
- Да предпазва от зацикляне на 2 слой (switching loops) в мрежи с резервирани пътища между комутаторите. Правилен отговор
7. На един сүич е конфигурирана виртуална локална мрежа VLAN 2, към която са присвоени всички FastEthernet портове. Какво ще се случи, ако се конфигурира нов VLAN 3 и на него се присвоят част от портовете?
- Ще се създаде още един бродкаст домейн.
8. Кои са двете характеристики на "store and forward" switching (комутиране)?
- Закъснението през комутатора варира според дължината на фрейма.
 - Комутаторът получава целият кадър (фрейм), преди да започне да го прехвърля към изходен порт.
9. Броят на слоевете в еталонния модел ISO OSI е
- 7
10. Имате двоичното число 10011101. Преобразувайте го в 16-ен формат.
- 0x9D
11. Колко дълъг е IPv6 адреса?
- 16 шестнадесетични числа, 128 bits
12. На мрежата SUnet е дадена Class C мрежа 199.166.131.0. Администраторът прилага маска 255.255.255.240. Колко хоста ще има на всяка подмрежа?

- 14
13. Кой от следните IP адреси попада в CIDR блок 115.54.4.0/22?
- 115.54.5.255
 - 115.54.7.61
 - 115.54.5.128
14. На рутера е конфигуриран IP адрес 172.16.2.1/23 на интерфейс Eth0. Кои от следните IP адреси са валидни за компютри, които са в LAN-а, "закачен" за интерфейс Eth0 на рутера?
- 172.16.2.255
 - 172.16.3.0
15. Какви са предимствата на сегментирането на мрежата с рутер?
- Рутерът не прехвърля бродкастите от един сегмент в друг.
 - Можете да приложите филтриране по IP адреси.
16. SUnet има клас C мрежа и иска на 5 департамента да се присвои отделна подмрежа. Всяка подмрежка трябва да поеме най-малко 24 хоста. Каква ще е маската?
- /27
17. Кои от долуизброените протоколи оперират на Интернет слоя на TCP/IP модела?
- IPsec
 - RARP
18. Кой от следните IP адреси попада в супермрежата 115.64.4.0/22?
- 115.64.6.255
 - 115.64.7.64
 - 115.64.5.128
19. Каква е максималната препоръчана дължина на 10BaseT кабел?
- 100 meters
20. Посочете две характеристики на IPv6.
- anycast, multicast
21. РС в мрежов сегмент изпраща данни до друго РС на друг сегмент. Кой от следните отговори правилно описва точния ред на опаковане (encapsulation) на данните?
- Frame bit

Тест 2

1. NIC (мрежова карта) има MAC адрес 00-0F-66-81-19-A3 и открива маршрутизиращ префикс 2001:0:1::/64. Кой IPv6 адрес ще се присвои на картата? – 2001:1:5:20F:66FF:FE81:19A3
2. В IPv6 хедъра полето Traffic Class е подобно на следното поле в IPv4 хедъра – TOS (Type Of Service)
3. На мрежата SUnet е дадена Class C мрежа 199.166.131.0. Администраторът прилага маска 255.255.255.240. Колко хоста ще има всяка подмрежа? – 14
4. Кои от следните твърдения са верни за IPv6 unicast адресите? – глобалните адреси започват с 200::/3 ; има само един loopback адрес, който е ::1
5. Какъв е максималният брой IP адреси, които могат да бъдат присвоени на хостове в подмрежа с маска /27? – 30
6. Във всяка NAT (Network Address Translation) конфигурация кой е вътрешния глобален (Inside Global) IP адрес? – получен адрес, който представя вътрешен хост пред външната мрежа
7. Каква информация могат да извлекат два компютъра от съобщенията „timestamp request“ и „timestamp replay“ за IP пакет, който пътува между тях? – Round-trip time (RTT)
8. В структурата на IPv6 адреса, колко бита съдържа всяко поле (заградено с :) ? – 16
9. Кой е broadcast адреса на мрежа 89.51.100.0 с маска 255.255.254.0? – 89.51.101.255
10. Каква е целта на DHCP сървъра? – да осигурява IP конфигурация на хостовете.
11. Стратегията, която използват два компютъра с IPv6, за да комуникират помежду си през IPv4 мрежа е: - тунелиране
12. Има проблем с комуникациите между двата директно свързани компютри, произведени през 2017г. Как може да се реши? – Свързването да стане с помощта на рутер и маската на двете машини да се промени на 255.255.255.0
13. Кое е вярно за NAT конфигурацията на горната фигура? (най горния адрес е 172.16.1.254) – Числото 1 в командата ip nat inside source се отнася до филтъра (access-list) с номер 1, който дефинира вътрешните (частни) адреси, които ще се транслират в публични.

Тест 1

14. Физическо или логическо подреждане в мрежата е
а. омрежаване

b. маршрутизиране

c. топология

d. окабеляване

15. При "движението" на пакета с данни отгоре надолу по слоестата архитектура заглавията (headers) се

a. преаранжират

b. добавят

c. премахват

d. модифицират

16. Как се нарича съединение, което се споделя от три и повече устройства?

a. точка-точка

b. Няма верен отговор

c. многоточково

17. Каналният слой взима пакети от КОИ СЛОЙ и ги енкапсулира в кадри (frames)?

a. представителен

b. транспортен

c. физически

d. мрежов

e. сесиен

18. Разгледайте локалната мрежа с 2 FMI комутатора:

Мрежата съдържа два VLAN-а.

- ports 1 - 4 на всеки комутатор принадлежат на VLAN1

- ports 5 - 8 на всеки комутатор принадлежат на VLAN2.

- 802.1q trunk свързва двата комутатора.

Въз основа на горното, кое е вярно?

a. хост 2-1 не може да ping хост 2-2

b. хост 7-1 не може да не може да ping хост 2-2

c. хост 2-1 може да ping хост 7-2

d. хост 2-1 може да ping хост 2-2

e. хост 7-1 може да ping хост 7-2

19. Каква е целта на алгоритъма spanning-tree в комутираната LAN?

Изберете едно

a. Осигурява механизъм за следене на мрежи в среди с комутатори.

b. Да предпазва от зациклияне на 2 слой (switching loops) в мрежи с резервираны пътища между комутаторите.

c. Да управлява VLAN-и през множество комутатори.

d. Да сегментира мрежата на множество колизия домейни.

e. Да предпазва от зациклияне на маршрути routing loops) в мрежите.

20. В полуудуплекс (half-duplex) Ethernet LAN, два хоста се опитват едновременно да изпратят данни, което предизвиква колизия (колизия). Какво следва да направят двата хоста?

Изберете едно

- a. Сигналът „jam“ показва, че колизията е изчистена.
- b. Хостовете нищо няма да правят, тъй като по-горните слоеве са отговорни за корекция на грешки и повторно предаване.
- c. destination хост изпраща „молба“ до източника за повторно предаване на фрейма.
- d. Електрически импулс показва, че колизията е изчистена.
- e. Всеки един от двата хоста ще опита повторно предаване след произволен интервал от време.
- f. Рутерът, който е на сегмента, ще сигнализира, че колизията е изчистена.

21. Как комуникират мрежови устройства разпределени във виртуални локални мрежи (VLAN)?

Изберете едно

- a. Устройства от една виртуална локална мрежа (VLAN) комуникират с помощта на маршрутизатор
- b. Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта намагистрална (trunk) линия между комутаторите (комутатори)
- c. Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на протокола VTP
- d. Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта намаршрутизатор (router)

22. Искате да сегментирате LAN-а на множество broadcast domain-и. Коя технология ще приложите?

Изберете едно

- a. Virtual LANs
- b. Fragment-free switching (комутиране)
- c. Transparent bridging (прозрачен мост)
- d. Cut-through switching
- e. Store-and-forward switching

23. Кои от следните изречения отразяват предимствата на VLAN-те?

Изберете едно или повече:

- a. Увеличават броя на бродкаст домейните, като същевременно намаляват размерите им.
- b. Увеличава се броя на колизионните домейни.
- c. Увеличават размера на бродкаст домейните, като същевременно намаляват броя на колизионните домейни.
- d. Подобряват сигурността в мрежата.
- e. Позволяват логическо групиране на потребителите според функциите, които изпълняват.
- f. Конфигурирането на съич с VLAN-и е по-лесно.

24. Кой слой отговаря за отдалечените комуникации между процеси?

Изберете едно

- a. представителен
- b. транспортен
- c. мрежов
- d. канален
- e. сесиен

25. В транспортния слой на TCP/IP модела кои са валидните протоколи?

Изберете едно или повече:

- a.ARП
- b.RARP
- c.IР
- d.UDP
- e.TCP
- f.BootP
- g.ICMP

26. Хост изчислява контролната сума върху получен PDU и вижда, че е повреден и трябва да се изхвърли. На кой слой от OSI модела става това?

Изберете едно

- а. транспортен
- б. приложен
- с. мрежов
- d. канален
- е. сесиен

27. Кои от посочените са предимства на оптичните кабели при изграждане на мрежи:

Изберете едно или повече:

- a.устойчивост към електромагнитни смущения
- b.по-гъвкав от медните еквиваленти
- c.позволява информационен пренос на големи разстояния
- d.по-евтини мрежови карти (адаптори) отколкото за медни кабели
- e.нисък шанс за поразяване от мълния
- f.по-висока скорост от UTP

Прескоши на основното съдържание moodle

- Неизвестен  Снимка на Стайко Дафов
-  Моето табло 
-
-  Профил 
-  Оценки 
-  Съобщения 
-  Предпочитания 
-
-  Изход 

 Покажи менюто за съобщения

0

Съобщения

Ново съобщение

   Предпочитания за съобщенията

Няма чакащи съобщения



Виж всички

 Покажи менюто за уведомления

0

Уведомление

   Предпочитания за уведомленията

Нямате уведомления



Виж всички

- Български (bg)
 - English (en)
 - Български (bg)

Компютърни мрежи, сп. КН-1, летен семестър 2018/2019

Път през страниците

- [Начална страница](#) / ►
- Моите курсове / ►
- [Бакалаври, летен семестър 2018/2019](#) / ►
- [КН](#) / ►
- [Компютърни мрежи, сп. КН-1, летен семестър 2018/2019](#) / ►
- 15 април - 21 април / ►
- [Първи официален тест върху лекциите](#)

Започнат на

Състояние Завършен

Приключен на

Изминалото време

Точки 19,50/25,00

Оценка **7,80** от 10,00 (78%)

Въпрос 1

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

В случай на грешка "time exceeded", когато пакетът е влязъл в рутер, стойността на полето "time to live" се:

Изберете едно

- a. остава непроменена
- b. инкрементира се с 1
- c. декрементира се с 1  Правилен отговор
- d. декрементира се с 2

Забележка

Вашият отговор е верен.

Правилният отговор е: декрементира се с 1

Въпрос 2

Неправилен отговор

0,00 от максимално 1,00 точки



Текст на въпроса

С коя команда се присвоява последния използваем IP адрес от префикса 192.168.32.128/28 на интерфейса на рутера?

Изберете едно

- a.

SUA(config-if)# ip адрес 192.168.32.158 255.255.255.240

- b.

SUA(config-if)# ip адрес 192.168.32.158 255.255.255.240

- c.

SUA(config-if)# ip адрес 192.168.32.143 255.255.255.240  Неправилен отговор

- d.

SUA(config-if)# ip адрес 192.168.32.144 255.255.255.240

- e.

SUA(config-if)# ip адрес 192.168.32.142 255.255.255.240

Забележка

Правилният отговор е:

```
SUA(config-if)# ip адрес 192.168.32.142 255.255.255.240
```

Въпрос 3

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Имате class C мрежа и трябва да я разделите така, че да имате поне 13 подмрежи с по минимум 12 хоста. Коя маска ще приложите?

Изберете едно



225.225.255.0



225.225.240.0



225.225.255.240 Правилен отговор



255.255.255.224



225.225.224.0

Забележка

Правилният отговор е:

Въпрос 4

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан

Текст на въпроса

На мрежата SUnet е даден префикс 165.100.27.0/24. Колко подмрежи с по колко хоста поддържа този префикс?

Изберете едно

a.

30 мрежи с по 64 хоста.

b.

254 мрежи с по 65,534 хоста.

c.

Една мрежа с 254 хоста.  Правилен отговор

d.

65534 мрежи с по 255 хоста.

e.

254 мрежи с по 254 хоста.

Забележка

Правилният отговор е:

Една мрежа с 254 хоста.

Въпрос 5

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан

Текст на въпроса

Транспортният слой се имплементира в:

Изберете едно

- a. комуникационната среда
- b. крайната система  Правилен отговор
- c. рутера
- d. ЛМ Етернет

Забележка

Вашият отговор е верен.

Правилният отговор е: крайната система

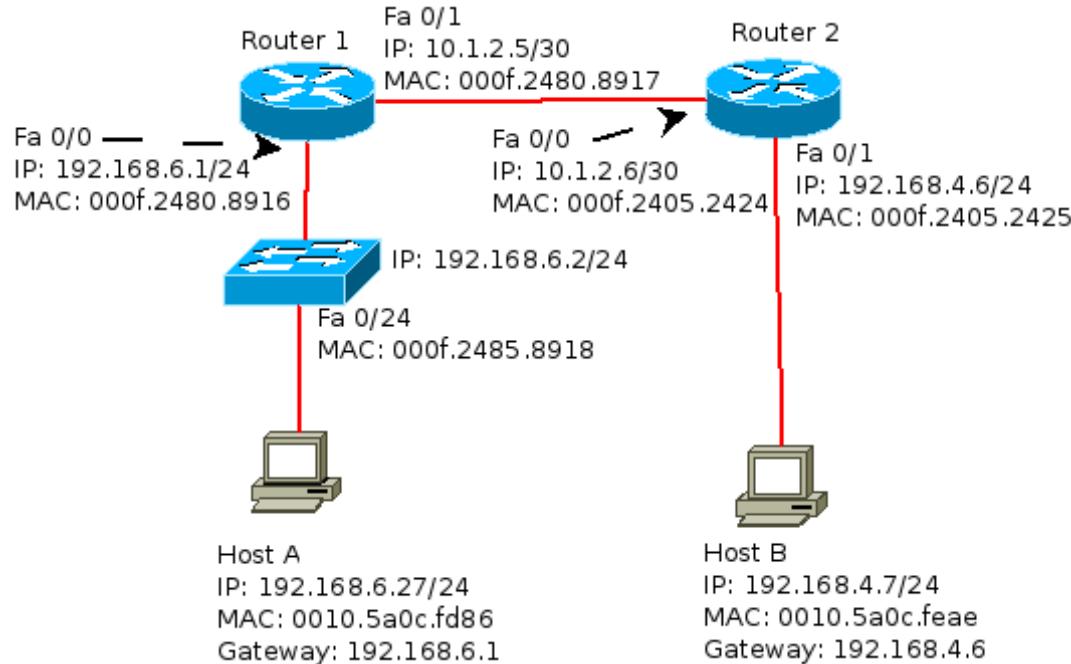
Въпрос 6

Неправилен отговор

0,00 от максимално 1,00 точки

 Неотбелязан

Текст на въпроса



HostA ping-ва HostB. Кой от долните записи е валиден за ARP кеша на HostA след изпълнението на командата ping:

- | IP | MAC |
|---------------|----------------|
| A 192.168.4.7 | 000f.2480.8916 |
| B 192.168.4.7 | 0010.5a0c.feaе |
| C 192.168.6.1 | 0010.5a0c.feaе |
| D 192.168.6.1 | 000f.2480.8916 |
| E 192.168.6.2 | 0010.5a0c.feaе |
| F 192.168.6.2 | 000f.2485.8918 |

Изберете едно

- a. Запис D  Неправилен отговор
- b. Запис В
- c. Запис Е
- d. Запис С
- e. Запис А
- f. Запис F

Забележка

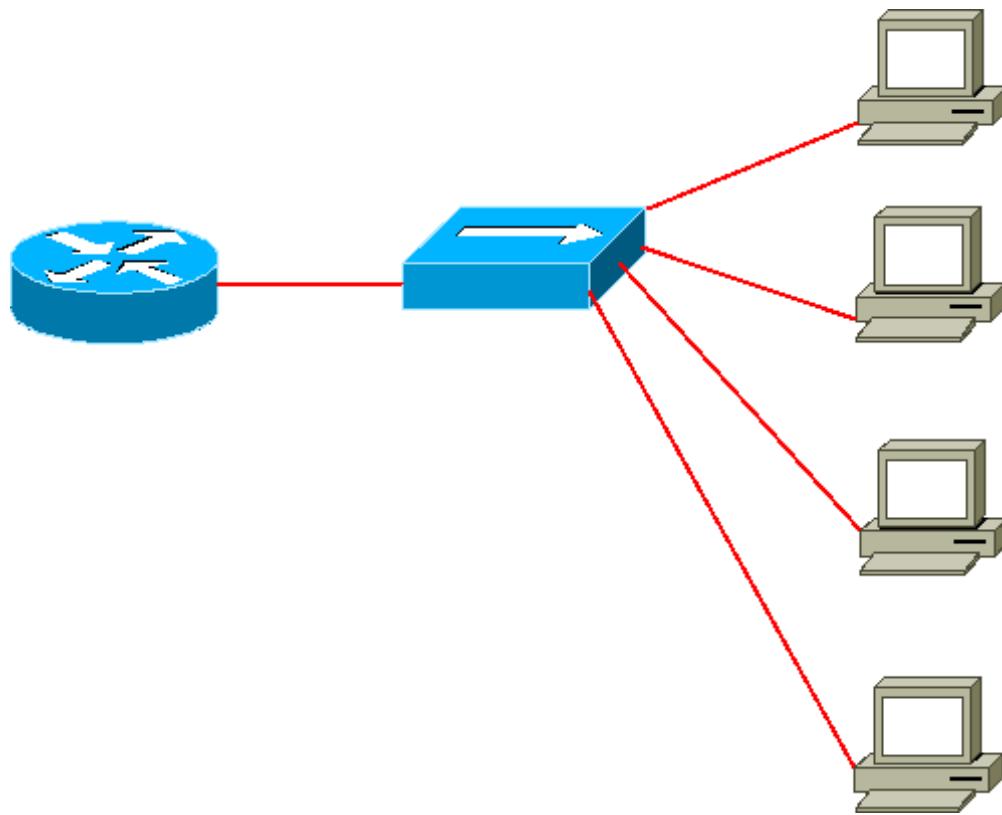
Вашият отговор не е верен.
Правилният отговор е: Запис F

Въпрос 7

Частично правилен отговор
0,50 от максимално 1,00 точки



Текст на въпроса



На горната фигура, ако заменим хъба със суич (комутатор), какво ще се случи?

Изберете едно или повече:

- a. Броят на колизионните домейни ще ое увеличи.  Правилен отговор
- b. Броят на бродкаст домейните ще намалее.
- c. Броят на бродкаст домейните ще се увеличи.
- d. Броят на колизионните домейни ще остане същият.
- e. Броят на колизионните домейни ще намалее.
- f. Броят на бродкаст домейните ще остане същият.

Забележка

Вашият отговор отчасти е верен.

Вие правилно сте избрали 1.

2 верни отговора

Правилните отговори са: Броят на колизионните домейни ще се увеличи., Броят на бродкаст домейните ще остане същият.

Въпрос 8

Частично правилен отговор

0,50 от максимално 1,00 точки



Текст на въпроса

Кои от долуизброените протоколи оперират на Интернет слоя на TCP/IP модела?

Изберете едно или повече:



SONET/SDH



RARP



IPsec Правilen отговор



BOOTP



DHCP Неправilen отговор



SNMP



DNS

 h.

HDLC

Забележка

Правилните отговори са:

RARP,

IPsec

Въпрос 9

Неправилен отговор

0,00 от максимално 1,00 точки

  Неотбелязан

Текст на въпроса

Във всяка NAT (Network Address Translation) конфигурация кой е вътрешния глобален (Inside Global) IP адрес?

Изберете едно

 a.

Сумаризираният (summarized) адрес на всички вътрешни подмрежкови адреси.  Неправилен отговор

 b.

Публичен адрес, който представя вътрешен хост пред външната мрежа.

 c.

Частен IP адрес присвоени на хост във вътрешната мрежа.

 d.

Уникален IP адрес, който се използва във вътрешната мрежа

Забележка

Правилният отговор е:

Публичен адрес, който представя вътрешен хост пред външната мрежа.

Въпрос 10

Неправилен отговор

0,00 от максимално 1,00 точки



Неотбелязан

Текст на въпроса

Администраторът изпълнява команда “ping 127.0.0.1” от компютър с хост име PC1. Ако е получен ICMP reply, какво потвърждава?

Изберете едно

- a. PC1 има свързаност с устройство на 3 слой.
- b. Протоколният стек TCP/IP е правилно инсталзиран на PC1.
- c. PC1 има свързаност до 5 слой на OSI модела.
- d. PC1 е с правилно конфигуриран default gateway.
- e. PC1 има свързаност с локален хост.



Неправилен отговор

Забележка

Вашият отговор не е верен.

Правилният отговор е: Протоколният стек TCP/IP е правилно инсталзиран на PC1.

Въпрос 11

Правилен отговор

1,00 от максимално 1,00 точки



Неотбелязан

Текст на въпроса

Какви ползи ще извлече от VLAN технологията една голяма корпорация?

Изберете едно или повече:



a.

VLAN-те значително улесняват добавяне, преместване или промяна на хостове в мрежата.  Правилен отговор



b.

VLAN-те осигуряват метод за комуникации между IP адреси в големи мрежи.



c.

VLAN-те позволяват мрежовите услуги да се организират по отдели, а не по физическо разположение.  Правилен отговор



d.

VLAN-те дефинират сегментирани broadcast domain-и в мрежи с комутатори.  Правилен отговор



e.

VLAN-те осигуряват комуникации с ниско закъснение и висока пропускателна способност.



f.

VLAN-те повишават сигурността чрез филтриране на пакети.

Забележка

Правилните отговори са:

VLAN-те позволяват мрежовите услуги да се организират по отдели, а не по физическо разположение.,

VLAN-те дефинират сегментирани broadcast domain-и в мрежи с комутатори.,

VLAN-те значително улесняват добавяне, преместване или промяна на хостове в мрежата.

Въпрос 12

Правилен отговор

1,00 от максимално 1,00 точки



Неотбелязан

Текст на въпроса

Кое поле от фрейма разглежда схемата за разпознаване на грешки, за да изпълни своята функция?

Изберете едно

a.

MAC

b.

ERR

c.

Flag

d.

PDU

e.

MTU

f.

FCS  Правилен отговор

Забележка

Правилният отговор е:

FCS

Въпрос 13

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан

Текст на въпроса

Как се създава EUI-64 формат на interface ID от 48-битов MAC адрес?

Изберете едно

- a. Поставяне на 0xFF пред MAC адреса и добавяне на 0xFF след него.
- b. Поставяне на 0xFFEE пред MAC адреса.
- c. Чрез прикрепяне на 0xFF към MAC адреса.
- d. Поставяне на 0xF пред MAC адреса и добавяне на 0xF след него.
- e. Чрез вмъкване на 0xFFFFE между първите три и вторите три байта на MAC адреса.

address Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: Чрез вмъкване на 0xFFFFE между първите три и вторите три байта на MAC адреса.

address

Въпрос 14

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан

Текст на въпроса

На долната схема е показана клоновата мрежата:

Колко колизионни домейни има в тази мрежа?

Изберете едно

- a. 5
- b. 1

- c. 14
- d. 2 Правилен отговор
- e. 3
- f. 4
- g. 6

Забележка

Правилният отговор е: 2

Въпрос 15

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

С кое от следните устройства администраторът може да сегментира локалната си мрежа?

Изберете едно или повече:



комутатори (суичове) Правилен отговор



мостове (Bridges) Правилен отговор



хъбове



Маршрутизатори (рутери) Правилен отговор



Медиа конвертори (FO-UTP)



f.

рипитери

Забележка

Правилните отговори са:

комутатори (суичове),

мостове (Bridges),

Маршрутизатори (рутери)

Въпрос 16

Правилен отговор

1,00 от максимално 1,00 точки



Неотбелязан

Текст на въпроса

Какъв е максималният брой на IP адресите, които може да бъдат присвоени на хостове в подмрежа с маска 255.255.255.224?

Изберете едно

a. 16

b. 30

c. 12

d. 15

Забележка

Вашият отговор е верен.

Правилният отговор е: 30

Въпрос 17

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Физическо или логическо подреждане в мрежата е

Изберете едно

- a. окабеляване
- b. маршрутизиране
- c. омрежаване
- d. топология  Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: топология

Въпрос 18

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Физическият слой осигрява

Изберете едно

- a. Всички отговори са верни  Правилен отговор

- b. електрически спецификации на сигналите по комуникационните линии
- c. спецификации на лъчите по оптическите кабели
- d. механични спецификации на електрическите конектори и кабели

Забележка

Вашият отговор е верен.

Правилният отговор е: Всички отговори са верни

Въпрос 19

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Определен брой старши битове в IPv6 адреса определят категорията му. Как се наричат?

Изберете едно

- a. резервирали
- b. локални
- c. постфикс
- d. префикс  Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: префикс

Въпрос 20

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Посочете валидния IPv6 адрес.

Изберете едно

- a. 2031:0:130F::9C0:876A:130B  Правилен отговор
- b. 2001:0db8:0:130H::87C:140B
- c. 2001:0db8:0000:130F:0000:0000:08GC:140B
- d. 2031::130F::9C0:876A:130B

Забележка

Вашият отговор е верен.

Правилният отговор е: 2031:0:130F::9C0:876A:130B

Въпрос 21

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Към коя виртуална локална мрежа (VLAN) по поддържане принадлежи една магистрална (trunked) линия?

Изберете едно

- a.

първата дефинирана виртуална локална мрежа (VLAN)

- b.

към дефинирана виртуална локална мрежа (VLAN) с най-малък номер

- c.

последната дефинирана виртуална локална мрежа (VLAN)

- d.

към всички дефинирани виртуални локални мрежи (VLAN)  Правилен отговор

Забележка

Правилният отговор е:

към всички дефинирани виртуални локални мрежи (VLAN)

Въпрос 22

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан

Текст на въпроса

Коя от следните разновидности на NAT реализира политиката множество портове и частни IP адреси да излизат с един единствен публичен IP адрес?

Изберете едно

a.

port loading

b.

Port Address Translation  Правилен отговор

c.

статичен NAT

d.

Dynamic NAT

Забележка

Правилният отговор е:

Port Address Translation

Въпрос 23

Частично правилен отговор
0,50 от максимално 1,00 точки



Текст на въпроса

Основната причина за преход от IPv4 към IPv6 е:

Изберете едно или повече:

- a. Огромният брой системи и хостове в internet
- b. Изчерпване на IPv4 адресите  Правилен отговор
- c. Осигуряване на стандартни адреси
- d. Малкият брой автономни системи в internet

Забележка

Вашият отговор отчасти е верен.
Вие правилно сте избрали 1.

2 верни отговора

Правилните отговори са: Огромният брой системи и хостове в internet, Изчерпване на IPv4 адресите

Въпрос 24

Правилен отговор
1,00 от максимално 1,00 точки



Текст на въпроса

CRC означава:

Изберете едно

- a. cyclic redundancy check  Правилен отговор
- b. Няма верен отговор
- c. cyclic repeat check
- d. code repeat check

Забележка

Вашият отговор е верен.

Правилният отговор е: cyclic redundancy check

Въпрос 25

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

В IPv6 адреса колко бита са включени във всяко поле, разделено със знака :

Изберете едно

- a. 3
- b.

4

- c.

24

- d. 16  Правилен отговор

Забележка

Правилният отговор е: 16

Записване състоянието на отбелязването

[Край на прегледа](#)

[!\[\]\(4a8e2020a4067a549da15b5f231f8fbb_img.jpg\) Маршрутен протокол OSPF в IPv4 и IPv6.](#)

Отиди на ... [Отиди на ...](#)

[Прескочи Навигация в теста](#)



Навигация в теста

[Въпрос 1 Тази страница](#) [Въпрос 2 Тази страница](#) [Въпрос 3 Тази страница](#) [Въпрос 4 Тази страница](#) [Въпрос 5 Тази страница](#) [Въпрос 6 Тази страница](#)
[Въпрос 7 Тази страница](#) [Въпрос 8 Тази страница](#) [Въпрос 9 Тази страница](#) [Въпрос 10 Тази страница](#) [Въпрос 11 Тази страница](#) [Въпрос 12 Тази страница](#)
[Въпрос 13 Тази страница](#) [Въпрос 14 Тази страница](#) [Въпрос 15 Тази страница](#) [Въпрос 16 Тази страница](#) [Въпрос 17 Тази страница](#) [Въпрос 18 Тази страница](#)
[Въпрос 19 Тази страница](#) [Въпрос 20 Тази страница](#) [Въпрос 21 Тази страница](#) [Въпрос 22 Тази страница](#) [Въпрос 23 Тази страница](#)
[Въпрос 24 Тази страница](#) [Въпрос 25 Тази страница](#)
[Показване по един въпрос на страница](#) [Край на прегледа](#)

Вие сте влезли в системата като [Стайко Дафов \(Изход\)](#)

[C425510S2](#)

[Get the mobile app](#)

[Прескоши на основното съдържание](#)
[moodle](#)

- [Димитро Богдев](#)  Снимка на Дмитро Богдев

-  [Моето табло](#)  [Моето табло](#)

-

-  [Профил](#)  [Профил](#)

-  [Оценки](#)  [Оценки](#)

-  [Съобщения](#)  [Съобщения](#)

-  [Предпочитания](#)  [Предпочитания](#)

-

-  [Изход](#)  [Изход](#)

 Покажи менюто за съобщения

0

Съобщения

[Ново съобщение](#)

 [Mark all as read](#)   [Предпочитания за съобщенията](#)

Няма чакащи съобщения

[Виж всички](#)

 Покажи менюто за уведомления

0

Уведомление

 [Mark all as read](#)   [Предпочитания за уведомленията](#)

Нямате уведомления

[Виж всички](#)

- [Български \(bg\)](#)
 - [English \(en\)](#)
 - [Български \(bg\)](#)

•

Компютърни мрежи, сп. Софт. Инж., летен семестър 2018/2019

Път през страниците

- [Начална страница](#) / ►
- Моите курсове / ►
- [Бакалаври, летен семестър 2018/2019](#) / ►
- [СИ](#) / ►
- [Компютърни мрежи, сп. Софт. Инж., летен семестър 2018/2019](#) / ►
- 22 април - 28 април / ►
- [Първи официален тест върху лекциите](#)

Започнат на понеделник, 22 април 2019, 20:01

Състояние Завършен

Приключен на понеделник, 22 април 2019, 20:39

Изминалото време 38 мин. 32 сек.

Точки 19,17/25,00

Оценка 7,67 от 10,00 (77%)

Въпрос 1

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Кои от долните твърдения са верни за IPv6 адресите?

Изберете едно или повече:



На един интерфейс може да се присвойт множество IPv6 адреси от различен тип.  Правилен отговор



b.

Всеки IPv6 интерфейс съдържа един loopback адрес.  Правilen отговор



c.

Водещите нули в 16-bit шестнадесетичното поле на IPv6 адресите се изписва задължително.



d.

Първите 64 бита са динамично създадения интерфейс ID.

Забележка

Правилните отговори са:

На един интерфейс може да се присвойт множество IPv6 адреси от различен тип.,

Всеки IPv6 интерфейс съдържа един loopback адрес.

Въпрос 2

Правilen отговор

1,00 от максимално 1,00 точки



 Неотбелязан

Текст на въпроса

Корпоративната LAN е един „плосък“ Ethernet сегмент. Искате да я разделите на 2 сегмента с помощта на рутер. Какво ще постигнете с това?

Изберете едно



a.

Ще се увеличи броя на колизиите.



b.

Ще се намали броя на broadcast домейните.



c.

Бродкастите от сегмент 1 няма да се пренасят в сегмент 2.  Правилен отговор



d.

Бродкастването на трафика между сегментите ще е по-ефективно.

Забележка

Правилният отговор е:

Бродкастите от сегмент 1 няма да се пренасят в сегмент 2.

Въпрос 3

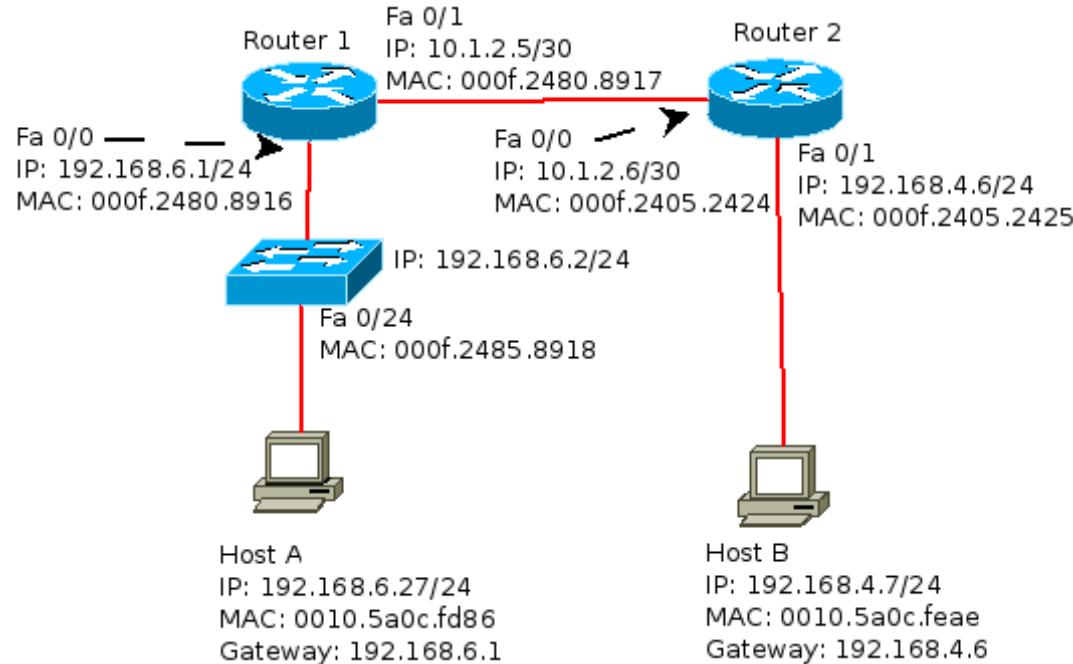
Правилен отговор

1,00 от максимално 1,00 точки



Неотбелязан

Текст на въпроса



HostA ping-ва HostB. Кой от долните записи е валиден за ARP кеша на HostA след изпълнението на командата ping:

- | IP | MAC |
|---------------|----------------|
| A 192.168.4.7 | 000f.2480.8916 |
| B 192.168.4.7 | 0010.5a0c.feaе |
| C 192.168.6.1 | 0010.5a0c.feaе |
| D 192.168.6.1 | 000f.2480.8916 |
| E 192.168.6.2 | 0010.5a0c.feaе |
| F 192.168.6.2 | 000f.2485.8918 |

Изберете едно

- a. Запис С
- b. Запис D
- c. Запис Е
- d. Запис А
- e. Запис F  Правилен отговор
- f. Запис В

Забележка

Вашият отговор е верен.

Правилният отговор е: Запис F

Въпрос 4

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Вие сте мрежов администратор на BULLEO. Мрежата ви се състои от две подмрежи, както на показаната схема по-долу:

Подмрежата Subnet A съдържа 25 клиентски компютъра, които получават TCP/IP настройки от DHCP сървър. Обхвата на подмрежата Subnet A е от адрес 131.107.50.64 до адрес 131.107.50.95.

Подмрежа Subnet B съдържа единствено пощенски сървър с име BULLEO1.

Потребителите от подмрежа Subnet A съобщават, че не могат да се свържат с BULLEO1.

Стартирайки команда ping 131.107.50.126 от клиентски компютър от подмрежа Subnet A, Вие получавате следното съобщение за грешка: "Request timed out".

Трябва да осигурите свързаност на компютрите от подмрежа Subnet A до сървъра BULLEO1.

Какво трябва да направите?

Изберете едно

a.

Ще промените IP адреса на интерфейса на рутер1 към подмрежа Subnet A на 131.107.50.65.

b.

Ще промените маската на подмрежата на клиентските компютри от подмрежа Subnet A на 255.255.255.224.

c.

Ще промените IP адреса на BULLEO1 на 131.107.50.130.  Правилен отговор

d.

Ще промените маската на подмрежата на BULLEO1 на 255.255.255.224.

Забележка

Правилният отговор е:

Ще промените IP адреса на BULLEO1 на 131.107.50.130.

Въпрос 5

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан

Текст на въпроса

Dual-stack означава

Изберете едно

a. Няма верен отговор

b. Един възел поддържа и IPv4, и IPv6  Правилен отговор

c. Реализираме два IPv6 стека

d. Реализираме два IPv4 стека

Забележка

Вашият отговор е верен.

Правилният отговор е: Един възел поддържа и IPv4, и IPv6

Въпрос 6

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

На кой слой от OSI модела оперират TTL филтрите, използвани от някои интернет доставчици?

Изберете едно



приложен



Presentation



транспортен



сесиен



мрежов Правилен отговор

Забележка

Правилният отговор е:

мрежов

Въпрос 7

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Към виртуална локална мрежа (VLAN) 1 трябва да се добави ново мрежово устройство. Маршрутизаторът (рутер) RA е конфигуриран както е указано по-горе. Кой от посочените по-долу IP адреси трябва да получи новото мрежово устройство?

Изберете едно



192.168.1.1 /26



192.168.1.22 /28  Правилен отговор



192.168.1.11 /28



192.168.1.33 /28

Забележка

Правилният отговор е:

192.168.1.22 /28

Въпрос 8

Правилен отговор

1,00 от максимално 1,00 точки



Неотбелязан

Текст на въпроса

От време на време наблюдавате задръстване на локалната мрежа. Какви може да са причините?

Изберете едно или повече:



a.

broadcast domain с твърде много хостове. Правилен отговор



b.

Multicasting.



c.

Broadcast „бури“ storms. Правилен отговор



d.

Сегментиране на мрежата.



e.

Ниска скорост на линиите. Правилен отговор



f.

Работа в Full duplex (пълен дуплекс).

Забележка

Правилните отговори са:

broadcast domain с твърде много хостове.,

Broadcast „бури“ storms.,

Ниска скорост на линиите.

Въпрос 9

Частично правилен отговор
0,67 от максимално 1,00 точки
 Неотбелязан

Текст на въпроса

В полето за данни в IP пакета се записва следното:

Изберете едно или повече:

- a. TCP сегмент
- b. UDP дейтаграма Правилен отговор
- c. Няма верен отговор
- d. ICMP съобщение Правилен отговор
- e. Контролна suma Неправилен отговор

Забележка

Вашият отговор отчасти е верен.
Вие правилно сте избрали 2.

3 верни отговора

Правилните отговори са: TCP сегмент, UDP дейтаграма, ICMP съобщение

Въпрос 10

Правилен отговор
1,00 от максимално 1,00 точки
 Неотбелязан

Текст на въпроса

Имате IP адрес 192.168.10.19/28. Кои от следните IP адреси са валидни хост адреси о тази подмрежа?

Изберете едно или повече:

- a. 192.168.10.0
- b. 192.168.10.29  Правилен отговор
- c. 192.168.10.17  Правилен отговор
- d. 192.168.10.31
- e. 192.168.10.16

Забележка

Вашият отговор е верен.

2 верни отговора

Правилните отговори са: 192.168.10.29, 192.168.10.17

Въпрос 11

Правилен отговор

1,00 от максимално 1,00 точки

-  Неотбелязан

Текст на въпроса

Кой от следните е канален протокол?

Изберете едно

- a. HDLC
- b. PPP
- c. Ethernet
- d. Всички отговори са верни  Правилен отговор
- e. Token Ring

Забележка

Вашият отговор е верен.

Правилният отговор е: Всички отговори са верни

Въпрос 12

Неправилен отговор

0,00 от максимално 1,00 точки



Неотбелязан

Текст на въпроса

Internet Control Message Protocol(ICMP) е проектиран да изпълнява следните функции:

Изберете едно

- a. докладване за грешки Неправилен отговор
- b. заявки за управление и към хостове
- c. всички други отговори са верни
- d. корекция на грешки

Забележка

Вашият отговор не е верен.

Правилният отговор е: всички други отговори са верни

Въпрос 13

Неправилен отговор

0,00 от максимално 1,00 точки



Неотбелязан

Текст на въпроса

Колко подрежи и хостове към всяка от тях ще имате, ако приложите префикс /29 маска на мрежа 210.10.2.0?

Изберете едно

a.

32 подмрежи и 18 хоста.

b.

8 подмрежи и 30 хоста.

c.

30 подмрежи и 6 хоста.

d.

16 подмрежи и 4 хоста.  Неправилен отговор

e.

32 подмрежи и 6 хоста.

Забележка

Правилният отговор е:

32 подмрежи и 6 хоста.

Въпрос 14

Частично правилен отговор

0,50 от максимално 1,00 точки

 Неотбелязан

Текст на въпроса

Компютърна мрежа, която може да се разпространява в регион, държава, континент или по света се нарича:

Изберете едно или повече:

a. MAN  Неправилен отговор

b. LAN

c. VPN

d. WAN  Правилен отговор

Забележка

Вашият отговор отчасти е верен.
Вие правилно сте избрали 1.

2 верни отговора

Правилните отговори са: WAN, VPN

Въпрос 15

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан

Текст на въпроса

Коя от следните разновидности на NAT реализира политиката множество портове и частни IP адреси да излизат с един единствен публичен IP адрес?

Изберете едно

a.

статичен NAT

b.

Port Address Translation  Правилен отговор

c.

Dynamic NAT

d.

port loading

Забележка

Правилният отговор е:

Port Address Translation

Въпрос 16

Неправилен отговор

0,00 от максимално 1,00 точки



Текст на въпроса

Кой от следните адреси е валиден IPv6 адрес?

Изберете едно

- a. 2002:7654:A1AD:61:81AF:CCC1 Неправилен отговор
- b. 2001:0000:130F::099a::12a
- c. 2004:1:25A4:886F::1
- d. FEC0:ABCD:WXYZ:0067::2A4

Забележка

Вашият отговор не е верен.

Правилният отговор е: 2004:1:25A4:886F::1

Въпрос 17

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Следните два слоя идват в повече при модела OSI, когато се сравнява с модела TCP IP:

Изберете едно или повече:

- а. презентационен  Правilen отговор
- б. транспортен
- в. сесиен  Правilen отговор
- г. мрежов

Забележка

Вашият отговор е верен.

2 верни отговора

Правилните отговори са: презентационен, сесиен

Въпрос 18

Правilen отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Кое твърдение е вярно за IPv6?

Изберете едно

- а. Мултикастите изпълняват роля и на бродкасти.  Правilen отговор
- б. Имаме налични 2.7 милиарди адреси.
- в. Адресите не са йерархични и се присвояват на random принцип.
- г. Даден интерфейс може да бъде конфигуриран с един единствен IPv6 адрес

Забележка

Вашият отговор е верен.

Правилният отговор е: Мултикастите изпълняват роля и на бродкасти.

Въпрос 19

Неправилен отговор

0,00 от максимално 1,00 точки



Неотбелязан

Текст на въпроса

При включване на захранването **PC2** се опитва да се свърже с DHCP сървър. Как става това?

Изберете едно

a.

C Layer 3 multicast съобщение.

b. C Layer 3 broadcast съобщение.

c.

Без Layer 3 енкапсулация (опаковане).

съобщение.

d. C Layer 3 unicast съобщение. A small square icon with a diagonal line through it, indicating that the answer is incorrect.

Забележка

Вашият отговор не е верен.

Правилният отговор е: C Layer 3 broadcast съобщение.

Въпрос 20

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

При "движението" на пакета с данни отгоре надолу по слоестата архитектура заглавията (headers) се

Изберете едно

- a. модифицират
- b. добавят  Правилен отговор
- c. премахват
- d. преаранжират

Забележка

Вашият отговор е верен.

Правилният отговор е: добавят

Въпрос 21

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Кой IPv6 адрес е еквивалентен на IPv4 адреса 127.0.0.1?

Изберете едно

- a. 2000::/3
- b. ::1  Правилен отговор
- c. 0::/10
- d. ::

Забележка

Вашият отговор е верен.

Правилният отговор е: ::1

Въпрос 22

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Броят на слоевете в TCP/IP протоколния стек е

Изберете едно

- a. 5
- b. 7
- c. 4 Правилен отговор
- d. 6

Забележка

Вашият отговор е верен.

Правилният отговор е: 4

Въпрос 23

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Полето TTL има стойност 10. Кокъв е максималният брой на рутерите, които могат да обработват пакета?

Изберете едно

- a. 10 Правилен отговор
- b. 11
- c. 5
- d. 1

Забележка

Вашият отговор е верен.
Правилният отговор е: 10

Въпрос 24

Правилен отговор
1,00 от максимално 1,00 точки



Текст на въпроса

Конфигурирате PPP на интерфейс на рутер. Какви методи на аутентикация можете да изберете?

Изберете едно или повече:



CHAP Правилен отговор



LAPB



SLIP



PAP Правилен отговор



SSL



VNP

Забележка

Правилните отговори са:

PAP,

CHAP

Въпрос 25

Неправилен отговор

0,00 от максимално 1,00 точки

  Отбелязан Отбелязан

Текст на въпроса

Коя команда се изпълнява от компютър, за да се верифицира връзката към компютрите, които са свързани в един и същи LAN чрез суич?

Изберете едно

- a. tracert address
- b. arp address  Неправилен отговор
- c. traceroute address
- d. ping address

Забележка

Вашият отговор не е верен.

Правилният отговор е: ping address

[Край на прегледа](#)

[◀ Списък с IP ROUTE2 команди](#)

Отиди на ...

[Прескачи Навигация в теста](#)



Навигация в теста

[Въпрос 1 Тази страница](#) [Въпрос 2 Тази страница](#) [Въпрос 3 Тази страница](#) [Въпрос 4 Тази страница](#) [Въпрос 5 Тази страница](#) [Въпрос 6 Тази страница](#)
[Въпрос 7 Тази страница](#) [Въпрос 8 Тази страница](#) [Въпрос 9 Тази страница](#) [Въпрос 10 Тази страница](#) [Въпрос 11 Тази страница](#) [Въпрос 12 Тази страница](#)
[Въпрос 13 Тази страница](#) [Въпрос 14 Тази страница](#) [Въпрос 15 Тази страница](#) [Въпрос 16 Тази страница](#) [Въпрос 17 Тази страница](#) [Въпрос 18 Тази страница](#)
[Въпрос 19 Тази страница](#) [Въпрос 20 Тази страница](#) [Въпрос 21 Тази страница](#) [Въпрос 22 Тази страница](#) [Въпрос 23 Тази страница](#)
[Въпрос 24 Тази страница](#) [Въпрос 25 Тази страница](#) [Отбелоязан](#)

[Показване по един въпрос на страница](#) [Край на прегледа](#)

Вие сте влезли в системата като [Димитро Боглев \(Изход\)](#)

[C425540S2](#)

[Get the mobile app](#)

Прескоши на основното съдържание moodle

- Богдан Карабаджак Снимка на Богдан Карабаджак
- Моето табло Moeto tablo
-
- Профил Profil
- Оценки Ocenki
- Съобщения Sobshcheniya
- Предпочитания Predposhitaniya
-
- Изход Izход

Покажи менюто за съобщения

0

Съобщения

Ново съобщение

Mark all as read Предпочитания за съобщенията

Няма чакащи съобщения

Виж всички

Покажи менюто за уведомления

0

Уведомление

Mark all as read Предпочитания за уведомленията

Нямате уведомления

Виж всички

- Български (bg)
 - English (en)
 - Български (bg)

•

Компютърни мрежи, сп. Софт. Инж., летен семестър 2018/2019

Път през страниците

- [Начална страница](#) / ►
- Моите курсове / ►
- [Бакалаври, летен семестър 2018/2019](#) / ►
- [СИ](#) / ►
- [Компютърни мрежи, сп. Софт. Инж., летен семестър 2018/2019](#) / ►
- 22 април - 28 април / ►
- [Първи официален тест върху лекциите](#)

Започнат на понеделник, 22 април 2019, 20:00

Състояние Завършен

Приключен на понеделник, 22 април 2019, 20:40

Изминалото време 39 мин. 5 сек.

Точки 25,00/25,00

Оценка **10,00** от 10,00 (100%)

Въпрос 1

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Как се нарича енкапсулирането (опаковане) на IPv6 пакети вътре в IPv4 пакети?

Изберете едно

- a. маршрутизация
- b. тунелиране Правилен отговор

- c. NAT
- d. хеширане

Забележка

Вашият отговор е верен.

Правилният отговор е: тунелиране

Въпрос 2

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кое е PDU-то в мрежовия слой?

Изберете едно

- a. пакет Правилен отговор
- b. сегмент
- c. кадър (frame)

Забележка

Вашият отговор е верен.

Правилният отговор е: пакет

Въпрос 3

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кои от следните предизвикват задръстване в LAN трафика?

Изберете едно или повече:



a.

Твърде много хостове в broadcast domain  Правилен отговор



b.

тясна честотна лента (bandwidth), т.е ниска скорост  Правилен отговор



c.

Broadcast storms (бури)  Правилен отговор



d.

сегментиране



e.

Multicasting  Правилен отговор



f.

Full duplex операции

Забележка

Правилните отговори са:

Твърде много хостове в broadcast domain,

Broadcast storms (бури),

Multicasting,

тясна честотна лента (bandwidth), т.е ниска скорост

Въпрос 4

Правилен отговор

1,00 от максимално 1,00 точки



Отбелязване на въпроса

Текст на въпроса

Кои от долуизброените протоколи оперират на Интернет слоя на TCP/IP модела?

Изберете едно или повече:

 a.

SNMP

 b.

BOOTP

 c.

HDLC

 d.

DNS

 e.

DHCP

 f.

RARP Правилен отговор

 g.

SONET/SDH

 h.

IPsec Правилен отговор

Забележка

Правилните отговори са:

RARP,

Въпрос 5

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кой от следните IP адреси е използваем (usable) за конфигуриране на мрежово устройство в мрежата 150.25.0.0 с маска 255.255.224.0?

Изберете едно или повече:

- a. 150.25.0.29 Правилен отговор
- b. 150.25.31.23 Правилен отговор
- c. 150.25.40.24
- d.

150.25.224.30

Забележка

Правилните отговори са: 150.25.0.29, 150.25.31.23

Въпрос 6

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Имате Class C IP мрежа (префикс) и връзка „точка-точка“ (point-to-point). Искате да приложите VLSM. Кой префикс е най-ефективен?

Изберете едно

- a.

/28

b.

/30  Правилен отговор

c.

/32

d.

/29

e.

/24

Забележка

Правилният отговор е:

/30

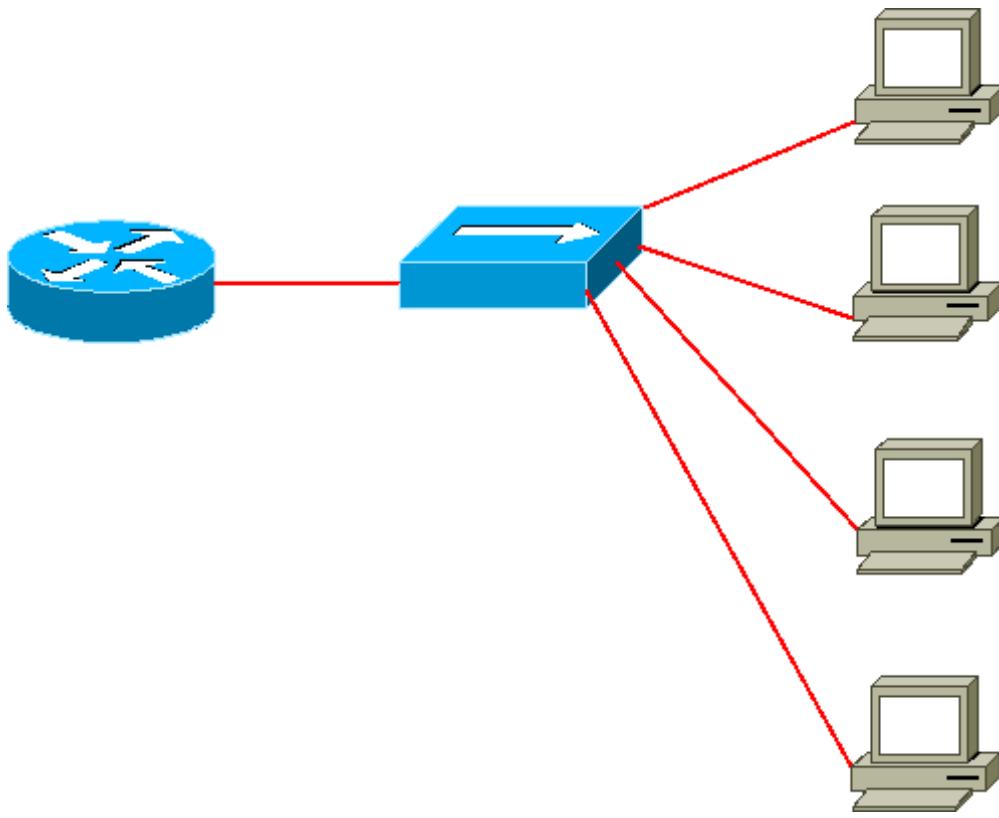
Въпрос 7

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса



На горната фигура, ако заменим хъба със суич (комутатор), какво ще се случи?

Изберете едно или повече:

- a. Броят на колизионните домейни ще остане същият.
- b. Броят на бродкаст домейните ще намалее.
- c. Броят на колизионните домейни ще се увеличи.
- d. Броят на бродкаст домейните ще остане същият.
- e. Броят на бродкаст домейните ще се увеличи.
- f. Броят на колизионните домейни ще намалее.

Забележка

Вашият отговор е верен.

2 верни отговора

Правилните отговори са: Броят на колизионните домейни ще се увеличи., Броят на бродкаст домейните ще остане същият.

Въпрос 8

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

PC в мрежов сегмент изпраща данни до друго PC на друг сегмент. Кой от следните отговори правилно описва точния ред на опаковане (encapsulation) на данните?

Изберете едно

a.

данни, Frame, сегмент, пакет, Bit

b.

данни, пакет, сегмент, Frame, Bit

c.

данни, Frame, пакет, сегмент, Bit

d.

данни, пакет, Frame, сегмент, Bit

e.

данни, сегмент, Frame, пакет, Bit

f.

данни, сегмент, пакет, Frame, Bit Правилен отговор

Забележка

Правилният отговор е:

данни, сегмент, пакет, Frame, Bit

Въпрос 9

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кои от следните изречения отразяват предимствата на VLAN-те?

Изберете едно или повече:

- a. Конфигурирането на суич с VLAN-и е по-лесно.
- b. Позволяват логическо групиране на потребителите според функциите, които изпълняват. Правилен отговор
- c. Увеличават размера на бродкаст домейните, като същевременно намаляват броя на колизионните домейни.
- d. Увеличават броя на бродкаст домейните, като същевременно намаляват размерите им. Правилен отговор
- e. Увеличава се броя на колизионните домейни.
- f. Подобряват сигурността в мрежата. Правилен отговор

Забележка

Вашият отговор е верен.

3 верни отговора.

Правилните отговори са: Позволяват логическо групиране на потребителите според функциите, които изпълняват., Подобряват сигурността в мрежата., Увеличават броя на бродкаст домейните, като същевременно намаляват размерите им.

Въпрос 10

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кои са типични характеристики на VLAN?

Изберете едно или повече:

a.

Trunk каналите носят трафика на множество VLAN-и.  Правilen отговор

b.

VLAN-те логически разделят суича (комутатора) на множество независими суичове на слой 2.  Правilen отговор

c.

VLAN-те увеличават броя на необходимите комутатори

d.

VLAN се разпростира през множество комутатори.  Правilen отговор

e.

VLAN-те намаляват броя на необходимите комутатори

f.

VLAN значително увеличава трафика заради добавената trunking информация.

Забележка

Правилните отговори са:

VLAN-те логически разделят суича (комутатора) на множество независими суичове на слой 2.,

Trunk каналите носят трафика на множество VLAN-и.,

VLAN се разпростира през множество комутатори.

Въпрос 11

Правilen отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Коя команда се изпълнява от компютър, за да се верифицира връзката към компютрите, които са свързани в един и същи LAN чрез суич?

Изберете едно

- a. arp address
- b. tracert address
- c. traceroute address
- d. ping address



Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: ping address

Въпрос 12

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Кое от следните ще уговори LCP (1-а фаза на PPP) при установяване на PPP връзка?

Изберете едно или повече:

- a.

Q.931

- b.

multilink



c.

CHAP



Правилен отговор



d.

callback



e.

IPCP



Забележка

Правилните отговори са:

IPCP

,

CHAP

Въпрос 13

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кой е адреса на подмрежата за следния IP адрес на хост 201.100.5.58/29?

Изберете едно

a.

201.100.5.65

b.

201.100.5.0

c.

201.100.5.56 Правилен отговор

d.

201.100.5.31

e.

201.100.5.32

f.

201.100.5.1

Забележка

Правилният отговор е:

201.100.5.56

Въпрос 14

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Физическо или логическо подреждане в мрежата е

Изберете едно

- a. окабеляване
- b. маршрутизиране
- c. топология Правилен отговор
- d. омрежаване

Забележка

Вашият отговор е верен.

Правилният отговор е: топология

Въпрос 15

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

С кое от следните устройства администраторът може да сегментира локалната си мрежа?

Изберете едно или повече:

- a.

хъбове

- b.

мостове (Bridges) Правилен отговор

c.

Медиа конвертори (FO-UTP)

d.

рипитери

e.

комутатори (суичове) Правилен отговор

f.

Маршрутизатори (рутери) Правилен отговор

Забележка

Правилните отговори са:

комутатори (суичове),

мостове (Bridges),

Маршрутизатори (рутери)

Въпрос 16

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кой от следните IP адреси е частен IP адрес?

Изберете едно

a.

192.168.42.34 Правилен отговор

b.

172.33.194.30

c.

12.0.0.1

d.

172.20.14.36

e.

168.172.19.39

Забележка

Правилният отговор е:

192.168.42.34

Въпрос 17

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кой слой на OSI модела в процеса на енкапсулиране не добавя хедър информация към пакета данни?

Изберете едно

a.

Каналният слой (data link)

b.

Транспортният слой

c.

Мрежовият слой

d.

Физическият слой  Правилен отговор

Забележка

Правилният отговор е:

Физическият слой

Въпрос 18

Правилен отговор

1,00 от максимално 1,00 точки

 НеотбелязанОтбелязване на въпроса

Текст на въпроса

Коя от следните разновидности на NAT реализира политиката множество портове и частни IP адреси да излизат с един единствен публичен IP адрес?

Изберете едно

a.

port loading

b.

статичен NAT

c.

Dynamic NAT

d.

Port Address Translation  Правилен отговор

Забележка

Правилният отговор е:

Port Address Translation

Въпрос 19

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Скоростта на предаване в bit/s се определя от:

Изберете едно

- a. транспортния слой
- b. физическия слой Правилен отговор
- c. сесийния слой
- d. приложния слой
- e. мрежовия слой

Забележка

Вашият отговор е верен.

Правилният отговор е: физическия слой

Въпрос 20

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

В модела OSI, устройство А изпраща данни до устройство В, 5-ти слой, който ще получи данни при В, се нарича:

Изберете едно

- a. канален
- b. представителен
- c. физически
- d. сесиен  Правилен отговор
- e. приложен

Забележка

Вашият отговор е верен.

Правилният отговор е: сесиен

Въпрос 21

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Докато се опитвате да откриете проблем със свързаността на дадено PC, получавате следната информация:

Local PC IP адрес: 190.0.3.35/24

Default Gateway: 190.0.3.1

Remote Server: 190.0.5.250/24

След това изпълнявате следните команди от PC-то:

Ping 127.0.0.1 - Unsuccessful

Ping 190.0.3.35 - Successful

Ping 190.0.3.1 - Unsuccessful

Ping 190.0.5.250 - Unsuccessful

Каква е причината, предизвикала този проблем?

Изберете едно

a.

TCP/IP не е инсталиран  Правилен отговор

b.

Локален проблем във физическия слой

c.

Отдалечен проблем във физическия слой

d.

Мрежовият контролер (NIC) не работи

Забележка

Правилният отговор е:

TCP/IP не е инсталиран

Въпрос 22

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Администраторът трябва да присвои статични IP адреси на сървърите в мрежата. За IP мрежа 192.168.20.24/29, на рутера е присвоен първият използваем (хост) адрес, а на сървър "Продажби" е даден последният използваем (хост) адрес. Кои от следните адреси ще бъдат въведени в "IP properties" полетата на сървър "Продажби"?

Изберете едно

a. IP address: 192.168.20.30

Subnet Mask: 255.255.255.240

Default Gateway: 192.168.20.25

b. IP address: 192.168.20.30

Subnet Mask: 255.255.255.248

Default Gateway: 192.168.20.25  Правилен отговор

c. IP address: 192.168.20.14

Subnet Mask: 255.255.255.248

Default Gateway: 192.168.20.9

d. IP address: 192.168.20.254

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.20.1

e. IP address: 192.168.20.30

Subnet Mask: 255.255.255.240

Default Gateway: 192.168.20.17

Забележка

Вашият отговор е верен.

Правилният отговор е: IP address: 192.168.20.30

Subnet Mask: 255.255.255.248

Default Gateway: 192.168.20.25

Въпрос 23

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан  Отбелязване на въпроса

Текст на въпроса

Имате мрежа, която трябва да разделите на 29 подмрежи с оптимален брой хостове във всяка. Колко бита трябва да вземете назаем от хост полето на IP адреса на мрежата, за да получите точната маска?

Изберете едно

- a. 3
- b. 5  Правilen отговор
- c. 2
- d. 4

Забележка

Вашият отговор е верен.

Правилният отговор е: 5

Въпрос 24

Правilen отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Как се нарича съединение, което се споделя от три и повече устройства?

Изберете едно

- a. Няма верен отговор
- b. точка-точка
- c. многоточково  Правilen отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: многоточково

Въпрос 25

Правilen отговор

1,00 от максимално 1,00 точки



НеотбелязанОтбелязване на въпроса

Текст на въпроса

Какъв е максималният брой на IP адресите, които може да бъдат присвоени на хостове в подмрежа с маска 255.255.255.224?

Изберете едно

- a. 12
- b. 16
- c. 15
- d. 30

Забележка

Вашият отговор е верен.

Правилният отговор е: 30

Край на прегледа

[◀ Списък с IP ROUTE2 команди](#)

Отиди на ...

[Прескачи Навигация в теста](#)



Навигация в теста

[Въпрос 1 Тази страница](#) [Въпрос 2 Тази страница](#) [Въпрос 3 Тази страница](#) [Въпрос 4 Тази страница](#) [Въпрос 5 Тази страница](#) [Въпрос 6 Тази страница](#)

[Въпрос 7 Тази страница](#) [Въпрос 8 Тази страница](#) [Въпрос 9 Тази страница](#) [Въпрос 10 Тази страница](#) [Въпрос 11 Тази страница](#) [Въпрос 12 Тази страница](#)

[Въпрос 13 Тази страница](#) [Въпрос 14 Тази страница](#) [Въпрос 15 Тази страница](#) [Въпрос 16 Тази страница](#) [Въпрос 17 Тази страница](#) [Въпрос 18 Тази страница](#)

[Въпрос 19 Тази страница](#) [Въпрос 20 Тази страница](#) [Въпрос 21 Тази страница](#) [Въпрос 22 Тази страница](#) [Въпрос 23 Тази страница](#)

[Въпрос 24 Тази страница](#) [Въпрос 25 Тази страница](#)

[Показване по един въпрос на страница](#) [Край на прегледа](#)

Вие сте влезли в системата като [Богдан Карабалжак \(Изход\)](#)

[C425540S2](#)

[Get the mobile app](#)

Прескоши на основното съдържание moodle

- Борис Ангелов Снимка на Борис Ангелов
- Моето табло
-
- Профил
- Оценки
- Съобщения
- Предпочитания
-
- Изход

Покажи менюто за съобщения

0

Съобщения

Ново съобщение

Mark all as read Предпочитания за съобщенията

Няма чакащи съобщения

Виж всички

Покажи менюто за уведомления

0

Уведомление

Mark all as read Предпочитания за уведомленията

Нямате уведомления

Виж всички

- Български (bg)
 - English (en)
 - Български (bg)

Компютърни мрежи, сп. КН-1, летен семестър 2018/2019

Път през страниците

- [Начална страница](#) / ►
- Моите курсове / ►
- [Бакалаври, летен семестър 2018/2019](#) / ►
- [КН](#) / ►
- [Компютърни мрежи, сп. КН-1, летен семестър 2018/2019](#) / ►
- 15 април - 21 април / ►
- [Първи официален тест върху лекциите](#)

Започнат на неделя, 21 април 2019, 13:00

Състояние Завършен

Приключен на неделя, 21 април 2019, 13:40

Изминало време 40 мин.

Точки 19,00/25,00

Оценка 7,60 от 10,00 (76%)

Въпрос 1

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Как комуникират мрежови устройства разпределени във виртуални локални мрежи (VLAN)?

Изберете едно



a.

Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на протокола VTP

b.

Устройства от една виртуална локална мрежа (VLAN) комуникират с помощта на маршрутизатор

c.

Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на магистрална (trunk) линия между комутаторите (комутатори)

d.

Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на маршрутизатор (рутер)

 Правилен отговор

Забележка

Правилният отговор е:

Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на маршрутизатор (рутер)

Въпрос 2

Неправилен отговор

0,00 от максимално 1,00 точки

 Неотбелязан
Отбелязване на въпроса

Текст на въпроса

Представителният слой включва следните функции:

Изберете едно

- a. Всички отговори са верни
- b. описание на данните
- c. компресиране на данните
- d. криптиране на данните  Неправилен отговор

Забележка

Вашият отговор не е верен.

Правилният отговор е: Всички отговори са верни

Въпрос 3

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Стандартът IEEE 802.3 е за:

Изберете едно



a.

ATM технология;



b.

Token-Ring технология



c.

Ethernet технология

Правилен отговор



d.

FDDI технология;

Забележка

Правилният отговор е:

Ethernet технология

Въпрос 4

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Какво означава “one-to-nearest” (един - до - най-близкия) в IPv6 адресацията?

Изберете едно

- a. multicast
- b. anycast Правилен отговор
- c. неопределен адрес
- d. глобални unicast

Забележка

Вашият отговор е верен.

Правилният отговор е: anycast

Въпрос 5

Неправилен отговор

0,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кой от посочените адреси е адрес на мрежа от клас C?

Изберете едно

- a.

255.255.255.0

- b.

224.100.0.0



c.

195.255.256.0  Неправилен отговор



d.

223.254.254.0

Забележка

Правилният отговор е:

223.254.254.0

Въпрос 6

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

Коректни IP адреси са:

Изберете едно или повече:



a.

87.154.48.265



b.

254.184.48.74  Правилен отговор



c.

158.189.582.215



d.

44.188.255.58  Правилен отговор



e.

878.26.56.65

f.

187.181.66.178  Правилен отговор

g.

47.15.0.848

Забележка

Правилните отговори са:

44.188.255.58,

187.181.66.178,

254.184.48.74

Въпрос 7

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кой от следните е валиден хост unicast IPv6 адрес?

Изберете едно

a.

2001:0:240E::0AC0:3428:121C  Правилен отговор

b.

2001::240E::0AC0:3428:121C

c.

2001:240E::0AC0:3428::

d.

2001::0000::240E::0000::0000::0AC0::3428::121C

Забележка

Правилният отговор е:

2001:0:240E::0AC0:3428:121C

Въпрос 8

Неправилен отговор

0,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Коя мрежова маска трябва да се приложи, така че адресният блок да бъде разделен между максимум 8 LANs, ато във всеки LAN да може да се включват между 5 и 26 хоста?

Изберете едно

a. 255.255.255.252

b. 255.255.255.240

c. 255.255.255.0 Неправилен отговор

d. 255.255.255.224

e. 0.0.0.240

Забележка

Вашият отговор не е верен.

Правилният отговор е: 255.255.255.224

Въпрос 9

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

IPv6 не използва следния тип адреси

Изберете едно

- a. Multicast
- b. няма верен отговор
- c. Anycast
- d. Broadcast Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: Broadcast

Въпрос 10

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

На мрежата SUnet е даден префикс 165.100.27.0/24. Колко подмрежи с по колко хоста поддържа този префикс?

Изберете едно

- a.

254 мрежи с по 65,534 хоста.

b.

Една мрежа с 254 хоста.  Правilen отговор

c.

30 мрежи с по 64 хоста.

d.

254 мрежи с по 254 хоста.

e.

65534 мрежи с по 255 хоста.

Забележка

Правилният отговор е:

Една мрежа с 254 хоста.

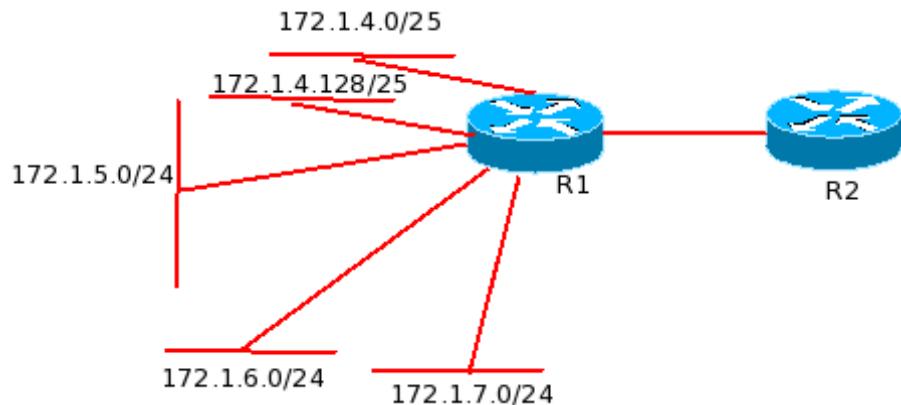
Въпрос 11

Неправilen отговор

0,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса



На горната фигура, кой префикс е най-подходящ за рекламиране към R2.

Изберете едно

- a. 172.1.0.0/22
- b. 172.1.0.0/21
- c. 172.1.4.0/24
- d. 172.1.4.0/22

Забележка

Вашият отговор не е верен.

Правилният отговор е: 172.1.4.0/22

Въпрос 12

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Рутер не може да маршрутизира (или хост да достави) пакет. Тогава пакетът се изхвърля и рутерът (или хостът) изпраща ICMP съобщение към възела - източник на пакета. Кое е то?

Изберете едно

- a. Source quench
- b. Time exceeded
- c. Router error
- d. Destination unreachable  Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: Destination unreachable

Въпрос 13

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Дадена е мрежата:

Кои от долните IP адреси са broadcast адреси на горните префикси?

Изберете едно или повече:

- a.

172.16.82.255

- b.

172.16.79.255 Правилен отговор

c.

172.16.95.255 Правилен отговор

d.

172.16.47.255 Правилен отговор

e.

172.16.64.255

f.

172.16.32.255

Забележка

Имате 3 верни отговора.

Правилните отговори са:

172.16.95.255,

172.16.47.255,

172.16.79.255

Въпрос 14

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Комутаторите Cisco Catalyst прилагат технология за идентифициране и предпазване от топологично зацикляне, както и гарантиране на точно определен път на потоците от данни. Коя е тази технология?

Изберете едно

a.

ISL

b.

802.1Q

c.

STP  Правилен отговор

d.

VTP

Забележка

Правилният отговор е:

STP

Въпрос 15

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

При преноса на данни между процеси с кой от следните методи комуникират два процеса?

Изберете едно

a. Трансфер на съобщения

b. клиент-сървър  Правилен отговор

c. източник-дестинация

d. Няма верен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: клиент-сървър

Въпрос 16

Неправилен отговор

0,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

При безкласовото адресиране (classless) IP адресите се предоставят на потребителите като:

Изберете едно

- a. блокове
- b. IP-та Неправилен отговор
- c. кодове
- d. размвери

Забележка

Вашият отговор не е верен.

Правилният отговор е: блокове

Въпрос 17

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кой адрес за получател използва един DHCP клиент, когато се опитва да получи IP адрес?

Изберете едно

a.

0.0.0.255

b.

0.0.0.0

c.

255.255.255.255  Правилен отговор

d.

127.0.0.1

Забележка

Правилният отговор е:

255.255.255.255

Въпрос 18

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кое от следните не е задача на каналния слой?

Изберете едно

a. управление на потока

b. кодиране на сигнала  Правилен отговор

c. формиране на кадри (frames)

d. контрол за грешки

Забележка

Вашият отговор е верен.

Правилният отговор е: кодиране на сигнала

Въпрос 19

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кои от следните адреси е пример за валиден unicast адрес?

Изберете едно

a.

255.255.255.255

b.

224.0.0.5

c.

FFFF.FFFF.FFFF

d.

172.31.128.255/18 Правилен отговор

e.

192.168.24.59/30

Забележка

Правилният отговор е:

172.31.128.255/18

Въпрос 20

Частично правилен отговор

0,50 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

Провайдерът ви предоставил една цяла клас В мрежа. Трябва да я разделите на най-малко 250 подмрежки, които да поддържат най-малко по 150 хоста. Кои от долните префикси удовлетворяват тези изисквания?

Изберете едно или повече:

a.

255.255.255.128

b.

255.255.254.0

c.

255.255.255.192

d.

255.255.255.248

e.

255.255.255.224

f.

255.255.255.0  Правилен отговор

Забележка

Правилните отговори са:

255.255.255.0,

255.255.254.0

Въпрос 21

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Инсталирали сте FTP сървър, достъпен от Internet. По отношение на OSI модела, Кой е най-високият слой, по който стават FTP сесиите.

Изберете едно

a.

сесиен

b.

приложен Правилен отговор

c.

транспортен

d.

представителен

e.

канален (Data Link)

f.

Internet

Забележка

Правилният отговор е:

приложен

Въпрос 22

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кой от следните IP адреси попада в CIDR блок 115.54.4.0/22?

Изберете едно или повече:



a.

115.54.7.61 Правилен отговор



b.

115.54.3.32



c.

115.54.12.128



d.

115.54.5.255 Правилен отговор



e.

115.54.5.128 Правилен отговор



f.

115.54.8.32

Забележка

Правилните отговори са:

115.54.7.61,

115.54.5.255,

Въпрос 23

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

С коя команда се присвоява последния използваем IP адрес от префикса 192.168.32.128/28 на интерфейса на рутера?

Изберете едно

a.

SUA(config-if)# ip адрес 192.168.32.144 255.255.255.240

b.

SUA(config-if)# ip адрес 192.168.32.158 255.255.255.240

c.

SUA(config-if)# ip адрес 192.168.32.142 255.255.255.240 Правилен отговор

d.

SUA(config-if)# ip адрес 192.168.32.143 255.255.255.240

e.

SUA(config-if)# ip адрес 192.168.32.158 255.255.255.240

Забележка

Правилният отговор е:

SUA(config-if)# ip адрес 192.168.32.142 255.255.255.240

Въпрос 24

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Не се предават следните IPV6 пакети:

Изберете едно

- a. Unicast
- b. Anycast
- c. Broadcast Правилен отговор
- d. Multicast

Забележка

Вашият отговор е верен.

Правилният отговор е: Broadcast

Въпрос 25

Частично правилен отговор

0,50 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

При OSI модела при движение на данните отдолу нагоре по слоевете хедърите се

Изберете едно или повече:

- a. премахват Правилен отговор
- b. декапсулират
- c. добавят
- d. енкапсулират

Забележка

Вашият отговор отчасти е верен.

Вие правилно сте избрали 1.

Правилните отговори са: премахват, декапсулират

[Край на прегледа](#)

[◀ Маршрутен протокол OSPF в IPv4 и IPv6.](#)

Отиди на ... [Отиди на ...](#)

[Прескочи Навигация в теста](#)



Навигация в теста

[Въпрос 1 Тази страница](#) [Въпрос 2 Тази страница](#) [Въпрос 3 Тази страница](#) [Въпрос 4 Тази страница](#) [Въпрос 5 Тази страница](#) [Въпрос 6 Тази страница](#)

[Въпрос 7 Тази страница](#) [Въпрос 8 Тази страница](#) [Въпрос 9 Тази страница](#) [Въпрос 10 Тази страница](#) [Въпрос 11 Тази страница](#) [Въпрос 12 Тази](#)

[страница](#) [Въпрос 13 Тази страница](#) [Въпрос 14 Тази страница](#) [Въпрос 15 Тази страница](#) [Въпрос 16 Тази страница](#) [Въпрос 17 Тази страница](#) [Въпрос 18](#)

[Тази страница](#) [Въпрос 19 Тази страница](#) [Въпрос 20 Тази страница](#) [Въпрос 21 Тази страница](#) [Въпрос 22 Тази страница](#) [Въпрос 23 Тази страница](#)

[Въпрос 24 Тази страница](#) [Въпрос 25 Тази страница](#)

[Показване по един въпрос на страница](#) [Край на прегледа](#)

Вие сте влезли в системата като [Борис Ангелов \(Изход\)](#)

[C425510S2](#)

[Get the mobile app](#)

[Прескоши на основното съдържание](#)
[moodle](#)

- [Недко Недев](#)  Снимка на Недко Недев

-  [Моето табло](#)  Моето табло

-

-  [Профил](#)  Профил

-  [Оценки](#)  Оценки

-  [Съобщения](#)  Съобщения

-  [Предпочитания](#)  Предпочитания

-

-  [Изход](#)  Изход

 Покажи менюто за съобщения

0

Съобщения

[Ново съобщение](#)

   [Предпочитания за съобщенията](#)

Няма чакащи съобщения



[Виж всички](#)

 Покажи менюто за уведомления

0

Уведомление

   [Предпочитания за уведомленията](#)

Нямате уведомления



[Виж всички](#)

- [Български \(bg\)](#)
 - [English \(en\)](#)
 - [Български \(bg\)](#)

Компютърни мрежи, сп. КН-2, летен семестър 2018/2019

Път през страниците

- [Начална страница](#) / ►
- Моите курсове / ►
- [Бакалаври, летен семестър 2018/2019](#) / ►
- [КН](#) / ►
- [Компютърни мрежи, сп. КН-2, летен семестър 2018/2019](#) / ►
- 22 април - 28 април / ►
- [Първи официален тест върху лекциите](#)

Започнат на вторник, 23 април 2019, 21:00

Състояние Завършен

Приключен на вторник, 23 април 2019, 21:39

Изминало време 38 мин. 53 сек.

Точки 21,33/25,00

Оценка **8,53** от 10,00 (85%)

Въпрос 1

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кои протоколи се осигуряват от PPP протокола за управление на връзката между двата възела (точки) в мрежата?

Изберете едно или повече:

- a. SPX
- b. NCP  Правилен отговор
- c. LCP  Правилен отговор
- d. TCP

Забележка

Вашият отговор е верен.

2 верни отговора

Правилните отговори са: LCP, NCP

Въпрос 2

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Приложният слой се имплементира в:

Изберете едно

- a. мрежовата карта
- b. рутера (маршрутизатора)
- c. всички отговори са верни
- d. крайната система  Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: крайната система

Въпрос 3

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Рутер не може да маршрутизира (или хост да достави) пакет. Тогава пакетът се изхвърля и рутерът (или хостът) изпраща ICMP съобщение към възела - източник на пакета. Кое е то?

Изберете едно

- a. Destination unreachable Правилен отговор
- b. Router error
- c. Source quench
- d. Time exceeded

Забележка

Вашият отговор е верен.

Правилният отговор е: Destination unreachable

Въпрос 4

Неправилен отговор

0,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Какво ще се случи, ако присвоите частен (private) IP адрес на публичния (WAN) на wireless рутерчето, който ви свързва към провайдера ви (ISP)?

Изберете едно

- a. Само рутерът на ISP ще има достъп до публичното Internet пространство. Неправилен отговор
- b. Частният адрес няма да бъде маршрутизиран в публичното Internet пространство.

- c. NAT процесът ще транслира този адрес в публичен IP адрес.
- d. Ще се случи конфликт на IP адреси, защото и други публични рутери може да използват адреси от същия обхват.

Забележка

Вашият отговор не е верен.

Правилният отговор е: Частният адрес няма да бъде маршрутизиран в публичното Internet пространство.

Въпрос 5

Правилен отговор

1,00 от максимално 1,00 точки



Отбелязване на въпроса

Текст на въпроса

Броят на слоевете в еталонния модел ISO OSI е

Изберете едно

- a. 6
- b. 7 Правилен отговор
- c. 4
- d. 5

Забележка

Вашият отговор е верен.

Правилният отговор е: 7

Въпрос 6

Правилен отговор

1,00 от максимално 1,00 точки



Отбелязване на въпроса

Текст на въпроса

Посочете валидния IPv6 адрес.

Изберете едно

- a. 2001:0db8:0:130H::87C:140B
- b. 2001:0db8:0000:130F:0000:0000:08GC:140B
- c. 2031:0:130F::9C0:876A:130B  Правилен отговор
- d. 2031::130F::9C0:876A:130B

Забележка

Вашият отговор е верен.

Правилният отговор е: 2031:0:130F::9C0:876A:130B

Въпрос 7

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Броят на слоевете в TCP/IP протоколния стек е

Изберете едно

- a. 7
- b. 5
- c. 4  Правилен отговор
- d. 6

Забележка

Вашият отговор е верен.

Правилният отговор е: 4

Въпрос 8

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Каква е целта на DHCP сървъра?

Изберете едно

- a. Да транслира URL в IP адрес.
- b. Да транслира IPv4 адреси в MAC адреси.
- c. Да осигурява IP конфигурация на хостовете. Правилен отговор
- d. За съхраняване на електронна поща.

Забележка

Вашият отговор е верен.

Правилният отговор е: Да осигурява IP конфигурация на хостовете.

Въпрос 9

Частично правилен отговор

0,67 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кои от следните твърдения са предимства на VLAN-те?

Изберете едно или повече:

- a.

Позволяват логическо групиране на потребителите по функции. Правилен отговор

- b.

Увеличават броя на broadcast домейните, като същевременно намаляват размера им.  Правilen отговор

c.

Увеличават рамера на broadcast домейните, като същевременно намаляват броя им.

d.

Подобряват сигурността на мрежата,  Неправilen отговор

e.

Увеличават размера на колизионните домейни.

f.

Опостяват администратора на комутатора.

Забележка

Правилните отговори са:

Позволяват логическо групиране на потребителите по функции.,

Увеличават броя на broadcast домейните, като същевременно намаляват размера им.,

Опостяват администратора на комутатора.

Въпрос 10

Правilen отговор

1,00 от максимално 1,00 точки

 НеотбелязанОтбелязване на въпроса

Текст на въпроса

RARP е протокол:

Изберете едно

a.

за динамично конфигуриране на IP адреса на хост, на базата на неговия MAC. Методът не изискава сървър;

b.

за динамично конфигуриране на IP адреса на хост, на базата на неговия MAC. Методът изискава сървър;  Правилен отговор

c.

за динамично намиране на MAC адреса на хост, чието IP ни е известно. Методът изискава сървър;

d.

за динамично намиране на IP адреса на хост, чийто MAC ни е известен. Методът не изискава сървър;

e.

за динамично намиране на MAC адреса на хост, чието IP ни е известно. Методът не изискава сървър;

f.

за динамично намиране на IP адреса на хост, чийто MAC ни е известен. Методът изискава сървър;

Забележка

Правилният отговор е:

за динамично конфигуриране на IP адреса на хост, на базата на неговия MAC. Методът изискава сървър;

Въпрос 11

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан  Отбелязване на въпроса

Текст на въпроса

Кой от следните не е клас от IP адреси?

Изберете едно

- a. клас D
- b. клас F  Правилен отговор
- c. клас E
- d. клас C

Забележка

Вашият отговор е верен.

Правилният отговор е: клас F

Въпрос 12

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан  Отбелязване на въпроса

Текст на въпроса

Мрежата 213.115.77.0 е разделена на подмрежки с префикс /28. Колко подмрежки и с по колко хоста ще се получат?

Изберете едно

- a.

16 мрежи с 14 хоста  Правилен отговор

- b.

16 мрежи с 16 хоста

- c.

6 мрежи с 30 хоста

- d.

62 мрежи с 2 хоста

- e.

2 мрежи с 62 хоста

Забележка

Правилният отговор е:

16 мрежи с 14 хоста

Въпрос 13

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

В подкатегориите на резервирните адреси в IPv6 има адрес, който се използва от хостовете да тестват самите себе си, без да излизат в мрежата. Кой е този адрес?

Изберете едно

- a. заместващ адрес
- b. Loopback Правилен отговор
- c. Неопределен
- d. уникален адрес

Забележка

Вашият отговор е верен.

Правилният отговор е: Loopback

Въпрос 14

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

ICMP винаги докладва за грешка на:

Изберете едно

- a. предишен рутер
- b. източника (сурса)  Правилен отговор
- c. дестинацията
- d. следващ рутер

Забележка

Вашият отговор е верен.

Правилният отговор е: източника (сурса)

Въпрос 15

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан  Отбелязване на въпроса

Текст на въпроса

Какъв е EUI-64 формата на идентификатора на интерфейса, ако MAC адресът е 00-0C-27-A2-13-1B?

Изберете едно

- a.

FEFE:C:27A2:131B

- b.

020C:27FF:FEA2:131B  Правилен отговор

- c.

C:27A2:131B

d.

000C:27A2:131B:0000:0000

Забележка

Правилният отговор е:

020C:27FF:FEA2:131B

Въпрос 16

Неправилен отговор

0,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

При безкласовото адресиране (classless) IP адресите се предоставят на потребителите като:

Изберете едно

- a. блокове
- b. размвери
- c. кодове
- d. IP-та Неправилен отговор

Забележка

Вашият отговор не е верен.

Правилният отговор е: блокове

Въпрос 17

Частично правилен отговор

0,67 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кое от следните е вярно по отношение на мрежа (префикс) с маска

255.255.248.0.

Изберете едно или повече:

a.

Първите (старшите) 21 бита са хост частта на адреса.

b.

Мрежовият адрес на последната подмрежа ще има 248 в 3-ти октет. Правилен отговор

c.

С тази маска може да се създадат 16 подмрежи.

d.

Номерата на подмрежите са кратни на 8. Правилен отговор

e.

Отнася се към Class A адрес с взети назем 13 бита.

f.

Отнася се към Class B адрес с взети назем 4 бита.

Забележка

Правилните отговори са:

Отнася се към Class A адрес с взети назем 13 бита.,

Мрежовият адрес на последната подмрежа ще има 248 в 3-ти октет.,

Номерата на подмрежите са кратни на 8.

Въпрос 18

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Коя е най-високоскоростната комуникационна среда?

Изберете едно

- a. влакнесто-оптически (FO) кабел Правилен отговор
- b. коаксиален кабел
- c. електрозахранващи кабели
- d. кабел тип "усукана двойка"

Забележка

Вашият отговор е верен.

Правилният отговор е: влакнесто-оптически (FO) кабел

Въпрос 19

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

100BASE-FX реализира Етернет (Ethernet)стандарта при скорост на предаване 100 Mbps:

Изберете едно

- a.

по дебел коаксиален кабел

b.

по кабел тип „усукана двойка“ (UTP)

c.

по оптичен кабел  Правилен отговор

d.

по тънък коаксиален кабел

Забележка

Правилният отговор е:

по оптичен кабел

Въпрос 20

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кое от долните твърдения не е стратегия за преход от IPv4 към IPv6 ?

Изберете едно

- a. Tunnelling (тунелиране)
- b. Dual stack
- c. транслирне на хедър
- d. Конвергиране  Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: Конвергиране

Въпрос 21

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Dual-stack означава

Изберете едно

- a. Няма верен отговор
- b. Реализираме два IPv4 стека
- c. Реализираме два IPv6 стека
- d. Един възел поддържа и IPv4, и IPv6 Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: Един възел поддържа и IPv4, и IPv6

Въпрос 22

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Дадена е долната схема:

В LAN-а на Branch рутера е инсталирано ново PC. PC-то не може да се свърже със сървъра.

Какъв е проблемът?

Изберете едно

a.

Сървърът има невалиден IP адрес

b.

default gateway на PC-то е зададен неточно  Правилен отговор

c.

IP адресът на рутера е неточен

d.

IP адресът на PC-то е невалиден

e.

Маската на PC-то е зададена неточна

Забележка

Правилният отговор е:

default gateway на PC-то е зададен неточен

Въпрос 23

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Физическият слой осигрява

Изберете едно

- a. спецификации на лъчите по оптическите кабели
- b. Всички отговори са верни Правилен отговор
- c. механични спецификации на електрическите конектори и кабели
- d. електрически спецификации на сигналите по комуникационните линии

Забележка

Вашият отговор е верен.

Правилният отговор е: Всички отговори са верни

Въпрос 24

Неправилен отговор

0,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

За да има коректна адресация, всеки един MAC адрес следва да е:

Изберете едно

- a.

уникален за Интернет (всички мрежи, до които имаме свързаност) Неправилен отговор

- b.

уникален за локалния сегмент на мрежата

c.

уникален за всички мрежи в организацията

d.

уникален за локалния сегмент на мрежата освен ако не е мултикастен

e.

уникален за Интернет (всички мрежи, до които имаме свързаност) освен ако не е мултикастен

f.

уникален за всички мрежи в организацията освен ако не е мултикастен

Забележка

Правилният отговор е:

уникален за локалния сегмент на мрежата освен ако не е мултикастен

Въпрос 25

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кои три IP адреса могат да бъдат присвоени на хостове, ако маската е /27 ?

Изберете едно или повече:

a. 129.33.192.192

- b. 135.1.64.34 Правилен отговор
- c. 17.15.66.128
- d. 66.55.128.1 Правилен отговор
- e. 192.168.5.63
- f. 10.15.32.17 Правилен отговор

Забележка

Вашият отговор е верен.

3 верни отговора.

Правилните отговори са: 10.15.32.17, 66.55.128.1, 135.1.64.34

[Край на прегледа](#)

[◀ Маршрутен протокол OSPF в IPv4 и IPv6.](#)

Отиди на ... [Отиди на ...](#)

[Some internet outages predicted for the coming month as '768k Day' approaches ►](#)

[Прескочи Навигация в теста](#)



Навигация в теста

[Въпрос 1 Тази страница](#) [Въпрос 2 Тази страница](#) [Въпрос 3 Тази страница](#) [Въпрос 4 Тази страница](#) [Въпрос 5 Тази страница](#) [Въпрос 6 Тази страница](#)
[Въпрос 7 Тази страница](#) [Въпрос 8 Тази страница](#) [Въпрос 9 Тази страница](#) [Въпрос 10 Тази страница](#) [Въпрос 11 Тази страница](#) [Въпрос 12 Тази страница](#)
[Въпрос 13 Тази страница](#) [Въпрос 14 Тази страница](#) [Въпрос 15 Тази страница](#) [Въпрос 16 Тази страница](#) [Въпрос 17 Тази страница](#) [Въпрос 18 Тази страница](#)
[Въпрос 19 Тази страница](#) [Въпрос 20 Тази страница](#) [Въпрос 21 Тази страница](#) [Въпрос 22 Тази страница](#) [Въпрос 23 Тази страница](#)
[Въпрос 24 Тази страница](#) [Въпрос 25 Тази страница](#)
[Показване по един въпрос на страница](#) [Край на прегледа](#)

Вие сте влезли в системата като [Недко Недев \(Изход\)](#)

[C425511S2](#)

[Get the mobile app](#)

[Прескоши на основното съдържание](#)
[moodle](#)

- [Велина Карналова](#)  Снимка на Велина Карналова

-  [Моето табло](#)  [Моето табло](#)
-
-  [Профил](#)  [Профил](#)
-  [Оценки](#)  [Оценки](#)
-  [Съобщения](#)  [Съобщения](#)
-  [Предпочитания](#)  [Предпочитания](#)
-
-  [Изход](#)  [Изход](#)

 Покажи менюто за съобщения

0

Съобщения

[Ново съобщение](#)

 [Mark all as read](#)   [Предпочитания за съобщенията](#)

Няма чакащи съобщения

 [Loading](#)

[Виж всички](#)

 Покажи менюто за уведомления

0

Уведомление

 [Mark all as read](#)   [Предпочитания за уведомленията](#)

Нямате уведомления

 [Loading](#)

[Виж всички](#)

- [Български \(bg\)](#)
 - [English \(en\)](#)
 - [Български \(bg\)](#)

Компютърни мрежи, сп. КН-2, летен семестър 2018/2019

Път през страниците

- [Начална страница](#) / ►
- Моите курсове / ►
- [Бакалаври, летен семестър 2018/2019](#) / ►
- [КН](#) / ►
- [Компютърни мрежи, сп. КН-2, летен семестър 2018/2019](#) / ►
- 22 април - 28 април / ►
- [Първи официален тест върху лекциите](#)

Започнат на вторник, 23 април 2019, 21:00

Състояние Завършен

Приключен на вторник, 23 април 2019, 21:39

Изминало време 39 мин. 19 сек.

Точки 24,00/25,00

Оценка **9,60** от 10,00 (96%)

Въпрос 1

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

В модела OSI, устройство А изпраща данни до устройство В, 5-ти слой, който ще получи данни при В, се нарича:

Изберете едно

- a. физически
- b. канален

- c. сесиен  Правилен отговор
- d. приложен
- e. представителен

Забележка

Вашият отговор е верен.

Правилният отговор е: сесиен

Въпрос 2

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан

Текст на въпроса

Мрежата 201.145.32.0 е разделена на подмрежи с префиксa /27. Колко подмрежи и с по колко хоста ще се получат?

Изберете едно

- a.

8 мрежи с по 30 хоста  Правилен отговор

- b.

64 мрежи с по 4 хоста

- c.

6 подмрежи с по 30 хоста

- d.

8 подмрежи с по 32 хоста

- e.

32 мрежи с по 2 хоста

Забележка

Правилният отговор е:

8 мрежи с по 30 хоста

Въпрос 3

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

В подкатегориите на резервирните адреси в IPv6 има адрес, който се използва от хостовете да тестват самите себе си, без да излизат в мрежата. Кой е този адрес?

Изберете едно

- a. Неопределен
- b. заместващ адрес
- c. Loopback Правилен отговор
- d. уникален адрес

Забележка

Вашият отговор е верен.

Правилният отговор е: Loopback

Въпрос 4

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Dual-stack означава

Изберете едно

- a. Реализираме два IPv6 стека
- b. Реализираме два IPv4 стека
- c. Един възел поддържа и IPv4, и IPv6  Правилен отговор
- d. Няма верен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: Един възел поддържа и IPv4, и IPv6

Въпрос 5

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Един комуникационен канал може да се споделя от сигнали от множество потребители с помощта на:

Изберете едно

- a. мултиплексиране  Правилен отговор
- b. аналогова модулация
- c. цифрова модулация
- d. Няма верен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: мултиплексиране

Въпрос 6

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Кой от адресите е unicast?

Изберете едно



224.1.5.2



FFFF. FFFF. FFFF



192.168.24.23/30



172.31.96.255/19 Правилен отговор



255.255.255.255

Забележка

Правилният отговор е:

172.31.96.255/19

Въпрос 7

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Посочете IPv6 link-local адреса.

Изберете едно

- a. FE08::280e:611:a:f14f:3d69
- b. FFE:0345:5f1b::e14d:3d69
- c. FE80::380e:611a:e14f:3d69  Правилен отговор
- d. FE81::280f:512b:e14f:3d69

Забележка

Вашият отговор е верен.

Правилният отговор е: FE80::380e:611a:e14f:3d69

Въпрос 8

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Кой е префикса на хост с IP адрес 201.100.5.68/28?

Изберете едно

- a.

201.100.5.64 

- b.

201.100.5.65

- c.

201.100.5.0

- d.

201.100.5.1

e.

201.100.5.32

f.

201.100.5.31

Забележка

Правилният отговор е:

201.100.5.64

Въпрос 9

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан

Текст на въпроса

Две устройства са в компютърна мрежа, ако

Изберете едно

- a. Няма верен отговор
- b. процеси, работещи върху различни устройства имат еднакви PIDs
- c. процес върху едното устройство може да обменя информация с процес върху другото  Правилен отговор
- d. даден процес работи едновременно и върху двете

Забележка

Вашият отговор е верен.

Правилният отговор е: процес върху едното устройство може да обменя информация с процес върху другото

Въпрос 10

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

DHCP (dynamic host configuration protocol) осигурява следното на клиентите:

Изберете едно

- a. IP адрес Правилен отговор
- b. URL
- c. Няма верен отговор
- d. MAC адрес

Забележка

Вашият отговор е верен.

Правилният отговор е: IP адрес

Въпрос 11

Неправилен отговор

0,00 от максимално 1,00 точки



Текст на въпроса

Коя е максималната скорост, определена от IEEE 802.11n стандарта за безжични LAN?

Изберете едно

- a.

54 Mbps

- b.

150-300 Mbps



c.

10 Mbps



d.

100 Mbps  Неправилен отговор

Забележка

Правилният отговор е:

150-300 Mbps

Въпрос 12

Правилен отговор

1,00 от максимално 1,00 точки



 Неотбелязан

Текст на въпроса

Избройте три характеристики на IPv6 anycast адреса?

Изберете едно или повече:

- a. Уникален IPv6 адрес за всяко устройство в групата.
- b. Комуникационен модел "един-към-много".
- c. Един и същ адрес за множество устройства в групата.  Правилен отговор
- d. Комуникационен модел "от един източник към най-близката дестинация".  Правилен отговор
- e. Комуникационен модел "any-to-many".
- f. Насочване на пакетите към интерфейс от групата, който е най-близо до изпращащото устройство.  Правилен отговор

Забележка

Вашият отговор е верен.

Три верни отговора.

Правилните отговори са: Насочване на пакетите към интерфейс от групата, който е най-близо до изпращащото устройство., Един и същ адрес за множество устройства в групата., Комуникационен модел "от един източник към най-близката дестинация".

Въпрос 13

Правилен отговор

1,00 от максимално 1,00 точки



Неотбелязан

Текст на въпроса

Кой слой осигурява директно услуги за потребителя?

Изберете едно

- a. транспортен
- b. сесиен
- c. физически
- d. представителен
- e. приложен

Забележка

Вашият отговор е верен.

Правилният отговор е: приложен

Въпрос 14

Правилен отговор

1,00 от максимално 1,00 точки



Неотбелязан

Текст на въпроса

Скоростта на предаване в bit/s се определя от:

Изберете едно

- a. мрежовия слой
- b. приложния слой
- c. транспортния слой
- d. физическия слой  Правилен отговор
- e. сесийния слой

Забележка

Вашият отговор е верен.

Правилният отговор е: физическия слой

Въпрос 15

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

На кой слой от OSI модела оперират TTL филтрите, използвани от някои интернет доставчици?

Изберете едно

- a.

сесиен

- b.

транспортен

- c.

мрежов  Правилен отговор

- d.

приложен

e.

Presentation

Забележка

Правилният отговор е:

мрежов

Въпрос 16

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан

Текст на въпроса

ARP изпраща заявки, които са:

Изберете едно

a.

multicast на 2ри слой от OSI модела и broadcast на 3ти;

b.

broadcast на 2ри слой от OSI модела и unicast на 3ти;  Правилен отговор

c.

multicast на 2ри слой от OSI модела и multicast на 3ти;

d.

broadcast на 2ри слой от OSI модела и broadcast на 3ти;



e.

broadcast на 2ри слой от OSI модела и multicast на 3ти;

Забележка

Правилният отговор е:

broadcast на 2ри слой от OSI модела и unicast на 3ти;

Въпрос 17

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Представителният слой включва следните функции:

Изберете едно

- a. криптиране на данните
- b. описание на данните
- c. компресиране на данните
- d. Всички отговори са верни  Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: Всички отговори са верни

Въпрос 18

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

На долната схема е показана клоновата мрежата:

Колко колизионни домейни има в тази мрежа?

Изберете едно

- a. 4
- b. 1
- c. 2 Правilen отговор
- d. 5
- e. 3
- f. 14
- g. 6

Забележка

Правилният отговор е: 2

Въпрос 19

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Посочете валидния IPv6 адрес.

Изберете едно

- a. 2001:0db8:0:130H::87C:140B
- b. 2031::130F::9C0:876A:130B
- c. 2031:0:130F::9C0:876A:130B  Правилен отговор
- d. 2001:0db8:0000:130F:0000:0000:08GC:140B

Забележка

Вашият отговор е верен.

Правилният отговор е: 2031:0:130F::9C0:876A:130B

Въпрос 20

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

При "движението" на пакета с данни отгоре надолу по слоестата архитектура заглавията (headers) се

Изберете едно

- a. премахват
- b. преаранжират
- c. модифицират
- d. добавят  Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: добавят

Въпрос 21

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Какъв вид съобщение издава PING, изпратен да тества свързаност?

Изберете едно



Source quench



ICMP echo request Правилен отговор



Timestamp reply



information interrupt request

Забележка

Правилният отговор е:

ICMP echo request

Въпрос 22

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Кой от следните адреси е broadcast адрес на клас В мрежа с маска по подразбиране?

Изберете едно

- a. 172.255.255.255
- b. 255.255.255.255
- c. 172.16.255.255  Правилен отговор
- d. 172.16.10.255

Забележка

Вашият отговор е верен.

Правилният отговор е: 172.16.255.255

Въпрос 23

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Какъв е EUI-64 формата на идентификатора на интерфейса, ако MAC адресът е 00-0C-27-A2-13-1B?

Изберете едно

- a.

020C:27FF:FEA2:131B  Правилен отговор

- b.

FEFE:C:27A2:131B

- c.

C:27A2:131B

- d.

000C:27A2:131B:0000:0000

Забележка

Правилният отговор е:

020C:27FF:FEA2:131B

Въпрос 24

Правилен отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Имате MAC адрес на интерфейс wlan0 = 00:0e:2e:d1:ab:15. Какъв ще бъде Host ID на IPv6 link local адреса на интерфейс wlan0? (Имайте предвид, че MAC адресът се маркира в този случай като локално администриран)

Изберете едно

a.

e:2ed1:ab15

b.

20e:2eff:fed1:ab15 Правилен отговор

c.

ff 00:0e2e:d1ab:1500

d.

0:e2e:d1ab:15ff

e.

20e:2eff:ffd1:ab15

Забележка

Правилният отговор е:

Въпрос 25

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан

Текст на въпроса

Кое поле определя времето на живот на IPv6 пакета?

Изберете едно

- a. Hop limit  Правилен отговор
- b. Няма верен отговор
- c. TTL
- d. Next header

Забележка

Вашият отговор е верен.

Правилният отговор е: Hop limit

Записване състоянието на отбелязването

[Край на прегледа](#)

[◀ Маршрутен протокол OSPF в IPv4 и IPv6.](#)

Отиди на ... [Отиди на ...](#)

[Some internet outages predicted for the coming month as '768k Day' approaches ►](#)

[Прескочи Навигация в теста](#)

Навигация в теста

[Въпрос 1 Тази страница](#) [Въпрос 2 Тази страница](#) [Въпрос 3 Тази страница](#) [Въпрос 4 Тази страница](#) [Въпрос 5 Тази страница](#) [Въпрос 6 Тази страница](#)

[Въпрос 7 Тази страница](#) [Въпрос 8 Тази страница](#) [Въпрос 9 Тази страница](#) [Въпрос 10 Тази страница](#) [Въпрос 11 Тази страница](#) [Въпрос 12 Тази](#)

[страница](#) [Въпрос 13 Тази страница](#) [Въпрос 14 Тази страница](#) [Въпрос 15 Тази страница](#) [Въпрос 16 Тази страница](#) [Въпрос 17 Тази страница](#) [Въпрос 18](#)

[Тази страница](#) [Въпрос 19](#) [Тази страница](#) [Въпрос 20](#) [Тази страница](#) [Въпрос 21](#) [Тази страница](#) [Въпрос 22](#) [Тази страница](#) [Въпрос 23](#) [Тази страница](#)
[Въпрос 24](#) [Тази страница](#) [Въпрос 25](#) [Тази страница](#)
[Показване по един въпрос на страница](#) [Край на прегледа](#)

Вие сте влезли в системата като [Велина Карналова](#) ([Изход](#))

[C425511S2](#)

[Get the mobile app](#)

[Прескочи на основното съдържание](#)
[moodle](#)

- [Български \(bg\)](#)
 - [English \(en\)](#)
 - [Български \(bg\)](#)
-
- Вие сте влезли в системата като [Мария Кунчева \(Изход\)](#)

Компютърни мрежи, сп. ИС, уч. 2014-15

Път през страниците

- [Начална страница](#) / ►
- [Моите курсове](#) / ►
- [Бакалаври, летен семестър 2014/2015](#) / ►
- [ИС](#) / ►
- [Компютърни мрежи, сп. ИС, уч. 2014-15](#) / ►
- 20 април - 26 април / ►
- [Първи официален тест върху лекциите](#)

Започнат на сряда, 22 април 2015, 21:30

Състояние Завършен

Приключен на сряда, 22 април 2015, 22:10

Изминалото време 39 мин. 39 сек.

Точки 15,75/25,00

Оценка **6,30** от 10,00 (63%)

Въпрос 1

Неправилен отговор

0,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кое от полетата на IPv4 header не е идентично с поле в IPv6 header?

Изберете едно



a.

TTL



b.

Version



c.

Checksum



d.

ToS  Неправилен отговор

Забележка

Правилният отговор е:

TTL

Въпрос 2

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Имате class C мрежа и трябва да я разделите така, че да имате поне 5 подмрежи с по минимум 18 хоста. Коя маска ще приложите?

Изберете едно

a.

225.225.255.0

b.

225.225.224.0

c.

255.255.255.224  Правилен отговор

d.

225.225.240.0

e.

225.225.255.240

Забележка

Правилният отговор е:

255.255.255.224

Въпрос 3

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Имате Class C мрежа и ви трябват 10 подмрежи. Каква маска ще изберете, за да имате оптимален брой хост адреси?

Изберете едно

a.

255.255.255.248

b.

255.255.255.192

c.

255.255.255.240  Правилен отговор

d.

255.255.255.224

Забележка

Правилният отговор е:

255.255.255.240

Въпрос 4

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

На мрежата SUnet е даден префикс 165.100.27.0/24. Колко подмрежи с по колко хоста поддържа този префикс?

Изберете едно

a.

254 мрежи с по 65,534 хоста.

b.

254 мрежи с по 254 хоста.

c.

65534 мрежи с по 255 хоста.

d.

30 мрежи с по 64 хоста.



e.

Една мрежа с 254 хоста. Правилен отговор

Забележка

Правилният отговор е:

Една мрежа с 254 хоста.

Въпрос 5

Неправилен отговор

0,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кои две редукции на IPv6 адреса 2001:0d02:0000:0000:0014:0000:0000:0095 са валидни?

Изберете едно или повече:



a.

2001:0d02::0014::0095 Неправилен отговор



b.

2001:d02::14:0:0:95



c.

2001:d02:0:0:14::95



d.

2001:d02::14::95 Неправилен отговор

Забележка

Правилният отговор е:

2001:d02:0:0:14::95,

2001:d02::14:0:0:95

Въпрос 6

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кои са двете характеристики а “store and forward” switching (комутиране)?

Изберете едно или повече:



a.

Комутаторът получава целият кадър (фрейм), преди да започне да го прехвърля към изходен порт. Правилен отговор



b.

Закъснението през комутатора варира според дължината на фрейма. Правилен отговор



c.

Флуктуации в закъснението независещи от размера на фрейма.



d.

Комутаторът проверява адреса на дестинацията при получаван на заглавната част на фрейма (header).

Забележка

Правилният отговор е:

Комутаторът получава целият кадър (фрейм), преди да започне да го прехвърля към изходен порт.,

Закъснението през комутатора варира според дължината на фрейма.

Въпрос 7

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

На СУнет е предоставен class C IP префикс 189.66.1.0. Ако приложите маската 255.255.255.224, колко хоста ще има на всяка подмрежа?

Изберете едно

a.

32

b.

62

c. 64

d.

14

e. 30 Правилен отговор

f.

16

Забележка

Правилният отговор е: 30

Въпрос 8

Неправилен отговор

0,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

В даден момент един маршрутизатор притежава следната маршрутна таблица:

```
=====
```

Network	Destination	Netmask	Gateway	interface	Metric
---------	-------------	---------	---------	-----------	--------

0.0.0.0	0.0.0.0	195.73.25.1	195.73.25.254	2	
---------	---------	-------------	---------------	---	--

127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1	
-----------	-----------	-----------	-----------	---	--

195.73.25.254	255.255.255.255	127.0.0.1	127.0.0.1	1	
---------------	-----------------	-----------	-----------	---	--

195.73.25.255	255.255.255.0	195.73.25.254	195.73.25.254	1	
---------------	---------------	---------------	---------------	---	--

207.15.140.0	255.255.255.0	207.15.140.10	207.15.140.10	1	
--------------	---------------	---------------	---------------	---	--

207.15.140.10	255.255.255.255	127.0.0.1	127.0.0.1	1	
---------------	-----------------	-----------	-----------	---	--

207.15.140.255	255.255.255.255	207.15.140.10	207.15.140.10	1	
----------------	-----------------	---------------	---------------	---	--

207.15.150.0	255.255.255.0	207.15.140.20	207.15.140.10	2	
--------------	---------------	---------------	---------------	---	--

207.15.160.0 255.255.255.0 207.15.140.20 207.15.140.10 2

207.15.170.0 255.255.255.0 207.15.140.20 207.15.140.10 3

224.0.0.0 224.0.0.0 207.15.140.10 207.15.140.10 1

=====

Той трябва да изпрати TCP пакети до компютър с IP адрес 207.15.190.204. През кой интерфейс на маршрутизатора ще трябва да преминат пакетите и кой е IP адреса на следващия маршрутизатор, на който ще бъдат прехвърлени тези пакети?

Изберете едно

а. през интерфейс с IP адрес: 195.73.25.1

IP адрес на следващ маршрутизатор: 195.73.25.254

б. през интерфейс с IP адрес: 195.73.25.254

IP адрес на следващ маршрутизатор: 195.73.25.1  Неправилен отговор

в. през интерфейс с IP адрес: 207.15.140.20

IP адрес на следващ маршрутизатор: 207.15.140.10

Забележка

Правилният отговор е: а. през интерфейс с IP адрес: 195.73.25.1

IP адрес на следващ маршрутизатор: 195.73.25.254

Въпрос 9

Неправилен отговор

0,00 от максимално 1,00 точки



Отбелязване на въпроса

Текст на въпроса

Какво ще стане, ако IPv6 рутер, на който има 6to4, трябва да предава пакет към отдалечена дестинация, а следващият възел (хоп) е с адрес 2002::/16 ?

Изберете едно

a.

Пакетът се гтагва с IPv6 header и IPv6 префикс включително

b.

IPv6 пакет се опакова в IPv4 пакет, използвайки IPv4 protocol type 41

c.

IPv6 пакетът се изхвърля, защото тази дестинация не може да маршрутизира IPv6 пакети Неправилен отговор

d.

На IPv6 пакета му се маха header-а и се заменя с IPv4 header

Забележка

Правилният отговор е:

IPv6 пакет се опакова в IPv4 пакет, използвайки IPv4 protocol type 41

Въпрос 10

Неправилен отговор

0,00 от максимално 1,00 точки



Отбелязване на въпроса

Текст на въпроса

Кое действие от посочените трябва да се извърши, за да се конфигурира интерфейс “eth0” на един маршрутизатор за едновременно използване на адресите на няколко виртуални локални мрежи (VLAN trunking)?

Изберете едно

a.

Да се използва различен интерфейс за всеки под-интерфейс

b.

За всеки под-интерфейс да се конфигурира различна управляваща област (managementdomain)  Неправилен отговор

c.

Да се използват под-интерфейси (subinterface), и на всеки под-интерфейс да се конфигурира различна IP мрежа

d.

Да се използва по една магистрална (trunked) линия за всяка виртуална локална мрежа (VLAN)

Забележка

Правилният отговор е:

Да се използват под-интерфейси (subinterface), и на всеки под-интерфейс да се конфигурира различна IP мрежа

Въпрос 11

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

Какава е максималната скорост на един порт на 48-портов гигабитов суич?

Изберете едно

a.

48 Gb/s

b. 96 Mb/s

c.

100 Mb/s

d.

1000 Mb/s  Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е:

1000 Mb/s

Въпрос 12

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

NIC (мрежова карта) има MAC адрес 00-0F-66-81-19-A3 и открива маршрутизиращ префикс 2001:0:1:5::/64. Кой IPv6 адрес ще се присвои на картата?

Изберете едно

a.

FF02::1

b.

2001::1:5:20F:66FF:FE81:19A3  Правилен отговор

c.

FE80::20F:66FF:FE81:19A3

d.

::1

Забележка

Правилният отговор е:

2001::1:5:20F:66FF:FE81:19A3

Въпрос 13

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кои от следните твърдения са верни за IPv6 unicast адресите?

Изберете едно или повече:



a.

Link-local адресите започват с FF00::/10



b.

Глобалните адресите започват с 2000::/3 Правилен отговор



c.

Има само един loopback адрес, който е ::1 Правилен отговор



d.

Link-local адресите започват с FE00:/12

Забележка

Правилният отговор е:

Глобалните адресите започват с 2000::/3,

Има само един loopback адрес, който е ::1

Въпрос 14

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Свързвате PC към порт на комутатор, но PC-то няма достъп до ресурси на LAN-а. Какъв е на-вероятният проблем, след като другите PC-та не го изпитват?

Изберете едно

a.

В маршрутната таблица на рутера ням запис за новия хост

b.

Портът на комутатора, към който е свързан хоста, не е присвоен към точния VLAN Правилен отговор

c.

STP топологията (instance) с новия хост не е инициализирана

d.

Комутаторът няма твърдо закодиран MAC адрес в MAC адрес таблицата.

e.

MAC адресът на хоста е неправилно конфигуриран

Забележка

Правилният отговор е:

Портът на комутатора, към който е свързан хоста, не е присвоен към точния VLAN

Въпрос 15

Неправилен отговор

0,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

Мрежата АВТОнет е получила префиксa 192.168.55.0/24. Администраторите са приложили необходимите подмрежкови маски.

При тази постановка са ви дадени следните IP адреси:

192.168.55.57/27

192.168.55.29/28

192.168.55.1/30

192.168.55.132/25

192.168.55.0/30

192.168.55.127/26

На кои интерфейси ще ги присвоите според схемата:

Cars fa0/0 IP:

Trucks s0/1 IP:

Trucks fa0/0 IP:

Vans fa0/0 IP:

Cars fa0/0 IP: Отговор 1 Неправилен отговор

Trucks s0/1 IP: Отговор 2 Неправилен отговор

Vans fa0/0 IP: Отговор 3 Неправилен отговор

Trucks fa0/0 IP: Отговор 4 Неправилен отговор

Забележка

Правилният отговор е:

Cars fa0/0 IP:

– 192.168.55.29/28,

Trucks s0/1 IP:

– 192.168.55.1/30,

Vans fa0/0 IP:

– 192.168.55.57/27,

Trucks fa0/0 IP:

– 192.168.55.132/25

Въпрос 16

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан
Отбелязване на въпроса

Текст на въпроса

Вашият ISP ви е присвоил следната подмрежа и маска:

IP адрес: 199.141.27.0

Subnet маска: 255.255.255.240

Кои от следните адреси може да присвоите на хостове?

Изберете едно или повече:

a.

199.141.27.112

b.

199.141.27.208

c.

199.141.27.175

d.

199.141.27.11 Правилен отговор

e.

199.141.27.2 Правилен отговор

f.

199.141.27.13 Правилен отговор

Забележка

Правилният отговор е:

199.141.27.2,

199.141.27.13,

199.141.27.11

Въпрос 17

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

На IPv6 корпоративна (enterprise) мрежа се препоръчва да се присвои следния префикс:

Изберете едно

- a. /16
- b.

/8

- c.

/3

- d. /48

Забележка

Правилният отговор е: /48

Въпрос 18

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Посочете две причини, заради които мрежовият администратор ще сегментира мрежата с помощта на Layer 2 суич?

Изберете едно или повече:

- a.
елиминира виртуалните канали
- b.
изолира ARP request съобщенията от останалата част на мрежата
- c.
създава по-малко колизионни домейни
- d.
създава повече broadcast домейни
- e.
ще изолира трафика между сегментите 
- f.
разширява честотната лента за потребителя 

Забележка

Вашият отговор е верен.

2 верни отговора

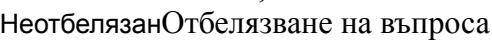
Правилният отговор е:

разширява честотната лента за потребителя,
ще изолира трафика между сегментите

Въпрос 19

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан 

Текст на въпроса

Имате задача да смените окабеляването в мрежата, така че да не бъде подвластно на електромагнитни смущения (EMI).

Какъв кабел ще изберете?

Изберете едно

a.

Тънък коаксиален (Thinnet coaxial cable).

b.

Fiber optic кабел (оптически).  Правилен отговор

c.

Дебел коаксиален (Thicknet coaxial cable).

d.

Category 5 STP кабел.

e.

Category 5 UTP кабел.

Забележка

Правилният отговор е:

Fiber optic кабел (оптически).

Въпрос 20

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Колко хост IP адреса има в една Class C мрежа?

Изберете едно

- a. 510
- b. 256
- c. 192
- d.

128

- e. 254  Правилен отговор

Забележка

Правилният отговор е: 254

Въпрос 21

Неправилен отговор

0,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Имате Class C IP мрежа (префикс) и връзка „точка-точка“ (point-to-point). Искате да приложите VLSM. Кой префикс е най-ефективен?

Изберете едно

- a.

255.255.255.254  Неправилен отговор

- b.

255.255.255.0

- c.

255.255.255.252

- d.

255.255.255.248

- e.

255.255.255.240

Забележка

Правилният отговор е:

255.255.255.252

Въпрос 22

Частично правилен отговор

0,50 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кои от долните адреси могат да се присвоят на хостове от подмржа

192.168.15.19/28?

Изберете едно или повече:

a.

192.168.15.16 Неправилен отговор

b.

192.168.15.29

c.

192.168.15.17 Правилен отговор

d.

192.168.15.31

e.

192.168.15.14 Неправилен отговор

Забележка

Правилният отговор е:

192.168.15.17,

192.168.15.29

Въпрос 23

Частично правилен отговор

0,50 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кое от следните ще уговори LCP (1-а фаза на PPP) при установяване на PPP връзка?

Изберете едно или повече:

a.

Q.931

b.

CHAP

c.

callback Неправилен отговор

d.

IPCP

 Правилен отговор

e.

multilink  Неправилен отговор

Забележка

Правилният отговор е:

IPCP

,

CHAP

Въпрос 24

Частично правилен отговор

0,75 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кои от следните предизвикват задръстване в LAN трафика?

Изберете едно или повече:



a.

сегментиране



b.

Multicasting



c.

Твърде много хостове в broadcast domain  Правilen отговор



d.

Broadcast storms (бури)  Правilen отговор



e.

тясна честотна лента (bandwidth), т.е ниска скорост  Правilen отговор



f.

Full duplex операции

Забележка

Правилният отговор е:

Твърде много хостове в broadcast domain,

Broadcast storms (бури),

Multicasting,

тясна честотна лента (bandwidth), т.е ниска скорост

Въпрос 25

Неправилен отговор

0,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

TCP/IP моделът се различава от OSI модела. Кой от слоевете принадлежи на TCP/IP модела?

Изберете едно или повече:

a.

приложен слой

b.

физически слой  Неправилен отговор

c.

канален (data link) слой  Неправилен отговор

d.

транспортен слой

e.

internet слой

f.

сесиен слой  Неправилен отговор

g.

мрежов слой

Забележка

Правилният отговор е:

приложен слой,

транспортен слой,

internet слой

[Край на прегледа](#)

[Прескочи Навигация в теста](#)

Навигация в теста

[Въпрос 1 Тази страница](#) [Въпрос 2 Тази страница](#) [Въпрос 3 Тази страница](#) [Въпрос 4 Тази страница](#) [Въпрос 5 Тази страница](#) [Въпрос 6 Тази страница](#)
[Въпрос 7 Тази страница](#) [Въпрос 8 Тази страница](#) [Въпрос 9 Тази страница](#) [Въпрос 10 Тази страница](#) [Въпрос 11 Тази страница](#) [Въпрос 12 Тази страница](#)
[Въпрос 13 Тази страница](#) [Въпрос 14 Тази страница](#) [Въпрос 15 Тази страница](#) [Въпрос 16 Тази страница](#) [Въпрос 17 Тази страница](#) [Въпрос 18 Тази страница](#)
[Въпрос 19 Тази страница](#) [Въпрос 20 Тази страница](#) [Въпрос 21 Тази страница](#) [Въпрос 22 Тази страница](#) [Въпрос 23 Тази страница](#)
[Въпрос 24 Тази страница](#) [Въпрос 25 Тази страница](#)
[Край на прегледа](#)

Вие сте влезли в системата като [Мария Кунчева \(Изход\)](#)

[С354740](#)

[Прескоши на основното съдържание](#)
[moodle](#)

- [Български \(bg\)](#)
 - [English \(en\)](#)
 - [Български \(bg\)](#)
-
- Вие сте влезли в системата като [Красимир Атанасов \(Изход\)](#)

Компютърни мрежи, сп. ИС, уч. 2014-15

Път през страниците

- [Начална страница](#) / ►
- [Моите курсове](#) / ►
- [Бакалаври, летен семестър 2014/2015](#) / ►
- [ИС](#) / ►
- [Компютърни мрежи, сп. ИС, уч. 2014-15](#) / ►
- 30 март - 5 април / ►
- [Първи тест за самостоятелна подготовка](#)

Въпрос 11

Незавършен

От максимално 1,00

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Относно DHCP (dynamic Host Configuration Protocol), кое от следните твърдения е вярно?

Изберете едно или повече:



а.

DHCP Discover съобщението не се изпраща на слой 2 адрес.

b.

DHCP Discover съобщението не се нуждае от протокол на транспортния слой.

c.

DHCP Discover съобщението използва TCP за протокол на транспортния слой.

d.

DHCP Discover съобщението се изпраща на специален слой 2 multicast адрес.

e.

DHCP Discover съобщението използва UDP за протокол на транспортния слой.

f.

DHCP Discover съобщението се изпраща на слой 2 адрес FF-FF-FF-FF-FF-FF.

Отметни

Въпрос 12

Незавършен

От максимално 1,00

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кои са трите адресни обхвата, принадлежащи на частните адреси според RFC 1918 и използвани в NAT?

Изберете едно или повече:

a.

127.0.0.0 to 127.255.255.255

b.

192.168.0.0 to 192.168.255.255

c.

172.16.0.0 to 172.16.255.255

d.

10.0.0.0 to 10.255.255.255

e.

0.0.0.0 to 255.255.255

f.

224.0.0.0 to 239.255.255.255

g.

172.16.0.0 to 172.31.255.255

Отметни

Въпрос 13

Незавършен

От максимално 1,00

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кой е префикаса на хост с IP адрес 201.100.5.68/28?

Изберете едно

a.

201.100.5.31

b.

201.100.5.32

c.

201.100.5.65

d.

201.100.5.64

e.

201.100.5.1

f.

201.100.5.0

Отметни

Въпрос 14

Незавършен

От максимално 1,00

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

SUnet има клас C мрежа и иска на 5 департамента да се присвои отделна подмрежа. Всяка подмрежа трябва да поеме най-малко 24 хоста.

Каква ще е маската?

Изберете едно

a.

255.255.255.192

b.

255.255.255.224

c.

255.255.255.254

d.

255.255.255.252

e.

255.255.255.240

f.

255.255.255.248

Отметни

Въпрос 15

Незавършен

От максимално 1,00

 Неотбелязан Отбелязан на въпроса

Текст на въпроса

IP мрежата 210.106.14.0 е разделена на подмрежки с префикс /24. Колко мрежи и с по колко хостове ще се получат?

Изберете едно

a.

8 мрежи с 36 хоста

b.

6 мрежи с 64 хоста

c.

4 мрежи с 128 хоста

d.

2 мрежи с 24 хоста

e.

1 мрежа с 254 хоста

Отметни

Следваща

[Прескочи](#) [Навигация в теста](#)

Навигация в теста

[Въпрос 1](#) [Въпрос 2](#) [Въпрос 3](#) [Въпрос 4](#) [Въпрос 5](#) [Въпрос 6](#) [Въпрос 7](#) [Въпрос 8](#) [Въпрос 9](#) [Въпрос 10](#) [Въпрос 11](#) [Тази страница](#) [Въпрос 12](#) [Тази страница](#)
[Въпрос 13](#) [Тази страница](#) [Въпрос 14](#) [Тази страница](#) [Въпрос 15](#) [Тази страница](#)
[Приключване на опита...](#)

Оставащо време 0:39:23

Вие сте влезли в системата като [Красимир Атанасов \(Изход\)](#)

[C354740](#)

Прескоши на основното съдържание

moodle

- [Атанас Груев](#)  Снимка на Атанас Груев

-  [Моето табло](#)  [Моето табло](#)

-

-  [Профил](#)  [Профил](#)

-  [Оценки](#)  [Оценки](#)

-  [Съобщения](#)  [Съобщения](#)

-  [Предпочитания](#)  [Предпочитания](#)

-

-  [Изход](#)  [Изход](#)

 Покажи менюто за съобщения

0

Съобщения

[Ново съобщение](#)

 [Mark all as read](#)   [Предпочитания за съобщенията](#)

Няма чакащи съобщения

[Виж всички](#)

 Покажи менюто за уведомления

0

Уведомление

 [Mark all as read](#)   [Предпочитания за уведомленията](#)

Нямate уведомления

[Виж всички](#)

- [Български \(bg\)](#)
 - [English \(en\)](#)
 - [Български \(bg\)](#)

Компютърни мрежи, сп. КН-2, летен семестър 2018/2019

Път през страниците

- [Начална страница](#) / ►
- Моите курсове / ►
- [Бакалаври, летен семестър 2018/2019](#) / ►
- [КН](#) / ►
- [Компютърни мрежи, сп. КН-2, летен семестър 2018/2019](#) / ►
- 22 април - 28 април / ►
- [Първи официален тест върху лекциите](#)

Започнат на вторник, 23 април 2019, 21:00

Състояние Завършен

Приключен на вторник, 23 април 2019, 21:40

Изминало време 39 мин. 32 сек.

Точки 22,00/25,00

Оценка **8,80** от 10,00 (88%)

Въпрос 1

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кое е PDU-то в мрежовия слой?

Изберете едно

- a. кадър (frame)
- b. сегмент

с. пакет  Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: пакет

Въпрос 2

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Опитвате се да откриете проблеми в локалната си мрежа. С кои от следните команди ще откриете проблеми с LAN свързаността?

Изберете едно или повече:

a.

ping  Правилен отговор

b.

show hosts

c.

show ip route  Правилен отговор

d.

winipcfg

e.

ipconfig

f.

show interfaces  Правилен отговор

Забележка

Правилните отговори са:

ping,

show ip route,

show interfaces

Въпрос 3

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Имате задача 3-те уеб сървъра на фирмата да са в една IP подмрежа. Същевременно трябва да осигурите максимален брой подмрежки. Каква маска ще приложите за подмрежката с 3-те уеб сървъра?

Изберете едно

- a. 192.168.252.8 255.255.255.248 Правилен отговор
- b. 192.168.252.16 255.255.255.240
- c. 192.168.252.0 255.255.255.252
- d. 192.168.252.16 255.255.255.252
- e. 192.168.252.8 255.255.255.252

Забележка

Вашият отговор е верен.

Правилният отговор е: 192.168.252.8 255.255.255.248

Въпрос 4

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Мрежов администратор верифицира конфигурацията на новоинсталиран хост, като установява FTP конекция към отдалечен сървър. Кой е най-високият слой в протоколния стек, използван в този случай?

Изберете едно

- a. приложен Правилен отговор
- b. сесиен
- c. интернет
- d. транспортен
- e. презентационен

Забележка

Вашият отговор е верен.

Правилният отговор е: приложен

Въпрос 5

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Как комуникират мрежови устройства разпределени във виртуални локални мрежи (VLAN)?

Изберете едно

- a.

Устройства от една виртуална локална мрежа (VLAN) комуникират с помощта на маршрутизатор

- b.

Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на магистрална (trunk) линия между комутаторите (комутатори)

c.

Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на маршрутизатор (рутер)

 Правилен отговор

d.

Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на протокола VTP

Забележка

Правилният отговор е:

Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на маршрутизатор (рутер)

Въпрос 6

Неправилен отговор

0,00 от максимално 1,00 точки

 НеотбелязанОтбелязване на въпроса

Текст на въпроса

В софтуерна компания се изгражда локална мрежа. На фигурата е посочен броят на компютрите във всеки отдел на компанията, които трябва да бъдат свързани в мрежата. Поставено е изискване компютрите от всеки отдел да бъдат в различни подмрежки на една клас „C” мрежа. Коя мрежова маска ще използвате?

Изберете едно

a.

255.255.255.240

b.

255.255.255.224  Неправилен отговор

c.

255.255.255.192

d.

255.255.255.128

Забележка

Правилният отговор е:

255.255.255.128

Въпрос 7

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кой от следните IP адреси попада в CIDR блок 115.54.4.0/22?

Изберете едно или повече:

a.

115.54.7.61 Правилен отговор

b.

115.54.3.32

c.

115.54.5.255 Правилен отговор

d.

115.54.8.32

e.

115.54.5.128 Правилен отговор

f.

115.54.12.128

Забележка

Правилните отговори са:

115.54.7.61,

115.54.5.255,

115.54.5.128

Въпрос 8

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кое е вярно за Ethernet технологията?

Изберете едно

a.

хостовете са в логическа шинна топология Правилен отговор

b.

хостовете са директно свързани към концентратор, наречен MSAU.

c.

хостовете трябва да чакат електронен сигнал, за да предават данни.

d.

хостовете са в логическа кръгова топология.

Забележка

Правилният отговор е:

хостовете са в логическа шинна топология

Въпрос 9

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кое от следните не е от типа съобщения за докладване на грешки (error-reporting messages):

Изберете едно

- a. Destination unreachable
- b. Router error  Правилен отговор
- c. Source quench
- d. Time exceeded

Забележка

Вашият отговор е верен.

Правилният отговор е: Router error

Въпрос 10

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Какво означава “one-to-nearest” (един - до - най-близкия) в IPv6 адресацията?

Изберете едно

- a. anycast  Правилен отговор
- b. глобални unicast
- c. multicast
- d. неопределен адрес

Забележка

Вашият отговор е верен.

Правилният отговор е: anycast

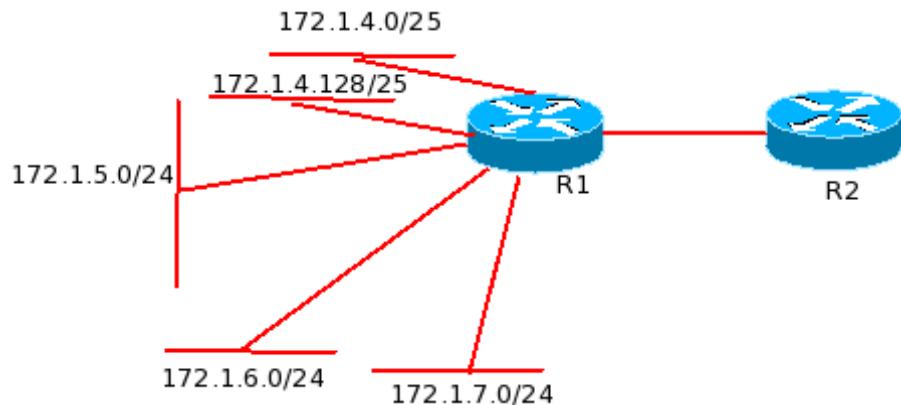
Въпрос 11

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса



На горната фигура, кой префикс е най-подходящ за рекламиране към R2.

Изберете едно

- a. 172.1.4.0/22
- b. 172.1.4.0/24
- c. 172.1.0.0/21
- d. 172.1.0.0/22

Забележка

Вашият отговор е верен.

Правилният отговор е: 172.1.4.0/22

Въпрос 12

Неправилен отговор

0,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Internet Control Message Protocol(ICMP) е проектиран да изпълнява следните функции:

Изберете едно

- a. всички други отговори са верни
- b. корекция на грешки
- c. докладване за грешки  Неправилен отговор
- d. заявки за управление и към хостове

Забележка

Вашият отговор не е верен.

Правилният отговор е: всички други отговори са верни

Въпрос 13

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

TCP/IP няма такъв слой, но OSI моделът го има. Кой е той?

Изберете едно

- a. сесиен  Правилен отговор
- b. мрежов
- c. транспортен
- d. приложен

Забележка

Вашият отговор е верен.

Правилният отговор е: сесиен

Въпрос 14

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Имате IP адресен блок от обхвата на class B. Каква маска ще приложите, за да имате 100 подмрежи с по 500 хост адреса всяка?

Изберете едно

a.

255.255.224.0

b.

255.255.0.0

c.

255.255.255.224

d.

255.255.254.0 Правилен отговор

e.

255.255.255.0

Забележка

Правилният отговор е:

255.255.254.0

Въпрос 15

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кой е префикса на хост с IP адрес 201.100.5.68/28?

Изберете едно

a.

201.100.5.32

b.

201.100.5.64  Правилен отговор

c.

201.100.5.31

d.

201.100.5.1

e.

201.100.5.0

f.

201.100.5.65

Забележка

Правилният отговор е:

201.100.5.64

Въпрос 16

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Колко подмрежи и хостове към всяка от тях ще имате, ако приложите префикс /29 маска на мрежа 210.10.2.0?

Изберете едно



a.

16 подмрежи и 4 хоста.



b.

30 подмрежи и 6 хоста.



c.

8 подмрежи и 30 хоста.



d.

32 подмрежи и 18 хоста.



e.

32 подмрежи и 6 хоста.  Правилен отговор

Забележка

Правилният отговор е:

32 подмрежи и 6 хоста.

Въпрос 17

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан  Отбелязване на въпроса

Текст на въпроса

Структурата (формата) на данните се нарича

Изберете едно



a. конструкция



b. синтаксис  Правилен отговор

- c. няма верен отговор
- d. семантика

Забележка

Вашият отговор е верен.

Правилният отговор е: синтаксис

Въпрос 18

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кой слой на модела OSI отговаря за установяване на надеждно съединение от-край-до-край (end-to-end)?

Изберете едно

- a.

мрежов

- b.

приложен

- c.

сесиен

- d.

транспортен Правилен отговор

- e.

Presentation

Забележка

Правилният отговор е:

транспортен

Въпрос 19

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кое поле помага да се провери подреждането на фрагментите?

Изберете едно

- a. TTL
- b. flag
- c. identifier
- d. offset

Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: offset

Въпрос 20

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Как се създава EUI-64 формат на interface ID от 48-битов MAC адрес?

Изберете едно

- a. Чрез прикрепяне на 0xFF към MAC адреса.
- b. Поставяне на 0xF пред MAC адреса и добавяне на 0xF след него.
- c. Поставяне на 0xFFEE пред MAC адреса.
- d. Поставяне на 0xFF пред MAC адреса и добавяне на 0xFF след него.
- e. Чрез вмъкване на 0xFFFFE между първите три и вторите три байта на MAC адреса.

address  Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: Чрез вмъкване на 0xFFFFE между първите три и вторите три байта на MAC адреса.

address

Въпрос 21

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

За да има коректна адресация, всеки един MAC адрес следва да е:

Изберете едно

- a. уникален за локалния сегмент на мрежата освен ако не е мултикастен  Правилен отговор
- b.

уникален за всички мрежи в организацията освен ако не е мултикастен

- c.

уникален за Интернет (всички мрежи, до които имаме свързаност)

- d.

уникален за Интернет (всички мрежи, до които имаме свързаност) освен ако не е мултикастен

e.

уникален за всички мрежи в организацията

f.

уникален за локалния сегмент на мрежата

Забележка

Правилният отговор е:

уникален за локалния сегмент на мрежата освен ако не е мултикастен

Въпрос 22

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан
Отбелязване на въпроса

Текст на въпроса

SUnet има клас C мрежа и иска на 5 департамента да се присвои отделна подмрежа. Всяка подмрежа трябва да поеме най-малко 24 хоста.

Каква ще е маската?

Изберете едно

a.

/31

b.

/28

c.

/27  Правilen отговор

d.

/30

e.

/26

f.

/29

Забележка

Правилният отговор е:

/27

Въпрос 23

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

Каква маска трябва да приложите на подмрежа, в която ще има поне 16 хоста?

Изберете едно

a. /29

b. /27  Правilen отговор

c. /28

d. /26

Забележка

Вашият отговор е верен.
Правилният отговор е: /27

Въпрос 24

Неправилен отговор
0,00 от максимално 1,00 точки
НеотбелязанОтбелязване на въпроса

Текст на въпроса

Определен брой старши битове в IPv6 адреса определят категорията му. Как се наричат?

Изберете едно

- а. локални Неправилен отговор
- б. резервирали
- в. префикс
- г. постфикс

Забележка

Вашият отговор не е верен.
Правилният отговор е: префикс

Въпрос 25

Правилен отговор
1,00 от максимално 1,00 точки
НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кое от следните е вярно по отношение на мрежа (префикс) с маска

255.255.248.0.

Изберете едно или повече:

a.

Мрежовият адрес на последната подмрежа ще има 248 в 3-ти октет.  Правилен отговор

b.

Първите (старшите) 21 бита са хост частта на адреса.

c.

Номерата на подмрежите са кратни на 8.  Правилен отговор

d.

Отнася се към Class B адрес с взети назем 4 бита.

e.

Отнася се към Class A адрес с взети назем 13 бита.  Правилен отговор

f.

С тази маска може да се създадат 16 подмрежи.

Забележка

Правилните отговори са:

Отнася се към Class A адрес с взети назем 13 бита.,

Мрежовият адрес на последната подмрежа ще има 248 в 3-ти октет.,

Номерата на подмрежите са кратни на 8.

[Край на прегледа](#)

[◀ Маршрутен протокол OSPF в IPv4 и IPv6.](#)

Отиди на ...

[Some internet outages predicted for the coming month as '768k Day' approaches ►](#)

[Прескочи Навигация в теста](#)

Навигация в теста

[Въпрос 1 Тази страница](#) [Въпрос 2 Тази страница](#) [Въпрос 3 Тази страница](#) [Въпрос 4 Тази страница](#) [Въпрос 5 Тази страница](#) [Въпрос 6 Тази страница](#)
[Въпрос 7 Тази страница](#) [Въпрос 8 Тази страница](#) [Въпрос 9 Тази страница](#) [Въпрос 10 Тази страница](#) [Въпрос 11 Тази страница](#) [Въпрос 12 Тази страница](#)
[Въпрос 13 Тази страница](#) [Въпрос 14 Тази страница](#) [Въпрос 15 Тази страница](#) [Въпрос 16 Тази страница](#) [Въпрос 17 Тази страница](#) [Въпрос 18 Тази страница](#)
[Въпрос 19 Тази страница](#) [Въпрос 20 Тази страница](#) [Въпрос 21 Тази страница](#) [Въпрос 22 Тази страница](#) [Въпрос 23 Тази страница](#)
[Въпрос 24 Тази страница](#) [Въпрос 25 Тази страница](#)
[Показване по един въпрос на страница](#) [Край на прегледа](#)

Вие сте влезли в системата като [Атанас Груев \(Изход\)](#)

[C425511S2](#)

[Get the mobile app](#)

[Прескоши на основното съдържание](#)
[moodle](#)

- [Калоян Караиванов](#)  Снимка на Калоян Караиванов
-  [Моето табло](#) 
-
-  [Профил](#) 
-  [Оценки](#) 
-  [Съобщения](#) 
-  [Предпочитания](#) 
-
-  [Изход](#) 

 Покажи менюто за съобщения
0

Съобщения

[Ново съобщение](#)
   [Предпочитания за съобщенията](#)
Няма чакащи съобщения

[Виж всички](#)
 Покажи менюто за уведомления
0

Уведомление

   [Предпочитания за уведомленията](#)
Нмате уведомления

[Виж всички](#)

- [Български \(bg\)](#)
 - [English \(en\)](#)
 - [Български \(bg\)](#)

Компютърни мрежи, сп. ИС, летен семестър 2018/2019

Път през страниците

- [Начална страница](#) / ►
- Моите курсове / ►
- [Бакалаври, летен семестър 2018/2019](#) / ►
- [ИС](#) / ►
- [Компютърни мрежи, сп. ИС, летен семестър 2018/2019](#) / ►
- 22 април - 28 април / ►
- [Първи официален тест върху лекциите](#)

Започнат на понеделник, 22 април 2019, 21:01

Състояние Завършен

Приключен на понеделник, 22 април 2019, 21:38

Изминалото време 37 мин. 32 сек.

Точки 21,17/25,00

Оценка 8,47 от 10,00 (85%)

Въпрос 1

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

На кой OSI слой заглавната част съдържа адрес на хост, който е дестинация и се намира в отдалечена мрежа?

Изберете едно



a.

физически

b.

транспортен

c.

мрежов  Правилен отговор

d.

канален (data link)

e.

сесиен

f.

приложен

g.

представителен

Забележка

Правилният отговор е:

мрежов

Въпрос 2

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Как се нарича енкапсулирането (опаковане) на IPv6 пакети вътре в IPv4 пакети?

Изберете едно

- a. хеширане
- b. маршрутизация
- c. тунелиране  Правилен отговор
- d. NAT

Забележка

Вашият отговор е верен.

Правилният отговор е: тунелиране

Въпрос 3

Частично правилен отговор

0,50 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кои от следните съкращения са коректни за IPv6 адреса 2001:0d02:0000:0000:0014:0000:0000:0095?

Изберете едно или повече:

- a.

2001:d02::14::95

- b.

2001:0d02::0014::0095

- c.

2001:d02::14:0:0:95  Правилен отговор

- d.

2001:d02:0:0:14::95

Забележка

Правилните отговори са:

2001:d02:0:0:14::95,

2001:d02::14:0:0:95

Въпрос 4

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Колко дълъг е IPv6 адреса?

Изберете едно

a.

32 bits

b.

32 десетични числа

c.

16 шестнадесетични числа

d.

128 bits Правilen отговор

Забележка

Правилният отговор е:

128 bits

Въпрос 5

Неправилен отговор

0,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кое от долните твърдения не е стратегия за преход от IPv4 към IPv6 ?

Изберете едно

- a. Tunnelling (тунелиране) Неправилен отговор
- b. транслирне на хедър
- c. Dual stack
- d. Конвергиране

Забележка

Вашият отговор не е верен.

Правилният отговор е: Конвергиране

Въпрос 6

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Имате IP адрес 192.168.10.19/28. Кои от следните IP адреси са валидни хост адреси о тази подмрежа?

Изберете едно или повече:

- a. 192.168.10.17 Правилен отговор

- b. 192.168.10.31
- c. 192.168.10.0
- d. 192.168.10.16
- e. 192.168.10.29  Правилен отговор

Забележка

Вашият отговор е верен.

2 верни отговора

Правилните отговори са: 192.168.10.29, 192.168.10.17

Въпрос 7

Частично правилен отговор

0,50 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Протоколите ICMPv4 и ICMPv6 се използват за:

Изберете едно или повече:

- a. диагностика  Правилен отговор
- b. прехвърляне на пакетите  Неправилен отговор
- c. адресиране
- d. откриване на MAC адреса на съседа във физическия сегмент

Забележка

Вашият отговор отчасти е верен.

Вие правилно сте избрали 1.

2 верни отговора

Правилните отговори са: диагностика, откриване на MAC адреса на съседа във физическия сегмент

Въпрос 8

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Какъв е типа на информацията относно VLAN, която се вмъква в заглавната част на кадъра (фрейма)?

Изберете едно

a.

802.1Q Правилен отговор

b.

ISL

c.

LLC

d.

VTP

e.

CDP

Забележка

Правилният отговор е:

802.1Q

Въпрос 9

Частично правилен отговор

0,50 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кои два елемента се прилагат при stateless автоконфигурирането?

Изберете едно или повече:



a.

Advertised (рекламиран) интерфейс ID



b.

EUI-64 format интерфейс ID Правилен отговор



c.

Advertised (рекламиран) префикс



d.

Multicast префикс Неправилен отговор

Забележка

Правилните отговори са:

Advertised (рекламиран) префикс,

EUI-64 format интерфейс ID

Въпрос 10

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Как се създава EUI-64 формат на interface ID от 48-битов MAC адрес?

Изберете едно

- a. Поставяне на 0xFFEE пред MAC адреса.
- b. Поставяне на 0xFF пред MAC адреса и добавяне на 0xFF след него.
- c. Чрез вмъкване на 0xFFFFE между първите три и вторите три байта на MAC адреса.
address  Правилен отговор
- d. Чрез прикрепяне на 0xFF към MAC адреса.
- e. Поставяне на 0xF пред MAC адреса и добавяне на 0xF след него.

Забележка

Вашият отговор е верен.

Правилният отговор е: Чрез вмъкване на 0xFFFFE между първите три и вторите три байта на MAC адреса.

address

Въпрос 11

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

По отношение а мостове (bridge-ве) и комутатори, кое от следните твърдения е вярно?

Изберете едно или повече:

- a.

Комутаторите имат повече портове от bridge-те.  Правилен отговор

- b.

И bridge-ве, и комутатори вземат решения за направляване на трафика на базата на адреси на 2 слой.  Правилен отговор

- c.

И bridge-ве, и комутатори направляват на 2 слой broadcast-те.  Правилен отговор

d.

Bridge-те дефинират broadcast домейн, докато комутаторите дефинират колизионни домейни.

e.

Комутаторите са предимно софтуерно базирани bridge-ве.

f.

Bridge-те са по-бързи от комутаторите.

Забележка

Правилните отговори са:

И bridge-ве, и комутатори направляват на 2 слой broadcast-те.,

Комутаторите имат повече портове от bridge-те.,

И bridge-ве, и комутатори вземат решения за направляване на трафика на базата на адреси на 2 слой.

Въпрос 12

Частично правилен отговор

0,67 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Вашият ISP ви е присвоил следната подмрежа и маска:

IP адрес: 199.141.27.0/27

Кои от следните адреси може да присвоите на хостове?

Изберете едно или повече:

a.

199.141.27.112



b.

199.141.27.11  Правилен отговор

c.

199.141.27.32



d.

199.141.27.2  Правилен отговор

e.

199.141.27.175



f.

199.141.27.30

Забележка

Правилните отговори са:

199.141.27.2,

199.141.27.30,

199.141.27.11

Въпрос 13

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

След смяна на NIC карта на PC в LAN мрежа комутаторът показва нов MAC адрес, присъединен към неговия port. Кои от следните отговори правилно описват MAC адреса?
Изберете едно или повече:



a.

Публичен IP адрес.



b.

Това е логически адрес



c.

Глобален уникален 48 bit адрес  Правилен отговор



d.

Използван е като част от IPX/SPX конфигурация.



e.

Осигурен е от производителя на NIC картата.  Правилен отговор

Забележка

Правилните отговори са:

Глобален уникален 48 bit адрес,

Осигурен е от производителя на NIC картата.

Въпрос 14

Неправилен отговор

0,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

Ако хост в мрежа има адрес 172.16.45.17/30, какъв ще е префикса, към който принадлежи хоста?

Изберете едно



a.

172.16.45.12

b.

172.16.45.0

c.

172.16.45.15  Неправилен отговор

d.

172.16.45.8

e.

172.16.45.16

Забележка

Правилният отговор е:

172.16.45.16

Въпрос 15

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Мрежата 213.115.77.0 е разделена на подмрежи с префикс /28. Колко подмрежи и с по колко хоста ще получат?

Изберете едно

a.

6 мрежи с 30 хоста

b.

16 мрежи с 14 хоста  Правилен отговор

c.

16 мрежи с 16 хоста

d.

62 мрежи с 2 хоста

e.

2 мрежи с 62 хоста

Забележка

Правилният отговор е:

16 мрежи с 14 хоста

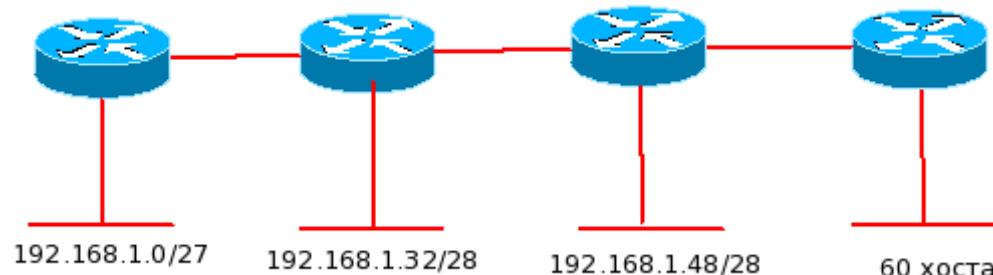
Въпрос 16

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса



В горната мрежа се добавя подмрежа с 60 хоста (компютъра). Кой е най-подходящият префикс?

Изберете едно

- a. 192.168.1.56/26
- b. 192.168.1.64/27
- c. 192.168.1.56/27
- d. 192.168.1.64/26  Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: 192.168.1.64/26

Въпрос 17

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан  Отбелязване на въпроса

Текст на въпроса

Кой от следните IP адреси е използваем (usable) за конфигуриране на мрежово устройство в мрежата 150.25.0.0 с маска 255.255.224.0?

Изберете едно или повече:

- a. 150.25.0.29  Правилен отговор
- b. 150.25.40.24
- c.

150.25.224.30

- d. 150.25.31.23  Правилен отговор

Забележка

Правилните отговори са: 150.25.0.29, 150.25.31.23

Въпрос 18

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кое поле от фрейма разглежда схемата за разпознаване на грешки, за да изпълни своята функция?

Изберете едно

a.

FCS Правилен отговор

b.

ERR

c.

MAC

d.

PDU

e.

Flag

f.

MTU

Забележка

Правилният отговор е:

FCS

Въпрос 19

Правилен отговор

1,00 от максимално 1,00 точки



Отбелязване на въпроса

Текст на въпроса

Каква е максималната препоръчана дължина на 10BaseT кабел?

Изберете едно

a.
100 yards

b.
100 feet

c.
100 meters Правилен отговор

d.
200 meters

Забележка

Правилният отговор е:

100 meters

Въпрос 20

Правилен отговор

1,00 от максимално 1,00 точки



Отбелязване на въпроса

Текст на въпроса

Броят на слоевете в еталонния модел ISO OSI е

Изберете едно

- a. 6
- b. 7  Правилен отговор
- c. 4
- d. 5

Забележка

Вашият отговор е верен.
Правилният отговор е: 7

Въпрос 21

Правилен отговор
1,00 от максимално 1,00 точки
НеотбелязанОтбелязване на въпроса

Текст на въпроса

В полудуплекс (half-duplex) Ethernet LAN, два хоста се опитват едновременно да изпратят данни, което предизвиква колизия (колизия). Какво следва да направят двата хоста?
Изберете едно

- a.

Рутерът, който е на сегмента, ще сигнализира, че колизията е изчистена.

- b.

destination хост изпраща „молба“ до източника за повторно предаване на фрейма.

- c.

Всеки един от двата хоста ще опита повторно предаване след произволен интервал от време.  Правилен отговор

- d.

Хостовете нищо няма да правят, тъй като по-горните слоеве са отговорни за корекция на грешки и повторно предаване.

- e.

Сигналът „jam“ показва, че колизията е изчистена.

- f.

Електрически импулс показва, че колизията е изчистена.

Забележка

Правилният отговор е:

Всеки един от двата хоста ще опита повторно предаване след произволен интервал от време.

Въпрос 22

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Докато се опитвате да откриете проблем със свързаността на дадено PC, получавате следната информация:

Local PC IP адрес: 190.0.3.35/24

Default Gateway: 190.0.3.1

Remote Server: 190.0.5.250/24

След това изпълнявате следните команди от PC-то:

Ping 127.0.0.1 - Unsuccessful

Ping 190.0.3.35 - Successful

Ping 190.0.3.1 - Unsuccessful

Ping 190.0.5.250 - Unsuccessful

Каква е причината, предизвикала този проблем?

Изберете едно

a.

Мрежовият контролер (NIC) не работи

b.

Отдалечен проблем във физическия слой

c.

Локален проблем във физическия слой

d.

TCP/IP не е инсталиран  Правilen отговор

Забележка

Правилният отговор е:

TCP/IP не е инсталиран

Въпрос 23

Правilen отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

На рутера е конфигуриран IP адрес 172.16.2.1/23 на интерфейс Eth0. Кои от следните IP адреси са валидни за компютри, които са в LAN-а, "закачен" за интерфейс Eth0 на рутера?

Изберете едно или повече:

- a. 172.16.3.0  Правilen отговор
- b. 172.16.2.255  Правilen отговор
- c. 172.16.1.198
- d. 172.16.1.100

Забележка

Вашият отговор е верен.

2 верни отговора

Правилните отговори са: 172.16.2.255, 172.16.3.0

Въпрос 24

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Мрежов администратор верифицира конфигурацията на новоинсталиран хост, като установява FTP конекция към отдалечен сървър. Кой е най-високият слой в протоколния стек, използван в този случай?

Изберете едно

- a. интернет
- b. транспортен
- c. сесиен
- d. презентационен
- e. приложен Правilen отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: приложен

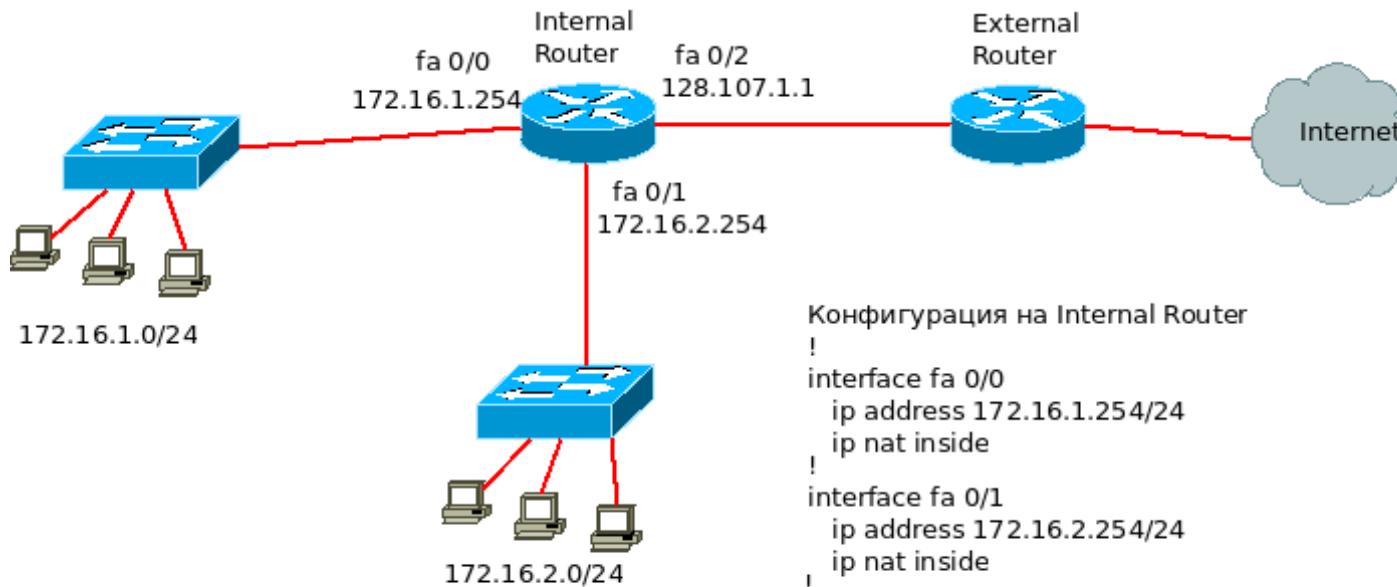
Въпрос 25

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязан на въпроса

Текст на въпроса



Конфигурация на Internal Router

```
!
interface fa 0/0
  ip address 172.16.1.254/24
  ip nat inside
!
interface fa 0/1
  ip address 172.16.2.254/24
  ip nat inside
!
interface fa 0/2
  ip address 128.107.1.1/30
  ip nat outside
!
ip nat inside source list 1 interface fa 0/2 overload
!
ip route 0.0.0.0/0 fa 0/2
!
access-list 1 permit 172.16.1.0/24
access-list 1 permit 172.16.2.0/24
```

Кое е вярното за NAT конфигурацията на горната фигура?

Изберете едно

- а. Заради адреса на интерфейс FastEthernet 0/1, адресът на интерфейс FastEthernet 0/2 не може да поддържа NAT.

- b. ExternalRouter трябва да бъде конфигуриран със статични маршрути към мрежи 172.16.1.0/24 и 172.16.2.0/24.
- c. Показаната конфигурация осигурява неадекватно външно адресно пространство, в което да се транслират вътрешните адреси.
- d. Числото 1 в командата ip nat inside source се отнася до филтъра (access-list) с номер 1, който дефинира вътрешните (частни) адреси, които ще се транслират в публични.  Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: Числото 1 в командата ip nat inside source се отнася до филтъра (access-list) с номер 1, който дефинира вътрешните (частни) адреси, които ще се транслират в публични.

[Край на прегледа](#)

[!\[\]\(4b60441d8dd2ba32eb342c68c655f659_img.jpg\) Списък с ip route2 команди](#)

Отиди на ...



[План на упражнение 2 ►](#)

[Прескочи Навигация в теста](#)

Навигация в теста

[Въпрос 1 Тази страница](#) [Въпрос 2 Тази страница](#) [Въпрос 3 Тази страница](#) [Въпрос 4 Тази страница](#) [Въпрос 5 Тази страница](#) [Въпрос 6 Тази страница](#)
[Въпрос 7 Тази страница](#) [Въпрос 8 Тази страница](#) [Въпрос 9 Тази страница](#) [Въпрос 10 Тази страница](#) [Въпрос 11 Тази страница](#) [Въпрос 12 Тази страница](#)
[Въпрос 13 Тази страница](#) [Въпрос 14 Тази страница](#) [Въпрос 15 Тази страница](#) [Въпрос 16 Тази страница](#) [Въпрос 17 Тази страница](#) [Въпрос 18 Тази страница](#)
[Въпрос 19 Тази страница](#) [Въпрос 20 Тази страница](#) [Въпрос 21 Тази страница](#) [Въпрос 22 Тази страница](#) [Въпрос 23 Тази страница](#)
[Въпрос 24 Тази страница](#) [Въпрос 25 Тази страница](#)
[Показване по един въпрос на страница](#) [Край на прегледа](#)

Вие сте влезли в системата като [Калоян Караванов \(Изход\)](#)

[C425441S2](#)

[Get the mobile app](#)

Прескоши на основното съдържание moodle

- [Александър Станев](#)  Снимка на Александър Станев

-  [Моето табло](#)  Моето табло

-

-  [Профил](#)  Профил

-  [Оценки](#)  Оценки

-  [Съобщения](#)  Съобщения

-  [Предпочитания](#)  Предпочитания

-

-  [Изход](#)  Изход

 Покажи менюто за съобщения

0

Съобщения

[Ново съобщение](#)

   [Предпочитания за съобщенията](#)

Няма чакащи съобщения



[Виж всички](#)

 Покажи менюто за уведомления

0

Уведомление

   [Предпочитания за уведомленията](#)

Нямате уведомления



[Виж всички](#)

- [Български \(bg\)](#)
 - [English \(en\)](#)
 - [Български \(bg\)](#)

Компютърни мрежи, сп. КН-1, летен семестър 2018/2019

Път през страниците

- [Начална страница](#) / ►
- Моите курсове / ►
- [Бакалаври, летен семестър 2018/2019](#) / ►
- [КН](#) / ►
- [Компютърни мрежи, сп. КН-1, летен семестър 2018/2019](#) / ►
- 15 април - 21 април / ►
- [Първи официален тест върху лекциите](#)

Започнат на неделя, 21 април 2019, 13:01

Състояние Завършен

Приключен на неделя, 21 април 2019, 13:41

Изминалото време 39 мин. 59 сек.

Точки 23,00/25,00

Оценка **9,20** от 10,00 (92%)

Въпрос 1

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Списък от протоколи в слоиста архитектура - по един протокол на слой, се нарича

Изберете едно

- a. протоколна архитектура
- b. Няма верен отговор

- c. протоколен стек  Правилен отговор
 d. комплект от протоколи

Забележка

Вашият отговор е верен.

Правилният отговор е: протоколен стек

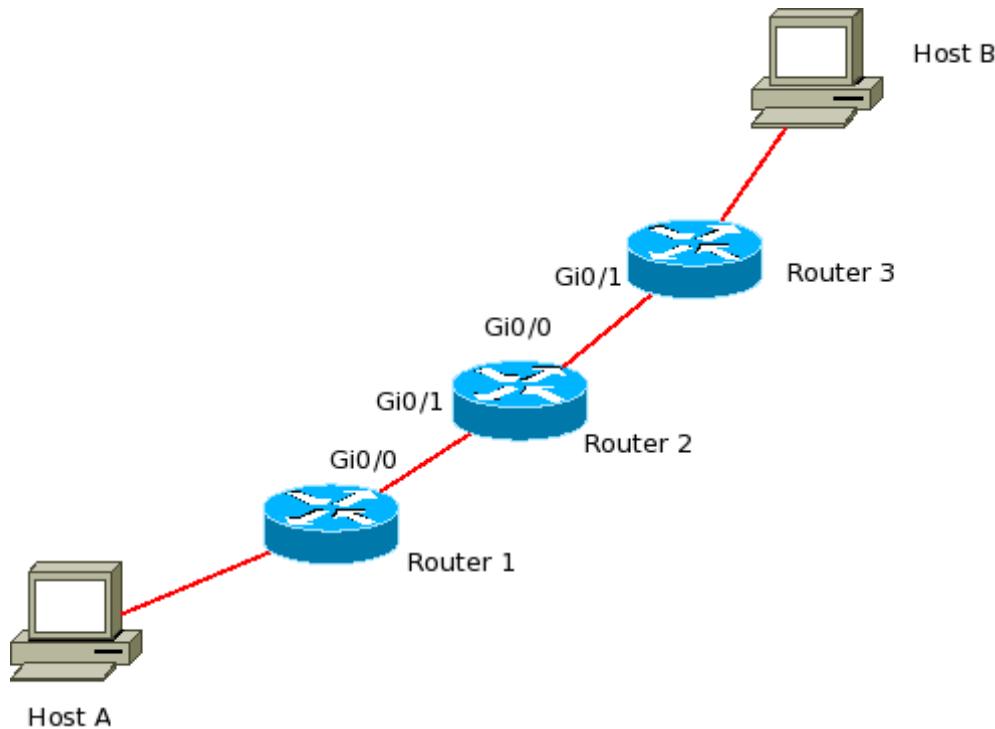
Въпрос 2

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса



Разгледайте горната картина. Host A ping-ва интерфейс Gi 0/1 на рутер 3. Каква е TTL стойността за този ping?

Изберете едно

- a. 252
- b. 255
- c. 254
- d. 253



Забележка

Вашият отговор е верен.

Правилният отговор е: 253

Въпрос 3

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

100BASE-FX реализира Етернет (Ethernet)стандарта при скорост на предаване 100 Mbps:

Изберете едно

a.

по оптичен кабел Правилен отговор

b.

по кабел тип „усукана двойка“ (UTP)

c.

по тънък коаксиален кабел

d.

по дебел коаксиален кабел

Забележка

Правилният отговор е:

по оптичен кабел

Въпрос 4

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Имате IP адресен блок от обхвата на class B. Каква маска ще приложите, за да имате 100 подмрежи с по 500 хост адреса всяка?

Изберете едно

a.

255.255.255.224

b.

255.255.254.0  Правилен отговор

c.

255.255.224.0

d.

255.255.0.0

e.

255.255.255.0

Забележка

Правилният отговор е:

255.255.254.0

Въпрос 5

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Имате IP адрес 172.16.13.5 с маска 255.255.255.128. От какъв клас е адреса, от коя IP мрежа и кой е broadcast адреса?

Изберете едно

- a. Клас А, IP мрежа 172.16.13.0, Broadcast address 172.16.13.127
- b. Клас В, IP мрежа 172.16.13.0, Broadcast address 172.16.13.255
- c. Клас В, IP мрежа 172.16.0.0, Broadcast address 172.16.255.255
- d. Клас В, IP мрежа 172.16.13.0, Broadcast address 172.16.13.127

 Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: Клас В, IP мрежа 172.16.13.0, Broadcast address 172.16.13.127

Въпрос 6

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

Какво означава NAT?

Изберете едно

- a.

Network Address Table

- b.

Network Address Translation  Правилен отговор

- c.

Network Architecture Translation

- d.

National Anthem of Toronto

Забележка

Правилният отговор е:

Network Address Translation

Въпрос 7

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Как се нарича комуникационния модел “от един източник към най-близката дестинация” в IPv6?

Изберете едно

- a. multicast
- b. anycast Правилен отговор
- c. неспецифициран адрес
- d. global unicast

Забележка

Вашият отговор е верен.

Правилният отговор е: anycast

Въпрос 8

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кои от посочените са предимства на оптичните кабели при изграждане на мрежи:

Изберете едно или повече:

a.

по-гъвкав от медните еквиваленти

b.

по-висока скорост от UTP

c.

по-евтини мрежови карти (адаптори) отколкото за медни кабели

d.

позволява информационен пренос на големи разстояния  Правилен отговор

e.

устойчивост към електромагнитни смущения  Правилен отговор

f.

нисък шанс за поразяване от мълния  Правилен отговор

Забележка

Правилните отговори са:

устойчивост към електромагнитни смущения,

позволява информационен пренос на големи разстояния,

нисък шанс за поразяване от мълния

Въпрос 9

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кое от следните полета в IPv4 пакета не се отнася до фрагментацията?

Изберете едно

- a. Offset
- b. TOS  Правилен отговор
- c. Флагове
- d. Identifier (Идентификатор)

Забележка

Вашият отговор е верен.

Правилният отговор е: TOS

Въпрос 10

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

На мрежата SUnet е дадена Class C мрежа 199.166.131.0. Администраторът прилага маска 255.255.255.240. Колко хоста ще има на всяка подмрежка?

Изберете едно

- a. 32
- b. 30
- c. 62
- d. 16
- e.

14  Правилен отговор

- f. 64

Забележка

Правилният отговор е:

14

Въпрос 11

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан
 Отбелязване на въпроса

Текст на въпроса

Коя от следните разновидности на NAT реализира политиката множество портове и частни IP адреси да излизат с един единствен публичен IP адрес?

Изберете едно

a.

Dynamic NAT

b.

статичен NAT

c.

Port Address Translation Правилен отговор

d.

port loading

Забележка

Правилният отговор е:

Port Address Translation

Въпрос 12

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Мрежовата маска е 255.255.255.224. Кои от следните адреси могат да се присвоят на хостове?

Изберете едно или повече:



a.

134.178.18.56

Правилен отговор



b.

92.11.178.93

Правилен отговор



c.

15.234.118.63



d.

192.168.16.87

Правилен отговор

Забележка

Вашият отговор е верен.

Правилните отговори са:

92.11.178.93

,

134.178.18.56

,

192.168.16.87

Въпрос 13

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан
Отбелязване на въпроса

Текст на въпроса

Кой от следните слоеве на TCP/IP модела най-добре съответства на мрежовия слой на OSI модела?

Изберете едно

a.

Internet Правилен отговор

b.

мрежов

c.

транспортен

d.

приложен

e.

Канален (Data Link)

Забележка

Правилният отговор е:

Въпрос 14

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

В IPv6 хедъра полето "traffic class" е подобно на следното поле в IPv4 хедъра:

Изберете едно

- a. Fast-switching
- b. ToS Правилен отговор
- c. Option
- d. Fragmentation

Забележка

Вашият отговор е верен.

Правилният отговор е: ToS

Въпрос 15

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кое е PDU-то в мрежовия слой?

Изберете едно

- a. сегмент

- b. пакет  Правилен отговор
 c. кадър (frame)

Забележка

Вашият отговор е верен.
Правилният отговор е: пакет

Въпрос 16

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кои са трите адресни обхвата, принадлежащи на частните адреси според RFC 1918 и използвани в NAT?

Изберете едно или повече:

a.

224.0.0.0 to 239.255.255.255

b.

172.16.0.0 to 172.16.255.255

c.

0.0.0.0 to 255.255.255

d.

10.0.0.0 to 10.255.255.255  Правилен отговор

e.

172.16.0.0 to 172.31.255.255  Правилен отговор

f.

192.168.0.0 to 192.168.255.255  Правилен отговор



g.

127.0.0.0 to 127.255.255.255

Забележка

Правилните отговори са:

10.0.0.0 to 10.255.255.255,

172.16.0.0 to 172.31.255.255,

192.168.0.0 to 192.168.255.255

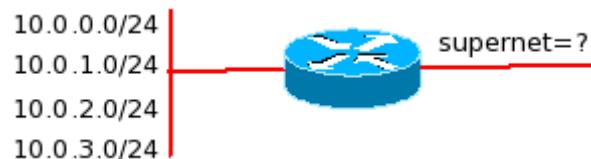
Въпрос 17

Неправилен отговор

0,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса



Кой от долните префикси е най-подходящ за агрегация? Т.е представяне на 4-те префикса /24 отляво като една "суперрежа".

Изберете едно

- a. 10.0.0.0 /22
- b. 10.0.0.0 /23
- c. 10.0.0.0 /24
- d. 10.0.0.0 /21

Неправилен отговор

Забележка

Вашият отговор не е верен.
Правилният отговор е: 10.0.0.0 /22

Въпрос 18

Правилен отговор
1,00 от максимално 1,00 точки
НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кое от следните разширява частната мрежа в обществените мрежи?

Изберете едно

- a. мрежа за съхранение на данни - storage area network (SAN)
- b. виртуална частна мрежа (VPN) Правилен отговор
- c. корпоративна частна мрежа
- d. локална мрежа (LAN)

Забележка

Вашият отговор е верен.
Правилният отговор е: виртуална частна мрежа (VPN)

Въпрос 19

Правилен отговор
1,00 от максимално 1,00 точки
НеотбелязанОтбелязване на въпроса

Текст на въпроса

Един маршрутизатор (рутер) има два серийни и два „FastEthernet“ интерфейси. Той трябва да свърже към Интернет основният офис и четири виртуални локални мрежи (VLANs) от мрежата на компанията. Как най-ефективно може да стане това?

Изберете едно

a.

Чрез използване на преходници (transceivers) от серийни към FastEthernet интерфейси за свързване на две от виртуалните локални мрежи (VLANs) към маршрутизатора, и свързване на останалите две виртуални локални мрежи (VLANs) директно към FastEthernet портовете на маршрутизатора

b.

Чрез магистрална (trunk) линия между FastEthernet интерфейсите на комутатора (комутатор) и маршрутизатора (рутер) и създаване на логически под-интерфейси (subinterfaces) за всяка виртуална локална мрежа (VLAN)

 Правилен отговор

c.

Чрез добавяне на два допълнителни FastEthernet интерфейса за свързване на виртуалните локални мрежи (VLANs)

d.

Чрез хъб (hub) за свързване на четирите виртуални локални мрежи (VLANs) с FastEthernet интерфейса на маршрутизатора (рутер)

Забележка

Правилният отговор е:

Чрез магистрална (trunk) линия между FastEthernet интерфейсите на комутатора (комутатор) и маршрутизатора (рутер) и създаване на логически под-интерфейси (subinterfaces) за всяка виртуална локална мрежа (VLAN)

Въпрос 20

Правилен отговор

1,00 от максимално 1,00 точки

 НеотбелязанОтбелязване на въпроса

Текст на въпроса

Корпоративната LAN е един „плосък“ Ethernet сегмент. Искате да я разделите на 2 сегмента с помощта на рутер. Какво ще постигнете с това?

Изберете едно

a.

Бродкастите от сегмент 1 няма да се пренасят в сегмент 2.  Правилен отговор

b.

Бродкастването на трафика между сегментите ще е по-ефективно.

c.

Ще се намали броя на broadcast домейните.

d.

Ще се увеличи броя на колизиите.

Забележка

Правилният отговор е:

Бродкастите от сегмент 1 няма да се пренасят в сегмент 2.

Въпрос 21

Неправилен отговор

0,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кое поле определя времето на живот на IPv6 пакета?

Изберете едно

- a. Няма верен отговор
- b. Hop limit
- c. TTL  Неправилен отговор
- d. Next header

Забележка

Вашият отговор не е верен.

Правилният отговор е: Hop limit

Въпрос 22

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

На кой слой от OSI модела оперират TTL филтрите, използвани от някои интернет доставчици?

Изберете едно

a.

Presentation

b.

приложен

c.

мрежов Правилен отговор

d.

сесиен

e.

транспортен

Забележка

Правилният отговор е:

мрежов

Въпрос 23

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Сравнявайки мостове (bridges) и комутатори, кои от следните твърдения са верни?

Изберете едно или повече:

a.

Комутаторът е многопортов bridge, Правилен отговор

b.

Bridge-ве и комутатори увеличават размера на колизионния домейн.

c.

Bridge-те и комутаторите научават MAC адреси чрез анализ на полето „source MAC адрес“ в заглавието на получния фрейм. Правилен отговор

d.

Bridge-те са по-бързи от комутаторите защото имат по-малко портове.

e.

bridge-ът прехвърля broadcast, но комутаторът не го прави.

Забележка

Правилните отговори са:

Комутаторът е многопортов bridge,,

Bridge-те и комутаторите научават MAC адреси чрез анализ на полето „source MAC адрес“ в заглавието на получния фрейм.

Въпрос 24

Правилен отговор

1,00 от максимално 1,00 точки



Отбелязване на въпроса

Текст на въпроса

Кой е префикс за IPv6 мултикаст?

Изберете едно



a.

F000::/16



b.

4000::/8



c.

FF00::/8 Правилен отговор



d.

0::/8

Забележка

Правилният отговор е:

FF00::/8

Въпрос 25

Правилен отговор

1,00 от максимално 1,00 точки



Отбелязване на въпроса

Текст на въпроса

Как комуникират мрежови устройства разпределени във виртуални локални мрежи (VLAN)?

Изберете едно

a.

Устройства от една виртуална локална мрежа (VLAN) комуникират с помощта на маршрутизатор

b.

Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на маршрутизатор (рутер)

 Правилен отговор

c.

Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на маршрутизатор (рутер) чрез намагистрална (trunk) линия между комутаторите (комутатори)

d.

Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на протокола VTP

Забележка

Правилният отговор е:

Устройства от различни виртуални локални мрежи (VLAN) комуникират с помощта на маршрутизатор (рутер)

[Край на прегледа](#)

[◀ Маршрутен протокол OSPF в IPv4 и IPv6.](#)

Отиди на ...



[Прескочи Навигация в теста](#)

Навигация в теста

[Въпрос 1 Тази страница](#) [Въпрос 2 Тази страница](#) [Въпрос 3 Тази страница](#) [Въпрос 4 Тази страница](#) [Въпрос 5 Тази страница](#) [Въпрос 6 Тази страница](#)

[Въпрос 7 Тази страница](#) [Въпрос 8 Тази страница](#) [Въпрос 9 Тази страница](#) [Въпрос 10 Тази страница](#) [Въпрос 11 Тази страница](#) [Въпрос 12 Тази](#)

[страница](#) [Въпрос 13 Тази страница](#) [Въпрос 14 Тази страница](#) [Въпрос 15 Тази страница](#) [Въпрос 16 Тази страница](#) [Въпрос 17 Тази страница](#) [Въпрос 18](#)

[Тази страница](#) [Въпрос 19 Тази страница](#) [Въпрос 20 Тази страница](#) [Въпрос 21 Тази страница](#) [Въпрос 22 Тази страница](#) [Въпрос 23 Тази страница](#)

[Въпрос 24 Тази страница](#) [Въпрос 25 Тази страница](#)

[Показване по един въпрос на страница](#) [Край на прегледа](#)

Вие сте влезли в системата като [Александър Станев \(Изход\)](#)

[C425510S2](#)

[Get the mobile app](#)

[Прескоши на основното съдържание](#)
[moodle](#)

- [Михаил Михайлов](#)  Снимка на Михаил Михайлов

-  [Моето табло](#)  [Моето табло](#)
-
-  [Профил](#)  [Профил](#)
-  [Оценки](#)  [Оценки](#)
-  [Съобщения](#)  [Съобщения](#)
-  [Предпочитания](#)  [Предпочитания](#)
-
-  [Изход](#)  [Изход](#)

 Покажи менюто за съобщения

0

Съобщения

[Ново съобщение](#)

 [Mark all as read](#)   [Предпочитания за съобщенията](#)

Няма чакащи съобщения

 [Loading](#)

[Виж всички](#)

 Покажи менюто за уведомления

0

Уведомление

 [Mark all as read](#)   [Предпочитания за уведомленията](#)

Нямате уведомления

 [Loading](#)

[Виж всички](#)

- [Български \(bg\)](#)
 - [English \(en\)](#)
 - [Български \(bg\)](#)

Компютърни мрежи, сп. КН-1, летен семестър 2018/2019

Път през страниците

- [Начална страница](#) / ►
- Моите курсове / ►
- [Бакалаври, летен семестър 2018/2019](#) / ►
- [КН](#) / ►
- [Компютърни мрежи, сп. КН-1, летен семестър 2018/2019](#) / ►
- 15 април - 21 април / ►
- [Първи официален тест върху лекциите](#)

Започнат на неделя, 21 април 2019, 13:00

Състояние Завършен

Приключен на неделя, 21 април 2019, 13:41

Изминалото време 40 мин. 1 сек.

Точки 22,67/25,00

Оценка **9,07** от 10,00 (91%)

Въпрос 1

Частично правилен отговор

0,67 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Имате 2 комутатори във FMI LAN, нямате рутери. Портове 1, 2 и 3 са присвоени на VLAN 1 в комутатори 1 и 2, а портове 4, 5 и 6 са присвоени на VLAN 2 в двата комутатора. Тези два комутатора са свързани чрез trunk канал.

С кои от долните действия ще докажете, че trunk и VLAN са правилно зададени?

Изберете едно или повече:



a.

хост 1 on VLAN 1 не може да ping хост 2 на VLAN 1  Неправилен отговор



b.

хост 4 on VLAN 2 не може да ping хост 1 на VLAN 1  Правилен отговор



c.

хост 4 on VLAN 2 може да ping хост 2 on VLAN 2  Правилен отговор



d.

хост 1 на VLAN 1 може да ping хост 4 на VLAN 2



e.

хост 1 на VLAN 1 може да ping хост 2 на VLAN 1

Забележка

Правилните отговори са:

хост 1 на VLAN 1 може да ping хост 2 на VLAN 1,

хост 4 on VLAN 2 не може да ping хост 1 на VLAN 1,

хост 4 on VLAN 2 може да ping хост 2 on VLAN 2

Въпрос 2

Правилен отговор

1,00 от максимално 1,00 точки

 ОтбелязанПремахване на отбелязването

Текст на въпроса

В модела OSI, устройство А изпраща данни до устройство В, 5-ти слой, който ще получи данни при В, се нарича:

Изберете едно

- a. канален
- b. приложен
- c. физически
- d. сесиен  Правилен отговор
- e. представителен

Забележка

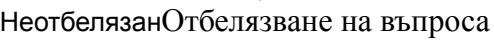
Вашият отговор е верен.

Правилният отговор е: сесиен

Въпрос 3

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан 

Текст на въпроса

На мрежата ви е даден префикс 172.12.0.0 (class B). На всяка подмрежа трябва да има 515 хоста. Коя маска ще използвате?

Изберете едно

- a.

255.255.224.0

- b.

255.255.0.0

- c.

255.255.254.0

- d.

255.255.252.0  Правилен отговор

Забележка

Правилният отговор е:

255.255.252.0

Въпрос 4

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кой слой отговаря за отдалечените комуникации между процеси?

Изберете едно

- a. сесиен
- b. представителен
- c. транспортен Правилен отговор
- d. мрежов
- e. канален

Забележка

Вашият отговор е верен.

Правилният отговор е: транспортен

Въпрос 5

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кои от долните твърдения са верни за IPv6 адресите?

Изберете едно или повече:

a.

Водещите нули в 16-bit шестнадесетичното поле на IPv6 адресите се изписва задължително.

b.

Всеки IPv6 интерфейс съдържа един loopback адрес.  Правilen отговор

c.

На един интерфейс може да се присвоят множество IPv6 адреси от различен тип.  Правilen отговор

d.

Първите 64 бита са динамично създадения интерфейс ID.

Забележка

Правилните отговори са:

На един интерфейс може да се присвоят множество IPv6 адреси от различен тип.,

Всеки IPv6 интерфейс съдържа един loopback адрес.

Въпрос 6

Правilen отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Посочете три характеристики на протокола IPv6.

Изберете едно или повече:

a. checksums

- b. Няма бродкасти  Правилен отговор
- c. фрагментиране на пакета по средата на пътя
- d. усложнен хедър
- e. автоконфигуриране  Правилен отговор
- f. IPv6 Mobile като опция  Правилен отговор

Забележка

Вашият отговор е верен.

3 верни отговора.

Правилните отговори са: IPv6 Mobile като опция, автоконфигуриране, Няма бродкасти

Въпрос 7

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кой е префикс за IPv6 мултикаст?

Изберете едно

a.

FF00::/8  Правилен отговор

b.

F000::/16

c.

4000::/8

d.

0::/8

Забележка

Правилният отговор е:

FF00::/8

Въпрос 8

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан  Отбелязване на въпроса

Текст на въпроса

Рутерът получава пакет на интерфейс 172.16.45.66/26. source IP на пакета е 172.16.45.127/26, a destination - 172.16.46.191/26.

Как рутерът ще обработи пакета?

Изберете едно

a.

destination е broadcast адрес, така че рутерът няма да прехвърли пакета.  Правилен отговор

b.

destination е хост на същата подмржа, така че рутерът ще прехвърли пакета.

c.

destination е мрежов адрес, така че рутерът ще прехвърли пакета.

d.

Дестинацията (destination) е хост на друга подмрежа, така че рутерът няма да прехвърли пакета.

Забележка

Правилният отговор е:

destination e broadcast адрес, така че рутерът няма да прехвърли пакета.

Въпрос 9

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Полето TTL има стойност 10. Кокъв е максималният брой на рутерите, които могат да обработват пакета?

Изберете едно

- a. 11
- b. 1
- c. 5
- d. 10

Забележка

Вашият отговор е верен.

Правилният отговор е: 10

Въпрос 10

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Стратегията, която използват два компютъра с IPv6, за да комуникират помежду си през IPv4 мрежа е:

Изберете едно

- a. Dual stack
- b. тунелиране  Правилен отговор
- c. транслиране на хедъри
- d. Конвергиране

Забележка

Вашият отговор е верен.

Правилният отговор е: тунелиране

Въпрос 11

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Мрежата АВТОнет е получила префиксa 192.168.55.0/24. Администраторите са приложили необходимите подмрежкови маски.

При тази постановка са ви дадени следните IP адреси:

192.168.55.57/27

192.168.55.29/28

192.168.55.1/30

192.168.55.132/25

192.168.55.0/30

На кои интерфейси ще ги присвоите според схемата:

Cars fa0/0 IP:

Trucks s0/1 IP:

Trucks fa0/0 IP:

Vans fa0/0 IP:

Cars fa0/0 IP: Отговор 1 Правилен отговор

Trucks s0/1 IP: Отговор 2 Правилен отговор

Trucks fa0/0 IP: Отговор 3 Правилен отговор

Vans fa0/0 IP: Отговор 4 Правилен отговор

Забележка

Правилният отговор е: Cars fa0/0 IP: → 192.168.55.29/28, Trucks s0/1 IP: → 192.168.55.1/30,

Trucks fa0/0 IP: → 192.168.55.132/25,

Vans fa0/0 IP: → 192.168.55.57/27

Въпрос 12

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан
 Отбелязване на въпроса

Текст на въпроса

Кой OSI слой е обвързан със следното: потвърждение напредаването, последователност и управление на потока през мрежата?

Изберете едно

a.

слой 2

b.

слой 5

c.

слой 4 Правилен отговор

d.

слой 6

e.

слой 3

Забележка

Правилният отговор е:

слой 4

Въпрос 13

Правилен отговор

1,00 от максимално 1,00 точки



Отбелязване на въпроса

Текст на въпроса

Физическият слой се занимава с

Изберете едно

- a. Няма верен отговор
- b. между процесни комуникации
- c. предаване бит по бит Правилен отговор
- d. комуникации между приложно програми

Забележка

Вашият отговор е верен.

Правилният отговор е: предаване бит по бит

Въпрос 14

Правилен отговор

1,00 от максимално 1,00 точки



Отбелязване на въпроса

Текст на въпроса

Физическият слой осигрява

Изберете едно

- a. Всички отговори са верни Правилен отговор
- b. спецификации на лъчите по оптическите кабели
- c. електрически спецификации на сигналите по комуникационните линии
- d. механични спецификации на електрическите конектори и кабели

Забележка

Вашият отговор е верен.

Правилният отговор е: Всички отговори са верни

Въпрос 15

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кои от следните твърдения са верни за IPv6 unicast адресите?

Изберете едно или повече:

a.

Link-local адресите започват с FE00:/12

b.

Има само един loopback адрес, който е ::1 Правилен отговор

c.

Link-local адресите започват с FF00::/10

d.

Глобалните адреси започват с 2000::/3 Правилен отговор

Забележка

Правилните отговори са:

Глобалните адреси започват с 2000::/3,

Има само един loopback адрес, който е ::1

Въпрос 16

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

IP адрес се присвоява на клиент от DHCP за:

Изберете едно

- a. Няма верен отговор
- b. не зависи от времето
- c. неограничен период от време
- d. определено време Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: определено време

Въпрос 17

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Имате IP адрес 192.168.10.19/28. Кои от следните IP адреси са валидни хост адреси о тази подмрежа?

Изберете едно или повече:

- a. 192.168.10.0
- b. 192.168.10.16

- c. 192.168.10.29  Правилен отговор
- d. 192.168.10.17  Правилен отговор
- e. 192.168.10.31

Забележка

Вашият отговор е верен.

2 верни отговора

Правилните отговори са: 192.168.10.29, 192.168.10.17

Въпрос 18

Правилен отговор

1,00 от максимално 1,00 точки

НеотбелязанОтбелязване на въпроса

Текст на въпроса

Интернет провайдерътви е дал адрес 223.6.14.6/29, който слагате на WAN интерфейса на безжичното рутерче. Също така той ви дава default gateway 223.6.14.7. След конфигуриране се оказва, че от рутера не можете да ping-те никое отдалечно устройство. Какъв е проблема?

Изберете едно

- a. IP адресът на рутера е невалиден клас D мулткаст адрес.
- b. IP адресът на рутера е broadcast адреса на подмрежата.
- c. default gateway не е адрес от същата подмрежа (префикс).
- d. default gateway е broadcast адреса на подмрежата.  Правилен отговор

Забележка

Вашият отговор е верен.

Правилният отговор е: default gateway е broadcast адреса на подмрежата.

Въпрос 19

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

В подкатегориите на резервирните адреси в IPv6 има адрес, който се използва от хостовете да тестват самите себе си, без да излизат в мрежата. Кой е този адрес?

Изберете едно

- a. Loopback Правилен отговор
- b. заместващ адрес
- c. уникален адрес
- d. Неопределен

Забележка

Вашият отговор е верен.

Правилният отговор е: Loopback

Въпрос 20

Правилен отговор

1,00 от максимално 1,00 точки

Неотбелязан Отбелязване на въпроса

Текст на въпроса

Хост е конфигуриран със статичен IP адрес, но default gateway е некоректен. Кой слой (слой) на модела OSI ще бъде засегнат първи от тази конфигурационна грешка?

Изберете едно

- a.

слой 5

- b.

слой 4

c.

слой 1

d.

слой 3

 Правилен отговор

e.

слой 2

Забележка

Правилният отговор е:

слой 3

Въпрос 21

Неправилен отговор

0,00 от максимално 1,00 точки

 НеотбелязанОтбелязване на въпроса

Текст на въпроса

Кои три IP адреса могат да бъдат присвоени на хостове, ако маската е /27 ?

Изберете едно или повече:

- a. 129.33.192.192  Неправилен отговор
- b. 17.15.66.128
- c. 192.168.5.63  Неправилен отговор
- d. 135.1.64.34
- e. 10.15.32.17

f. 66.55.128.1

Забележка

Вашият отговор не е верен.

3 верни отговора.

Правилните отговори са: 10.15.32.17, 66.55.128.1, 135.1.64.34

Въпрос 22

Правilen отговор

1,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

Възлите в компютърната мрежа са

Изберете едно

- a. всички отговори по-горе са верни  Правilen отговор
- b. компютрите, които са дестинация на съобщения
- c. компютрите, които определят маршрута на съобщенията
- d. компютрите, които са източник на съобщения

Забележка

Вашият отговор е верен.

Правилният отговор е: всички отговори по-горе са верни

Въпрос 23

Правilen отговор

1,00 от максимално 1,00 точки



Текст на въпроса

Физическият слой транслира заявки от логически комуникации от КОЙ СЛОЙ в чисто хардуерни операции?

Изберете едно

- a. приложен
- b. транспортен
- c. канален (DLL) Правилен отговор
- d. мрежов
- e. сесиен

Забележка

Вашият отговор е верен.

Правилният отговор е: канален (DLL)

Въпрос 24

Неправилен отговор

0,00 от максимално 1,00 точки



Текст на въпроса

Кое от полетата на IPv4 header не е идентично с поле в IPv6 header?

Изберете едно

- a.

ToS

- b.

Version

c.

TTL

d.

Checksum  Неправилен отговор

Забележка

Правилният отговор е:

TTL

Въпрос 25

Правилен отговор

1,00 от максимално 1,00 точки

 Неотбелязан Отбелязване на въпроса

Текст на въпроса

Кой от следните адреси е broadcast адрес на клас В мрежа с маска по подразбиране?

Изберете едно

a. 172.255.255.255

b. 172.16.10.255

c. 172.16.255.255  Правилен отговор

d. 255.255.255.255

Забележка

Вашият отговор е верен.

Правилният отговор е: 172.16.255.255

[Край на прегледа](#)

[◀ Маршрутен протокол OSPF в IPv4 и IPv6.](#)

Отиди на ... [Отиди на ...](#)

[Прескачи](#) [Навигация в теста](#)



Навигация в теста

[Въпрос 1 Тази страница](#) [Въпрос 2 Тази страница](#) [Отбелоязан](#) [Въпрос 3 Тази страница](#) [Въпрос 4 Тази страница](#) [Въпрос 5 Тази страница](#) [Въпрос 6 Тази страница](#) [Въпрос 7 Тази страница](#) [Въпрос 8 Тази страница](#) [Въпрос 9 Тази страница](#) [Въпрос 10 Тази страница](#) [Въпрос 11 Тази страница](#) [Въпрос 12 Тази страница](#) [Въпрос 13 Тази страница](#) [Въпрос 14 Тази страница](#) [Въпрос 15 Тази страница](#) [Въпрос 16 Тази страница](#) [Въпрос 17 Тази страница](#) [Въпрос 18 Тази страница](#) [Въпрос 19 Тази страница](#) [Въпрос 20 Тази страница](#) [Въпрос 21 Тази страница](#) [Въпрос 22 Тази страница](#) [Въпрос 23 Тази страница](#) [Въпрос 24 Тази страница](#) [Въпрос 25 Тази страница](#)

[Показване по един въпрос на страница](#) [Край на прегледа](#)

Вие сте влезли в системата като [Михаил Михайлов](#) ([Изход](#))

[C425510S2](#)

[Get the mobile app](#)

{882892054783560431}.txt

1. Кой е вторият хост адрес в IP мрежата 62.44.109.64/27
Хост адресите са 62.44.109.65-94

2. Кой е бродкаст адреса на IP мрежата 62.44.126.0/24
62.44.126.255

3. Кой е бродкаст адреса на IP мрежата 62.44.96.64/26
62.44.96.127

4. В мрежата на ФМИ има 512 хоста. Изберете дължина на мрежовата маска, при която да имаме минимално разхищение на IP адреси.
256 - 8 хост бита; 512 - 9 хост бита; т.e префикс /23, но спомнете си 2 на степен броя на хост битове - 2.

5. В мрежата на компанията "ABC Industries" има 1001 хоста. Изберете дължина на мрежовата маска, при която да имаме минимално разхищение на IP адреси.
256 - 8 хост бита; 512 - 9 хост бита; 1024 - 10 хост бита; т.e префикс /22

6. Кое от следните не е от типа съобщения за докладване на грешки (error-reporting messages)

a, b и c са съобщения за докладване на грешки, дефинирани в ICMP.

7. Адресът 172.0.0.1 е: публичен адрес

8. Най-младшият октет от мрежовата маска е 11111000 в двоичен формат. Как ще се представи с 10-но число?

В 16-ен код F8, т.e $15 * 16 + 8 = 248$

9. Вашият ISP ви е присвоил следната подмрежа и маска: IP адрес: 199.141.27.0/27
Кои от следните адреси може да присвоите на хостове?

Хост адреси: 199.141.27.1 - 30

10. На мрежата SUNet е даден префикса 165.100.27.0/24. Колко подмрежи с по колко хоста поддържа този префикс?

Една мрежа с префикс /24. 8 хост бита, следователно 254 хоста.

11. HostA ping-ва HostB. Кой от долните записи е валиден за ARP кеша на HostA след изпълнението на команда ping:

IP:192.168.6.2 MAC:000f.2485.8918. Единствено там има съответствие между IP адрес на интерфейс и MAC адрес - FastEthernet 0/24 на съича.

12. Кои твърдения са верни за IP адреса 10.16.3.65/23?

IP мрежата е 10.16.2.0/23, бродкаст 10.16.3.255

13. При класовото адресиране (classful addressing) гляма част от адресите се: пропиливат. Защо? Например, 10.0.0.0/8, а имате 5 компютъра...

14. Какво го има в IPv4, но го няма в IPv6?

Имаме фрагментиране (при сурса), Header checksum и Options

15. NIC (мрежова карта) има MAC адрес 00-0F-66-81-19-A3 и открива маршрутизиращ префикс 2001:0:1:5::/64. Кой IPv6 адрес ще се присвои на картата?
2001:0:1:5:020F:66FF:FE81:19A3/64. Обърнете внимание: защо 00 става 02 и къде се вмъква FFFE.

16. В IPv6 адреса колко бита са включени във всяко поле, разделено със знака :
4 16-ни цифри, 16 бита

17. Как се нарича комуникационния модел "от един източник към най-близката дестинация" в IPv6?
анукаст информацията, записана на даден възел (напр. БД) се реплицира на различни места в мрежата. Защо?

{882892054783560431}.txt

18. Кой от следните е валидно представяне на IPv6 адреса

B514:82C3:0000:0000:0029:EC7A:0000:EC72?

B514:82C3::0029:EC7A:0000:EC72 B514:82C3:0000:0000:0029:EC7A::EC72

19. Кой от долните е IPv6 link-local адрес?

FE80::380e:611a:e14f:3d69 link-local адреси са от следния префикс: fe80::/10

20. Точният формат на пакета при преход на IPv6 пакет през IPv4 мрежа (тунел) е:

За да мине IPv6 пакет през IPv4 мрежа: IPv4 header-IPv6 header-Payload

21. Кой съич ще избере STP (Spaning Tree Protocol) като root bridge?

Bridge ID: 32768: 11-22-33-44-55-65 (Priority:MAC) е с най-малка стойност.

{882892024718733885}.txt

1. Напишете най-характерното за работата на един комутатор (суич).

"Switch-ът функционира като един многопортов bridge. Работи на канално ниво и отговаря за успешното свързване на две мрежи. От получения кадър прочита адреса на получателя и така преценява по коя линия да изпрати същия този кадър."

Бих добавил: От получения кадър прочита MAC адреса на получателя. За целта поддържа "MAC Address Table" с две колони: "No. на порт" и "MAC Address" - MAC адресите, които са се "прилепили" към съответния порт. MAC Address Table е кеш, след определен timeout, запис, към който не е имало обръщение, се изтрива. Така се предпазваме от препълване на паметта. Интересен е случаят, когато даден Destination MAC не е открит в таблицата. Тогава суичът се превръща в хъб - препраща кадъра (фрейма) към всички портове с изключение на този, от който е получен. Ако на даден порт има устройство, което си познае MAC адреса, то връща отговор, като MAC адресът му е записан в полето "Source MAC". Така таблицата на суича се допълва, прочитайки полето "Source MAC". Този сценарий се практикува от атакуващите на 2 слой - задръства се таблицата с несъществуващи MAC адреси, което превръща суича в хъб. Разработени са защити срещу това.

Суичът може да работи и на 3 слой - добавя се още една колона към MAC Address Table - с Dest. IP:

https://documentation.meraki.com/MS/Layer_3_Switching/Layer_3_vs_Layer_2_Switching

Имаме също и L4 и L7 суичове, които комутират по TCP/UDP порт или по приложен протокол.

2. Две мрежи осигуряват надеждна услуга с установяване на сесии. Едната предлага надежден поток от байтове, а другата - надежден поток от съобщения. По какво са идентични и по какво се различават двете сесии?

"Сесията с надеждните байтове осигурява малко загуба на пакетите, а другата - надежност че ще пристигне цялото съобщение. Различават се по това, че при вторият вариант е гарантиран реда на получаване на пакетите, а при другият не."

Добър отговор. Може да се добави, че комутацията на съобщения създава условия за задръстване на линиите. Представете си съобщение, съдържащо 1 GB+ файл. При сегашните скорости е възможно блокиране на линиите. Това утежнява много проверките за грешки. Всъщност "надежден поток от байтове" е пакетната комутация. На транспортно ниво протоколът TCP връща Acknowledge при правилно получен поток от байтове, който е разделен на "chunk-вe", които IP протоколът "облича" като пакети. Но за това ще говорим като стигнем до темата за TCP.

3. Какво означава "договаряне" ("negotiation"), когато говорим за мрежови протоколи. Дайте пример.

"Двете страни се договарят кои мрежови протоколи да използват за комуникация. да ползват IPv6 например "

На съответния слой се договарят параметри, които са характерни за този слой. На физически слой - скорост на предаване, full/half duplex и др., на канален - MTU, CRC..., IP - QoS и приоритети, ако са зададени, на транспортно - дължина на сегмент или дейтаграма и т.н.

4. Файл, разбит на поредица от пакети, се трансферира между два компютъра. Има две възможности за гарантиране на надеждността на преноса. Едната е: получаването на всеки пакет се потвърждава поотделно, но не и на файла като цяло. Втората е: получаването на всеки пакет не се потвърждава, но се потвърждава получаването на целия файл. Анализирайте двета подхода.

{882892024718733885}.txt

"При потвърждаването на всеки пакет поотделно може по-бързо да се изпратят наново изгубените пакети.

При потвърждаването на целия файл може да се направи анализ кой пакети трябва да се изпратят наново след изтичането на delay-time-a. Или ако пакетите са много на брой може да се наложи да се изхвърлят някой, за да се получат наново пакети, за да се запази последователността. Вторият вариант е добър, когато връзката е надеждна."

Добър отговор - тук важат и разсъжденията от въпрос 2.

5. Едно изображение съдържа 1600×1200 пиксела (3 bytes/pixel). Предполагаме, че изображението се пренася по мрежата, без да е компресирано. Колко време ще отнеме да бъде предадено по модемна линия със скорост 64 kbps? Също така по 10 Mbps, 100 Mbps и 1000 Mbps Ethernet?

"64 kbps - 88 сек.

10 Mbps - 0.6 сек.

100 Mbps - 0.06 сек.

1000 Mbps - 0.006 сек."

"11 250, 70, 7, 0.7 сек."

За 64 kbps:

$$1600 \times 1200 \times 3 = 5760000 \text{ bytes} \times 8 = 46080000 \text{ bits} : 64000 = 720 \text{ s}$$

6. Президентът на Specialty Paint Corp. решава да произведе невидима бирена кутия (кен) съвместно с местната пивоварна. За целта се обръща към юридическия си отдел да уреди нещата. Те от своя страна се обръщат към инженерния отдел за помощ. За целта главният инженер кани колегата си от пивоварната, за да обсъдят техническите аспекти на проблема. Инженерите докладват резултатите на своите юридически отдели. Юристите от двете фирми обсъждат проблемите по телефона. Накрая президентите на двете фирми уреждат финансовите въпроси.

Кой принцип на многослойния протокол по отношение на OSI модела е нарушен тук?

"нарушава се принципа на ненуждното предаване на информация из другите слоеве."

"Нарушава се капсулатията, енкапсулатията"

"От горе надолу" липсва "договаряне" ("negotiation") на "слой" юридически.

7. Посочете две причини за прилагане на слоеста архитектура. Какъв е възможният недостатък на слоестите протоколи?

"Прозрачност - долните слоеве да не се интересуват от реализацията на долните Гъвкавост"

Също така Scalability. За Layered Architecture - Pros and Cons, вж.
<https://enqueuezero.com/layered-architecture.html#pros-and-cons>

8. Предполагаме, че се е наложила промяна в алгоритмите за реализация на функциите на слой k. Как това ще се отрази на операциите на слой k - 1 и на слой k + 1?

"няма да се отрази, защото това е идеята на прозначността между слоевете"

"Няма да се отрази по никакъв начин, понеже OSI моделът гарантира гъвкавост (промяна на реализацията на функциите без да се "счупи" цялостната концепция)."

"k-1 - никак Ако променим tcp и http е използвал tcp, то тогава и функционалността може да се промени иначе не" - в какъв смисъл? Напр., продължителността на timeout

за повторно предаване?

14. Имате 2 комутатори във FMI LAN, нямате рутери. Портове 1, 2 и 3 са присвоени на VLAN 1 в комутатори 1 и 2, а портове 4, 5 и 6 са присвоени на VLAN 2 в двата комутатора. Тези два комутатора са свързани чрез trunk канал. С кой от долните действия ще докажете, че trunk и VLAN са правилно зададени?

Изберете едно или повече:

- a. хост 1 на VLAN 1 може да ping хост 2 на VLAN 1 - верен
- b. хост 1 на VLAN 1 не може да ping хост 2 на VLAN 1
- c. хост 4 на VLAN 2 може да ping хост 2 на VLAN 2 - верен
- d. хост 4 на VLAN 2 не може да ping хост 1 на VLAN 1 - верен
- e. хост 1 на VLAN 1 може да ping хост 4 на VLAN 2

Възможно е ping-то САМО между хостовете в един и същи VLAN (1 или 2).

16. Две станции в LAN започват да предават в един и същи момент, което води до колизия. Какво става в мрежата при това положение?

Изберете едно или повече:

- a. Сигнал „jam“ информира всички устройства, че е настъпила колизия. - верен
 - b. След възстановяване на предаването устройствата, участващи в колизията, имат приоритет пред останалите.
 - c. Устройството, въвлечено в колизията, спира да предава за кратък период от време. - верен
 - d. Колизията стартира „random back-off algorithm“ (генратор на случайно число, след което предаването ще се повтори). - верен
 - e. Всяко устройство на Ethernet сегмента спира да предава кратък период от време.
- 3-те верни отговори илюстрират back-off алгоритъма при настъпване на колизия.

18. След смяна на NIC карта на PC в LAN мрежа комутаторът показва нов MAC адрес, присъединен към неговия port. Кои от следните отговори правилно описват MAC адреса?

Изберете едно или повече:

- a. Това е логически адрес
- b. Използван е като част от IPX/SPX конфигурация.
- c. Глобален уникален 48 bit адрес - верен
- d. Публичен IP адрес.
- e. Осигурен е от производителя на NIC картата. - верен

Това са характеристиките на MAC адреса

19. Кои от по-долните твърдения за OSI модела са верни:

Изберете едно или повече:

- a. преминаването на информацията между слоевете е само възходящо
- b. представлява отворен стандарт - верен
- c. състои се от 4ри слоя
- d. всеки слой се характеризира с определено представяне на информацията - верен (вж. PDU)
- e. описва метода за предаване на информация между мрежови устройства
- f. преминаването на информацията между слоевете е само низходящо

20. При OSI модела при движение на данните отдолу нагоре по слоевете хедърите се

...
изберете едно или повече:

- a. добавят
- b. премахват - верен (decapsulation)
- c. декапсулират
- d. енкапсулират

21. Кой суич ще избере STP (Spanning Tree Protocol) като root bridge?

{882892024718733885}.txt

- a. 32768: 11-22-33-44-55-66
- b. 32768: 22-33-44-55-66-77
- c. 32768: 22-33-44-55-66-78
- d. 32768: 11-22-33-44-55-65 - верен (най-ниска стойност на MAC адрес, съотв. най-малък Bridge ID)

КОМПЮТЪРНИ МРЕЖИ

ВЪВЕДЕНИЕ

Зашо изучавате КМ

Днешният свят е силно свързан. Живеем в едно глобално “дигитално село”.

И като потребители, и като създатели на компютърни продукти (хардуер и софтуер) сме с вързани ръце (и крака:)) без мрежова свързаност. Това налага да сме наясно (горе-долу) с мрежовите технологии.

По отношение на учебния процес във ФМИ:

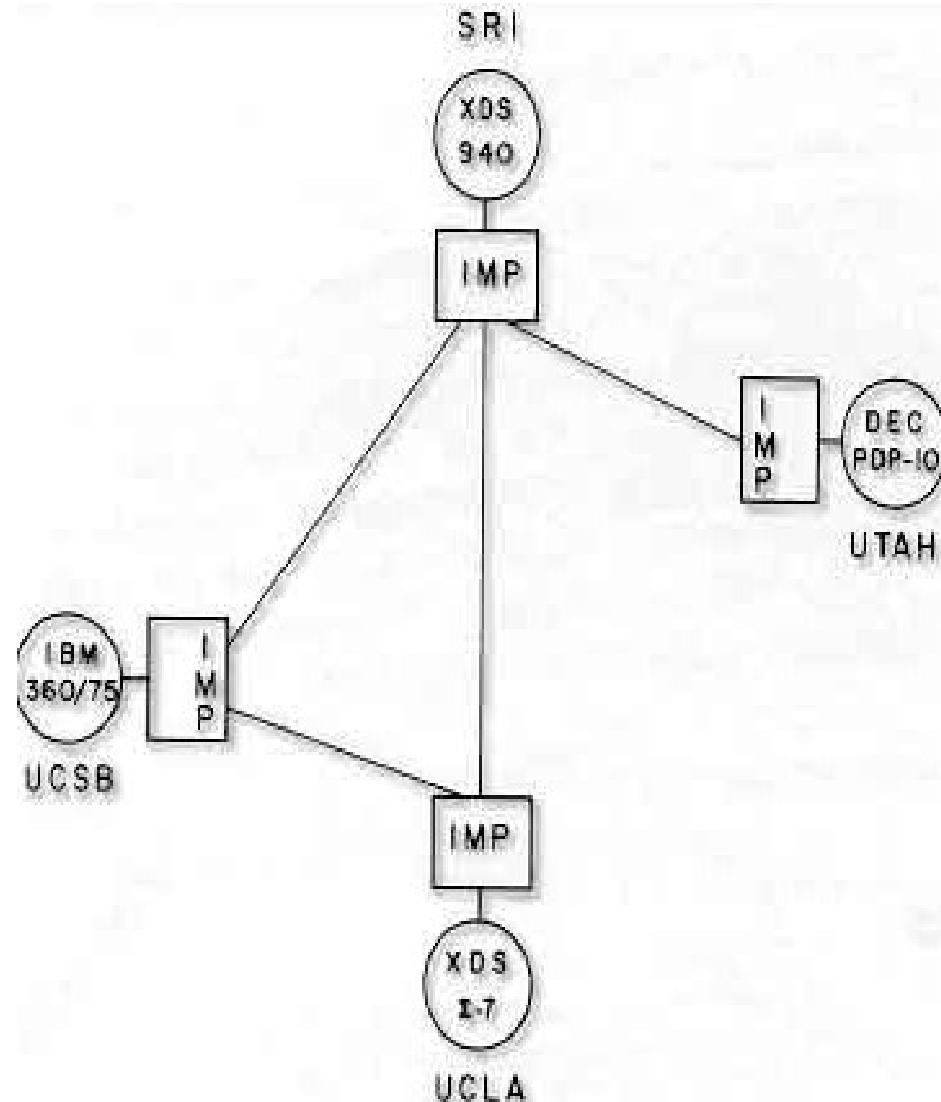
- Курсът въвежда в основните понятия на компютърните мрежи и комуникации – модели, среди, компоненти, услуги, протоколи, интерфейси, (по малко) защита и сигурност.
- Материалът е предпоставка за курсовете “Мрежово програмиране” (**на първо място**), по Web технологии и мн.др.

МАЛКО ИСТОРИЯ: 1960 - 1969

1958 В САЩ се формира Агенция за Съвременни Изследователски Проекти - Advanced Research Projects Agency ([ARPA](#)).

1964 Развиване на теорията за пакетни комуникационни мрежи. Paul Baran, RAND: " On Distributed Communications Networks"

1969 ARPANET е официално пусната в действие. Първоначално се състои от четири "възела" свързани с 50kbs линии предоставени от AT&T: UCLA, Stanford Research Institute (SRI), University of California Santa Barbara (UCSB), University of Utah.



Paul Baran (1926–2011) – изобретатель на packet switching



Paul Baran – Интернет пионер

Paul Baran (29.04.1926 – 26.03.2011) – американец от полски произход.

Разработва концепцията за оцеляваща и при апокалипсис комуникационна мрежа, когато работи за RAND Corp. в средата на 1960-те – Караиската криза.

Идеята за **packet switching** – движение на данни, разделени според Baran на "**message blocks**", в разпределена мрежа, намери реализация в ARPANET.

Идеята е революционна, че **AT&T** я отхвърля, нямало да сработи (по сведение на друг пионер Vinton Cerf).

MEMORANDUM
RM-3420-PR
AUGUST 1964

ON DISTRIBUTED COMMUNICATIONS:
I. INTRODUCTION TO
DISTRIBUTED COMMUNICATIONS NETWORKS

Paul Baran

PREPARED FOR:
UNITED STATES AIR FORCE PROJECT RAND

The **RAND** *Corporation*
SANTA MONICA • CALIFORNIA

Първият IMP

Len Kleinrock и
първият
Interface
Message
Processor.

(“прадядо” на
днешния
мрежов
контролер)



1970 - 1979

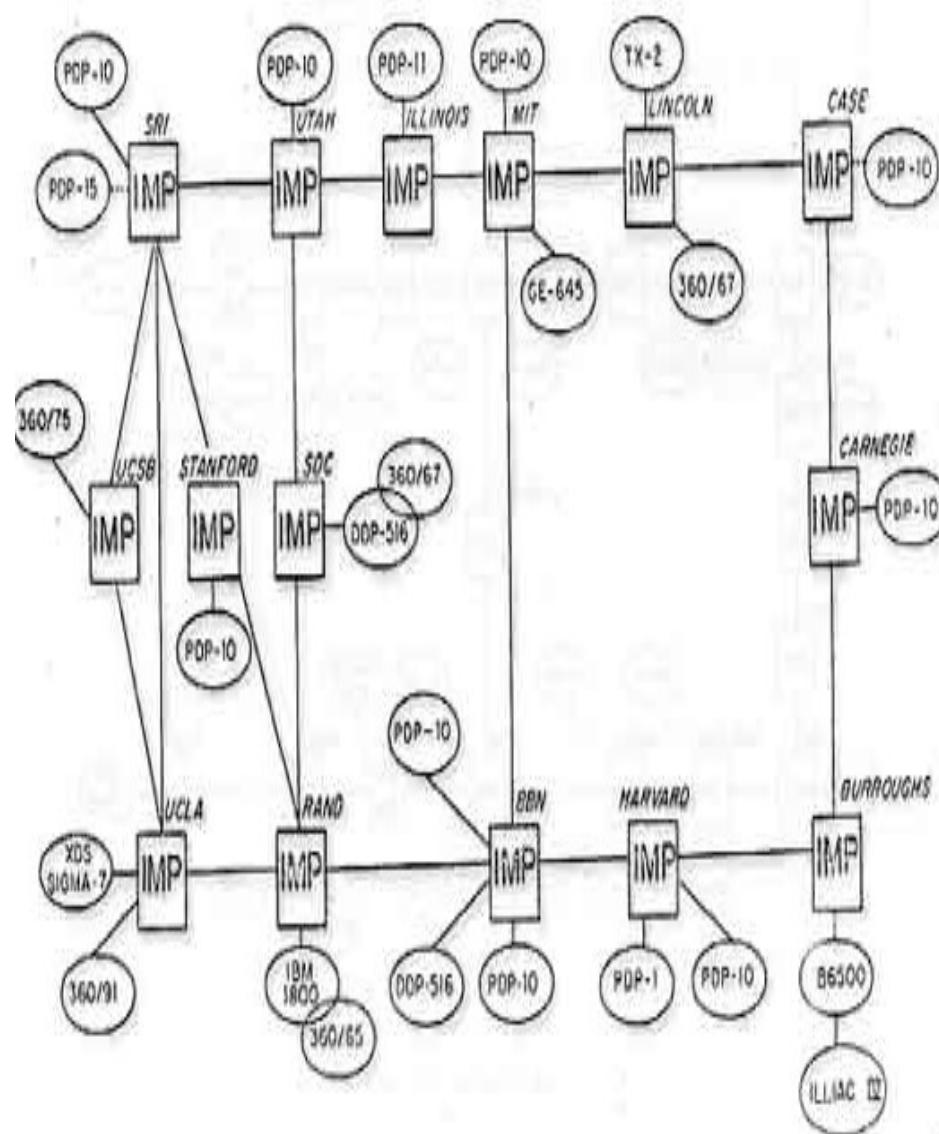
1970 Първа публикация на оригиналния ARPANET Host-Host протокол: C.S. Carr, S. Crocker, V.G. Cerf, "HOST-HOST Communication Protocol in the ARPA Network"

ALOHAnet, първата пакетна радио мрежа е разработена от Norman Abramson, Хавайски Университет, започва действие. През 1972 е свързана към ARPANET.

Компютрите в ARPANET започват да използват Network Control Protocol (NCP), първия host-to-host протокол.

1971 На 16 април е публикувана оригиналната спецификация на File Transfer Protocol (**FTP**) от Abhay Bhushan - RFC 114.

Ray Tomlinson от BBN изобретява **email** програма за изпращане на съобщения по компютърна мрежа.



1970 1979

1972 Ray Tomlinson модифицира програмата за ARPANET. Знакът @ е бил избран от пунктуационните клавиши на телетайп Tomlinson's модел 33 заради значението "at" "при".

Първи разговор (чат) по мрежата.

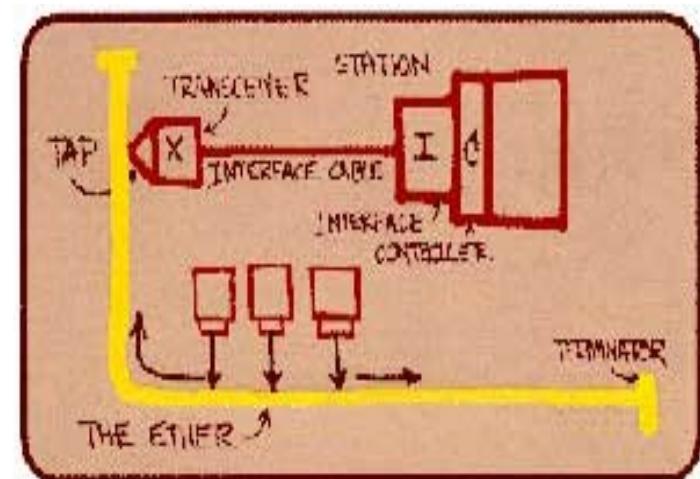
RFC 318: Telnet спецификация

1973 Първи международни връзки към ARPANET - UCL, Англия.

В докторската си теза **Bob Metcalfe** от Харвард изказва идеята си за **Ethernet**. Концепцията е проиграна в компютъра Alto на изследователския център на Xerox PARC в Алто, Калифорния. Там е създадена първата Ethernet мрежа.

Над 2000 потребители на ARPANET.

Изследване на ARPA сочи, че email съобщенията съставят 75% от целия трафик в ARPANET.



1970 – 1980... Стандарти

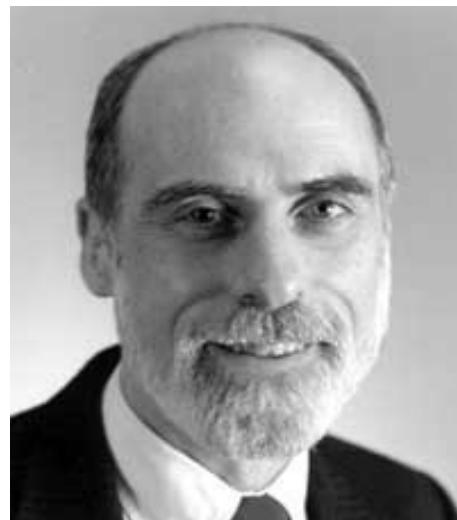
1974 [Vint Cerf](#) и [Bob Kahn](#) публикуват "Протокол за свързване чрез пакетна мрежа", който детайлно описва [TCP](#).

1978 През Март TCP се разделя на [TCP](#) и [IP](#).

Късните 1970 проект, управляем от International Organization for Standardization ([ISO](#)), друг - от International Telegraph and Telephone Consultative Committee ([CCITT](#))

1983 двата са слети в The Basic Reference Model for Open Systems Interconnection. Известен като **Open Systems Interconnection Reference Model (OSI Reference Model)**.

1984 публикуван от ISO като стандарт **ISO 7498**. И от CCITT ([ITU-T](#)) като стандарт **X.200**. OSI стъпва на опита на мрежите ARPANET, NPLNET, EIN, CYCLADES и разработките на [IFIP WG6.1](#).



1980 – 1989 Предпоставки за разрастване

1980 Първата реализация на **NTP** - Internet Engineering Note [IEN-173]; RFC 778 - Clock Service. NTP е въведен за първи път в RFC 958



1981 IBM PC стартира през август 1981

1984 Първият **Apple Macintosh**. Със съвременен графичен интерфейс:



Macintosh'89 = Windows 95
Локалната мрежа AppleTalk

1980 – 1989 (Unix и C)



През 1983 г. Ken Thompson и **Dennis Ritchie [1941-2011]** получават **Turing Award** за разработване на обща теория на операционните системи и по-специално **ОС UNIX**.

Ritchie е известен и като създател на **езика Си**.

Приносът на Ritchie към Unix е в универсалността: възможността за портване на различни машини и платформи.

1980 - 1989

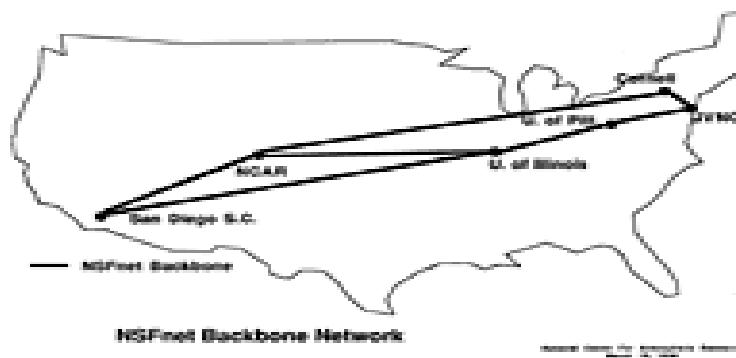
1982 DCA и ARPA налагат Transmission Control Protocol (TCP) и Internet Protocol (IP) познати като [TCP/IP](#) за стандартно ползване в ARPANET.

Това води до първите дефиниции на "интернет" като свързани мрежи, особено тези ползваващи TCP/IP, и "Интернет" като всички свързани TCP/IP интернети.

EUnet (European UNIX Network) е създаден от EUUG за осигуряване на email и USENET услуги. Мрежата е базирана на съществуващи връзки между Холандия, Дания, Швеция и Великобритания.

Exterior Gateway Protocol (RFC 827) спецификация. EGP се използва за входни точки между мрежите.

1984 Domain Name System ([DNS](#)) е въведена.

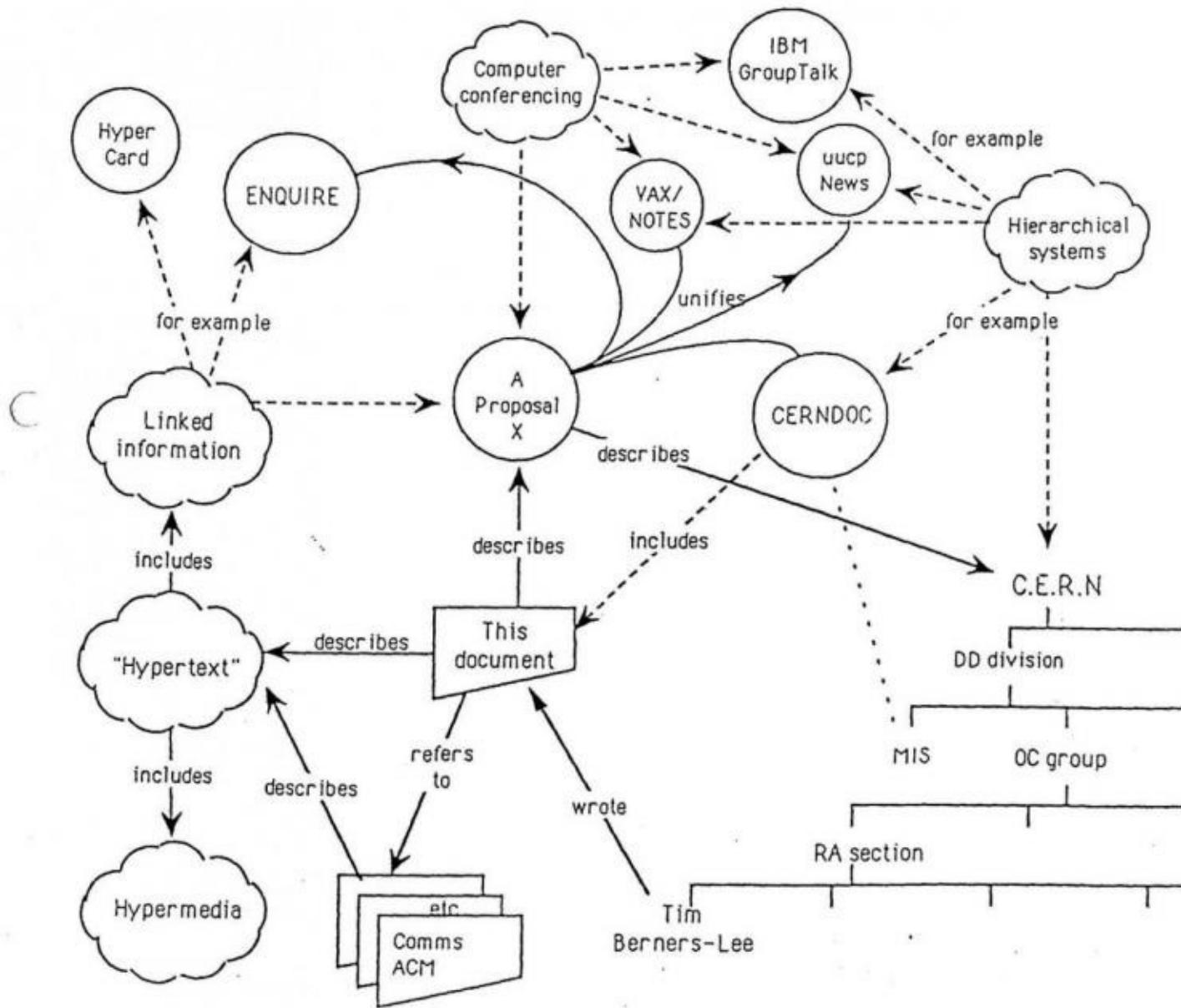


World Wide Web е родена в CERN през 1989

През март 1989 Tim Berners-Lee, работещ в CERN (European Organization for Nuclear Research), прави предложение за радикално нов начин за свързване и споделяне на информация по интернет.

Документът се нарича **Information Management: A Proposal (link is external)**. Така се ражда web.

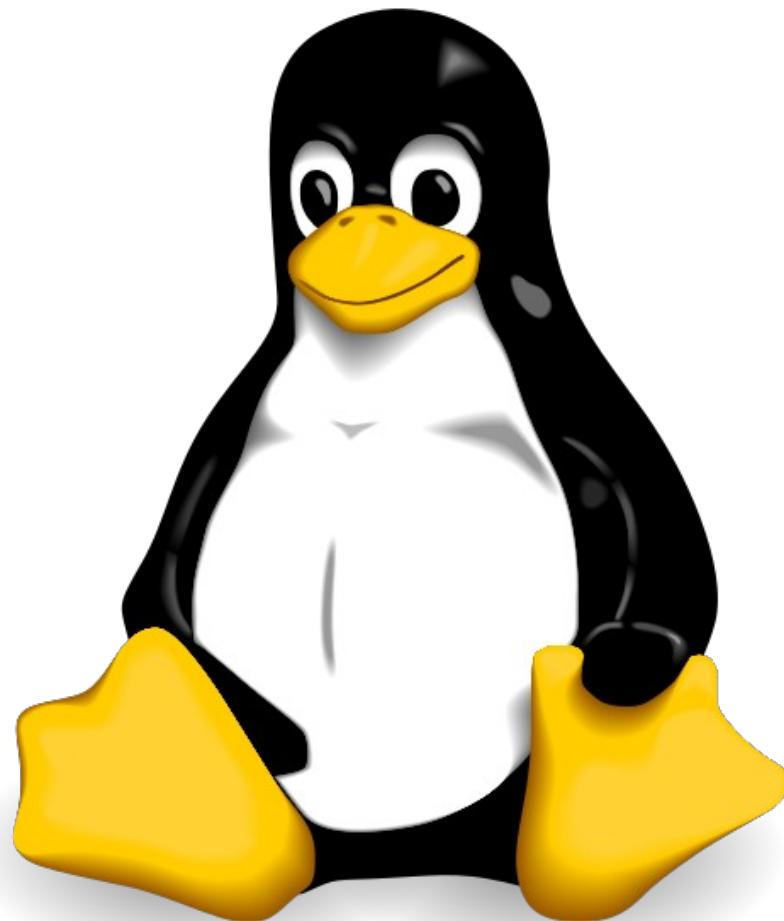
WWW в CERN през 1989



Linus Torvalds. Създателят на ядрото
на операционната система Linux.



Linux. Free and Open Source Software.
5 октомври 1991.



1980 - 1989

1985 На 15 Март Symbolics.com става първият регистриран домейн. Останалите първи: cmu.edu, purdue.edu, rice.edu, berkeley.edu, ucla.edu, rutgers.edu, bbn.com (24 Април); mit.edu (23 Май); think.com (24 Май); css.gov (Юни); mitre.org, .uk (Юли).

1986 **NSFNET** създаден със скорост от 56Kbps. NSF създава 5 центъра за суперкомпютърни изчисления и това позволява експлозия на връзките към Интернет, особено от университетите.

Network News Transfer Protocol (NNTP) е създаден за подобреие на предаването на Usenet новините по TCP/IP.

1980 - 1989

1987 Email връзка открита между Германия и Китай, първото съобщение изпратно от Китай на 20 Септември.

1988 2 Ноември - Интернет червей плъзва по Мрежата, засяга около 6000 от всички 60000 хоста в Интернет. CERT (Computer Emergency Response Team) е формиран от DARPA в отговор на инцидента с червея.

NSFNET гръбнакът е надграден до (1.544Mbps).

Internet Relay Chat (IRC) разработен от Jarkko Oikarinen.

1989 Над 100 000 хоста в Интернет. Австралия се свързва към NSFNET чрез Хавай на 23 Юни.

1990 ...

1998 IPv6 128-bit, RFC 2460

2000 Масивна атака за спиране на услугите ([Denial of Service](#)) е стартирана срещу главни уеб сайтове, включително Yahoo, Amazon, и eBay в началото на Февруари.

Размерът на световната мрежа преминава [1 милиард страници](#).

ASP (Active Server Pages), Napster (P2P технология)

Идващи технологии: безжички мрежови уреди, [IPv6](#) (2012)

Вируси на годината: Love Letter (Май)

Съдебни дела на годината: Napster, DeCSS

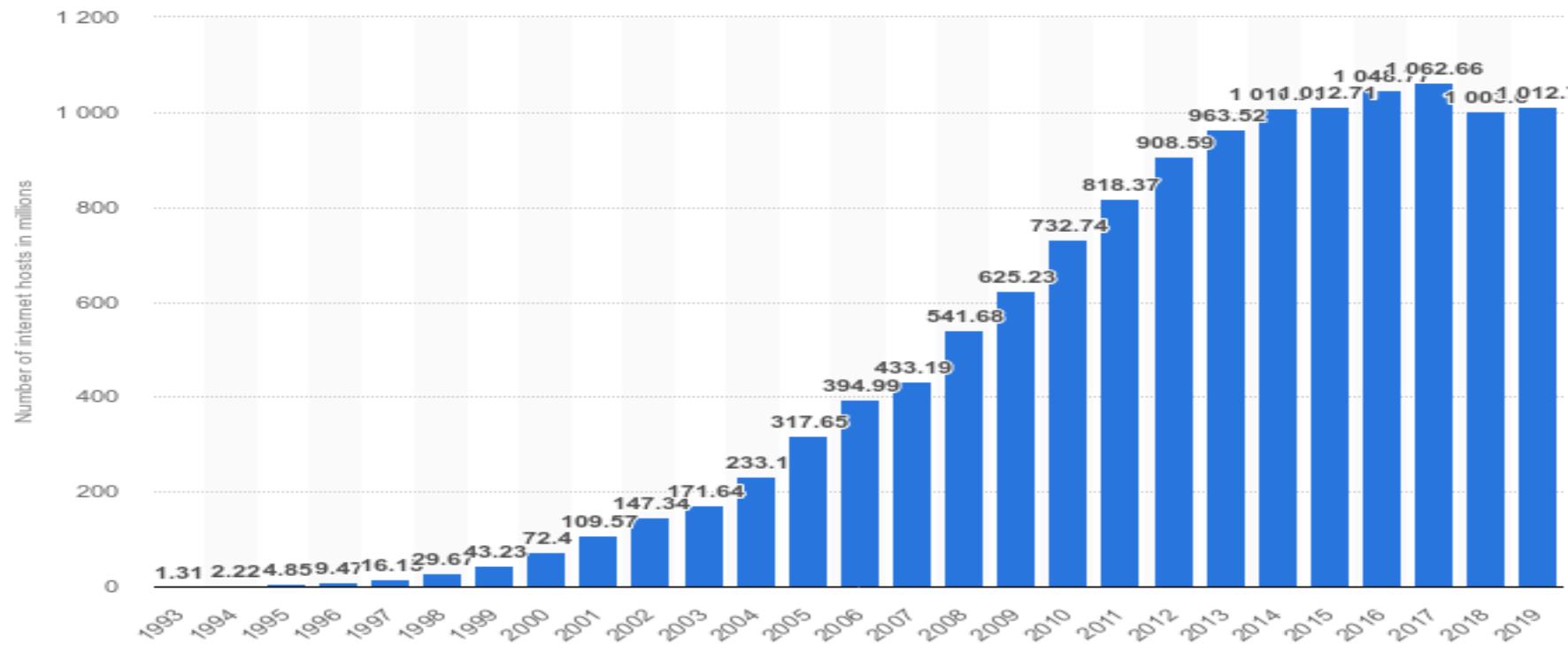
2001 Препращането на електронна поща става нелегално в Австралия след приемане на законът "Digital Agenda", тъй като то се гледа като техническо нарушаване на лични интелектуални права.

Домейните .biz и .info са добавени в DNS root сървъра на 27 Юни, възможни регистрации от Юли.

Червеят Code Red и вирусът Sircam проникват в хиляди уеб сървъри и сътв. пощенски кутии, причинявайки временна експлозия в трафика по Интернет и нарушенията на сигурността.

Интернет хостове към 2019

to 2019 (in millions)



Статистика от 1993 до 2019 г.

(<https://www.statista.com/statistics/264473/number-of-internet-hosts-in-the-domain-name-system/>)

През януари, 2019 имаме около 1.01×10^9 хоста.

Какво ще научим по-нататък

Що е то мрежа – компоненти, начин на свързване

Мрежа vs. разпределена система

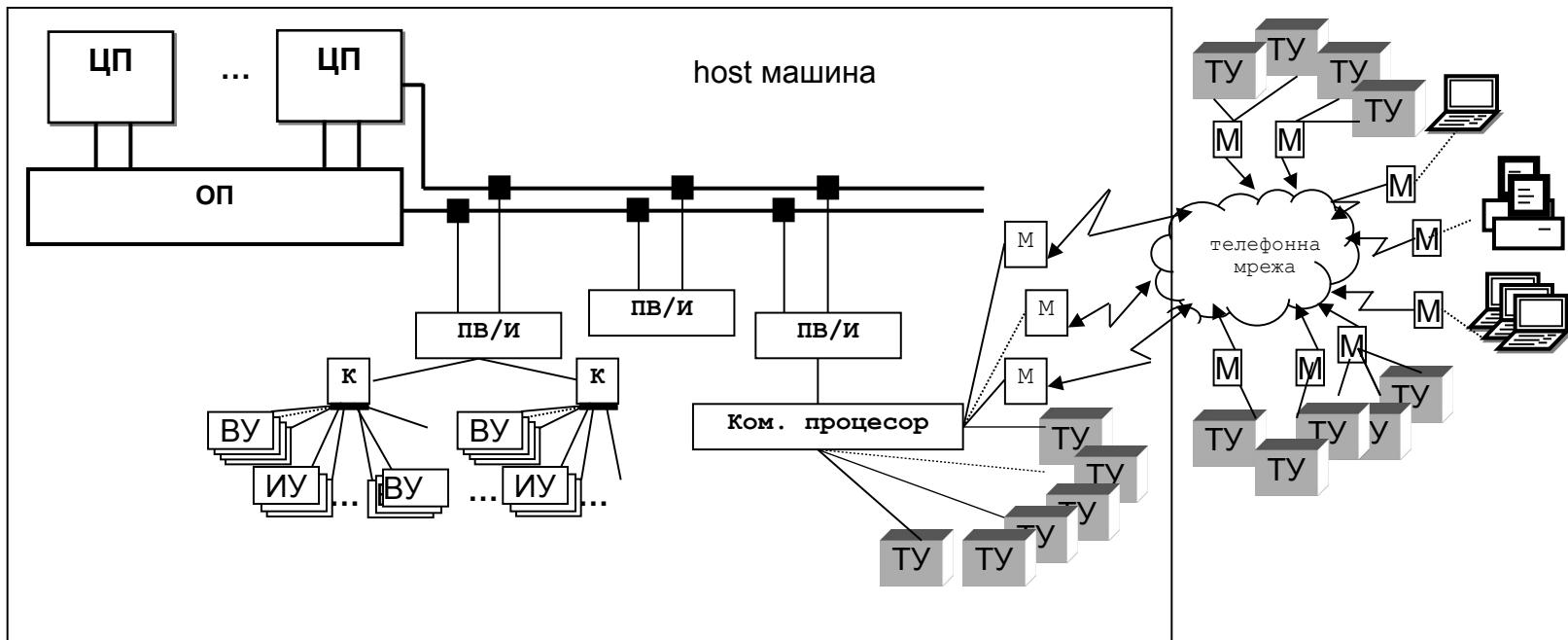
Видове мрежи според приложение, технологии, географски обхват и юридически права

Мрежови топологии

Мрежови стандарти

Терминални комплекси и мрежи

Предвестници – необходимостта от ефективен и удобен за потребителя достъп до ресурсите на тогавашните Големи машини (Mainframe). Йерархична структура.



Компютърни мрежи

Свързване на терминални мрежи помежду им – създаване на мрежи от компютри. Всеки потребител може да получи достъп до всяка приложна програма върху който и да е хост.

Терминалната мрежа е с йерархична структура с централизирано управление.

В компютърните мрежи имаме разпределение на управлението между съставящите я компоненти.

Компютърна мрежа – взаимно свързани чрез определена технология автономни машини.

Компютърна мрежа vs. Разпределена система

При Р.С. Връзката между компютрите е прозрачна за потребителя. Последният разглежда съвкупността от компютри като единна система (виртуални процесор, памет, дисково пространство).

К.М. – потребителят използва определена машина и управлява процеса на предаване на информация.

Общо между Р.С. и К.М. – пренос на файлове между няколко процесора.

Компютърни мрежи. Предпоставки за развитието.

През 1980-те години – персоналните компютри – голяма изчислителна мощност на бюрото. Възниква необходимост от тяхното свързване в рамките на една или повече сгради, достъп до обща Б.Д. или други изчислителни ресурси.

Оформят се:

на единия полюс - Глобална (**Global Network**) – огромни разстояния – обикновено се отнася за Internet ('Net)
на другия Локална (**Local Area Network**) – разстояние не повече от няколко километра. Ако свързва няколко сгради на ограничена територия: **Кампус мрежа**

(прод.) ...Предпоставки

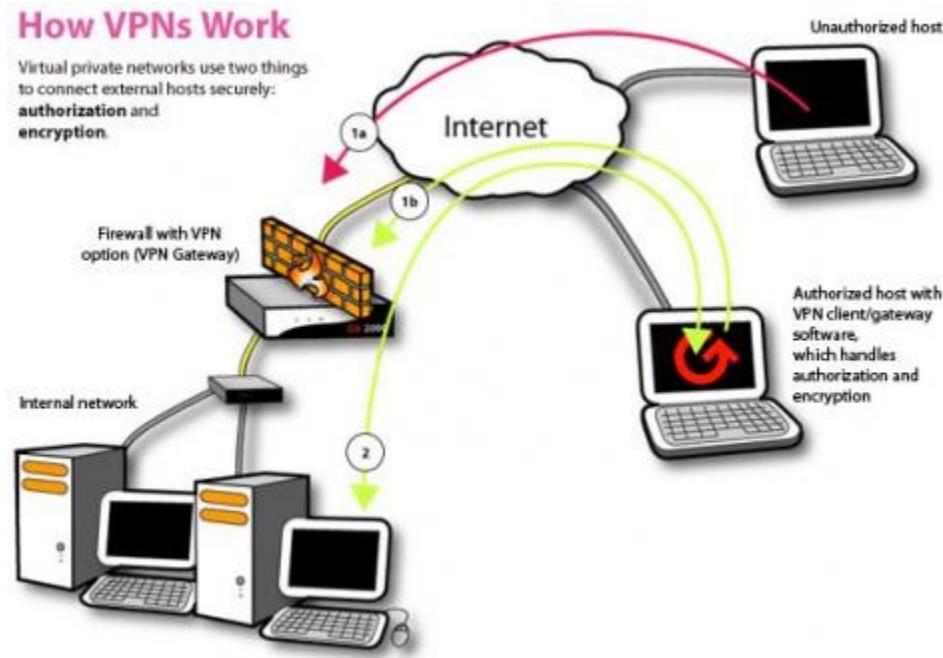
По "средата":

Градска (Metropolitan Area Network - MAN)

Регионална (Wide Area Network - WAN) – страна, континент; по-общо казано – външната връзка на една локална мрежа (напр. WAN порта на WiFi рутер)

Частна (Virtual Private Network - VPN) – защитени връзки – тунели (напр. криптиране) между офисите на една организация в рамките на публичната “Net.

VPN - пример



Класификация на мрежите

Основните типове мрежи се определят въз основа на две характеристики:

- Режим на предаване на данните;
- Физически размер на мрежата;
- Юридически права.

Видове мрежи според режима на предаване на данните

- Предаване до всички (общодостъпно – Broadcast). Прилага се при LAN. Общ комуникационен канал, който се разпределя между всички в мрежата. Пакети (съобщения) се получават от всички, но ги прочита този, който си познае адреса. Частен случай – групово предаване (multicast).
- Точка-точка (Point-to-point) – WAN мрежите се състоят от множество връзки “точка - точка” с произволна топология. Затова се налага маршрутизация – намиране на оптималния път.

Видове мрежи според физическия размер

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	
100 m	Building	Local area network
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	
1000 km	Continent	Wide area network
10,000 km	Planet	The Internet

PAN – многопроцесорна система

Юридически права

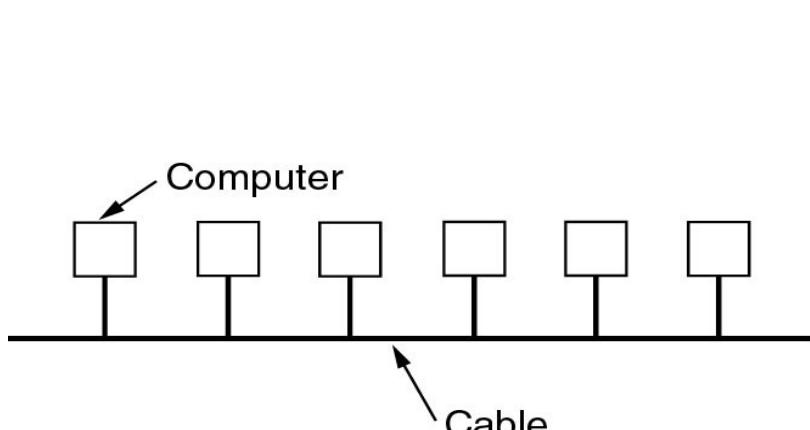
Имаме ли права върху земята, върху която се изгражда мрежата:

- **имаме**: локални, кампус мрежи – отговаряме за всичко – от кабели до приложения;
- **нямаме** (всички останали: MAN, WAN...), разчитаме на мрежов или телеком оператор.

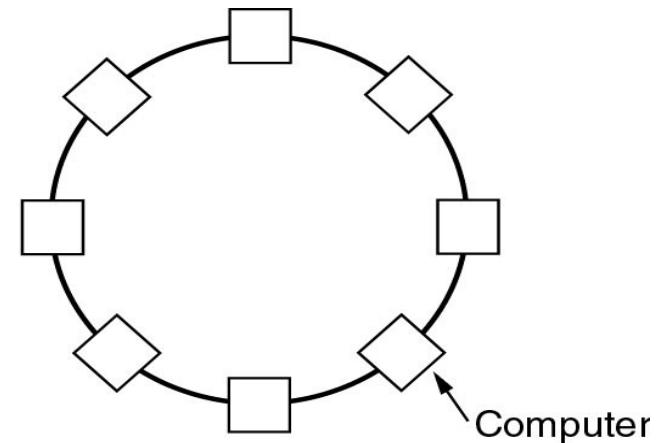
В днешно време това е **основния критерий**:

- имаме уеднаквяване (конвергенция) в скорости, технологии, напр. LAN и WAN портовете на WiFi рутерче – напълно еднакви.

Локални мрежи



(a)



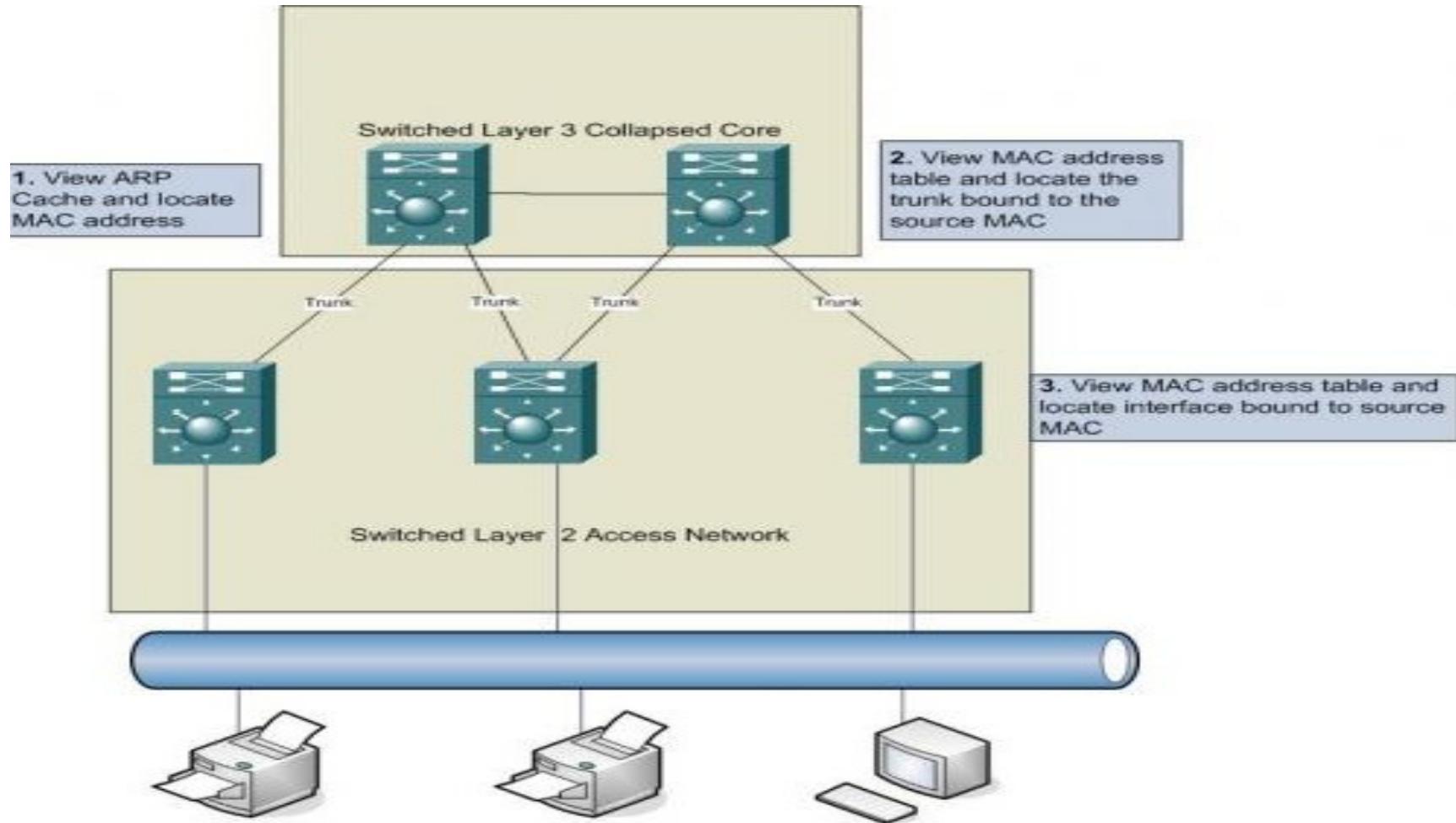
(b)

Старите локални мрежи (legacy LANs) бяха broadcast, с шинна (Bus) – Ethernet, или кръгова (Ring) – Token Ring, FDDI, топология (физическа и логическа).

Междинен етап Ethernet на база на хъбове (shared) с физическа топология “звезда”. TR и FDDI поради сложността им бяха изоставени (също имаха хъбове и суичове).

Съвременните мрежи Ethernet - **switched Ethernet**. Всяка станция има гарантирана скорост: 10, 100, 1000 Mbps, 10 Gbps. Логическата топология на практика е “всеки-с-всеки”.

Съвременна мрежа Ethernet



Metropolitan Area Networks (MAN)

MAN мрежата се състои от две основни части - опорна мрежа (backbone) и клиентски интерфейс.

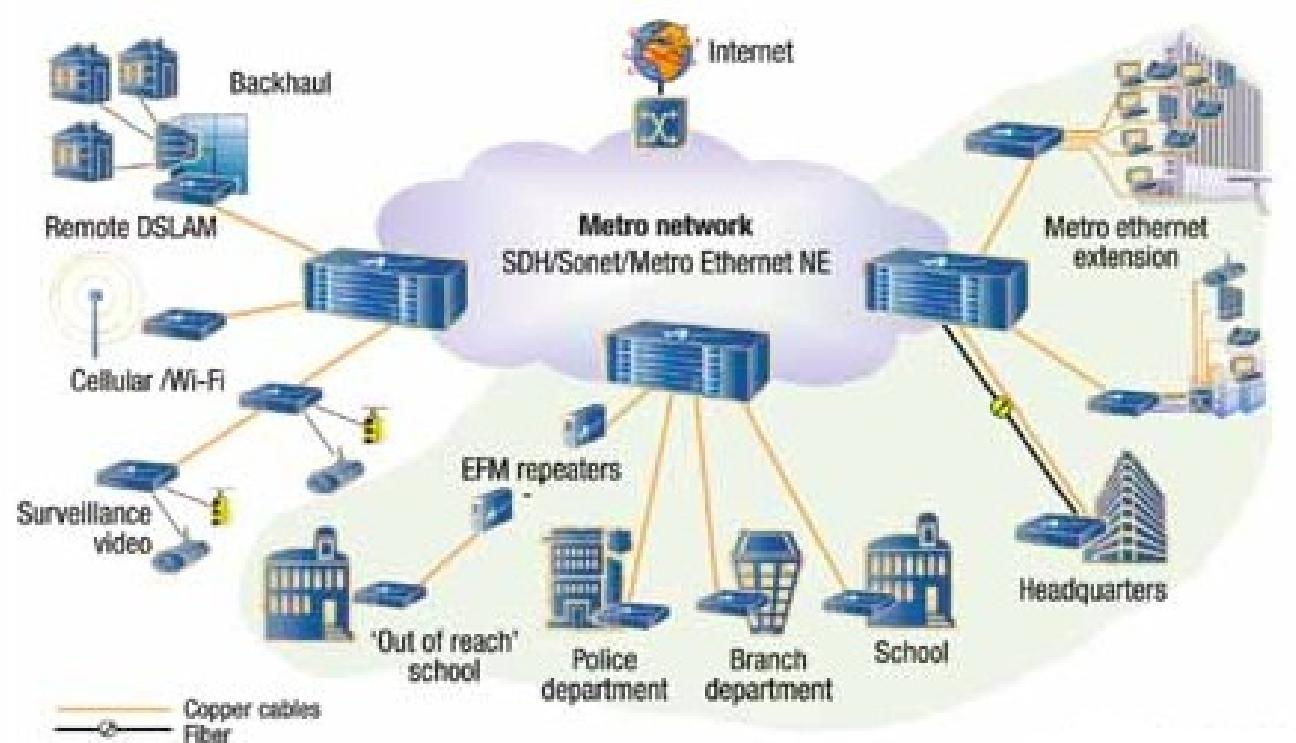
Съобщителна среда е оптически кабел. Използва инфраструктурата на телеком и кабелни оператори и технологията **switched Ethernet**. Затова се нарича още **Metro Ethernet**.

Топология - кръг, hub-and-spoke (звезда), напълно или частично свързана.

Опорната мрежа представлява набор от точки за достъп (POP - point of presence), в които има комутатори (на 2 и 3 слой) и/или маршрутизатори, свързани помежду си с високоскоростни връзки.

Клиентският интерфейс представлява оптичен кабел, прокаран между абоната и най-близката точка за достъп. За да се осъществи връзка между два или повече абонатни поста, в опорната мрежа се конфигурира виртуална локална мрежа (VLAN). Тъй като връзките в опорната мрежа са резервирани, MAN-връзката е дори по-надеждна от директен кабел (dark fiber), положен между две точки.

MAN



Глобални (рег.) мрежи - Wide Area Networks (WAN)

Обхватват широки географски области – страни, континенти... планета (Internet)... Галактика

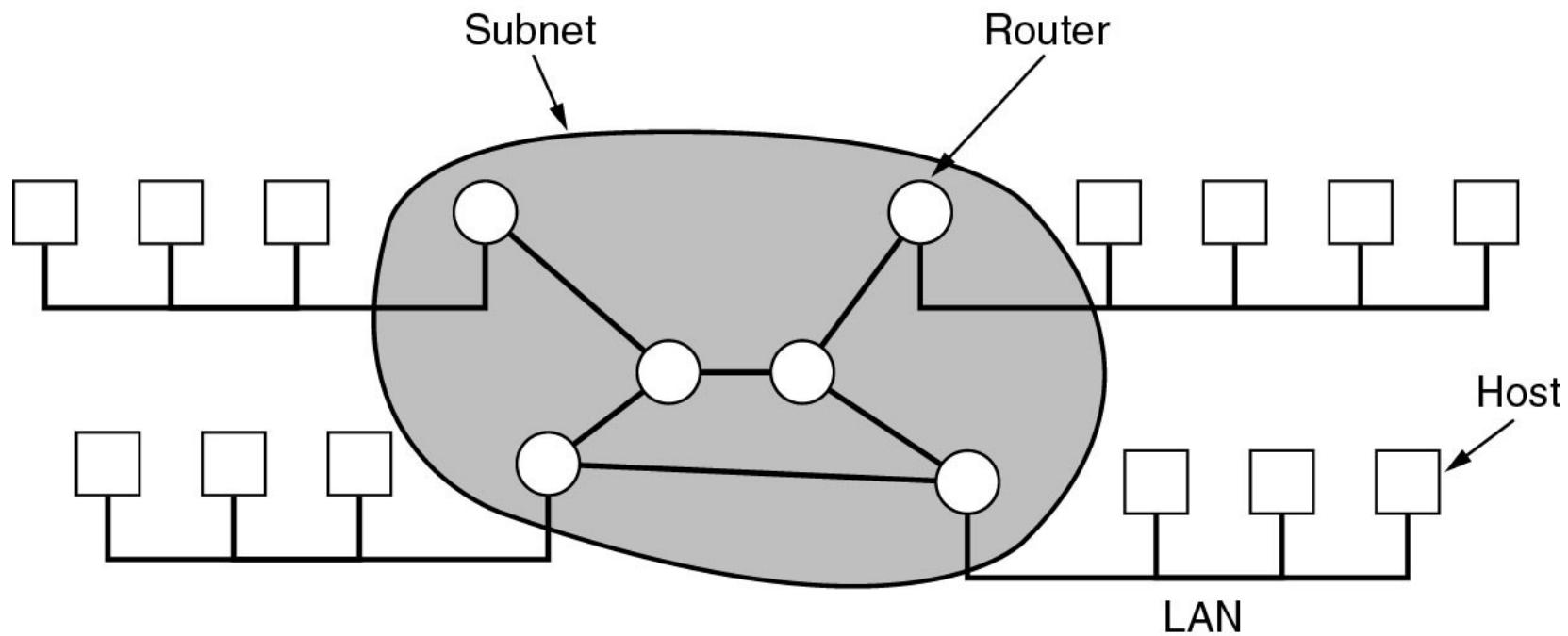
Хостове или LANs се свързват с помощта на комуникационна мрежа – собственост на телеком или I(Network)SP.

Комуникационна мрежа – състои се от предавателни линии (точка-точка), които свързват по 2 комуникационни устройства за маршрутизация и превключване (routers, L2&3 switches).

Линии - медни кабели (Cu); оптически влакна (Fiber Optics – FO), вече преобладават; безжични – радиорелейни и сателитни - (Wi)reless.

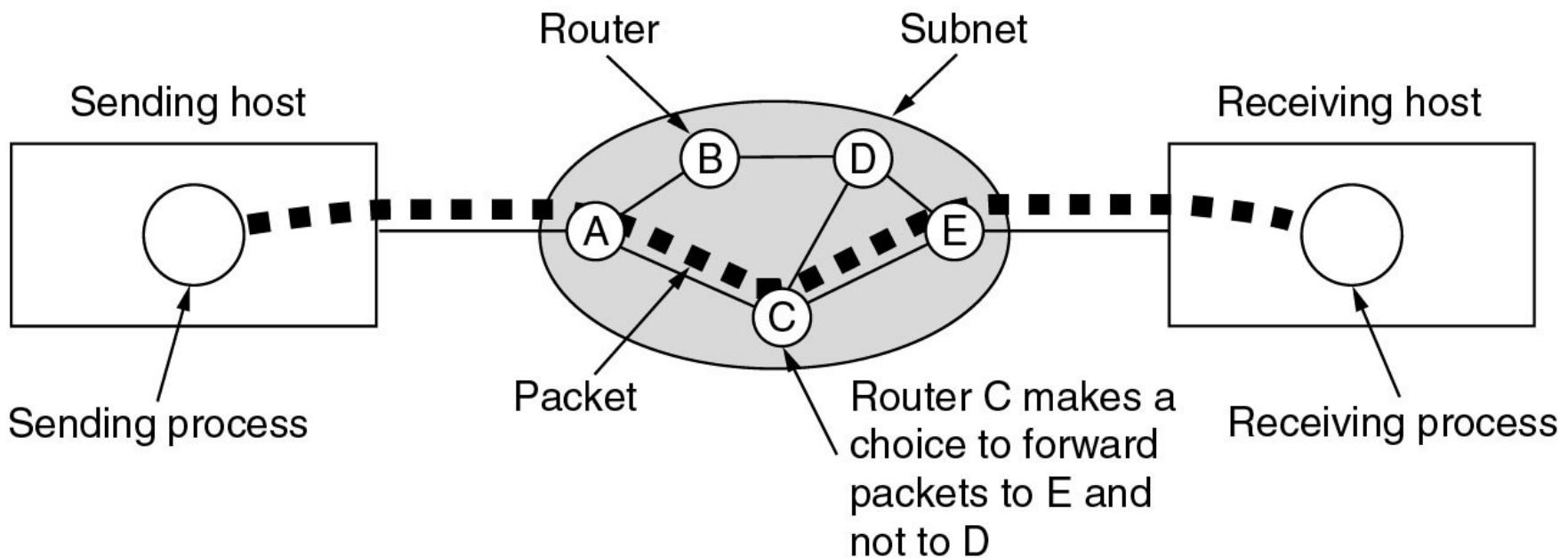
Комуникационни устройства – с два или повече интерфейси към съответни линии. Приема пакет на даден интерфейс, взема решение по коя линия да го препрати и го превключва към изходящ интерфейс (линия). Т.е...

WAN



WAN свързва хостове и LANs.

WAN



Изпращане на последователност от пакети от подател към получател. Не е задължително всички да минат по пътя ACE. Маршрутизаторите вземат решения.

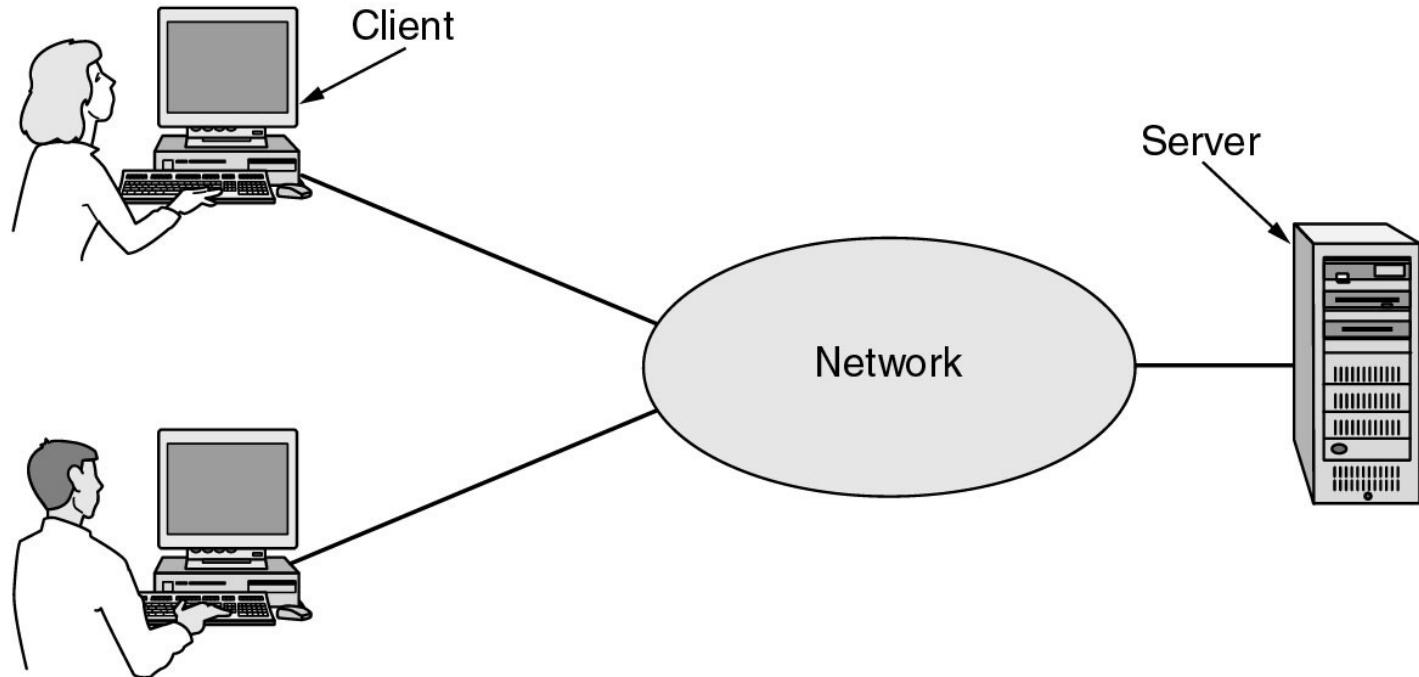
Модел Клиент-Сървър

Разпределено използване на ресурсите – напр. обща Б.Д. или общ принтер (скъпо удоволствие за всяко бюро, даже inkjet от 100 лв., но скъп консуматив)

Обща Б.Д. – на по-мощен компютър – **сървър** със системен администратор. Служителите достъпват до него от по-маломощни машини – **клиенти**. Или Web сървър (машина с **Apache**) – web клиент (PC с **браузър**).

Два основни процеса: на клиента и на сървъра.

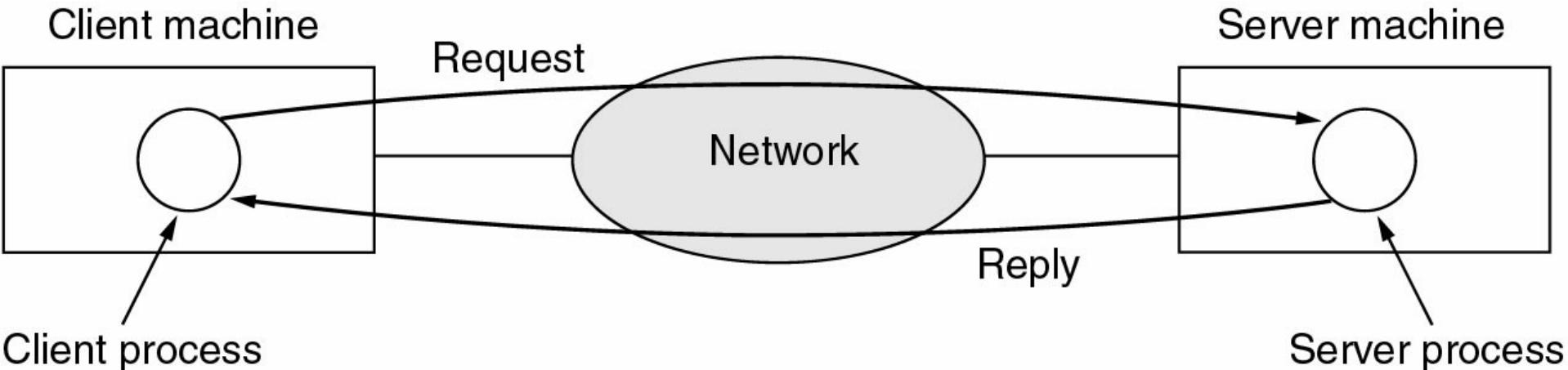
Модел Клиент-Сървър



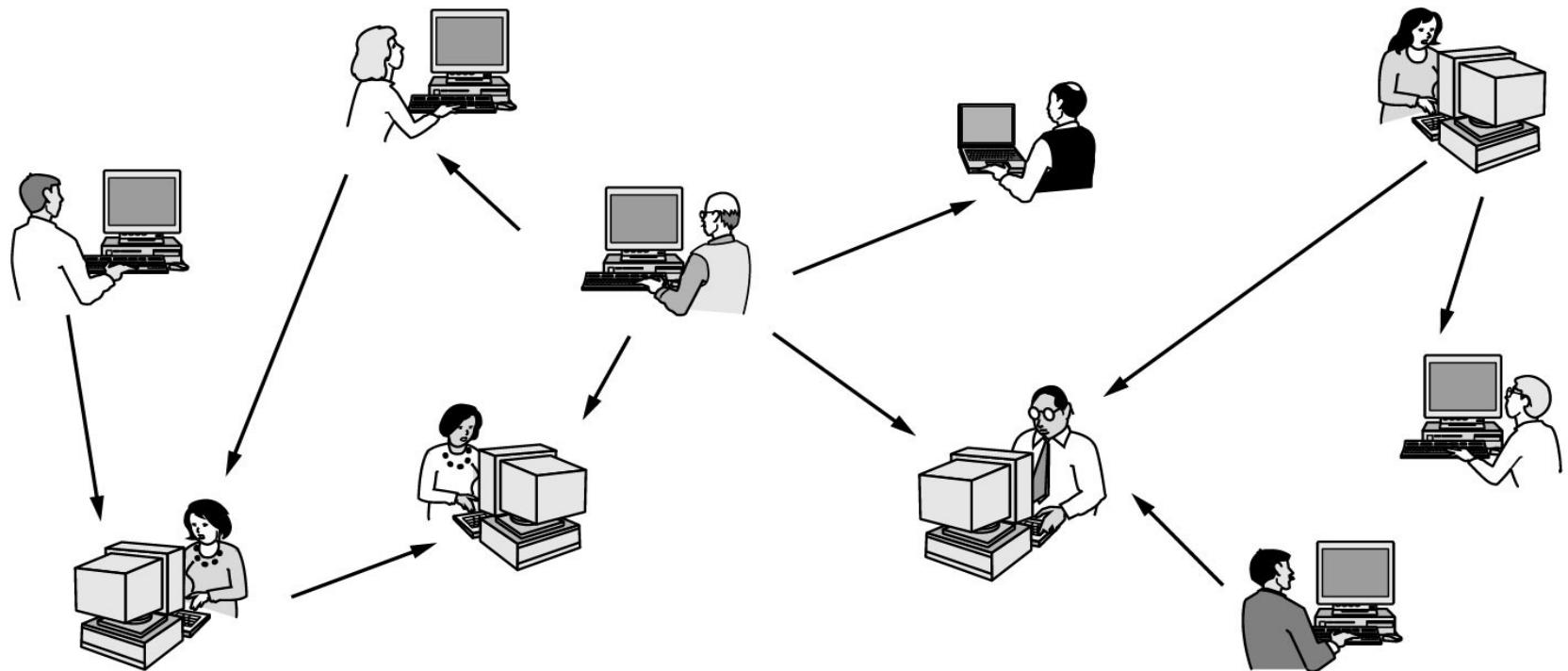
Мрежа от два клиента и един сървър

Модел Клиент-Сървър

- Клиентският процес изпраща заявка (request) до сървърския процес, който след съответната обработка връща отговор до клиента.
- Обменът на данните между клиент-сървър – по протокол. Това е набор от правила и съответни действия, които се извършват, за да се осъществи обмена.



Система с равностойни машини

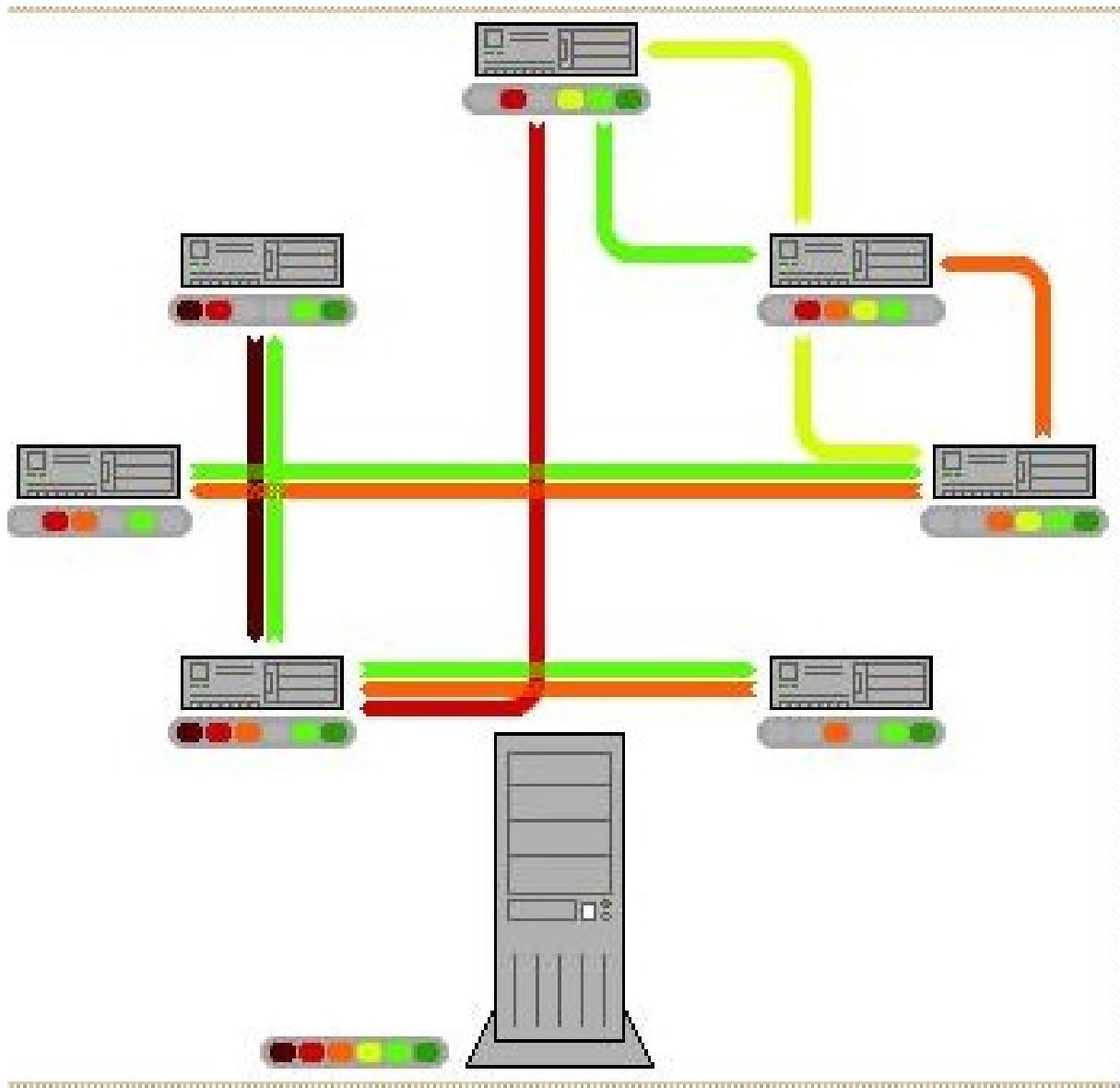


Или **peer-to-peer (P2P)** - няма фиксирани клиенти и сървъри.

Напр. File Sharing (споделяне на файлове) между Windows машини.

BitTorrent - P2P file sharing протокол за разпространение на големи обеми от данни (най-вече филми).

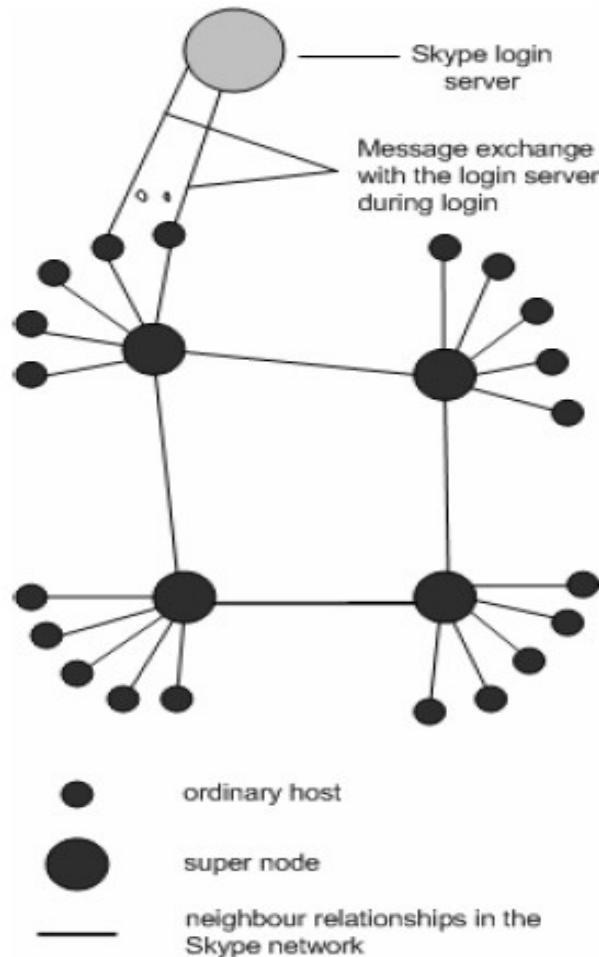
BitTorrent



Skype Peer-to-Peer Internet Telephony Protocol

С изключение на сървъра за първоначална аутентикация, няма друг централен сървър в Skype.

Skype използва 256-битово AES (Advanced Encryption Standard) криптиране.



Използване на компютърните мрежи

Бизнес приложения – електронна поща, е-
търговия, Б. Д.

Домашни приложения

Мобилни потребители

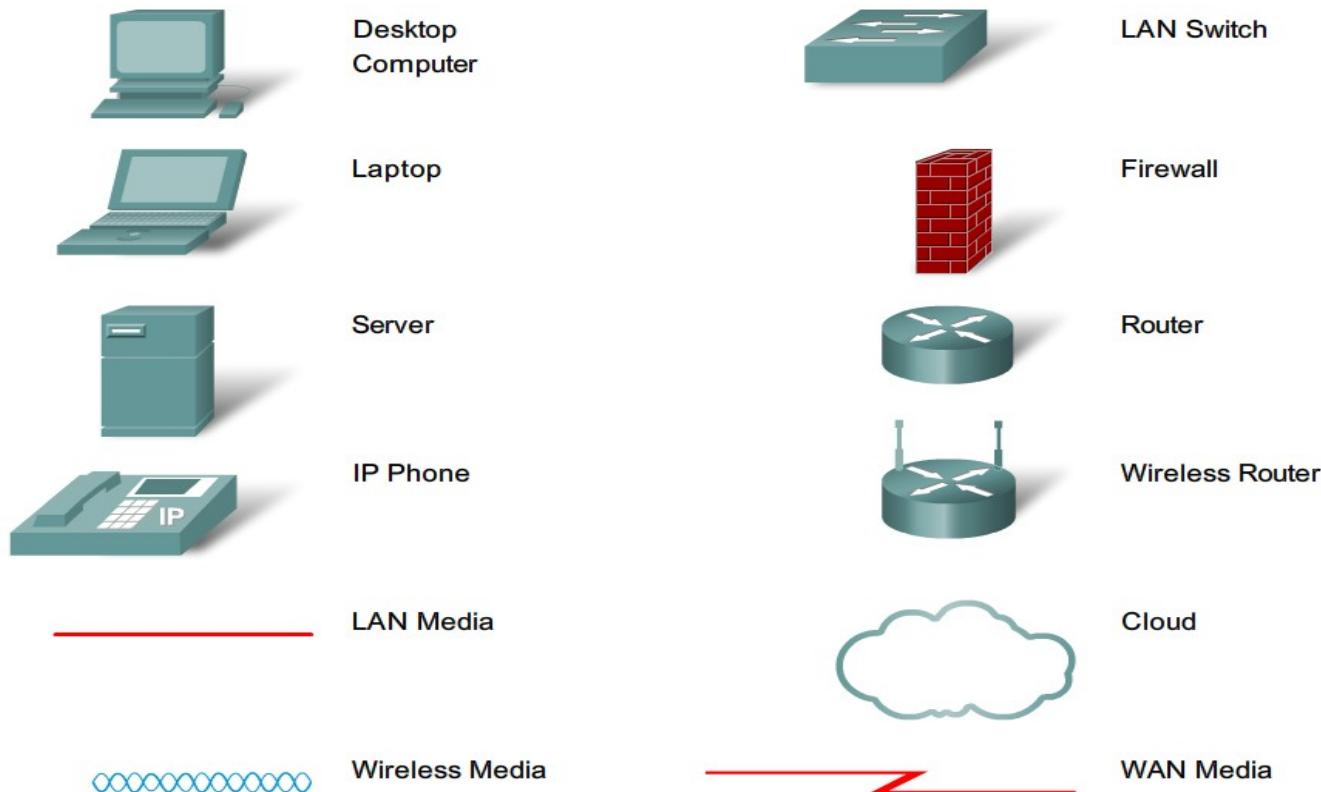
Социални аспекти – каква информация се
разпространява: вярна – невярна, цензура-
нецензурна, права на човека, етика в
отношенията, авторски права, атаки (DoS,
DDoS), хакери (остават скрити) и кракери
(извеждат системата от строя), phishing

Е-търговия

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books on-line
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products on-line
P2P	Peer-to-peer	File sharing

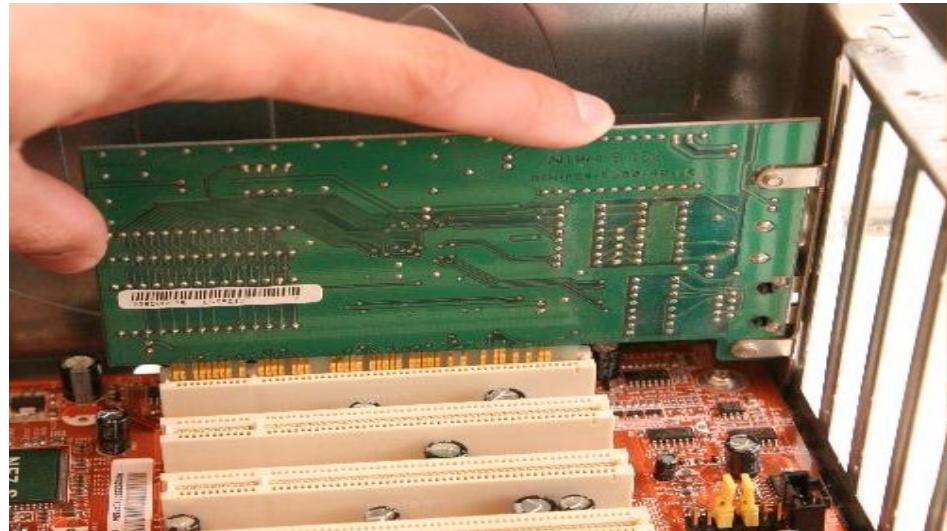
G2G – подписано споразумение по електронен път между президента Клинтън на САЩ и министър-председателя на Ирландия

Мрежов хардуер



Мрежов хардуер - адаптери

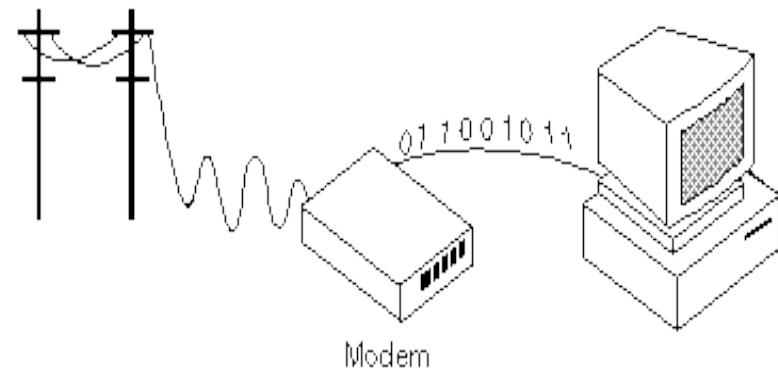
- PCI карта
- USB адаптер



Мрежов хардуер – модеми (история)

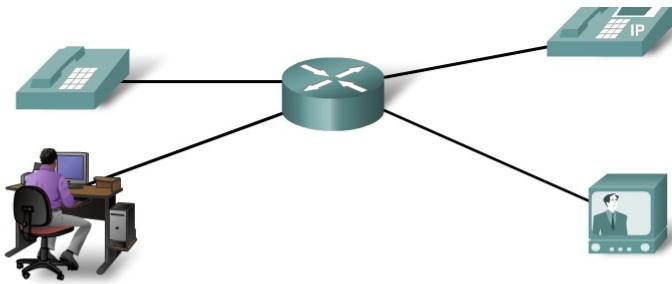
- **модулатор-демодулатор.**

Устройство, което позволява на компютъра да предава цифрови данни по аналогова (dial-up) или цифрова (DSL) телефонна линия.



Мрежов хардуер – съобщителни среди

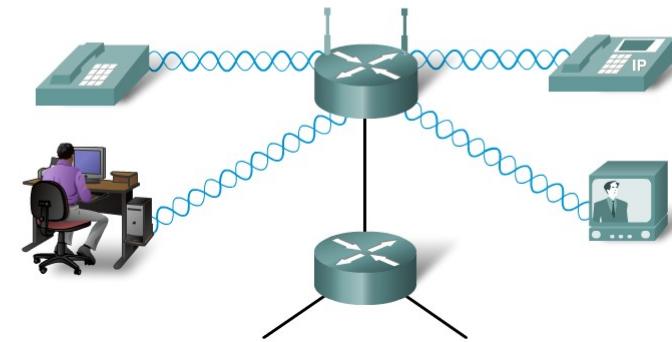
Wired networks used physical cables to connect devices.



Wireless networks use radio waves to communicate between devices.



Wireless networks are also connected to wired networks, at some point.



Жични – UTP, S(F)TP, коаксиални и далекосъобщителни медни и оптически (Fiber Optic - FO) кабели

Безжични среди - ефира

Топология на мрежата

Топология (от гръцки **τόπος**, "място", и **λόγος**, "учение") е област от математиката, която изучава форми и пространства.

Най-основните свойства на пространството - свързаност, непрекъснатост и граница.

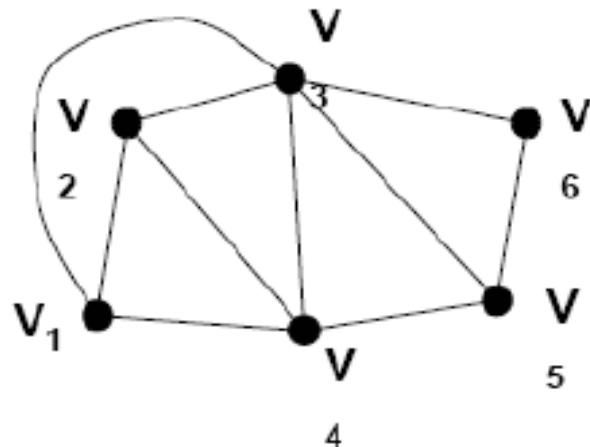
Топологията бива геометрична и алебрична - прилага теорията на множествата.

Ние обаче в компютърните мрежи говорим за топология, изхождайки от **теорията на графиките**.

Граф и мрежа

Графът е абстрактна структура, която представя връзките между отделните елементи на дадено множество.

Всеки член на това множество се нарича **връх** (**vertex**), а връзката между два върха се нарича **ребро** (**edge**).



Граф и мрежа

В практиката чрез графите се представят модели на реални обекти. Всред класическите примери са:

- **транспортна мрежа** — претеглен граф, където върховете изобразяват селищата, а свързващите ги ребра — пътищата между тях. Теглото на всяко ребро ще представлява дължината на пътя.
- **компютърна мрежа** — компютрите (върхове) и свързващите ги информационни канали (ребра).

Мрежови топологии

Три основни категории мрежови топологии:
физически, сигнални, логически

Физическата определя геометричното свързване
на физическите канали

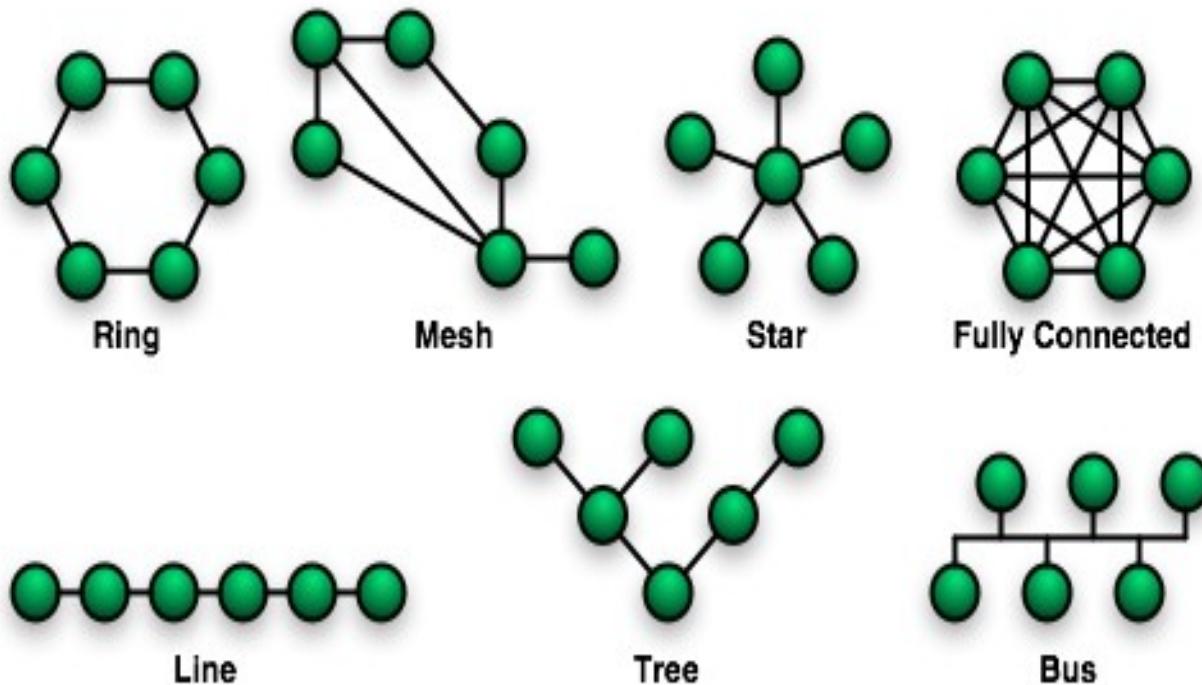
Сигналната отразява свързването между възлите
в мрежата от гледна точка на пътя на сигналите.
Често се смесва логическата топология, но тук
говорим конкретно за електрическите
(оптически) сигнали, а не за данни.

Мрежови топологии

Логическата отразява свързването между възлите в мрежата от гледна точка на пътя на данните. Определя се от **мрежовите протоколи**, т.е от това на **кой слой от мрежовата архитектура** (вж. следващата презентация) се осъществява комуникацията.

Пример: моделът **клиент-сървър** има логическа топология „**звезда**“ на приложен слой, на физическо е с произволна топология.

Видове топологии



Видове топологии

Централизирана (star) изиска всички абонати да имат връзка с централния възел, за да комуникират помежду си. Пример, физическа топология на локална мрежа в зала или на етаж, логическа – система клиент-сървър.

Дърводидната (tree, extended star) се прилага в структурните каблени системи (СКС) при изграждане на локални мрежи в сгради и кампуси (в този случай имаме *гора*).

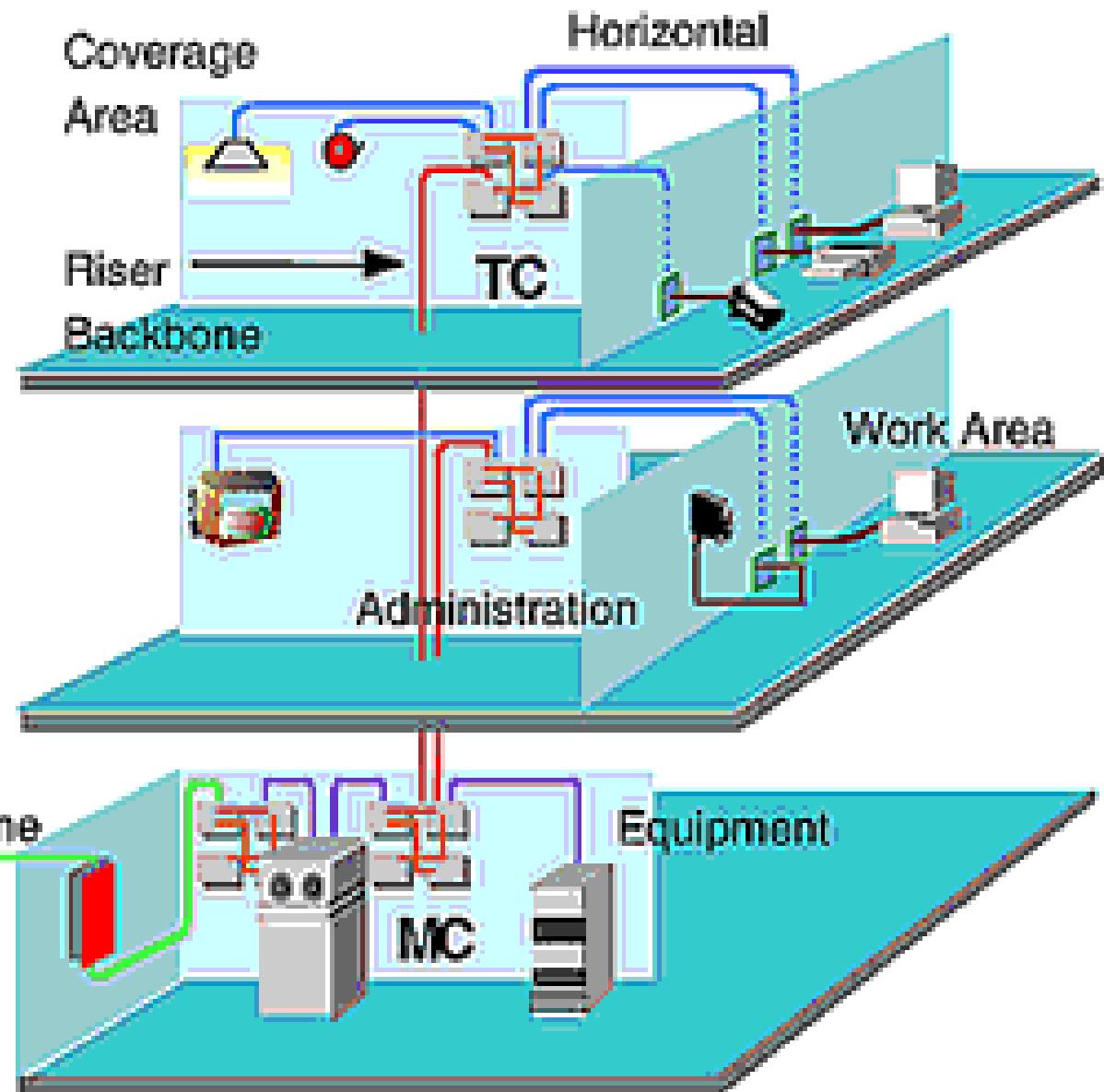
Кръгова (ring) – възлите са свързани в кръг. Пример: логическата топология на LAN Token Ring и FDDI, но физическата топология може да бъде звезда (централен възел MAU в IBM TR) или шина (3Com TR).

Частична или пълна свързаност (Mesh, Fully Mesh-Connected) – физически това са топологии на WAN мрежи, в общия случай Internet. Логическа: Peer-to-peer мрежа.

Шинна (bus) прилага се в LAN Ethernet (логическа). Първите реализации с коаксиален кабел физическата топология съвпадаше. В днешно време на UTP кабели имаме звезда и дърво.

Пример СКС (extended star)

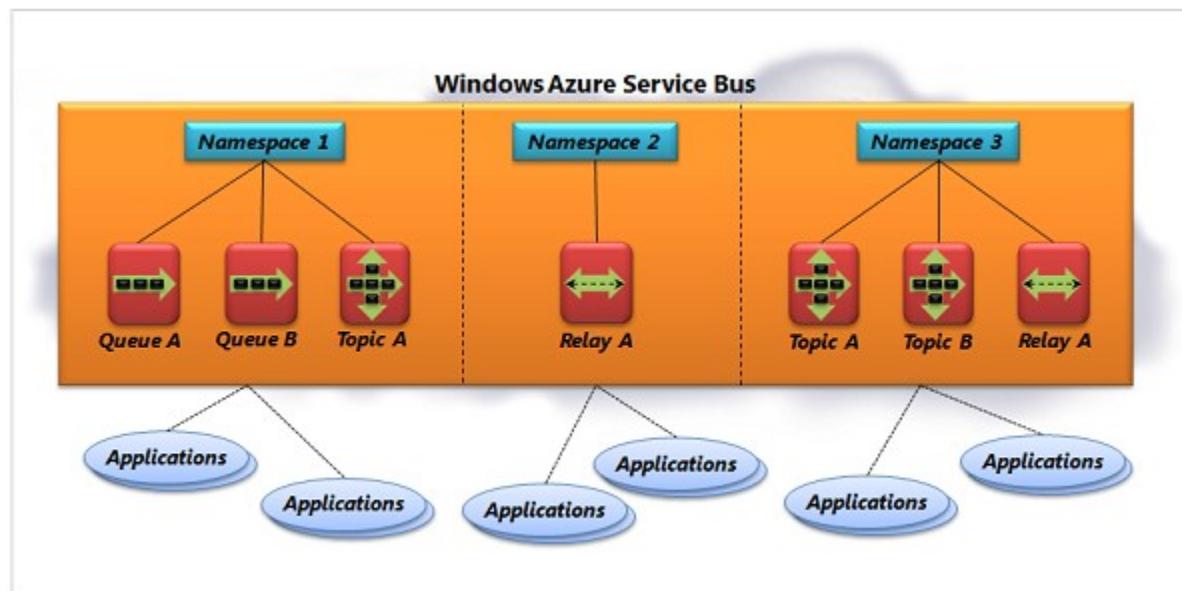
Structured Cabling Subsystems



Service Bus (шина на услугите)

Service Bus е облачна услуга, споделяна от много потребители.

(<https://azure.microsoft.com/en-us/documentation/articles/service-bus-fundamentals-hybrid-solutions/>)



Мрежови Стандарти

International Organization for Standardization (ISO) за международни стандарти. В нея влизат национални организации. **ISO/IEC Joint Technical Committee 1.** (International Electrotechnical Commission). Стандарти в областта на ИТ.

ITU (Международен съюз по телекомуникации), бивш **CCITT** Занимава се с развитие и стандартизация в областта на радио- и телекомуникациите.

Примери:

- V.35 – синхронни комуникации;
- V.92 – асинхронни (dial-up) модеми;
- X.400 (ISO/IEC 10021) – обмен на електронни съобщения;
- X.500 (ISO/IEC 9594-1) – директорийни услуги;
- X.509 (ISO/IEC 9594-8) – public key infrastructure (PKI), сертификати.

Стандарти на IEEE 802

Number	Topic
802.1	Overview and architecture of LANs
802.2 ↓	Logical link control
802.3 *	Ethernet
802.4 ↓	Token bus (was briefly used in manufacturing plants)
802.5	Token ring (IBM's entry into the LAN world)
802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 †	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
802.11 *	Wireless LANs
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number. Nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
802.15 *	Personal area networks (Bluetooth)
802.16 *	Broadband wireless
802.17	Resilient packet ring

Работните групи на 802. Най-важните *.
Отмиращите са ↓.

IETF и RFC

Internet Activities Board (**IAB** - RFC 1160) включващ два подкомитета: изследователски – **IRTF** (Internet Research Task Force - <https://irtf.org/>) и законодателен – **IETF** (Internet Engineering Task Force)

Internet Engineering Task Force (IETF - www.ietf.org) е отворена международна общност от мрежови проектанти, оператори, производители и изследователи, които се занимават с развитието на Internet архитектурата и експлоатацията.

Дейността на IETF се осъществява от **работни групи**, разпределени по тематики – маршрутизация, транспорт, сигурност и др.

Request for Comments (RFC) е меморандум, публикуван от IETF (www.ietf.org/rfc.html), който описва методи, поведения, проучвания или иновации, приложими към работата на Internet и свързани с нея системи.

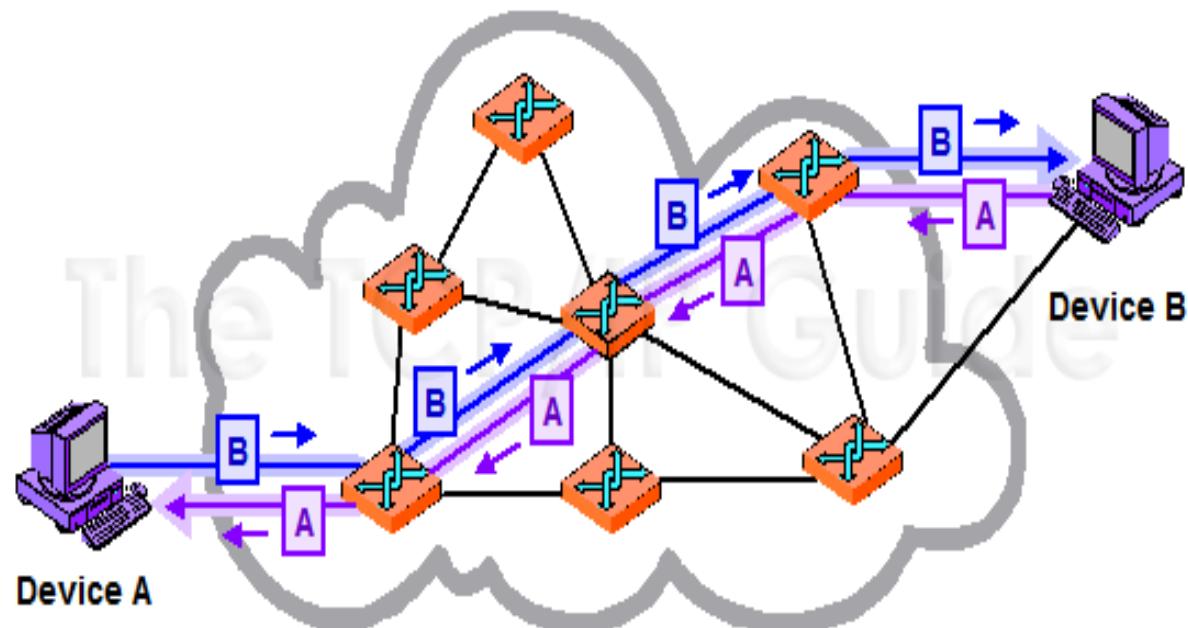
Предаване на съобщения в компютърните мрежи

Междупотребителите в мрежата информацията се обменя на части – съобщения.

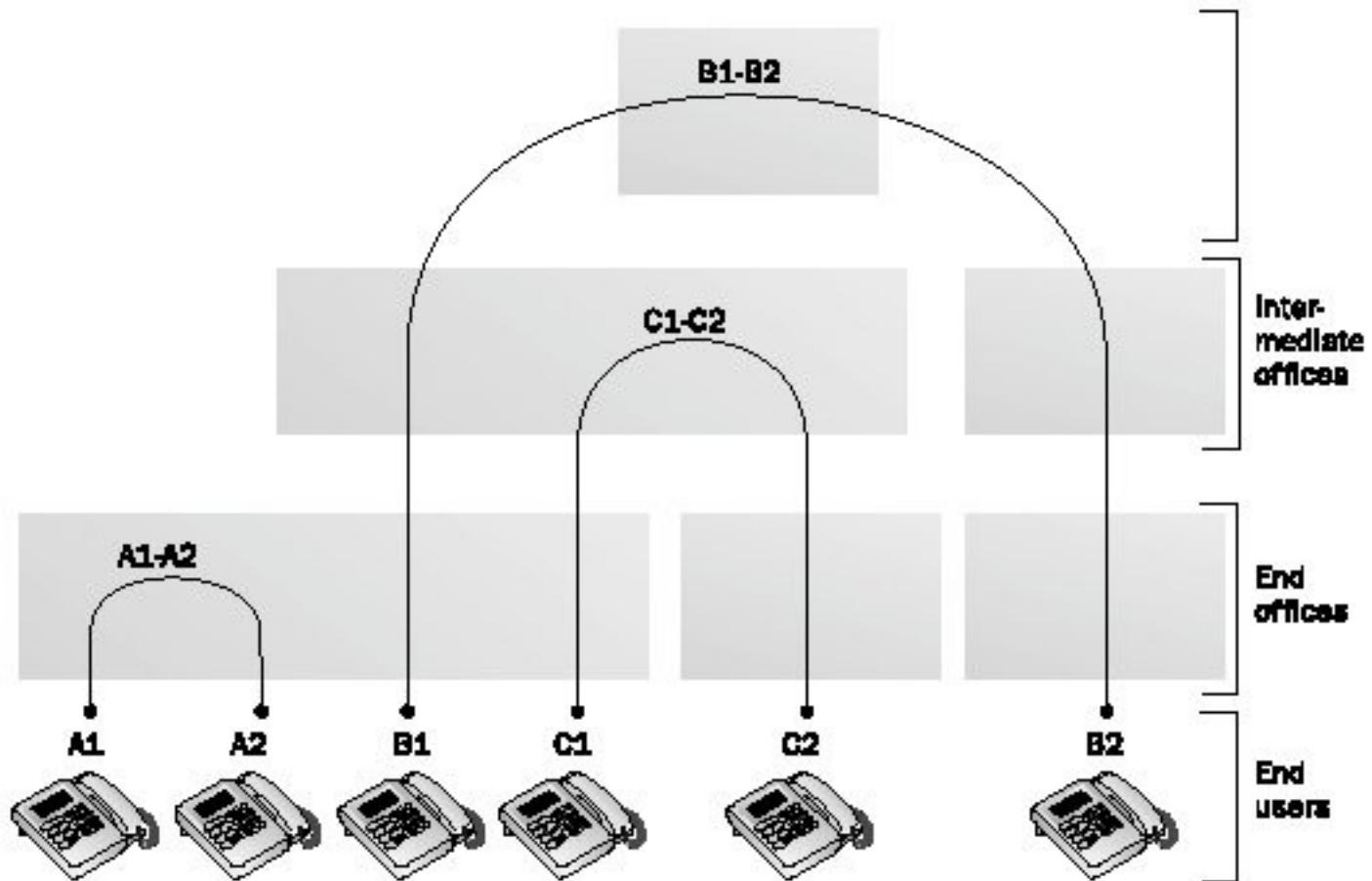
В зависимост от начина на предаване на съобщенията от подател до получател (източник-приемник):

- Комутация на канали;
- Комутация на съобщения;
- Комутация на пакети.

Комутиация на канали

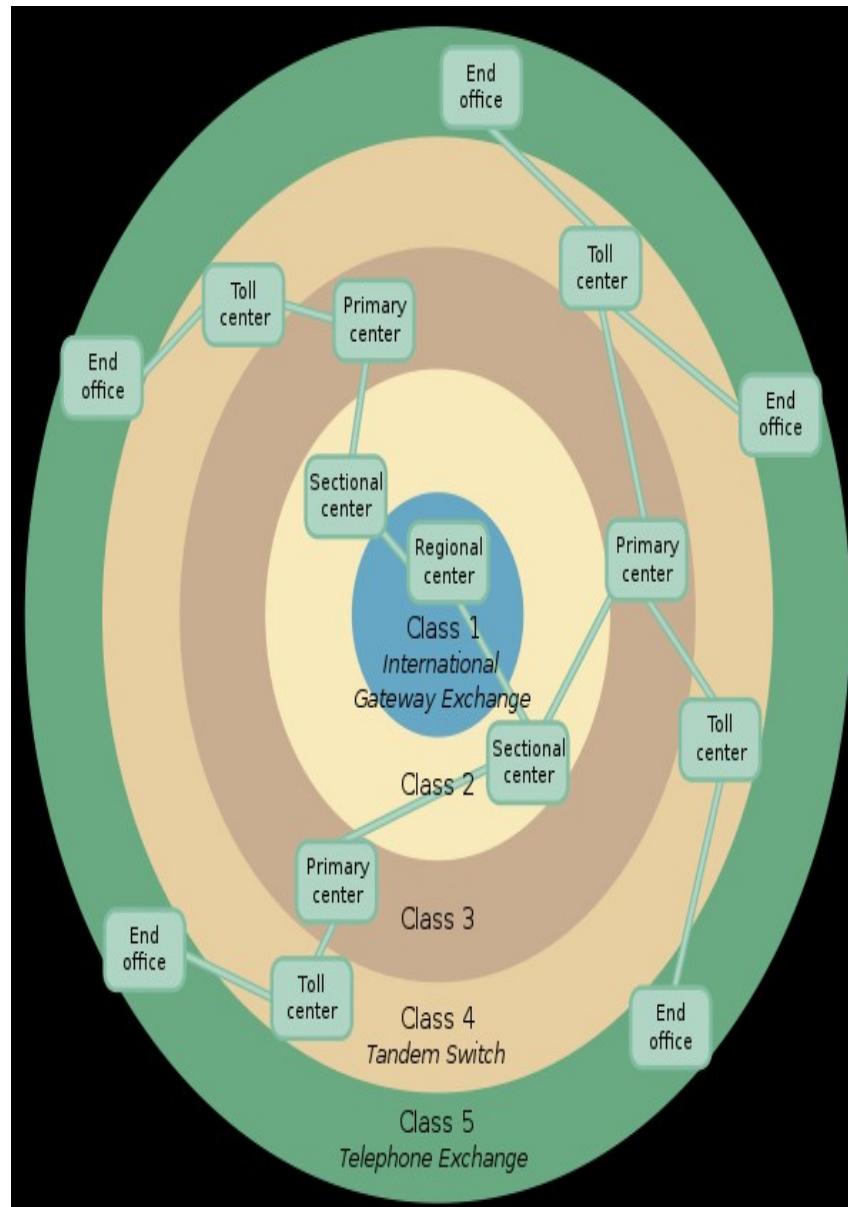


Комутиация на канали



Комутиация на канали

- Установява се физически канал между източник и приемник, по който се предава едно съобщение.
- След предаване на съобщението източникът освобождава канала.
- Подобен принцип в телефонните мрежи. След набиране на номера се нашракват релета (електромеханични или електронни) в централите по пътя до набираната страна. Така се изгражда канал между говорещите, който стои до разпадане на връзката – поставяне на слушалката върху вилката.



Комутиация на съобщения

Всяко съобщение за предаване се изпраща в комуникационната мрежа, която определя маршрута му до местоназначението (destination). Изиска повече буферна памет в маршрутизаторите, които да съхраняват дългите съобщения, докато се освободи изходяща линия. Неефективно, затова...

Комутиация на пакети (Paul Baran)

Мрежа с **комутация на пакети (packet-switched)**. Съобщение при подателя се разделя на сегменти с поредни номера (от 1500 байта до 8000+ при бързите мрежи >1 Gbps).

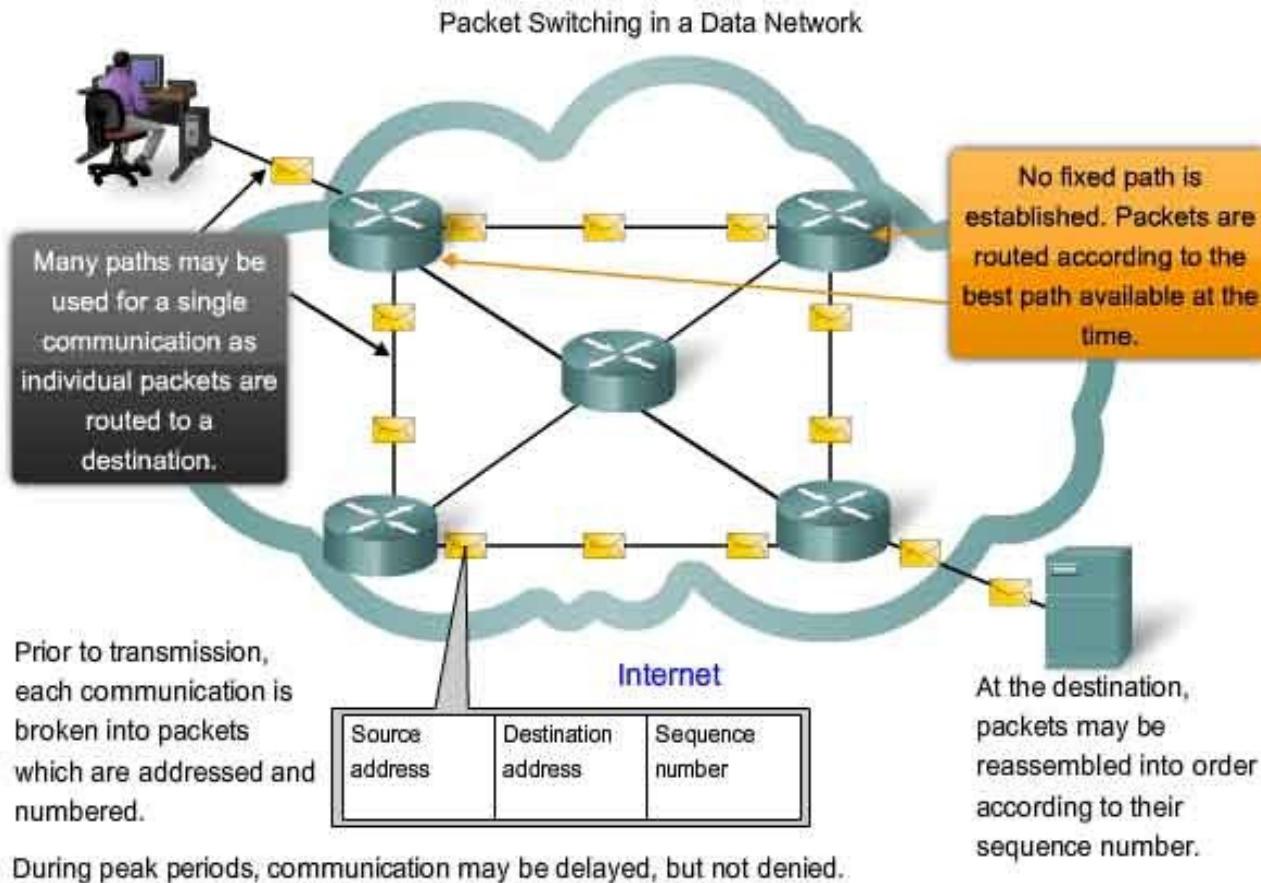
Последните се опаковат като пакети и “пътуват” самостоятелно до получателя, където става възстановяване на оригиналното съобщение (реасемблиране).

Обменът между възлите е по-бърз, по-добро уплътняване на каналите

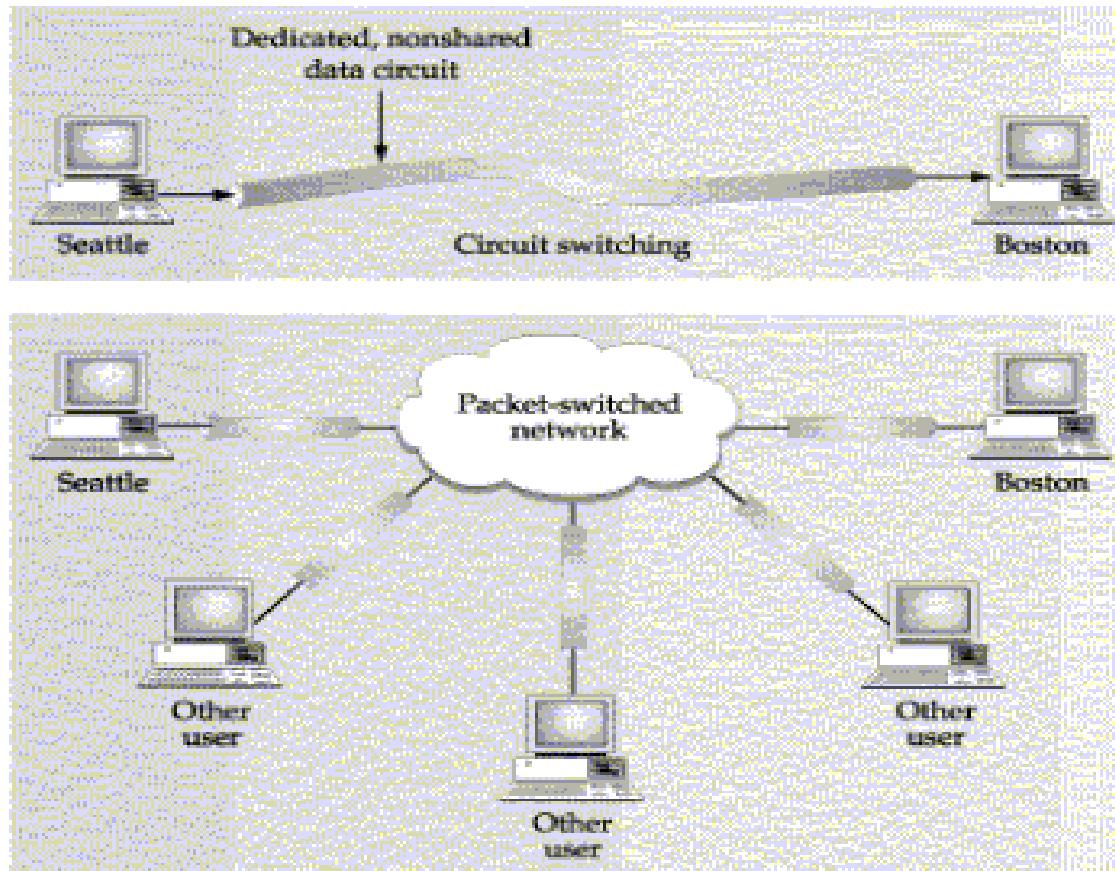
Всеки пакет с адрес на местоназначението и вътре в частта за данни има номер на сегмента от съобщението. Така се възстановява оригиналното съобщение.

Флаш демо: <https://www.youtube.com/watch?v=vSlcoQowe9I>

Комутиация на пакети (пример)



Комутиация на пакети vs. канали



Еталонен модел на мрежите

Характеристики на нивата.
Модел TCP/IP.

Какво ще научим

Зашо е избрана слоеста архитектура. Какво печелим.

Понятие за услуги, интерфейси, прозрачност.
Модел на ISO и модел TCP/IP.

Слоестата архитектура е взаимствана от системната. (Интернет е един **глобален компютър**.)

Ще бъде ли TCP/IP заместен от мрежовото кодиране, Named Data Networking?

Слоеста системна архитектура

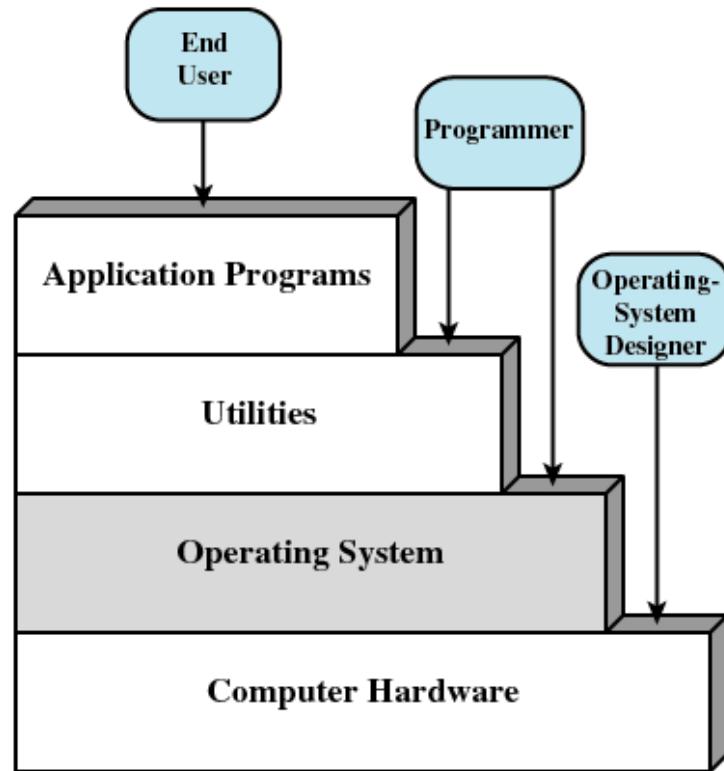


Figure 2.1 Layers and Views of a Computer System

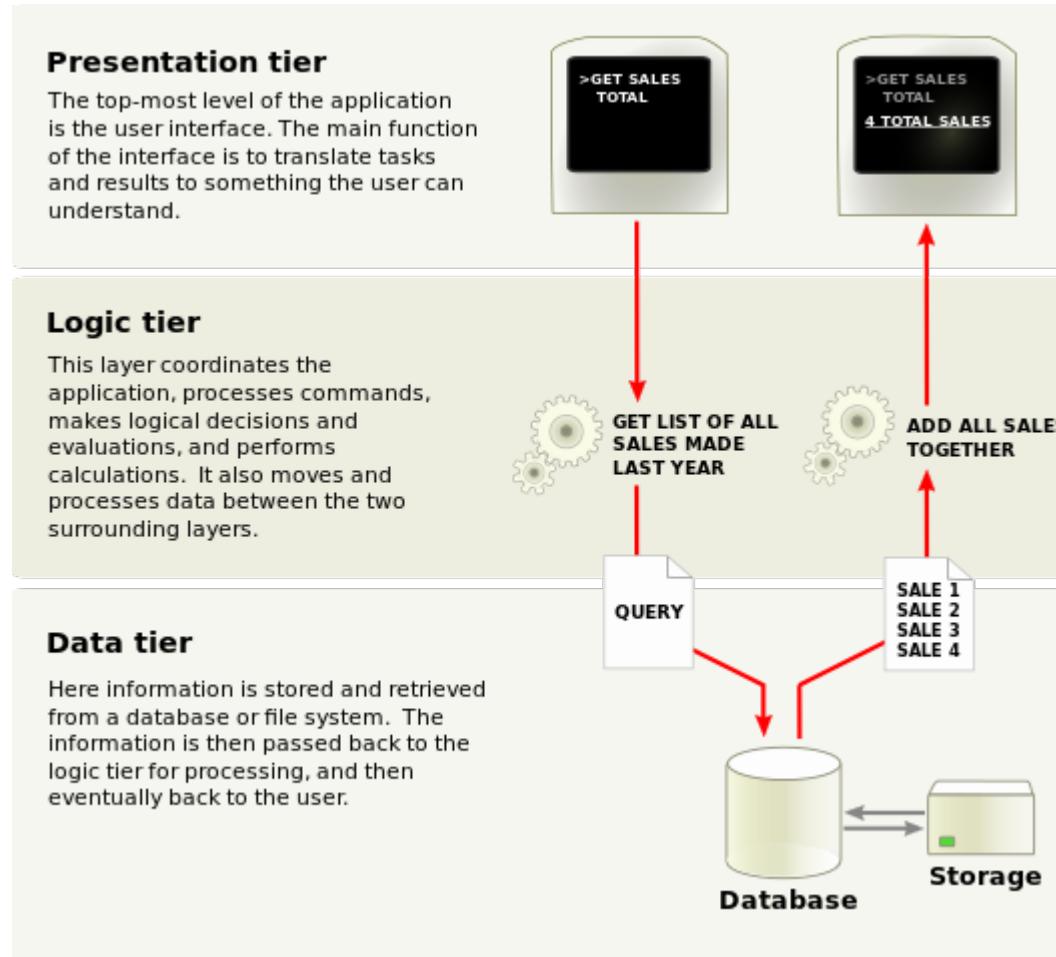
3-слойна архитектура на web сайт/ портал

Презентационен слой – основните портални компоненти за изграждане на потребителския интерфейс: портлети, HTML форми, JSP страници и др.

Бизнес слой – реализира бизнес логиката на решението (библиотеки от Java класове и Java Bean компоненти работещи в J2EE Server среда и услуги).

Бази от данни – реализира съхраняването и извличането на данните, независимо от конкретната СУБД и архитектура на данните.

3-слойна архитектура на web сайт/портал



Архитектура на мрежите

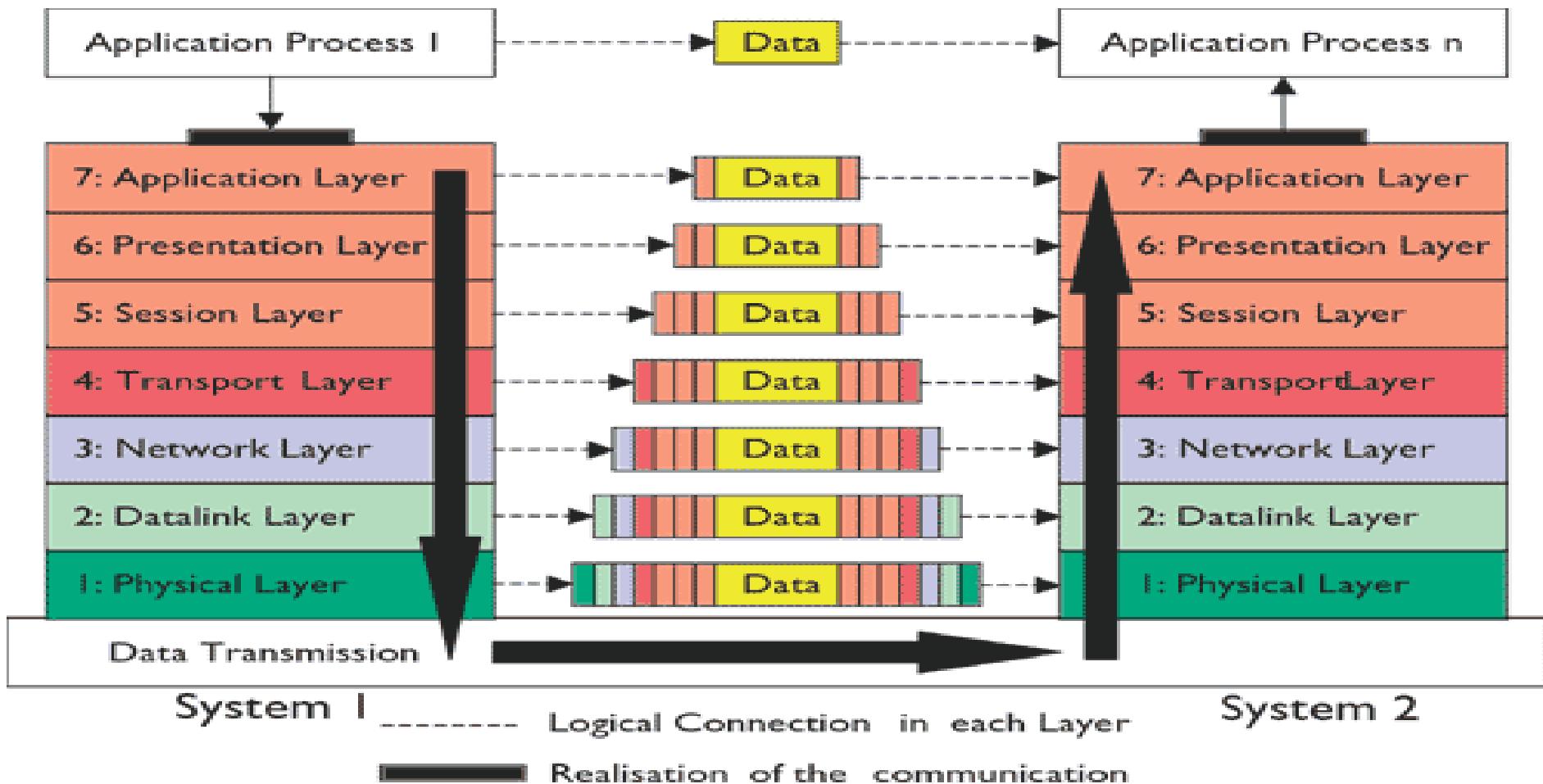
Основен принцип в съвременните мрежови архитектури е принципът за разслояване на функциите по управление на връзките, като всеки слой ползва услугите, предоставени от по-долните слоеве, без да знае как са реализирани тези услуги. Това е принципът на прозрачност.

Слоят n на една машина взаимодейства със слоят n (на същото ниво) на друга машина. Правилата, по които се осъществява това взаимодействие, се определят от протокола на n -то ниво.

Най-общо под протокол се разбира съгласувани правила между комуникиращите страни за това как да протича комуникацията.

На практика при комуникацията между съответните слоеве на двете машини не се предават данни. Всеки слой n предава данни и контролна информация (header+trailer) на непосредствено по-долния слой $n-1$, докато се достигне най-долния слой 1 , където се осъществява реалната комуникация между машините през физическата среда. В приемника получените данни се разпространяват в обратна посока - от слой 1 нагоре, като всеки слой премахва контролната информация, която се отнася до него. Опаковане и разопаковане (encapsulation – decapsulation).

Архитектура на мрежите



Данните+Контр. Инф. на слой n се наричат протоколен блок от данни (PDU). За слой $n-1$ PDU(n) са си обикновени данни. Чисто потребителските данни – payload.

Архитектура на мрежите

Всеки *слой n* предоставя **услуги** (множество от примитиви – операции) на *слой n+1*.

Всяка услуга е обвързана с **интерфейс** между двата слоя *n* и *n+1*. *Слой n+1* е потребител на услугата, а *слой n* – доставчик на услугата.

Интерфейсът показва на процеса как да достъпи услугата, определя параметрите на услугата и какъв резултат да се очаква.

Разслояването позволява да се промени изцяло реализацията на даден слой *n*, без да се променя реализацията на другите слоеве – достатъчно е да се запази множеството от услугите, които слой *n* осигурява на горния слой *n+1*. Прозрачност (**transparency**) и Гъвкавост (**flexibility**).

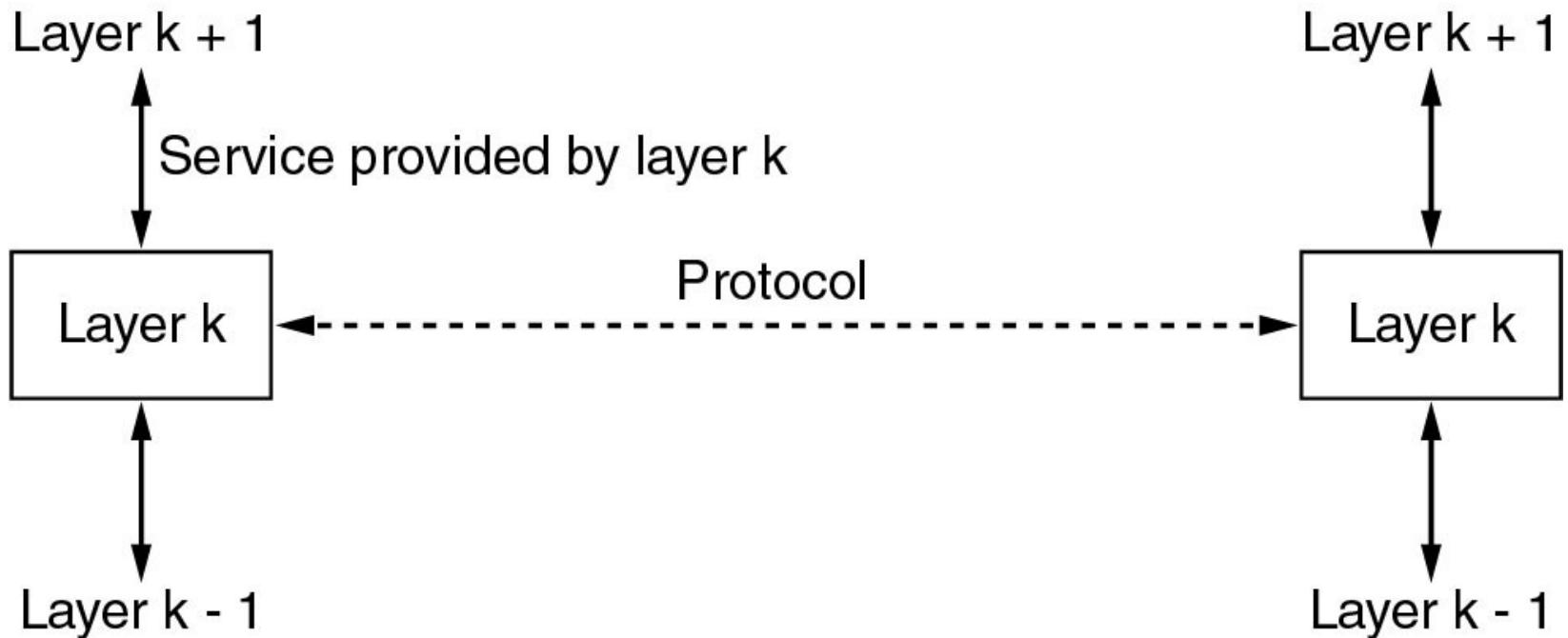
Архитектура на мрежите

Една **мрежова архитектура** се определя от **множеството на слоевете**, услугите които те предоставят и протоколите, по които се осъществява взаимодействие между слоевете.

Реализацията на слоевете, както и интерфейсът между отделните слоеве не е задължително да са едни и същи на машините в една мрежа – достатъчно е всеки слой *n* да може да комуникира със съответния слой *n* по определения протокол и да предоставя съответните услуги на по-горния слой. Машабируемост (**scalability**).

Списъкът от протоколи, използвани от една система, по един протокол за всеки слой се нарича **протоколен стек**.

Протоколи и услуги



Протоколи и услуги на едно ниво: k.

Моделът OSI

Съвременните мрежови архитектури следват принципите на **модела OSI (Open Systems Interconnection)**, създаден от Международната организация по стандартизация **ISO** (International Standards Organization) и Международния съюз по телекомуникации (**ITU-T**) за връзка между отворени системи.

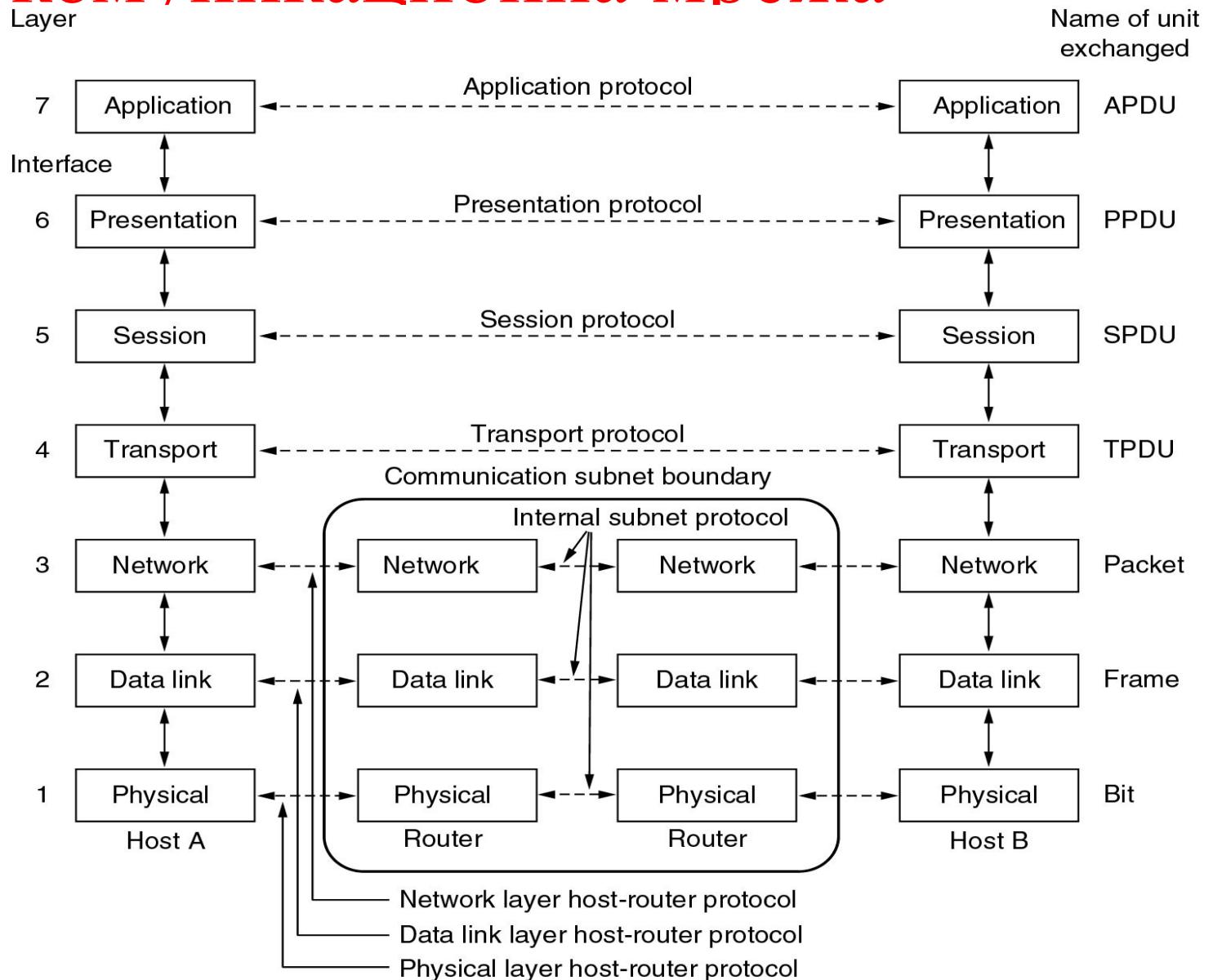
OSI цели създаване на мрежови стандарти, осигуряващи оперативна съвместимост на устройства, софтуер и системи от различни доставчици.

Отворена система е система, чиито ресурси могат да се използват от другите системи в мрежата.

OSI моделът е абстрактен модел на мрежова архитектура, който описва предназначението на слоевете, но не се обвързва с конкретен набор от протоколи. Поради това OSI моделът се нарича още **еталонен модел** и всъщност дава препоръки (**Reference Model**). Има **седем слоя**.

OSI RM – хост машини и комуникационна мрежа

The OSI reference model.



Физически слой

Физическият слой (physical layer) има за задача да реализира предаването на битове през физическата среда.

Основна функция на физическия слой е да управлява кодирането и декодирането на сигналите, представящи двоичните цифри 0 и 1. Той не се интересува от предназначението на битовете.

Физическият слой трябва да осигурява възможност на по-горния слой да активизира, поддържа и прекратява физическите съединения.

Обекти на този слой – хардуерни устройства, реализиращи предаването на 0-и и 1-ци през физическата среда – мрежови карти (NIC) и модули, модеми.

Канален слой

Основна функция на **каналният слой** (data-link layer) е управлението на канала от един възел до друг (точка-точка) според класическия модел, “точка-много точки” (напр. Frame Relay) или достъп до преносната среда (MAC) в LAN.

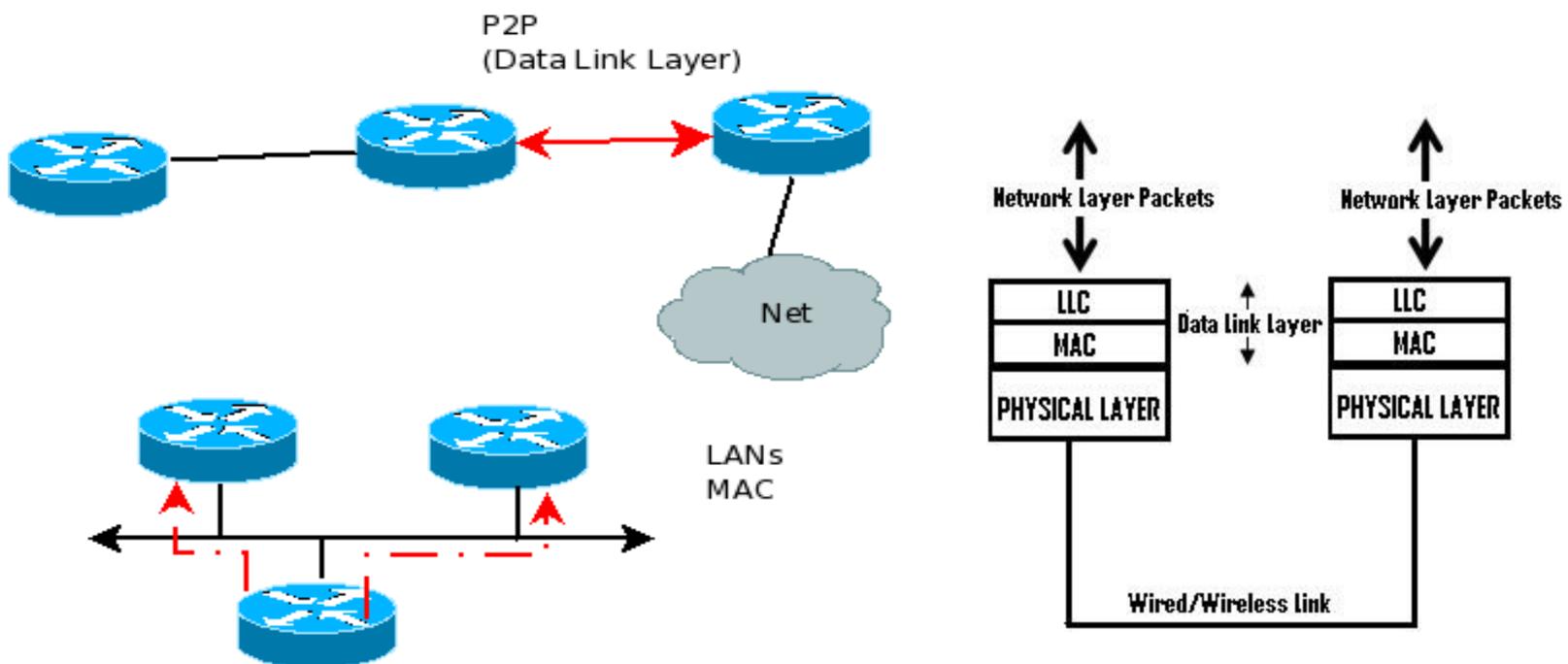
Откриването и евентуалното коригиране на грешки при предаването на данните.

Данните на канално ниво се обменят на порции (PDU), наречени **кадри (frames)**, обикновено с дължина от няколко стотин до няколко хиляди байта в зависимост от скоростта на линията.

В локалните мрежи каналният слой се разделя на два подслоя: Medium access control (**MAC**) – контролира как мрежовото устройство достъпва комуникационната среда и получава право да предава данни.

Logical link control (**LLC**) – идентифицира и “опакова” (encapsulate) протоколите от мрежовия слой, проверява за грешки и синхронизира кадрите.

Канален слой



Канален слой

При надеждна комуникация приемникът трябва да уведомява изпращача за всеки успешно получен кадър като му изпраща обратно потвърждаващ кадър.

Форматът на кадрите се определя от избрания протокол на канално ниво. Функциите на каналния слой обикновено се реализират смесено - аппаратно и програмно. Колкото повече функции са реализирани софтуерно (контролерът е реализиран на дънната платка), по-ниска е производителността.

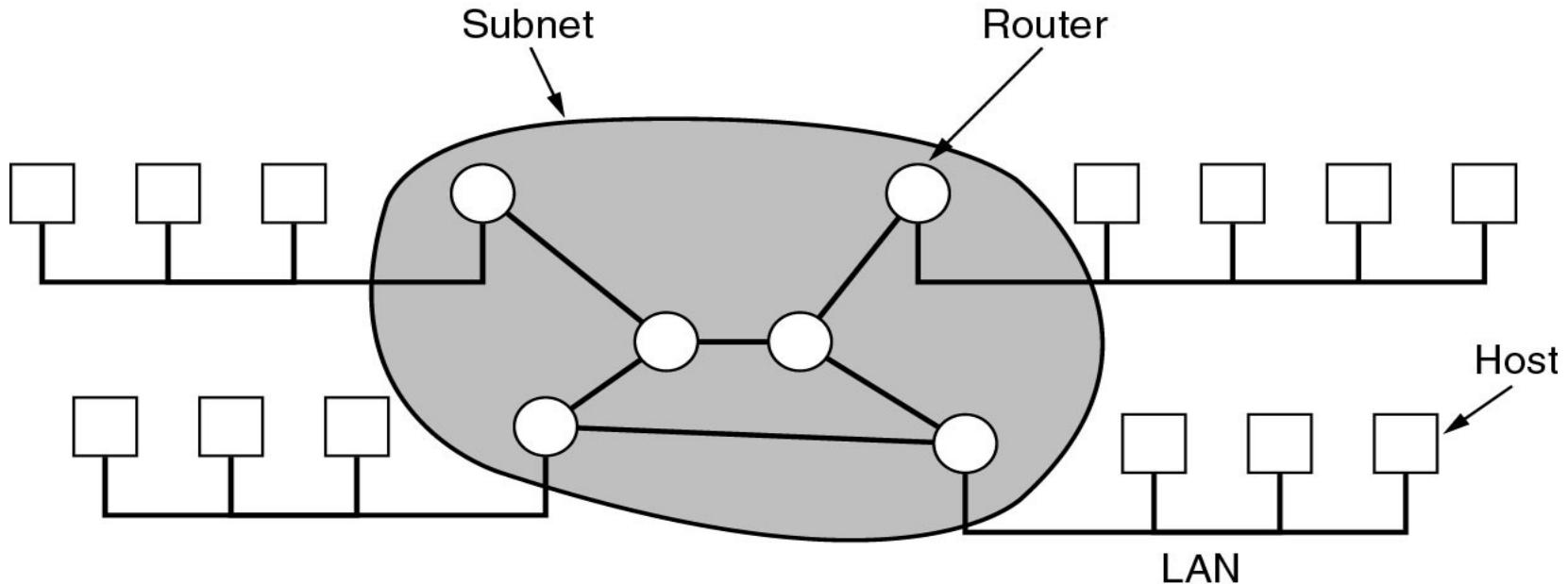
Мрежов слой

Мрежовият слой (network layer) отговаря за функционирането на комуникационната подмрежа.

Приложените програми, които се изпълняват в двете крайни системи взаимодействат помежду си посредством **сегменти** от данни, които в този слой се опаковат като **пакет**.

Пакетите са с фиксирана дължина в рамките на една мрежа. Но **при** преминаване от една КМ в друга е възможно пакетът да се раздели на части – **фрагментира**, след което да се възстанови. Напр. Преход: LAN-WAN-LAN

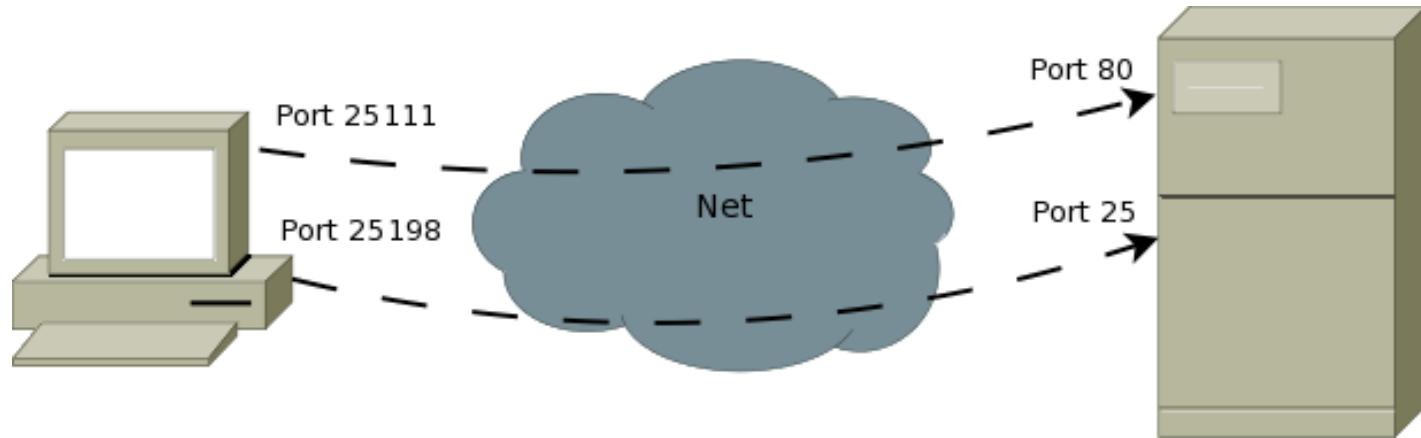
Мрежов слой



Основна задача на мрежовия слой е **маршрутизирането** на тези сегменти, опаковани като **пакети (PDU за мрежов слой)**.

За системите, реализиращи възлите на комуникационната подмрежа (**маршрутизатори - routers**) този слой е последен. Функциите на мрежовия слой, както и на по-горните слоеве се реализират програмно.

Транспортен слой



Транспортният слой (transport layer) осигурява транспортирането на съобщения от източника до получателя. Той е най-ниският слой, който реализира връзка от тип “край-край” между комуникиращите системи.

Изгражда програмен канал между портовете на приложения, които си “говорят” през мрежата.

Транспортен слой

В транспортния слой на изпращаща съобщенията се разбиват на **сегменти** (PDU за тр. слой) и се подават на мрежовия слой, където се опаковат като пакети, а в транспортния слой на получателя разопакованите от мрежовия слой сегменти се реасемблират.

Транспортният слой освобождава по-горния сесион слой от грижата за надеждното и ефективно транспортиране на данните между крайните системи.

Т.е транспортният слой отговаря за целостта на обменяните съобщения, което включва откриване на загубени сегменти и тяхното повторно предаване.

Сесиен слой

Сесийният слой (session layer) е отговорен за диалога между две комуникиращи програми. Съобщения се обменят, след като двета крайни абоната установят **сесия**.

Сесийният слой осигурява различни режими на диалог – двупосочен едновременен диалог (full duplex - FD), двупосочен алтернативен диалог (half duplex - HD), еднопосочен диалог (**simplex**).

Освен това той предоставя възможност за прекъсване на диалога и последващо възстановяване от мястото на прекъсването.

При липсата на сесиен слой всяко съобщение се предава независимо от другите съобщения.

Представителен слой

Представителният слой (presentation layer) е най-ниският слой, който разглежда значението на предаваната информация.

Първата функция на този слой е да определи общ синтаксис за предаване на съобщенията.

Втората функция на слоя е да унифицира вътрешната структура на представените данни в съобщенията.

По този начин за по-горния приложен слой няма значение дали двете крайни системи използват различни представления на данните.

UTF-8 (8-bit UCS/Unicode Transformation Format) представля всеки символ в Unicode стандарта и е **обратно съвместим с ASCII**. По тези причини е предпочитан за e-mail, web страници и др.

Извършва също криптиране на данните, компресия.

<https://developers.google.com/+web/>

До скоро се дефинираха базови размери за различните устройства:

За **десктоп** екрани: $\geq 992 \text{ px}$ размери

За **таблети**: (768 px, 992 px)

За **телефони**: $\leq 767\text{px}$

И се изискваше да се проектират отделни версии за всеки тип устройство.

Десктоп версия



English

Добре дошли в EGOV.BG - Порталът за достъп и информация относно всички електронни административни услуги и федерираните институционални сайтове в Република България.

Търсене в EGOV.BG

ТЪРСИ

Социални придобивки

Социално подпомагане, условия

Гражданско състояние

Гражданство, брак, отглеждане на деца, смърт

Бизнес и свободни професии

Бизнес и свободни професии
Управление и развитие на бизнеса

Работодатели и предпредимачи

Назначаване, осигуряване и заплащане

Околна среда и селско стопанство

Природни бедствия, рециклиране, програми

Имущество и комунални услуги

Недвижими имоти и местни услуги, данъци и такси

Данъци и такси

Данъци, социално и здравно осигуряване

Работа и пенсии

Работни дни, осигуряване и безработица

Популярни

Услугите в тази секция ще се поддържат автоматично според броя на поглед

Одобряване на технически и работни инвестиционни проекти за подобряване на техническата инфраструктура за повече от една област

Плащане на данъци и осигуряване по Интернет с лични карти

Подаване на наложени искане по §19ч, аз. 2/зл.4 от ПЗР на ЗЗО по електронен път

Предоставяне на справка за здравно осигуряване

ДДС върху електронните услуги - Регистрация

Категоризация на заведения за хранене и развлечения - Район Южен

Категоризация на средства за поддръжки и места за настаняване - Район Западен

Институциите на България

Президент

Парламент

Министерски съвет

Съдебна власт

14 Министерства

45 Агенции

28 Областни администрации

300 Общини и районна

152 Други

Научи повече

■ Как работи правителството на Република България

■ Символите на Република България

■ Електронното управление Програми, документи, статистика

Новини, анонси и прес-съобщения



МТИС успешно реализира проект за
обществен достъп до данни 17.09.2014
Създадените електронни услуги и
приложения, бяха дискутирани на
крыла маса.



Заявление на новина или анонс
25.02.14
Подготвянето на изображение в
подходящ вид и резолюция е още
трудно, но тък анонс с картичка има
много по-голям шанс да бъде
забелязан.



МТИС успешно реализира проект за
обществен достъп до данни за
железопътната инфраструктура
17.09.2014
Създадените електронни услуги и
приложения, бяха дискутирани на
крыла маса.

Нещо не е наред с тази страница?

Контакти

Условия за ползване

Достъпност

Карта на уеб сайта

За уеб сайта

Социални придобивки

Гражданско състояние

Бизнес и свободни професии

Правен ред

Хора с увреждания

Транспорт и автомобили

Работодатели и предпредимачи

Околна среда и селско стопанство

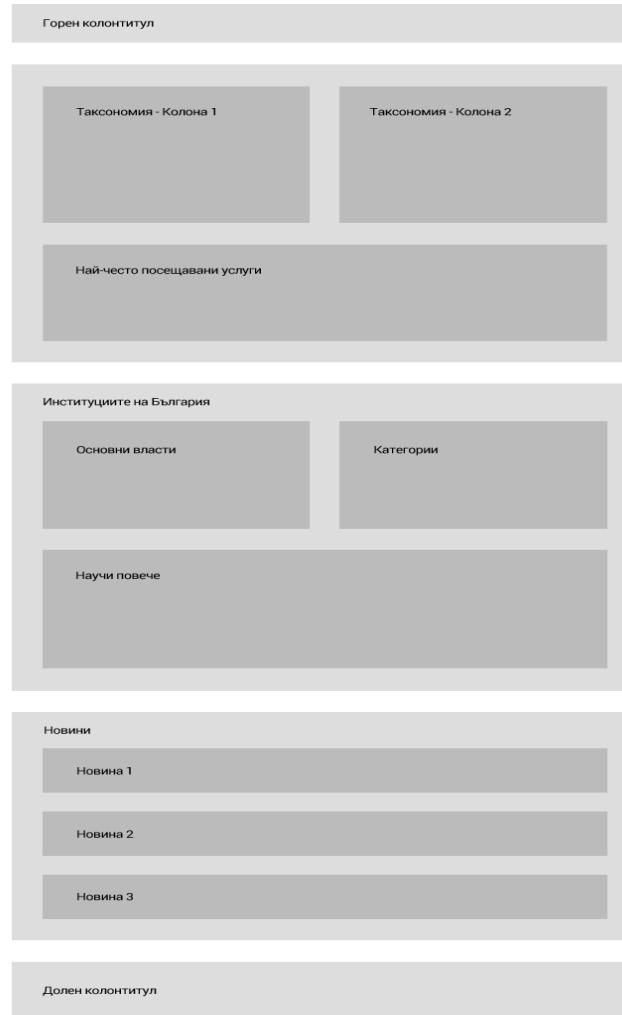
Имущество и комунални услуги

Данъци и такси

Паспорти, визи и имиграция

Работа и пенсии

Таблет версия



Версия за мобилен телефон

Горен колонитул

Таксономия

Най-често посещавани услуги

Институциите на България

Основни власти и категории

Научи повече

Новини

Новина 1

Новина 2

Новина 3

Долен колонитул

Responsive Web Design

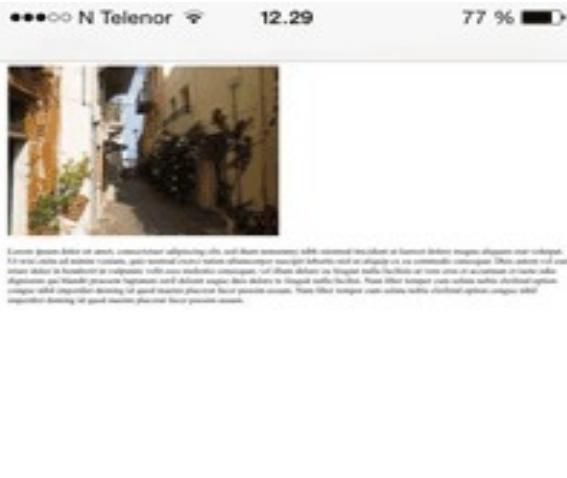
Вече имаме Responsive Web Design - прилага HTML и CSS (Cascading Style Sheets) за автоматично преоразмеряване на web сайт, за да изглежда еднакво добре на всяко устройство (десктоп, таблет, мобилен телефон).

На Web страниците се добавя елемент <meta> :

```
<meta name="viewport"  
content="width=device-width, initial-scale=1.0">
```

Responsive Web Design

Без viewport meta tag:



Etiam ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Nam liber tempor cum soluta nobis eleifend option conone nihil immediet domino.

Със viewport meta tag:



Etiam ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Nam liber tempor cum soluta nobis eleifend option conone nihil immediet domino.

Приложен слой

Приложният слой (application layer) е най-горният слой, към който се свързват потребителските процеси в двата крайни абоната.

Някои потребителски процеси са интерактивни - взаимодействват си в голям период от време с кратки съобщения от тип заявка-отговор (request-reply).

Други потребителски процеси взаимодействват с малко на брой големи по обем порции от данни.

За двата вида процеси се предвиждат различни протоколи на приложния слой - например протокол **FTP** (file transfer protocol) за обмен на цели файлове, протокол **HTTP** (hyper text transfer protocol) за обмен на уеб-страници и др.

Модел TCP/IP

Когато започват да се изграждат реални мрежи, използвайки OSI-модела и съществуващите протоколи се вижда, че те не отговарят на изискваните спецификации за обслужване.

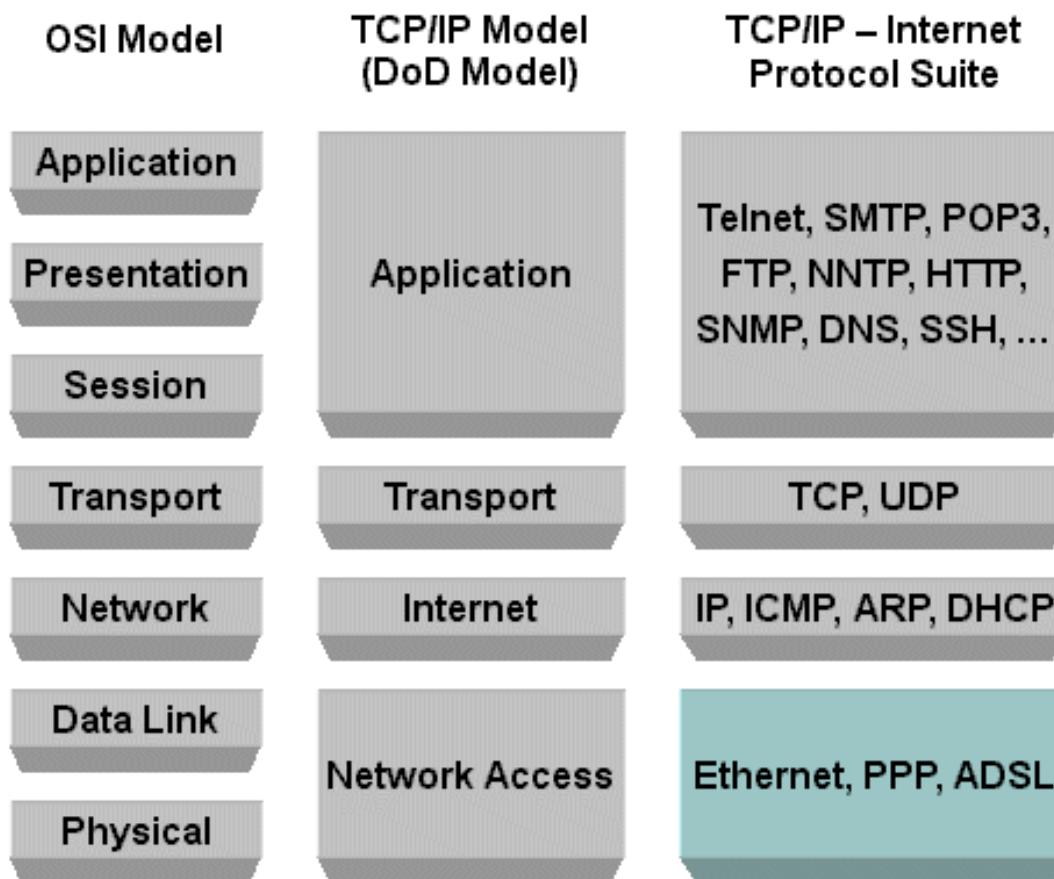
Въведен е за първи път през 1974 г. от V. Cerf и Kahn в ARPANET - първата компютърна мрежа, която прераства в Internet. Целта е била да позволи свързването на различни мрежи, да бъде жизненоспособна и гъвкава, да оцелее и в условията на ядрен апокалипсис.

Мрежа с комутация на пакети, базирана на обслужване с неустановена връзка (connectionless - без предварително уговоряне на параметрите на връзката между източник и приемник).

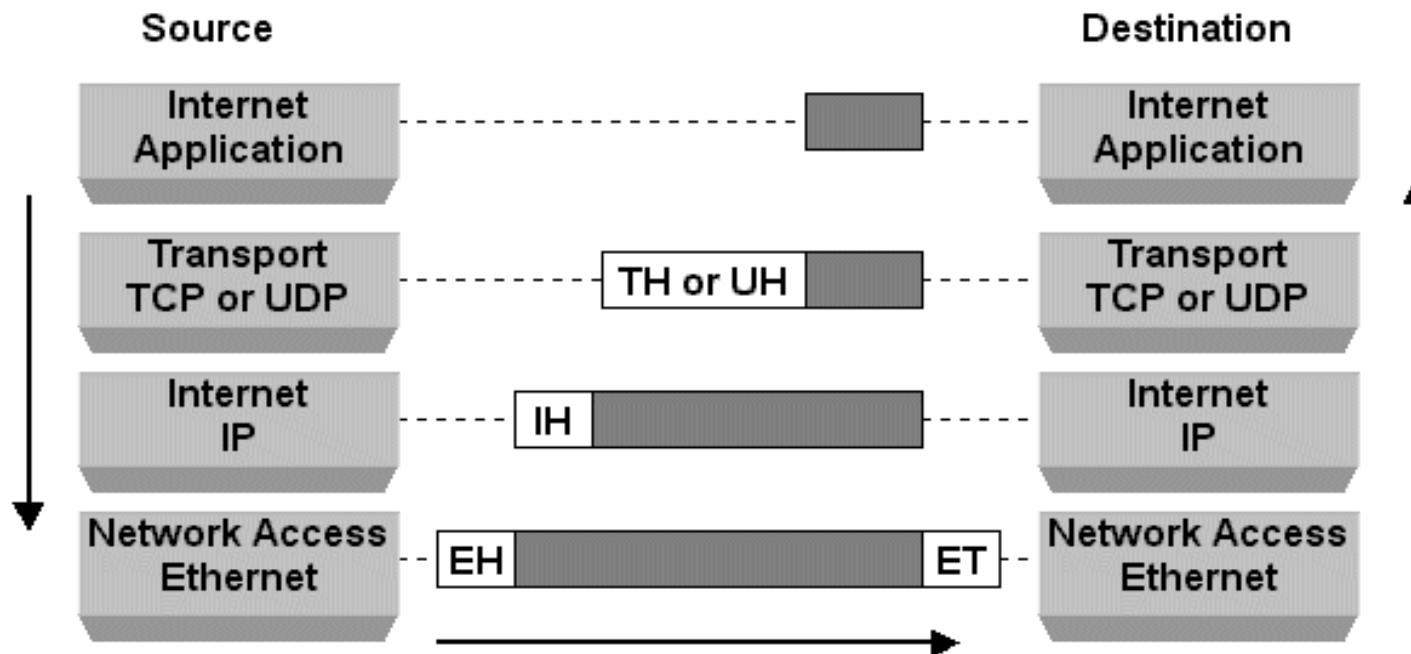
Това е мрежовото ниво – интернет нивото, където имаме “best effort delivery”.

Протоколът е Internet Protocol – IP, PDU - IP пакети.

OSI vs. TCP/IP



TCP/IP – мрежи, протоколи и услуги



Както Интернет, така и транспортният слой е подобен на OSI. Но транспортният:

TCP (Transmission Control Protocol) е connection-oriented. Потокът от байтове да бъде доставен без грешка. Съобщението се разбива на сегменти.

UDP (User Datagram Protocol) е connectionless за обмен на звук, къси съобщения: NTP, TFTP, SNMP.

Сравнение на OSI и TCP/IP

Общи свойства: единен стек от независими протоколи, подобни функции.

Три основни свойства на **OSI** (Създаден преди TCP/IP в условията на разделен свят.):

- Дефиниране на услуги
- Дефиниране на интерфейси
- Дефиниране на протоколи

Основно предимство на OSI: прави разграничение между тези три свойства.

TCP/IP (съответства на глобалното село) няма точно разграничение между трите.

Протоколите в OSI са по-добре обособени, отколкото в TCP/IP.

Могат да бъдат заменяни по-лесно.

Сравнение на OSI и TCP/IP

OSI – преди да е създадена концепцията за протоколите – доста^{тъчно общ}.

Канален слой – за връзки “точка-точка”. С поява на LAN – broadcast мрежите – нов подслой.

Подслоевете да бъдат изменяни в зависимост от различията в конкретните мрежи.

OSI създателите – всяка страна по една OSI мрежа под управлението на правителството. Не е мислено за международно свързване.

TCP/IP – първо се разработват протоколите. Моделът – реално описание на вече съществуващи протоколи. Т.е пасват перфектно, без да е необходима да са напасвани към модела, както при OSI.

Сравнение на OSI и TCP/IP

TCP/IP не е приложим за описание на мрежи, които не поддържат TCP/IP. Но днес всички производители го поддържат. Такива със собствени протоколни стекове. Novell се отказа от SPX/IPX, Apple – от AppleTalk, Microsoft – от NetBIOS и др.

Т.е TCP/IP стана световен мрежов стандарт.

Други разлики:

- На мрежово ниво - TCP/IP само connectionless; OSI – и connection oriented.
- На транспортно ниво - OSI – само connection oriented; TCP/IP – и двете (TCP и UDP).

Идва ли краят на TCP/IP?

Internet може да стане по-бърза и по-сигурна, като се изостави концепцията за пакети и корекцията на грешките, която забавя трафика заради повторните предавания.

Това предполагат учени от Aalborg University, Дания, в сътрудничество с MIT и Caltech (California Institute of Technology).

Te искат да заменят сегашния модел със система от линейни уравнения.

Методиката

Методиката се базира на мрежовото кодиране и декодиране, по-точно RLNC (**Random Linear Network Coding** – Случайно линейно мрежово кодиране)

Все едно, колите навлизат в кръстовище от всички посоки, без да се налага да се изчакват помежду си или да чакат да им светне “зелено”. Естествено, без да стават катастрофи :)

4-минутно видео се “сваля” 5 пъти по-бързо от клкото по традиционната технология.

Как работи

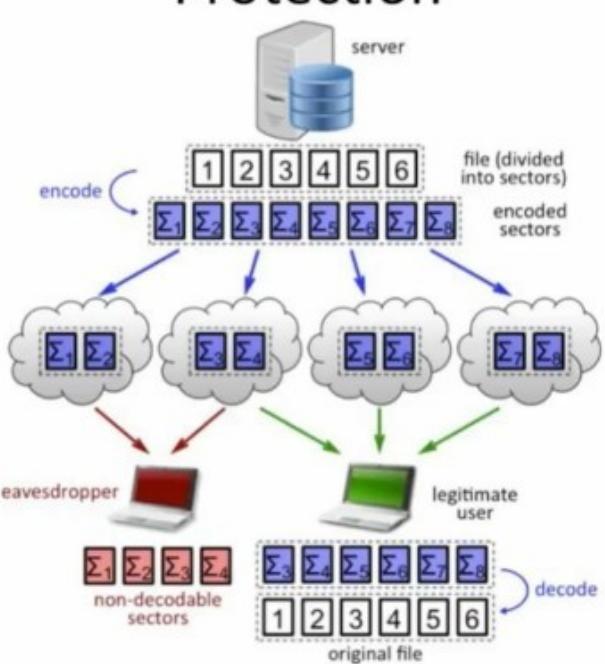
На съдържанието на пакета се гледа като на отделно число. Всеки възел в мрежата създава система от линейни уравнения от числата, извлечени от съдържанието на пакетите и множество от случайно генериирани коефициенти.

Ако си спомняте от гимназиалния курс по математика, необходими са ви **N линейни уравнения**, за да намерите стойностите на **N неизвестни**.

Всеки кодиран пакет съдържа по едно уравнение. Т.е на получателят му трябват **N** пакета (с различни коефициенти), за да може да декодира данните.

По-сигурна система. На “подслушвачите” ще им трябва да прихванат всички пакети, за да декодират информацията

Coding as a Measure Content of Protection



Противници

На нас ни предстои да се занимаваме с модела TCP/IP. Рано е да се каже, че е за изхвърляне. Трябва да отбележим, че:

Пакетите не е задължително да бъдат подредени. Протоколът TCP няма такова изискване. Сегментите, на които се разделя дадено съобщение, се номерират.

Благодарение на прозоречни механизми и др. техники, повторните предавания (ако се наложи) не забавят скоростта.

Нека имаме предвид и високото бързодействие на днешните интегрални схеми.

Все пак предлаганата технология сигурно ще намери приложение в **5G** мобилни мрежи, сателитни комуникации и **Internet of Things**.

Вече в Силиконовата долина

RLNC технологията е патентована и “опакована” в C++ софтуер от фирмата Steinwurf с марката Kodo. Steinwurf планира да я продава на хардуерни производители.

Steinwurf е основана от професор Frank Fitzek от Aalborg University и двама негови бивши студенти заедно с американските им колеги.

Компанията вече има офис и в Силиконовата долина, но управлението ѝ е все ще в Aalborg.

Named Data Networking

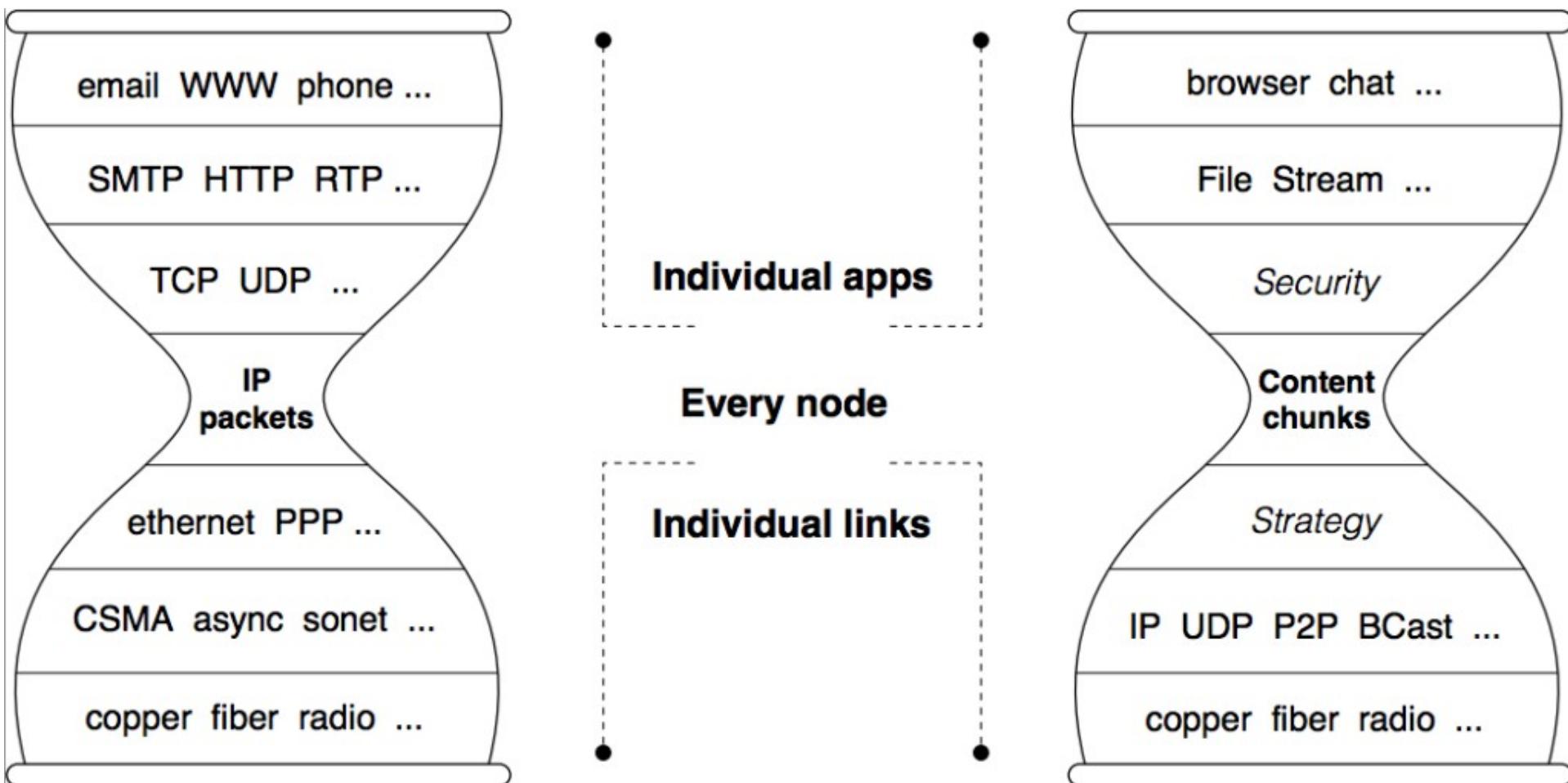
Проектът Named Data Networking (**NDN** - <http://named-data.net>) предлага нова Internet архитектура. Дават се **имена на данните**, а не на местоположението им.

Сегашната Internet подсигурява контейнера с данни, а **NDN** подсигурява **самото съдържание**. NDN Testbed в момента включва 43 възела с 121 връзки.

NDN е особено подходяща за новите мрежови среди като **edge computing** и **IoT**.

Участници в NDN проекта са над 60 академични и търговски институции от САЩ и др. страни.

Архитектура на NDN



Архитектура на NDN (6 основни принципи)

- (1) Оригиналният Internet е IP центриран. NDN – около обемите с данни.
- (2) придържа се към принципа end-to-end.
- (3) Маршрутизиращата и направляващата равнини и тук са разделени. NDN реализира най-добрата технология за направляване на данните, като се правят проучвания за нова система за маршрутизация.
- (4) NDN дава основна сигурност, като подписва всички именувани данни.
- (5) NDN включва балансиране на потоците с данни.
- (6) NDN полага усилия да даде инициативата в ръцете на крайния потребител и да стимулира конкуренцията.

Архитектура на NDN (формат на пакетите)

Interest packet

Content Name

Selector

(order preference, publisher filter, scope, ...)

Nonce

Data packet

Content Name

Signature

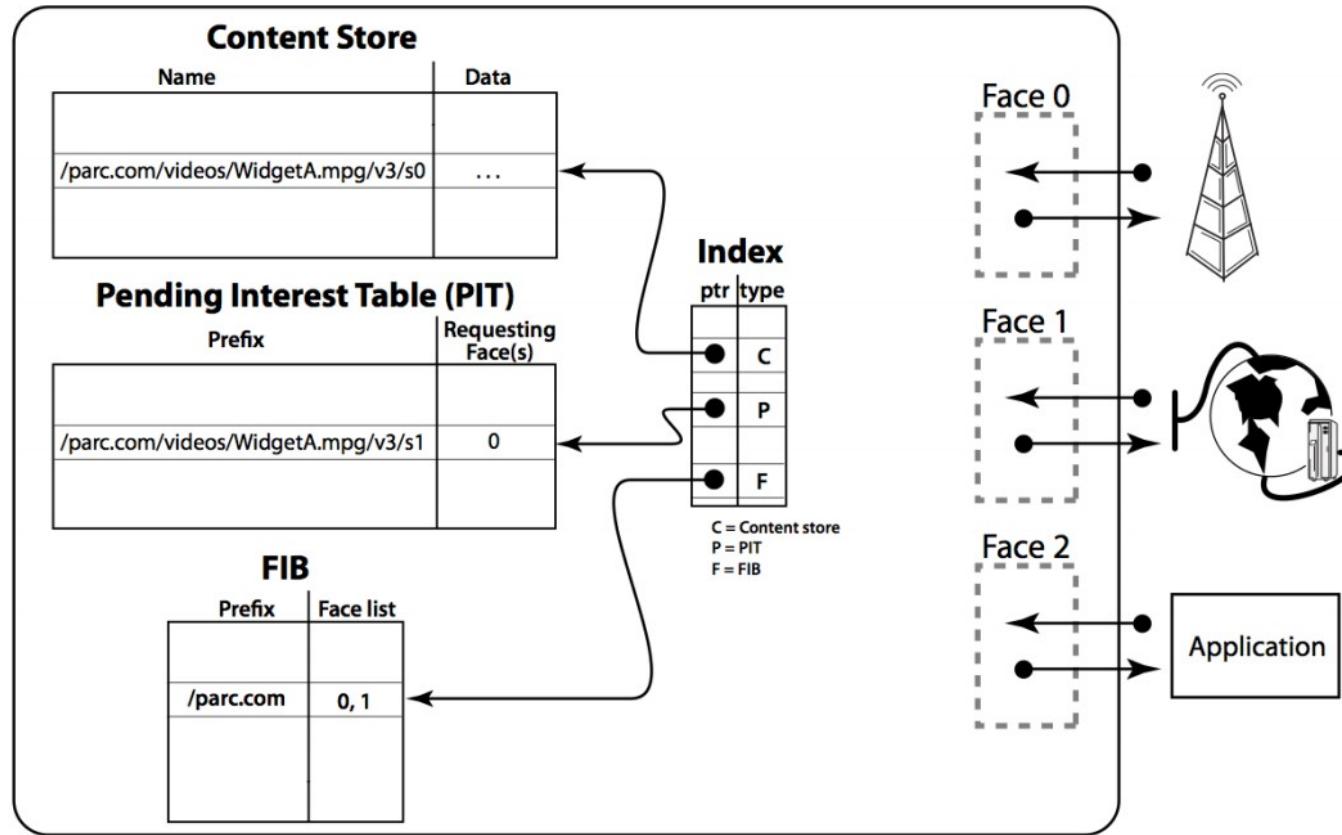
(digest algorithm, witness, ...)

Signed Info

(publisher ID, key locator, stale time, ...)

Data

Архитектура на NDN (NDN възел)



NDN комуникации

Комуникациите в NDN се водят от получателя, т.е. контейнерът с данни.

За да получи данни, консуматорът изпраща **Interest** пакет. Рутерът запомня интерфейса, от който идва заявката, след което пренасочва Interest пакета след справка за името във Forwarding Information Base (**FIB**), попълвана от протокол за маршрутизация **NLSR** - Named Data Link State Routing Protocol.

След като **Interest** достигне възел, съдържащ заявлените данни, обратно се връща **Data** пакет, носещ името и съдържанието на данните, подписани от създателя им.

Този **Data** пакет се връща обратно по пътя, по който е дошъл **Interest** пакета.

Забележете, нито **Interest** пакетът, нито **Data** пакетът носи никакъв адрес (напр. IP адрес).

Физическо ниво

Теоретически основи и среди за предаване

Какво ще научим

Аналогов и цифров сигнал

В компютрите и мрежите работим с дискретни (т.е цифрови) стойности – “0” и “1”. Как ги представяме по комуникационните линии. Тук има много математика – непрекъснати и дискретни функции, ред на Фурье и др.

Малко за цифровизацията.

Среди за пренос на данни:

- жични (медни и влакнесто-оптически)
- безжични (по въздуха и електрозахранващата мрежа)

Общи положения

Физическият слой дефинира механичните, електрически и времеви характеристики на мрежовия интерфейс.

Ограниченията, които поставя физическата среда върху скоростта на пренос.

Два вида преносна среда:

- жична (меден кабел или оптически влакна);
- безжична (наземна и сателитна).

Теоретични основи на преноса на данни

Информацията се пренася по жиците, изменяйки стойността на физическа величина: **ток или напрежение.**

Тази стойност се представя като **функция от времето, $f(t)$.**

Това позволява да се моделира поведението на сигнала и да се анализира математически.

В началото на 19 век френският математик **Jean-Baptiste Fourier** доказва, че всяка периодична функция с период T може да бъде представена като **сума от (на практика безброй) синуси и косинуси.**

Т.е като **ред на Фурье.**

Развитието в ред на дадена функция широко се използва в **числените методи.**

Ред на Фурие

Всяка периодична функция с период T може да се развие в следния ред:

$$f(t) = \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos\left(\frac{2\pi n}{T} t\right) + \sum_{n=1}^{\infty} b_n \sin\left(\frac{2\pi n}{T} t\right)$$

В частност, ако $T=2\pi$, редът добива особено опростен вид:

$$f(t) = \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos(nt) + \sum_{n=1}^{\infty} b_n \sin(nt)$$

Ред на Fourier. Коефициенти.

$f = 1/T$ е честотата, a_n и b_n са амплитудите на n -ти хармоник (член),
 $a_0/2$ е константа.

От ред на Fourier може да бъде възстановена оригиналната функция.
Коефициентите a_n , b_n и константата a_0 се намират от следните
интеграли:

$$a_0 = \frac{2}{T} \int_{-T/2}^{T/2} f(t) dt$$

$$a_n = \frac{2}{T} \int_{-T/2}^{T/2} f(t) \cos\left(\frac{2\pi n}{T} t\right) dt$$

$$b_n = \frac{2}{T} \int_{-T/2}^{T/2} f(t) \sin\left(\frac{2\pi n}{T} t\right) dt$$

Фурие и комуникациите

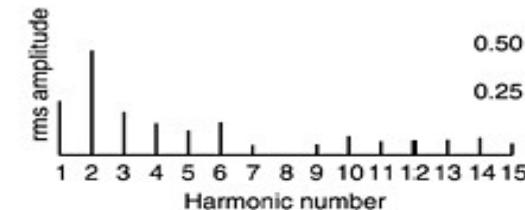
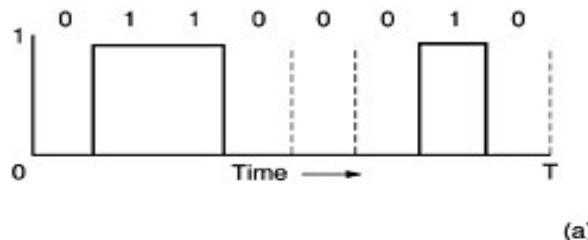
Да разгледаме примера:

Предаване на ASCII символ "b", кодиран като 8-битов байт.

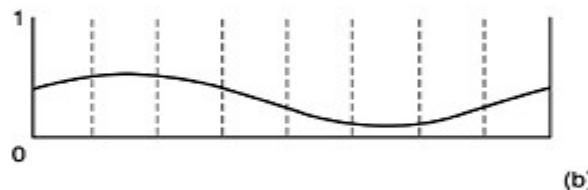
Илюстрация на Фуриеров синтез на периодична функция:

[https://commons.wikimedia.org/wiki/
File:Fourier_synthesis_square_wave_animated.gif](https://commons.wikimedia.org/wiki/File:Fourier_synthesis_square_wave_animated.gif)

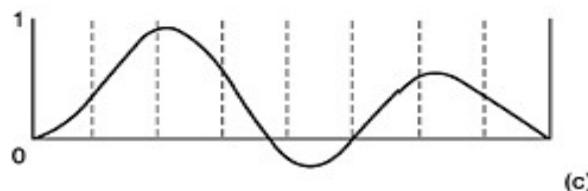
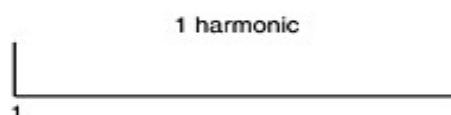
Буква b в ASCII код



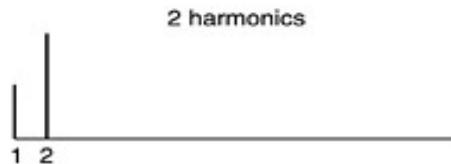
(a)



(b)

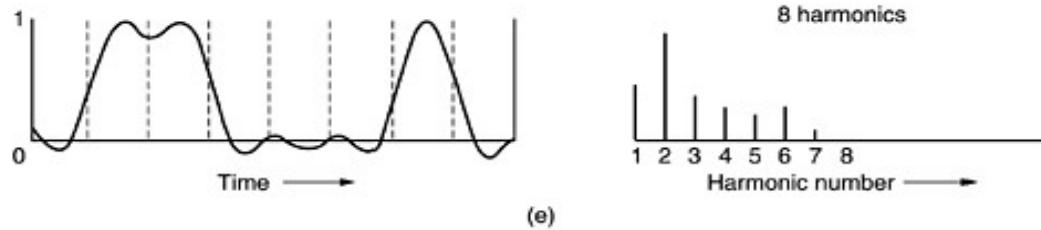
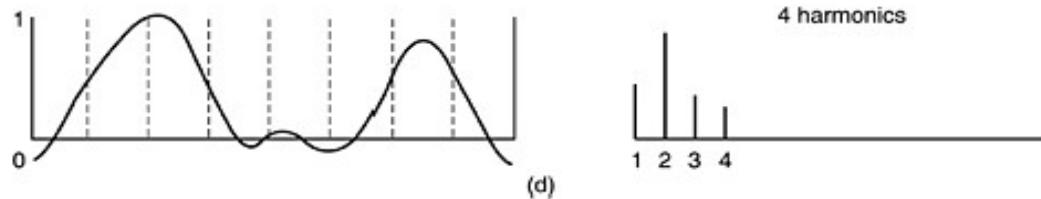


(c)



(b) апроксимация с първа хармонична сигнал \neq оригинал

Буква b в ASCII код



(c) – (e) апроксимация с по-голям брой честоти: сигнал \simeq оригинал

Фурие и честотна лента

Всяка преносна среда внася загуби, намалява силата на сигнала, за всеки от Fourier компонентите.

Амплитдите на различните Fourier компоненти намаляват различно, което води до **изкривяване**.

Амплитдите се предават без намаление при честоти **от 0 до f_c** [cycles/sec или Hertz (Hz)], над f_c която сигналът започва да отслабва.

Този обхват от честоти се нарича **честотна лента – bandwidth (bw)**.

bandwidth зависи от конструкция, дебелина и дължина на средата.

От слайд 16 и 17: символ “**b**” ще се предава **по-точно** при по-ширака честотна лента.

Електромагнитни вълни и честотна лента

Сигналите (вкл. битовете – 0 и 1) се разпространяват като електромагнитни вълни.

Във вакуум електромагнитните вълни се разпрострат със скоростта на светлината:

$$C = 3 \times 10^8 \text{ m/sec}$$

В **медни жици** и стъклени влакна тази скорост е около **$2/3$** от тази стойност и е честотно зависима.

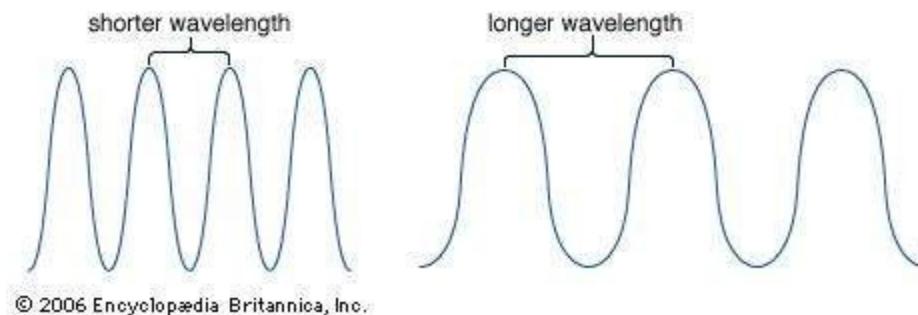
Връзката между **честотата f** и **дължината на вълната λ** се определя от формулата:

$$\lambda * f = C$$

Дължина на вълната - λ

Дължина на вълната (λ) е физическа величина, показваща разстоянието между **съответстващи точки** от две последователни вълни.

Съответстващи точки са две точки, които са в една и съща фаза, т.е. точки, които са завършили идентични части от периодичното им движение.



Честотна лента на електромагнитните вълни

Количеството информация, което може да пренесе електромагнитна вълна, има отношение към честотната лента. От горното уравнение, ако диференцираме по отношение на λ :

$$\frac{df}{d\lambda} = -\frac{c}{\lambda^2}$$

Ако заместим диференциалите с крайни разлики и отчетем само абсолютните стойности:

$$\Delta f = \frac{c \Delta \lambda}{\lambda^2}$$

Честотна лента на електромагнитните вълни

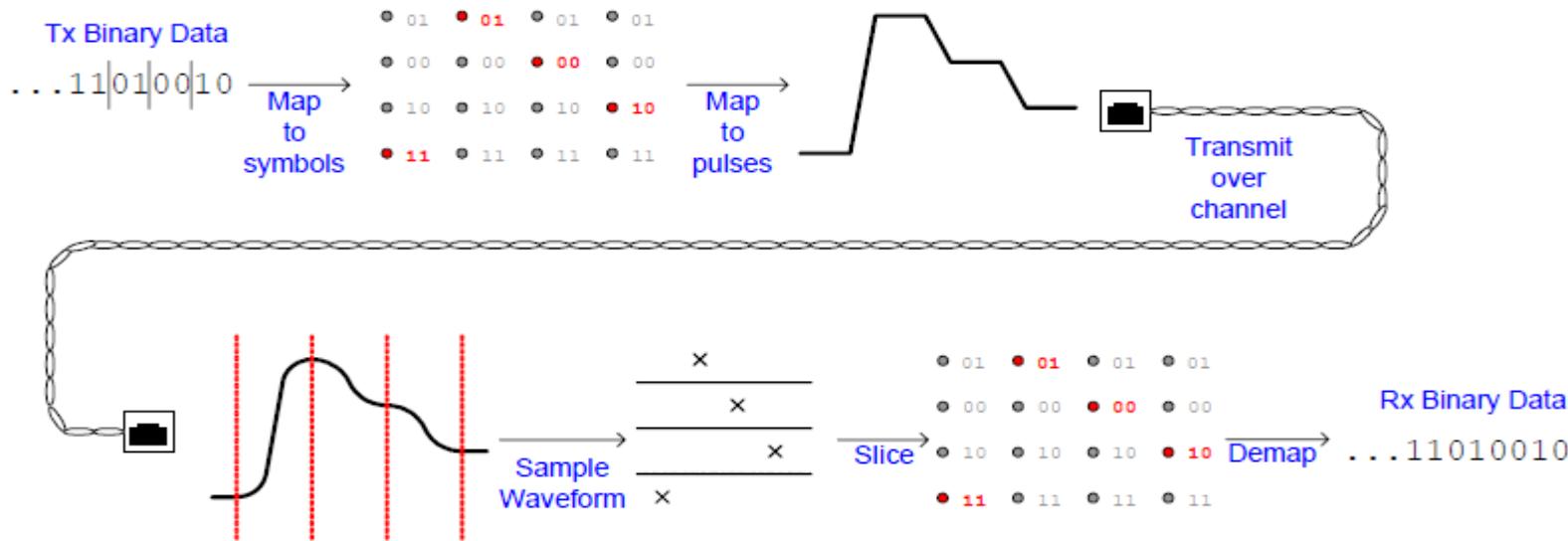
Честотната лента е обратно пропорционална на дълчината на вълната и право пропорционална на С и диапазона, в който се изменя дълчината на вълната.

Например, оптическото влакно (fiber optic – FO) е в 1.30 μm обхват:
 $\lambda = 1.3 \times 10^{-6}$ и $\Delta\lambda = 0.17 \times 10^{-6}$, следователно: $\Delta f \approx 30 \text{ THz}$.
При 8 bits/Hz: 240 Tbps.

Спектърът на електромагнитните вълни е показан по-нататък, в слайдовете за безжичните комуникации.

Влияние на преносната среда.

Сигнали с много нива



“Размиване” (изкривяване) на сигнала.

Предавайки сигнали с много нива на напрежение, кодираме групи от битове, а не с две нива да се кодира един единствен бит.

$$bw \sim 1/\text{бр.нива}$$

На фигурата имаме 4 нива, кодираме два бита на ниво.

Така по един и същ кабел предаваме 10/100/1000 Mbps.

Формула на Найкуист

През 1924 г. Henry Nyquist, инженер от AT&T, стига до извода, че всеки комуникационен канал има граничен капацитет.

И, колкото по-широка е **честотната лента**, толкова точно се възпроизвежда цифровият сигнал.

Найкуист извежда **формула**, показваща зависимостта на максималната скорост от честотната лента:

$$C = 2 \cdot B \cdot \log_2 L \text{ [bit/s]}$$

C – скорост на предаване на данните; **B**, Hz – честотна лента; **L** – брой на нивата на двоичния сигнал.

Формула на Найкуист

Например, $B = 3100 \text{ Hz}$ (частотна лента на обикновена телефонна линия); $L = 8$ нива (0-7):

$$C = 2 * 3100 * \log_2 8 = 18600 \text{ [bit/s]}$$

Ако $L=2$ (0 и 1): $C = 2 * 3100 * 1 = 6200 \text{ [bit/s]}$

На практика скоростта ще е по-ниска заради странични фактори: **шумове**.

Формула на Шенон

Шенон (Shannon, 1948) въвежда отношението **сигнал/шум** (Signal/Noise Ratio - SNR) в края на линията.

Отношението на **мощността** на полезния сигнал **S** към мощността на случайния шум **N**, измерени във ватове (**W**). Изразява се в **декабели**:

$$\text{SNR} = 10 \cdot \log_{10}(S/N), [\text{dB}]$$

Максимална теоретична скорост на предаване по формула Шенон-Хартли:

$$C = B \cdot \log_2(1 + S/N), [\text{bit/s}]$$

C, bit/s – скорост; **B, Hz** – честотна лента

Жични среди за предаване на сигнали (данни)

Медни кабели:

- Тип “усукана двойка” (Twisted Pair - ТР)
- Коаксиален кабел

Влакнестооптически кабели (Fiber Optics - FO)

Защо медни

Медта (**Cu**) е с най-добро съотношение цена/качество:

- ниско специфично съпротивление:
 $\rho = 0.016 \text{ } [\Omega \cdot \text{mm}^2/\text{m}]$;
- добра здравина и гъвкавост;
- широко разпространен в природата.

Медни кабели

Честотната лента
(bandwidth - bw), [bit/s],
зависи от сечението на
проводника (S) и
дължината (l). Според
разширения закон на Ом
(вдясно).

$$R = \rho \frac{l}{S}$$

Друг параметър е стъпката
на усукване:

Колкото повече на единица
дължина, толкова повече
 bw .

Twisted Pair (усукана двойка)

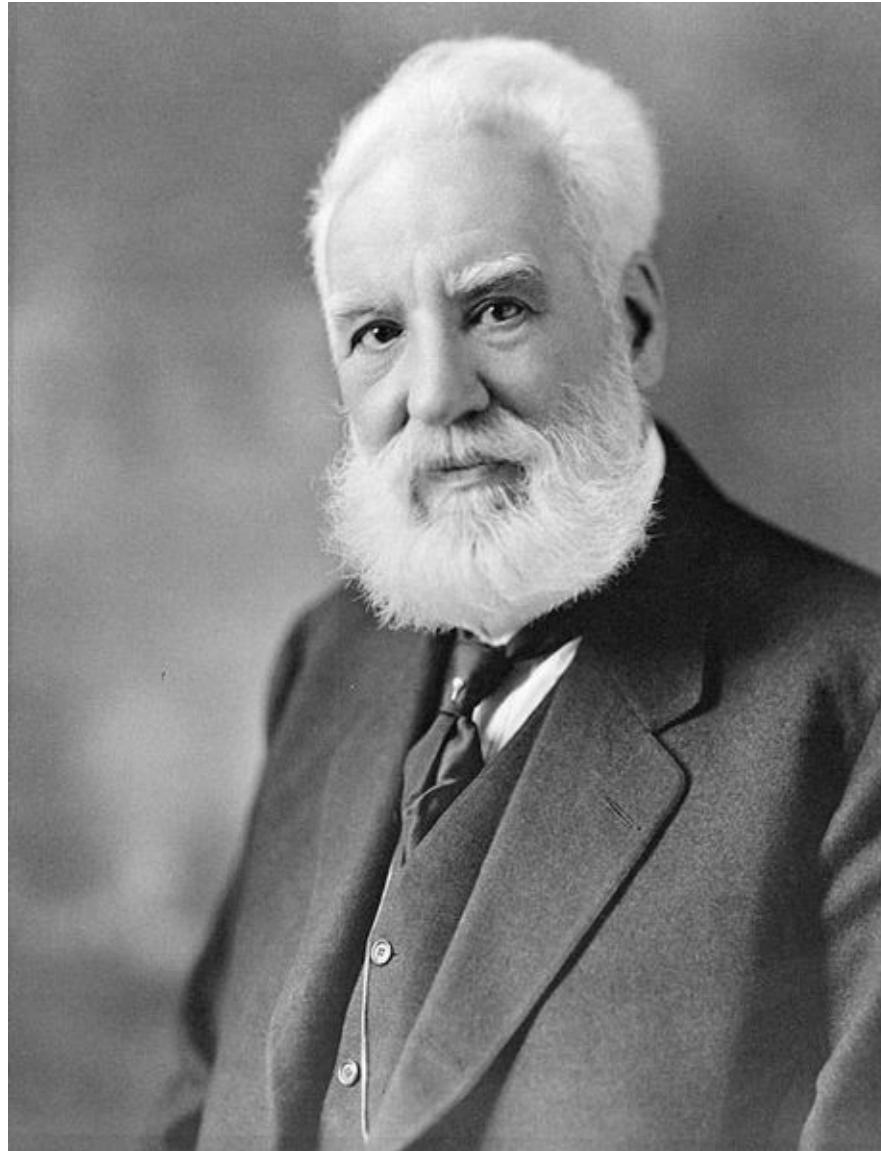
При кабелите тип “усукана двойка” (Twisted Pair) два проводника (прав и обратен) са усукани така, че да се анулира или подтисне електромагнитната интерференция (electromagnetic interference - EMI) на външни източници:

- съседни UTP кабели;
- прослушване (crosstalk) от съседни чифтове;
- други шумоизточници.

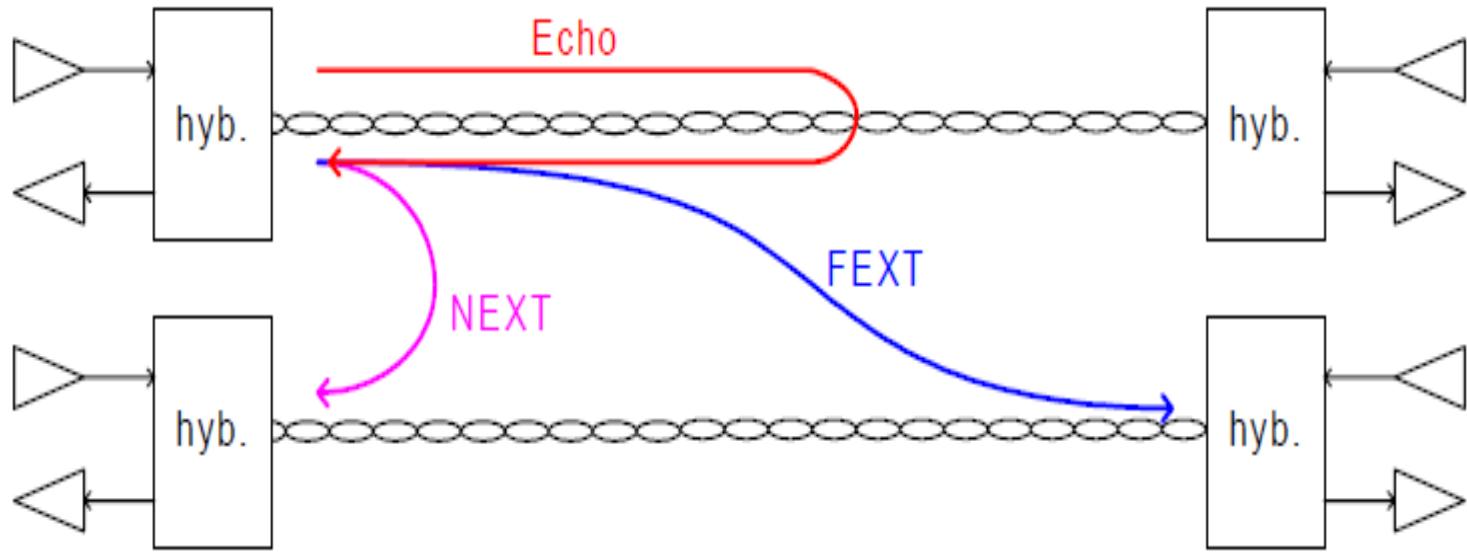
Изобретен от Alexander Graham Bell и патентован с US patent 244,426 Telephone-circuit (1881).

Прилага се диференциален режим на усилване на сигналите.

Alexander Graham Bell



NEXT. FEXT. Echo.



Near-end crosstalk (**NEXT**)

Far-end crosstalk (**FEXT**)

Диференциален режим

В усуканата двойка едната жица носи прав, а другата обратен сигнал.

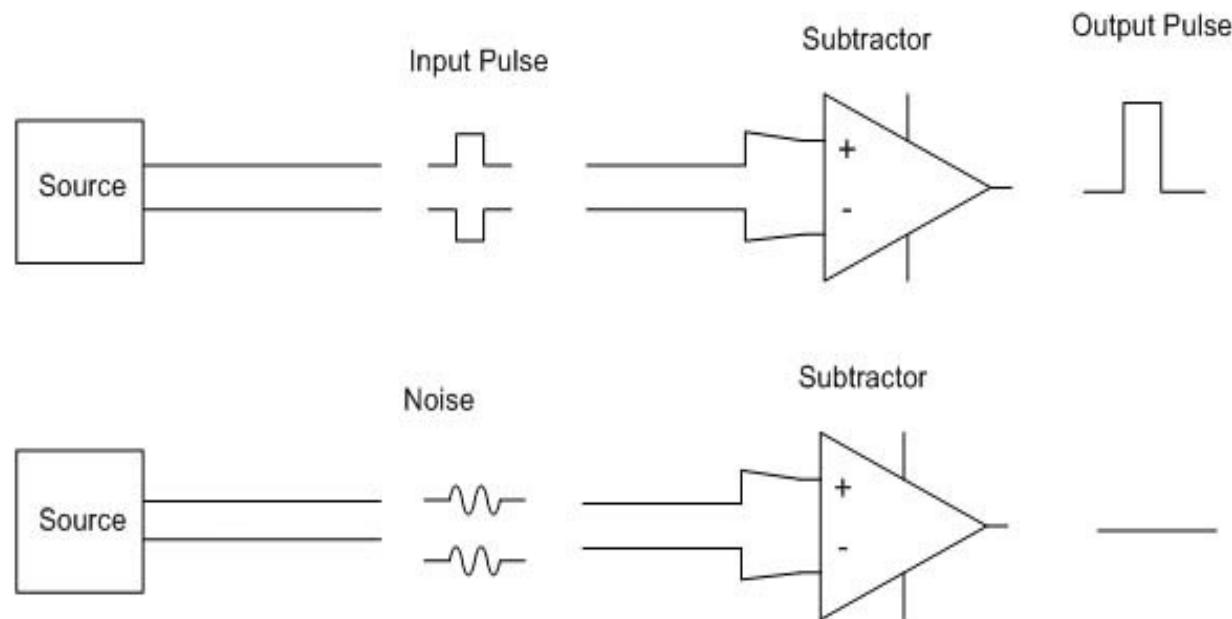
В крайната точка се приема разликата между двета:

$$S - (-S) = 2 \cdot S$$

Шумът се индуцира и в двета проводника в “права посока”. И така се анулира при приемника, който взима диференциалния сигнал:

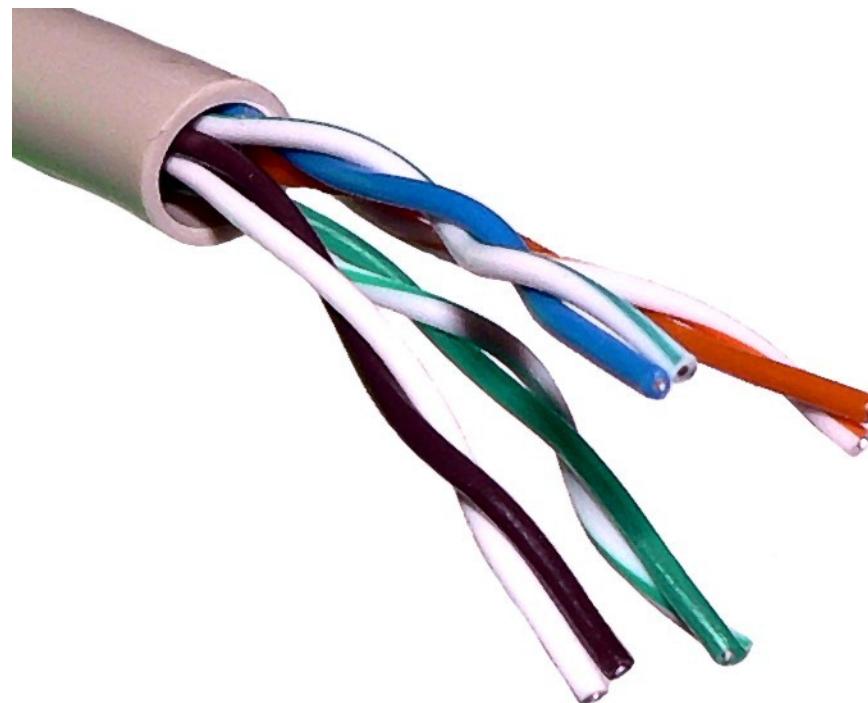
$$N - N = 0$$

Диф. режим. Схема.

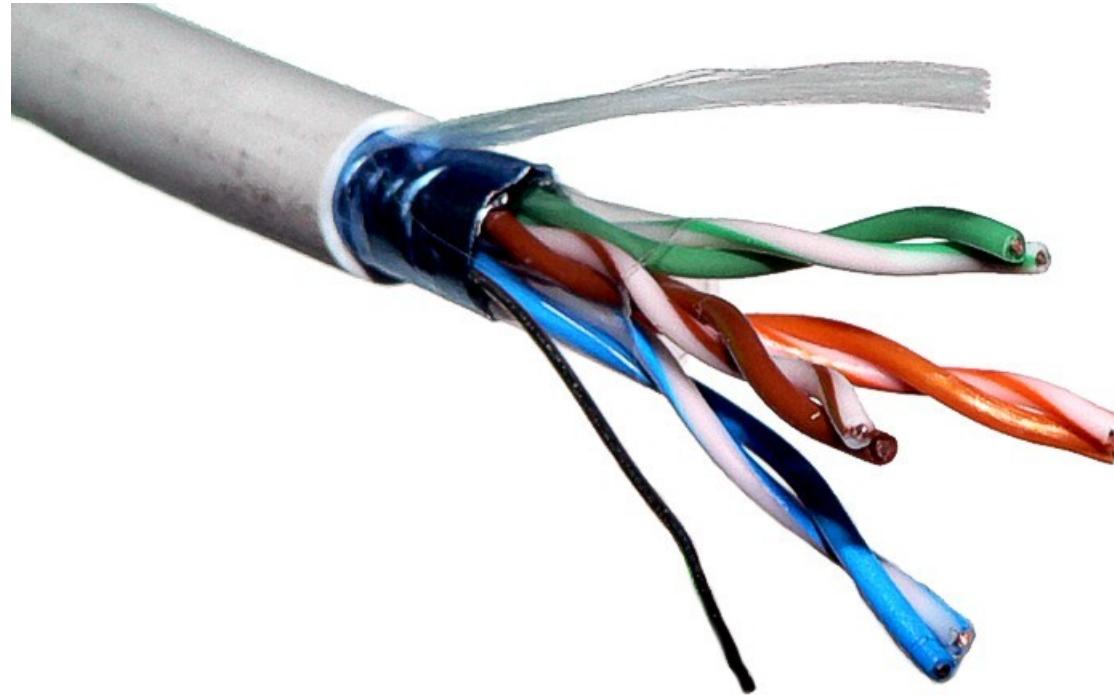


Unshielded twisted pair (UTP)

UTP се прилагат широко в телефонните мрежи и в локалните мрежи (LAN) Ethernet.



Екранирани кабели



S/UTP или FTP

Екранирани кабели



S/STP или S/FTP

Кабели с едно и многожилни проводници

- Кабелите с **едножилни** проводници се монтират за постоянно – вертикални и **хоризонтални** инсталации;
- Кабелите с **многожилни** проводници са гъвкави и се използват за свързващи (**пач**) кабели: например, компютър-розетка.

Категории Twisted Pair кабели

Категория	Стандарт	BW, MHz	Приложение
3	TIA/EIA-568-B	16	10 Mbit/s Ethernet
5	не	100	100 Mbit/s Ethernet
5e	TIA/EIA-568-B	100	100 Mbit/s и Gigabit Ethernet
6	TIA/EIA-568-B	250	Gigabit Ethernet и повече
6a	ANSI/TIA/EIA-568-B.2-10 и Amendment 1 and 2 of ISO/IEC 11801	500	10 Gigabit Ethernet
7	ISO/IEC 11801	600	S/FTP кабели
7a	Amendment 1 and 2 of ISO/IEC 11801	1000	S/FTP кабели

Cat 8 меден кабел за Data Center

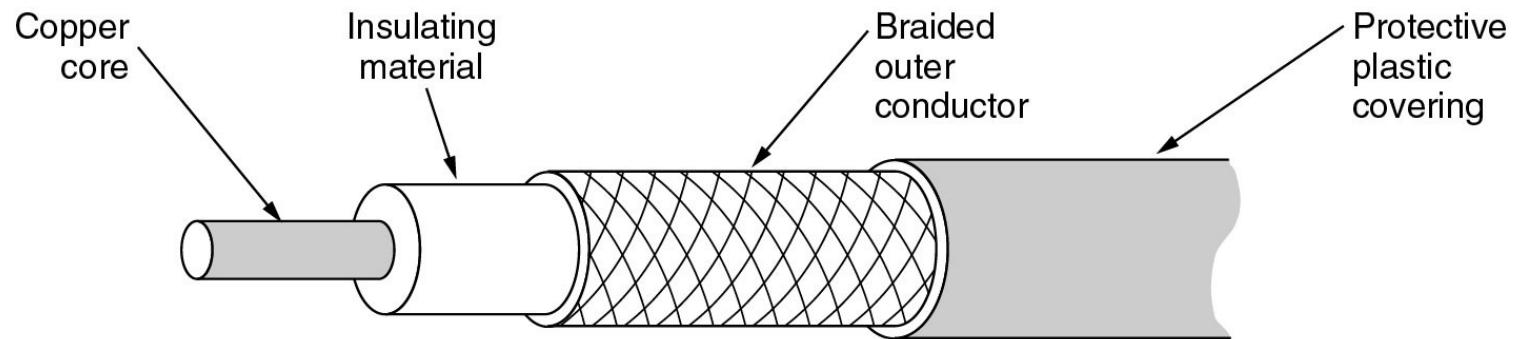


Although the standards have not been finalized, it is important for data center managers and suppliers to have a good sense of what Category 8 will look like, and how it will affect the data center infrastructure.

Bw: 2 GHz, за скорости от 40 Gbps в Data Center;

Конектор RJ-45 – подобен, обратно съвместим с Cat 6A, 7A.

Коаксиален кабел



Класическият Ethernet – 50Ω (тънък); CATV - 75Ω (дебел).

Влакнеста оптика. Принципи.



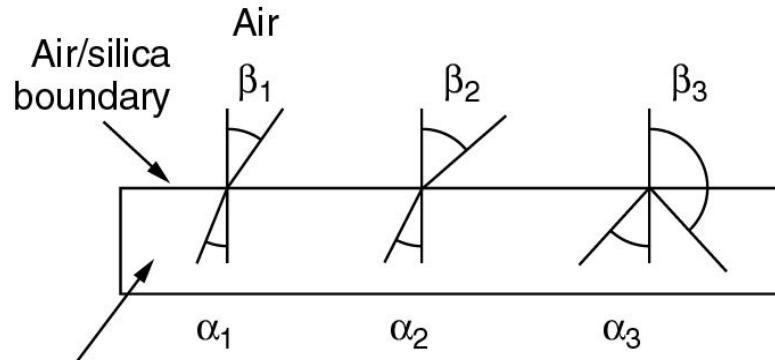
Една оптическа комуникационн система (Fiber Optics – FO):

Предавател: електрически в оптически (**светодиод или лазер**), преносна среда (тънка стъклена нишка – **optical fiber**) и фотоприемник (**фотодиод**) – оптически в електрически.

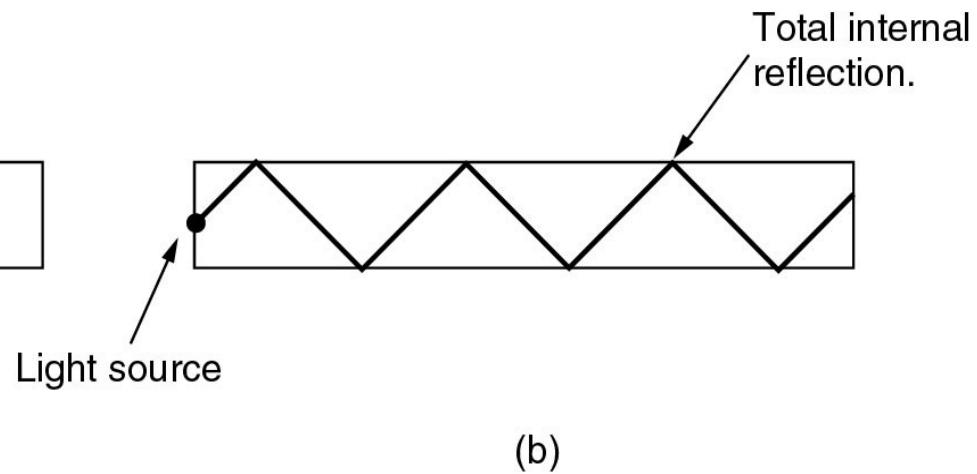
Един светлинен импулс (“лог. 1”), отсъствие (“лог. 0”)

Т.е **светне – 1**; **гасне – 0** и т.н.

Влакнестооптически кабели (Fiber Optics)



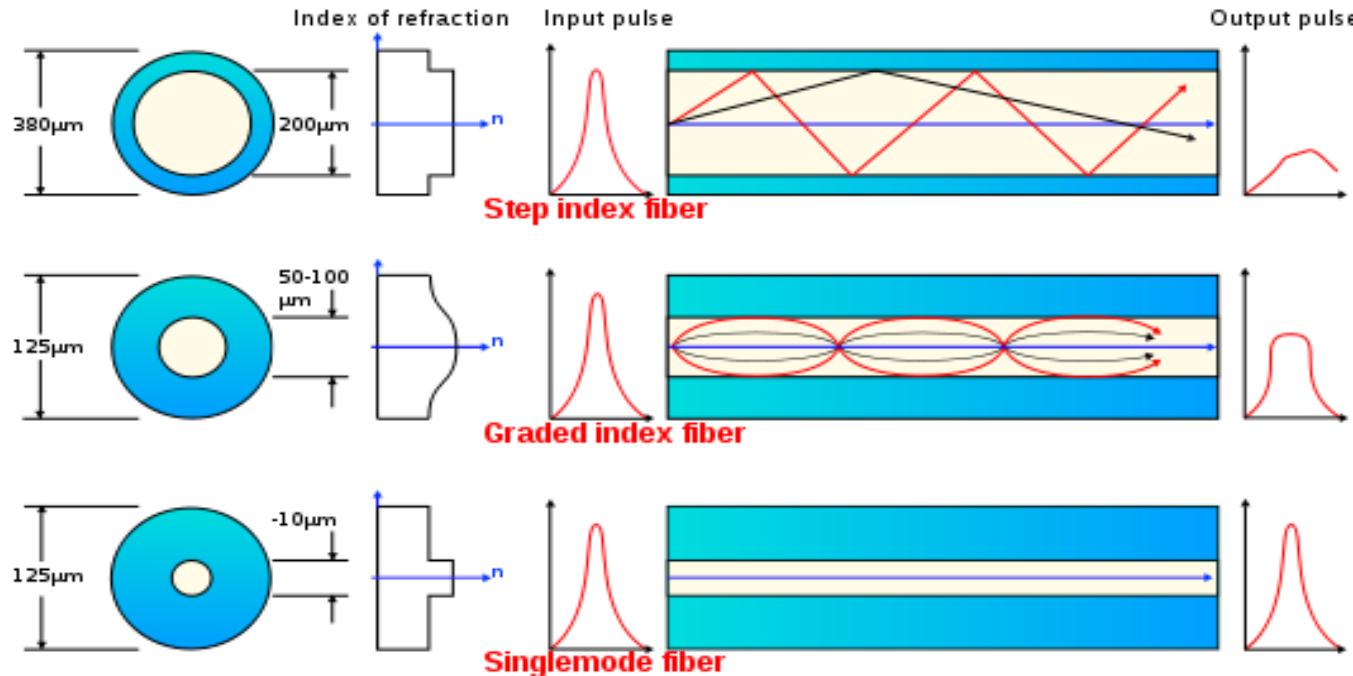
(a)



(b)

- (a) Светлинният лъч пада под различен ъгъл на границата “въздух-силиций”.
- (b) Пълно вътрешно отражение на светлинния лъч. Няма загуби на сигнал (т.е информация).

Видове оптически влакна



Многомодово (Multi-mode - MM) със стъпаловиден профил на коефициента на пречупване.

MM градиентно влакно.

Едномодово (Single-mode – SM) оптическо влакно.

Видове оптически влакна

ММ Светлините лъчи (модове) са разпръснати по многобройни пътища.

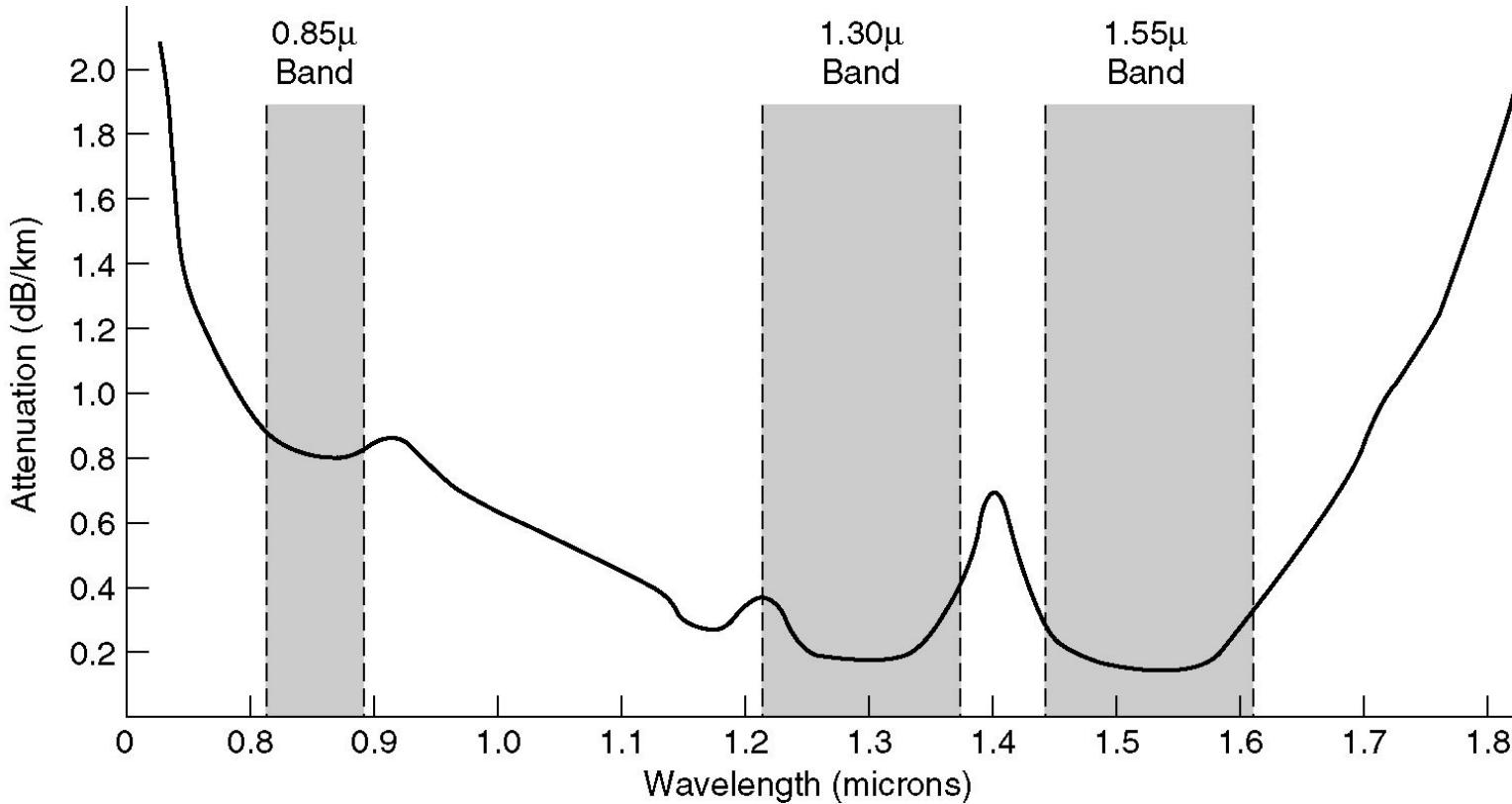
ММ влакната със стъпаловиден профил на коефициента на пречупване имат пълно вътрешно отражение на няколко дължини на вълната.

ММ градиентно влакно. Коефициентът на пречупване намалява постепенно. Както се вижда от фигурата са с по-добри характеристики.

Едномодово (**Single-mode – SM**) оптическо влакно. По него се разпространява един единствен лъч (мод).

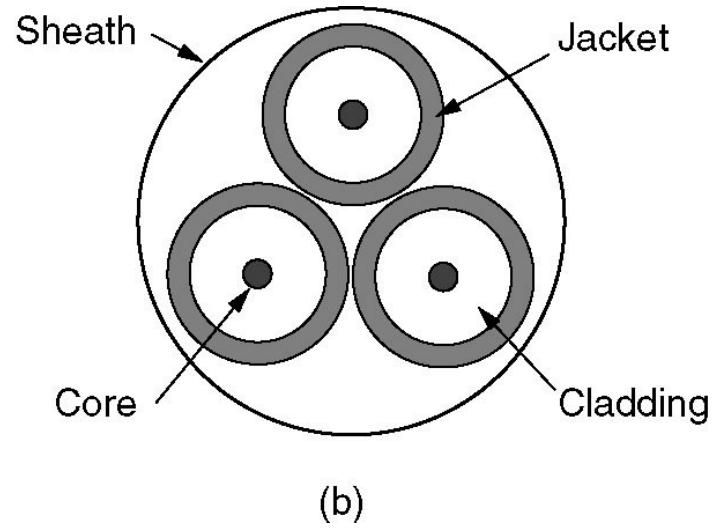
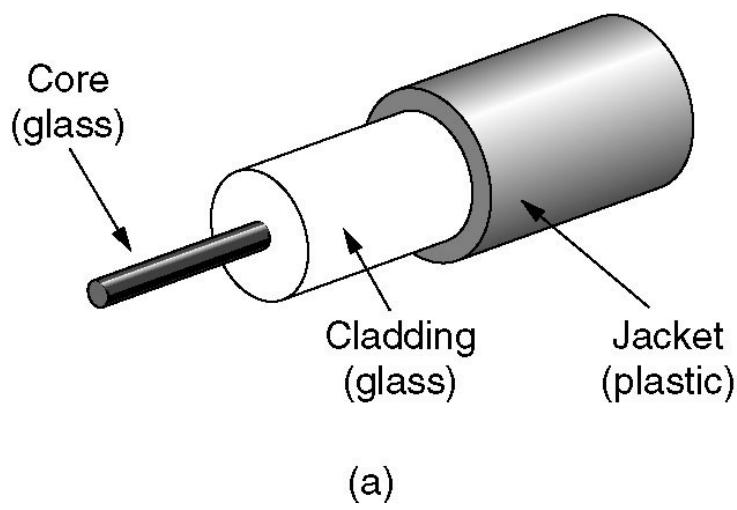
Основно предимство: не се влияе от външни шумове (ЕМI, влага и др.)

Честотни обхвати



Според коефициента на затихване във FO комуникациите имаме три честотни обхвата, центрирани около дължини на вълната 0.85, 1.30 и 1.55 μ m (850, 1300 и 1550 nm).

Оптически кабели. Конструкция.



(a) Едно влакно, поглед отстрани.

(b) Напречен разрез на кабел с три влакна.

Оптически кабели. Характеристики.

	MM	SM
core/clad	50/125 μm или 62.5/125 μm	10/125 μm
Дължина на вълната	850 nm и 1300 nm	1310 или 1550 nm
скорост/разстояние	100 Mbit/s / 2 km 1 Gbit/s / 220–550 m 10 Gbit/s / 300 m	10 Gbit/s / над 80 km (зависи от лазера) С усилватели и DWDM: $n \cdot 10^3$ km / 10 Gbit/s или $n \cdot 10^2$ km / 40 Gbit/s

Конструктивни изисквания към кабелите – FO и медни

При полагане под земя или под вода – да са
защитени от механични увреждания (гризачи,
вълни).

Инсталиране в сгради – изолацията да е
пожароустойчива – да не разпрострнява огъня и
да не изпуска задушливи газове.

Passive Optical Network

Passive optical network (**PON**) е **point-to-multipoint** архитектура за оптика до дома/офиса.

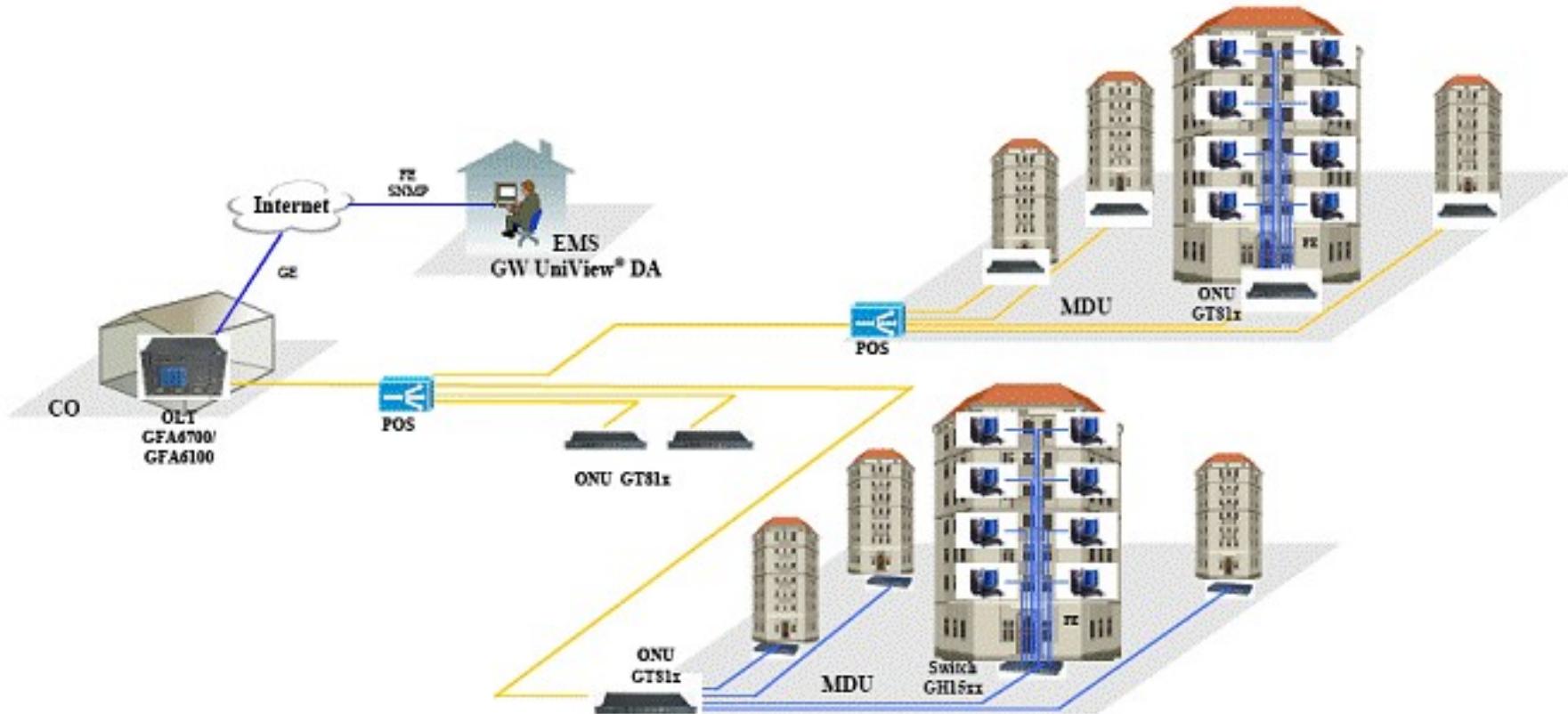
Пасивни сплитери, прилагащи “ъгъла на Brewster”, позволяват едно влакно да обслужва 32-128 крайни точки.

PON включва: optical line terminal (**OLT**) откъм провайдера и множество optical network units (**ONUs**) откъм потребителите.

Сигналите към потребителя (**Downstream**) се “broadcast” до всяка крайна точка, като споделят едно влакно. За защита на данните се прилага **криптиране**.

Сигналите към провайдера (**Upstream**) се мултиплексират с помощта на протокол за **множествен достъп**, какъвто е time division multiple access (**TDMA**).

Passive Optical Network

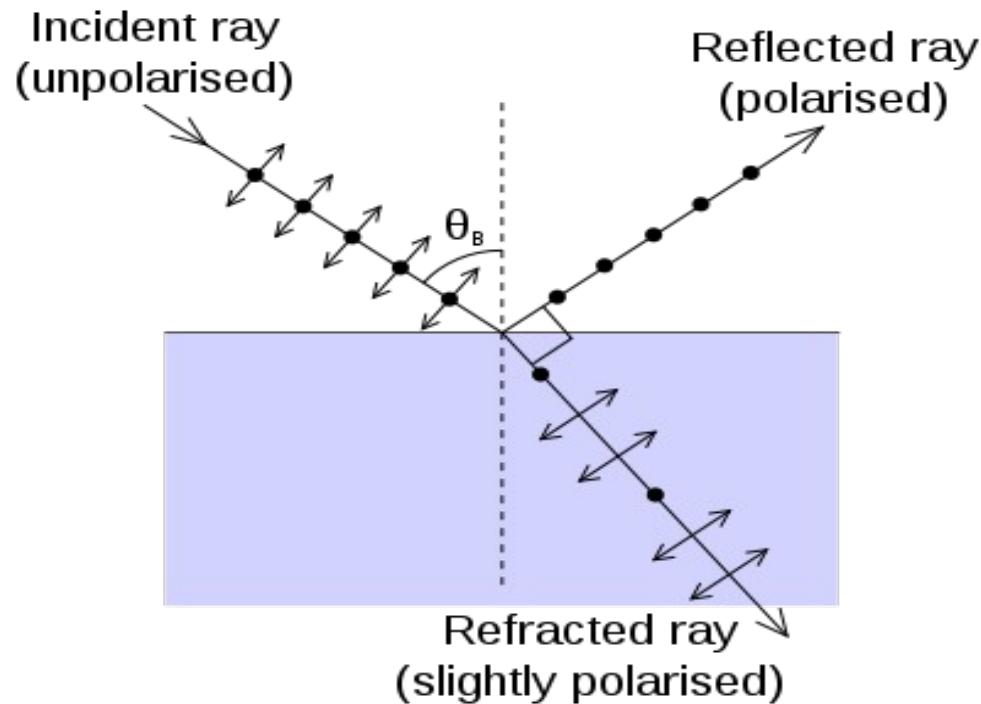


Passive optical network

В PON, както и всички съвременни оптически системи, се прилага мултплексиране по дължина на вълната (**wavelength division multiplexing - WDM**), което позволява:

- по едно и също влакно да върви двупосочен трафик (първите системи използваха едно влакно за downstream и друго за upstream), за всяка от посоките - отделна дължина на вълната;
- по едно и също влакно да върви трафик на различни потребители, за всеки потребител - отделна дължина на вълната.

Ъгъл на Brewster



Преминавайки м/у две среди с различен индекс на пречупване, част от светлината се отразява на границата. При определен ъгъл на падане, светлина с определена поляризация не може дабъде отразена. Това е ъгълът на Brewster, θ_B .

Мултиплексиране

Високочестотните характеристики на кабелите за предаване на данни (UTP, STP, FO и коаксиални) позволяват два режима:

- Директно предаване (**baseband**) – наличната честотна лента се предоставя на един канал, по който се предават поток от битове със скорости 10, 100, 1000 Mbit/s и т.н., които се кодират (**LANs**);
- Широколентов режим (**broadband**) – наличната честотна лента се разделя на определен брой подканали, всеки с част от общата честотна лента. Прилага се мултиплексиране и модулация (**WANs**).

Модулация. Обяснение. (за сведение)

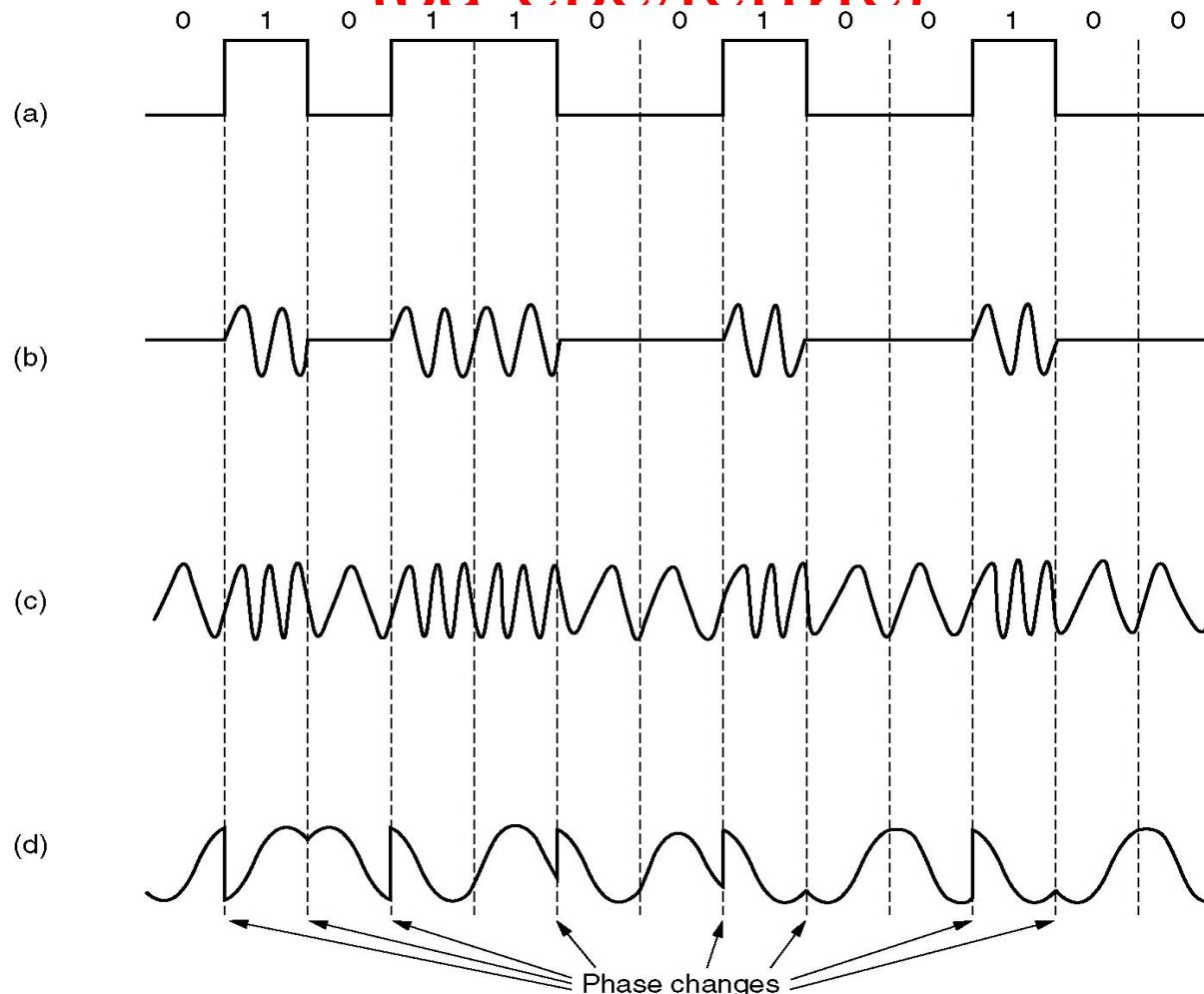
При тясна честотна лента (например при телефонните линии) цифровите сигнали не могат да се предават точно, поради което се използва **модулация**.

Въвежда се носещ сигнал (**носеща честота - carrier**) и информацията се предава чрез:

- смяна на неговата честота (**честотна модулация**);
- амплитуда (**амплитудна модулация**) или
- фаза (**фазова модулация**).

Прилагат се и по-сложни техники за модулация.

Модуляции. Модеми. (за свеление)



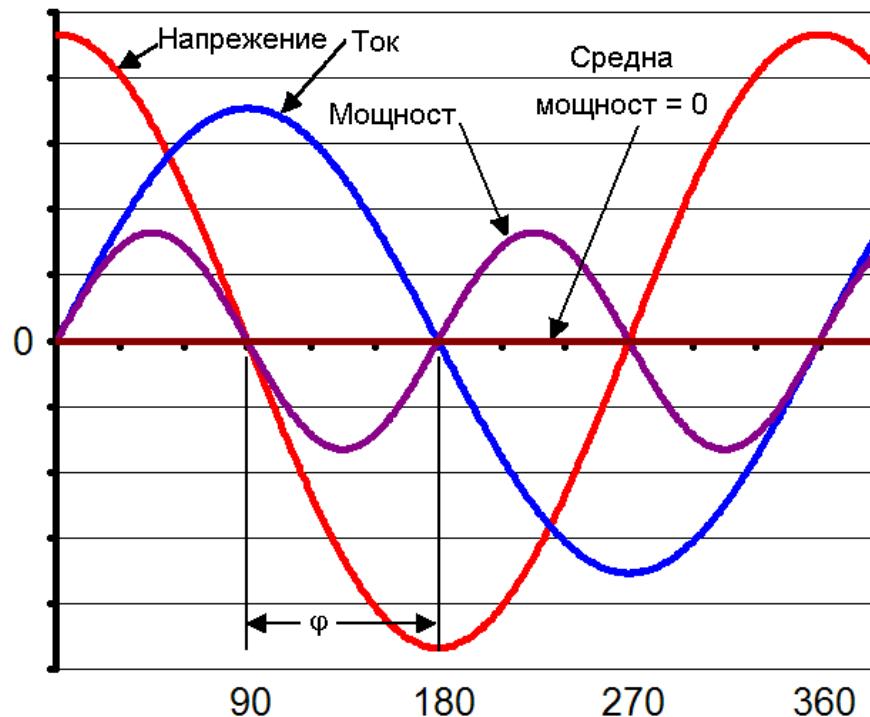
(a) двоичен сигнал

(b) амплитудна модулация

(c) честотна модулация

(d) фазова модулация

Фаза (пример - за сведение)



Wavelength Division Multiplexing (WDM)

В оптическите канали се използва мултиплексиране с разделяне на дълчините на вълните (**WDM**).

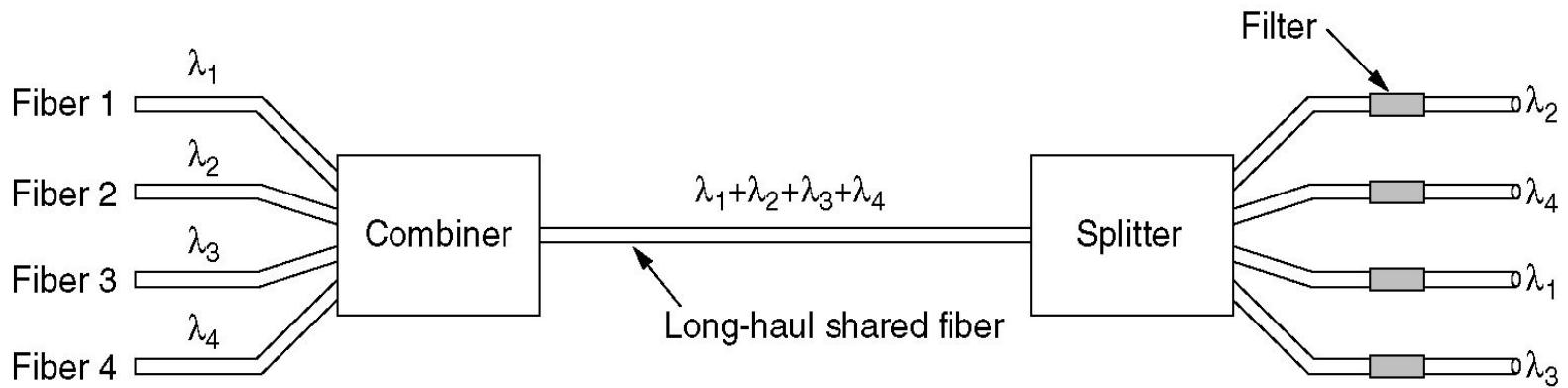
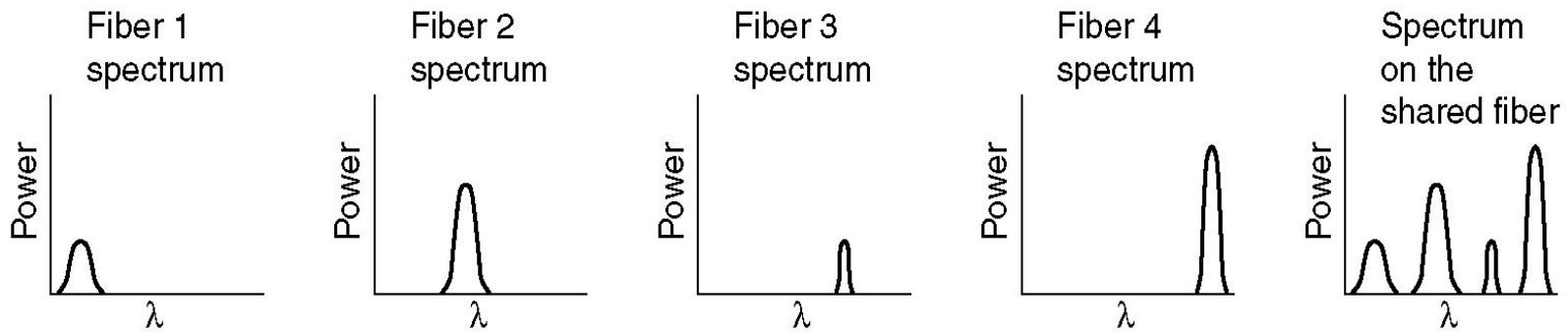
На фигурата по-долу лъчи от 4 влакна, всяко с различна λ постъпват в призма или дифракционна решетка.

Четирите лъча се обединяват в един лъч, който се пренася по общо FO.

В точката на приемане става разцепване в обратна посока.

Сега се използва Dense wavelength division multiplexing (**DWDM**).

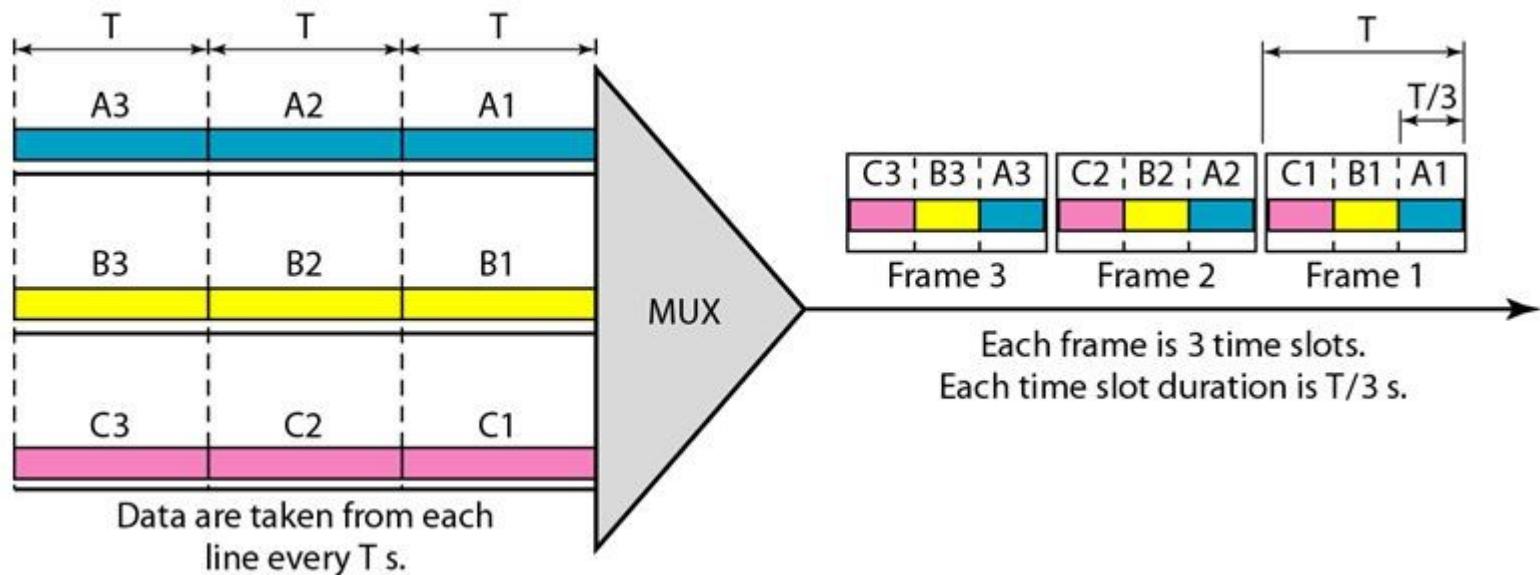
Wavelength Division Multiplexing



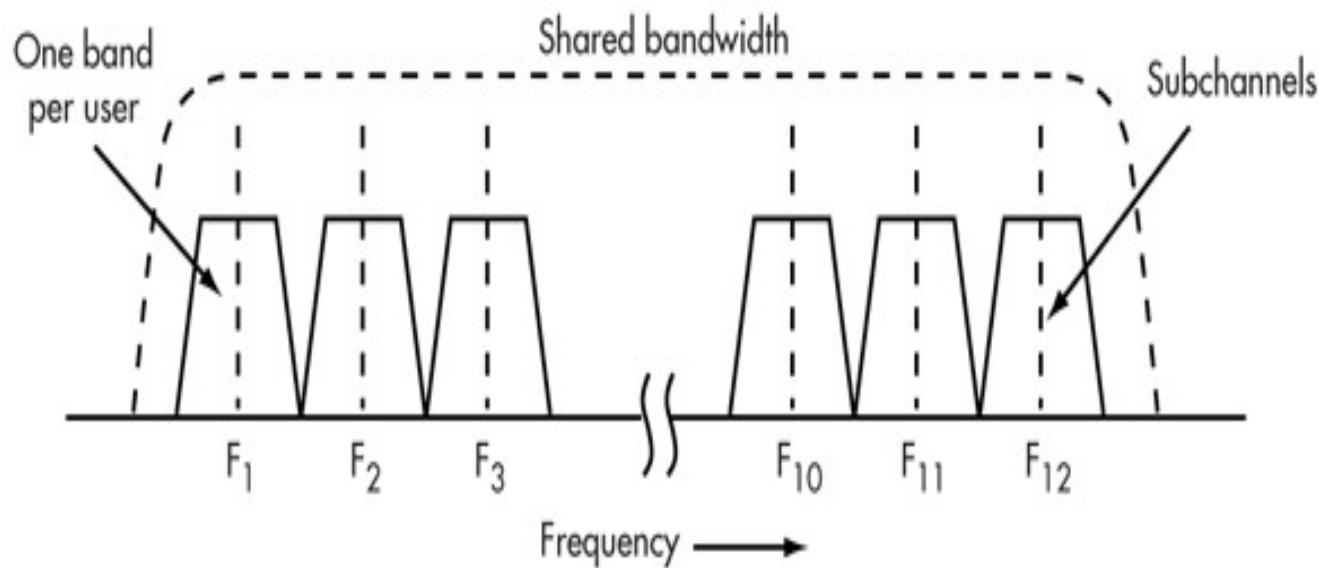
$\Delta f / \text{влакно} \approx 25000 \text{GHz}$. Т.е мултиплексират се огромен брой канали на големи разстояния.

Time Division Multiple Access (TDMA)

За всеки източник от информация се предвижда определен интервал от време (time slot), през който той разполага с канала.



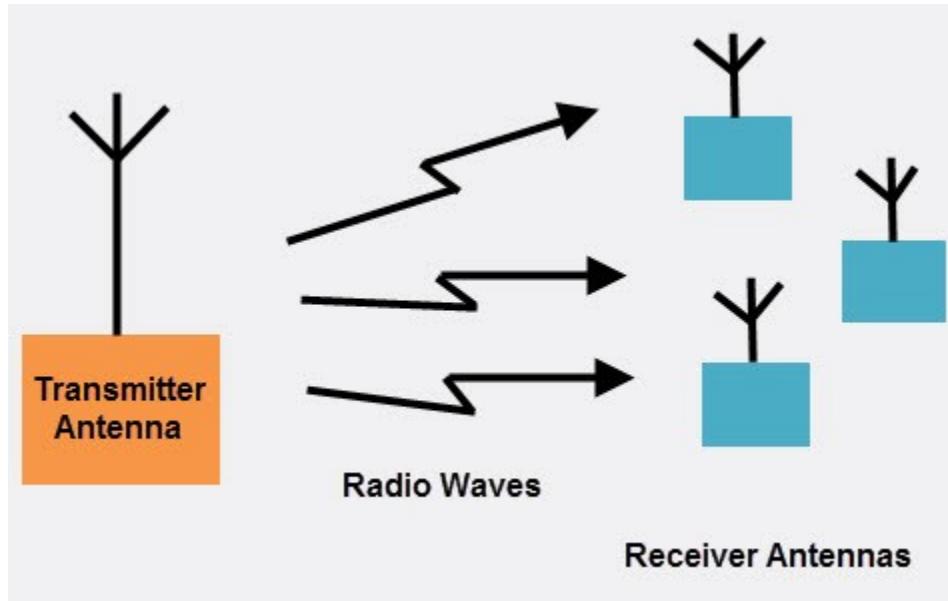
Frequency Division Multiple Access (FDMA)



FDMA алокира един или повече честотни обхвата (канали) на всеки потребител.

Заб. МА (Multiple Access) е технология за достъп на каналния слой, докато **Multiplexing** се отнася към физическия слой.

Безжични комуникации (Wireless Communication)



Безжични комуникации

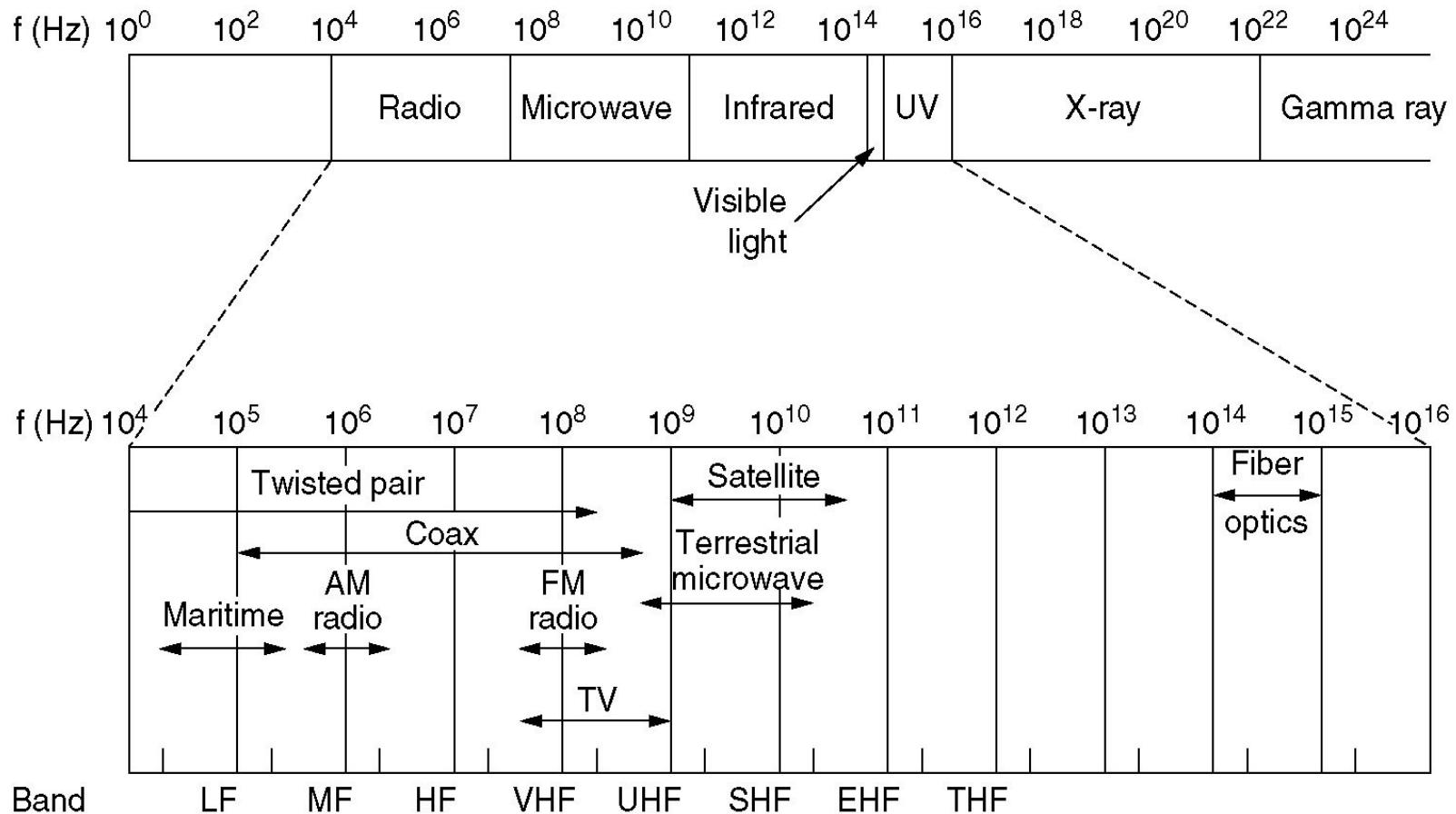
Бъдещето принадлежи на оптическите (външно окабеляване и вертикално в сгради) и безжичните (LAN – домашни и корпоративни) комуникации.

Основно предимство – нулеви разходи за преносна среда.

Достатъчна е точно оразмерена антена, прикрепена към предавател и информацията се носи от електромагнитните вълни. Посреща я също антена, прикрепена към приемник.

Покриваното разстояние зависи от честота, релеф, атмосферни условия.

Спектър на електромагнитните вълни



Спектър на електромагнитните вълни

За предаване на информация чрез вече известните модулации се използват **радио, микровълнов, инфрачервен** и обхвата на **видимата светлина** от спектъра.

Ултравиолетови, рентгенови (X-rays) и гама лъчите са даже по-добри (високи честоти), но са опасни за здравето.

В долната част на фигурата: **имена на обхватите** според **ITU**.

Разпределение на честотния спектър

За да се предотврати хаос, съществуват национални и международни споразумения за това кой и как да използва конкретни честоти:

За АМ и FM радио, TV, мобилни телефони, полиция, военни и т.н.
В глобален мащаб **ITU-R** координира.

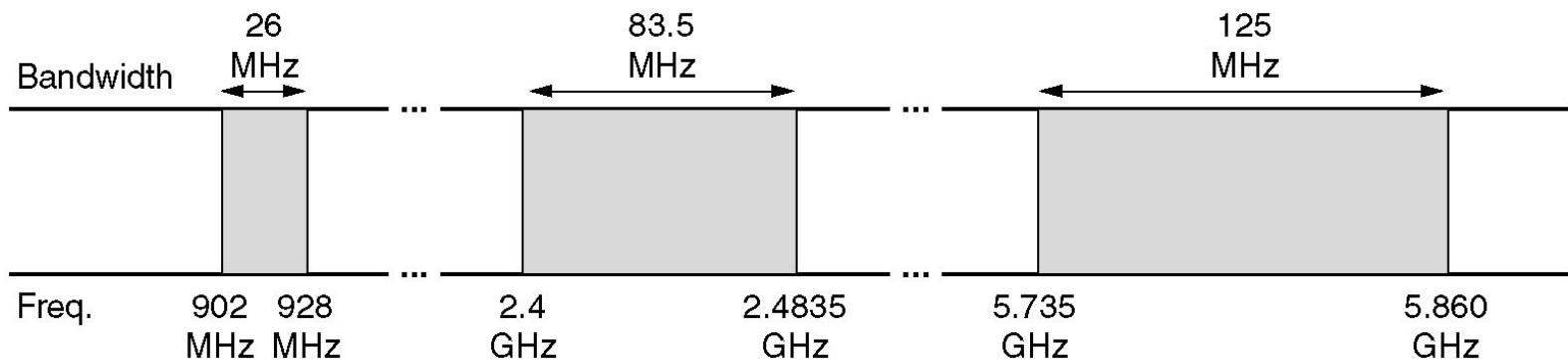
Всяка страна си има такава организация:

FCC (Federal Communication Commission) в САЩ;

KPC (Комисия за регулиране на съобщенията) у нас.

Имаме си “**Национален план за разпределение на радиочестотния спектър**” (<https://crc.bg/bg/rubriki/192/radiochestoten-spektyr>)

Нелицензиирани обхвати



Честотни ленти 26.957 - 27.283 MHz, 40.660 - 40.700 MHz, 433.050 - 434.790 MHz, **2400 - 2483.5 MHz**, **5725 - 5875 MHz**, 24 - 24.25 GHz, 120.06 - 126 GHz и 241 - 248 GHz се използват за устройства за промишлени, научни и медицински цели (**ISM**). (Това са **нелицензираните обхвати**)

Според заб. 77: 900+ MHz е даден на GSM операторите. (на фиг. важи за САЩ)

Безжични мрежи в нелицензираните обхвати

Wireless local area network (**WLAN**): популярна като WiFi (стандарти на работна група IEEE 802.11).

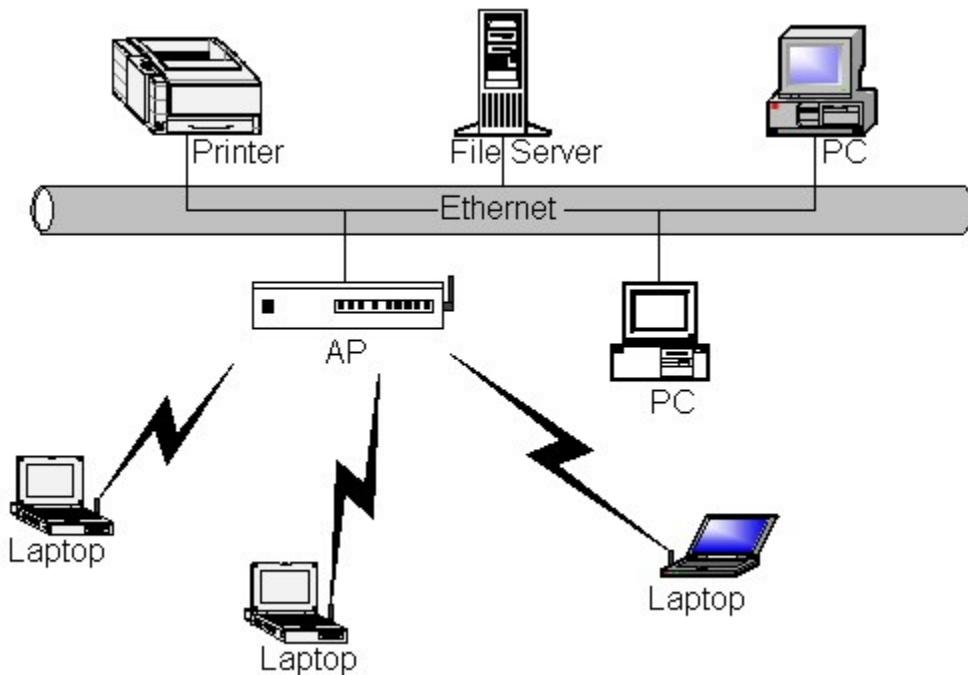
Wireless PAN (Personal Area Network): най-популярна Bluetooth (стандарти на работна група IEEE 802.15).

IEEE 802.11 стандарты

802.11 Wireless Standards

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

Безжична локална мрежа (WLAN)



Wi-Fi версии:

Wi-Fi 1: 802.11b (1999)

Wi-Fi 2: 802.11a (1999)

Wi-Fi 3: 802.11g (2003)

Wi-Fi 4: 802.11n (2009)

Wi-Fi 5: 802.11ac (2014)

Wi-Fi 6: 802.11ax (2018)

Ортогоналността...



В **компютърните науки**: промяна в поведението на даден компонент нито създава, нито прехвърля странични ефекти към други компоненти от системата.

Ортогонален набор от инструкции: всяка инструкция може да използва всеки регистър във всякакъв адресен режим.

В **кумуникациите** схемите с множествен достъп (**multiple-access**) са ортогонални, когато идеалният приемник може да отхвърли паразитните сигнали.

Примери: **TDMA, OFDM**.

... и високите скорости в безжични и др. среди...

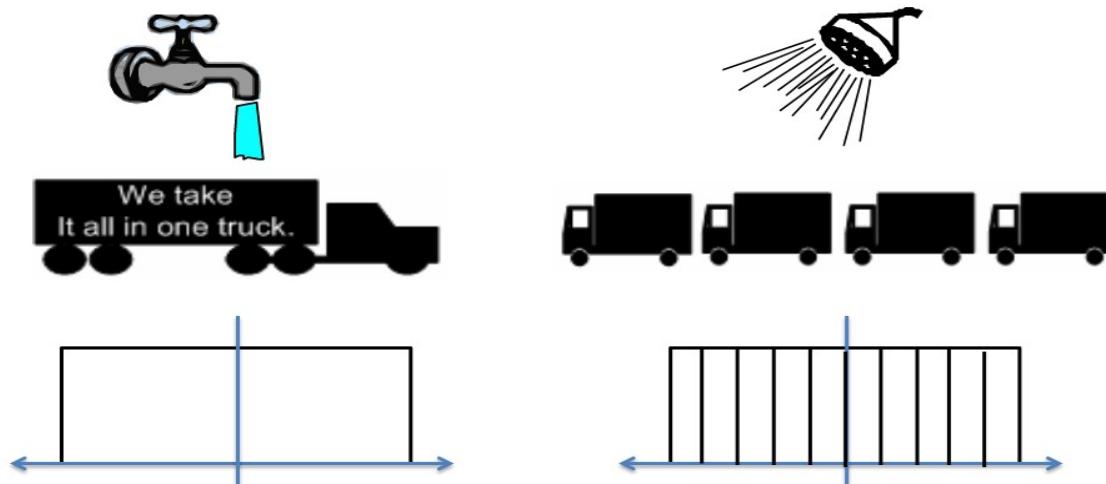
В Цифрова ТВ, ADSL, WiFi, WiMAX, комуникациите по електрозахранващи мрежи прилагат по-нетрадиционни идеи:

-**Модулация** на цифров сигнал с помощта на **много носещи**:

-Излъчваният поток от битове се разделя на **субпотоци** и се “носи” от много **субносещи**. Битовата скорост на всеки субканал е много по-ниска от общата.

-Много по-ефективно използване на спектъра се постига с “**ортогонални**” субносещи, чиито спекtri се припокриват, но поради ортогоналността си сигналите си влияят минимално.

...OFDM (Orthogonal frequency-division multiplexing)



(ляво) Използвате **цялата** честотна лента, за да изпратите данните.

(дясно) Изпращате данните на малки порции едновременно с помощта на множество **ортогонални подканали**.

Те са честотно отделени един от друг, така че да се гарантира “ортогоналността”: при демодулация да се получи точната честота на полезния сигнал, да няма отклонения и изкривявания.

MIMO-OFDM

MIMO (Multiple-Inputs Multiple-Outputs)-OFDM.

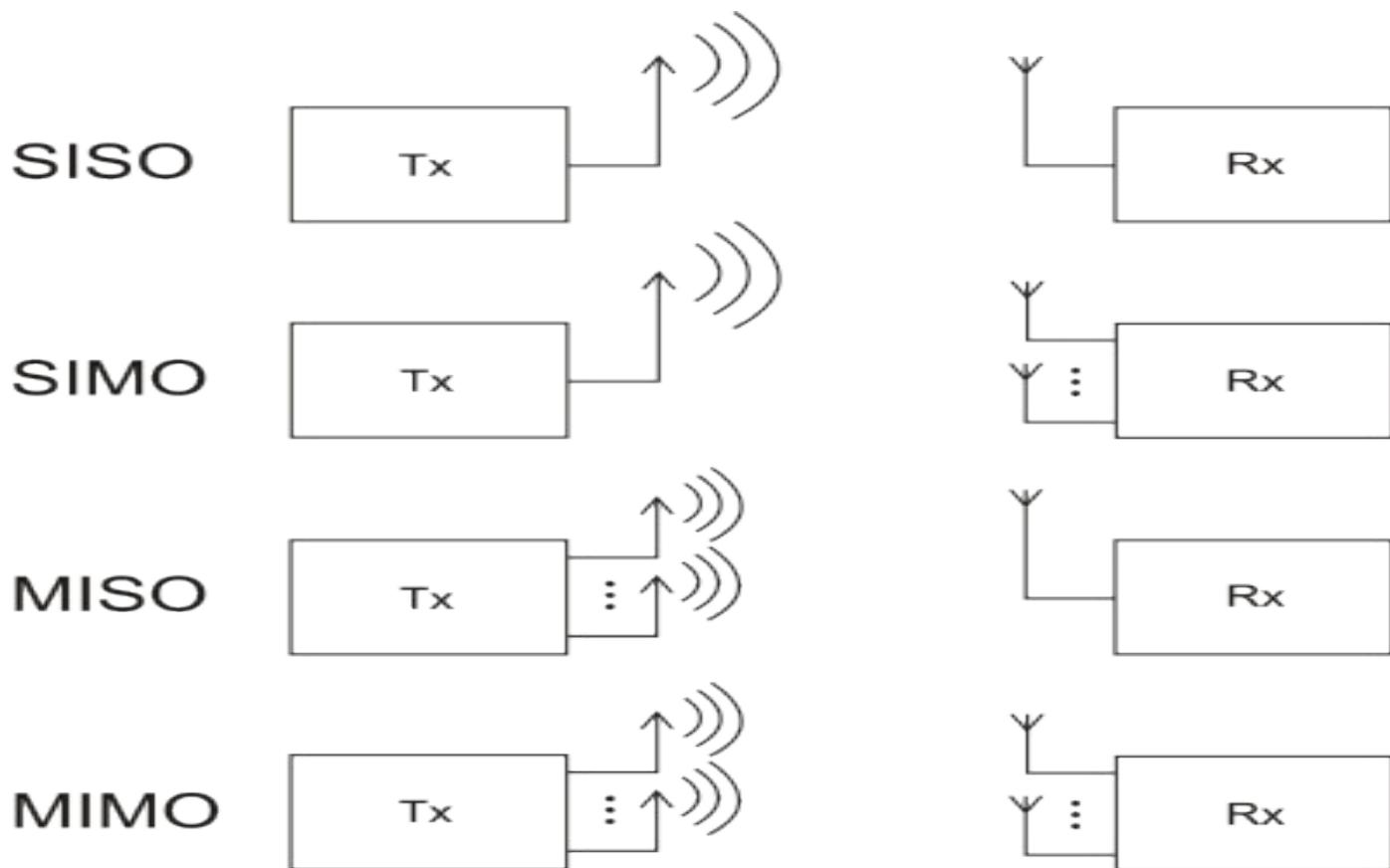
Използва множество антени за едновременно предаване на данни на малки порции.

Приемникът възстановява данните в оригиналния им вид.

Този процес се нарича още „пространствено мултиплексиране“.

Вдига скоростта на предаване пропорционално на броя на антените.

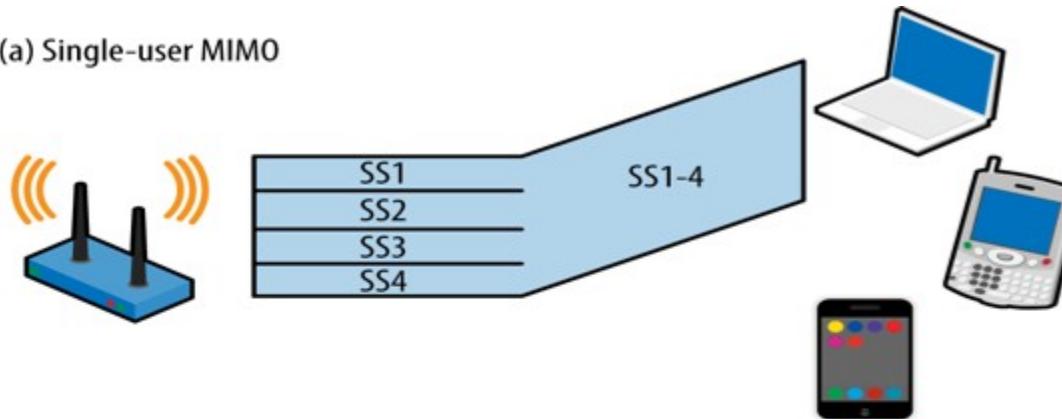
MIMO-OFDM



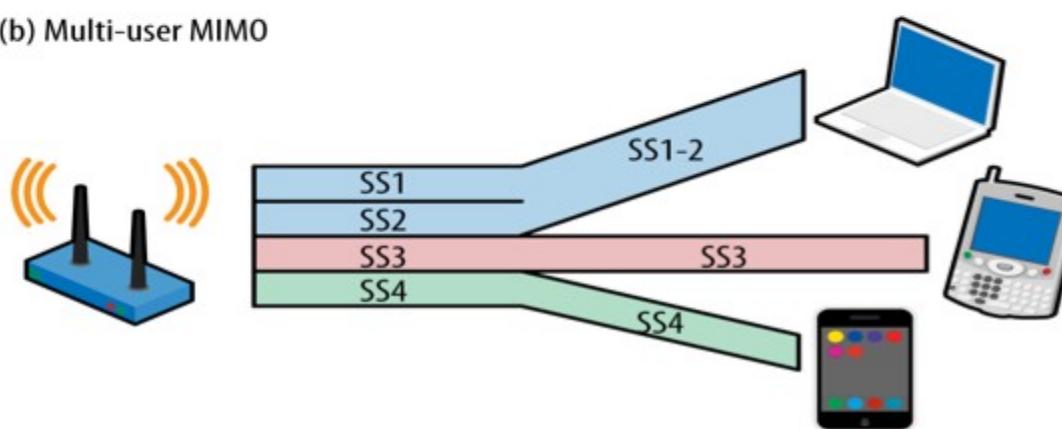
Прилага се и при [802.11n](#), [802.11ac/ad](#) и [802.16e](#) (WiMAX).
Прилага се във варианти SU (single-user) и MU (multi-user).

SU-MIMO и MU-MIMO

(a) Single-user MIMO



(b) Multi-user MIMO



Gigabit Wi-Fi: 802.11ac, ad, etc.

IEEE 802.11ac (5G Wi-Fi) е предвиден е за 5 GHz обхват. Поддържа скорости до 1.3 Gbps.

Разширява възможностите на безжичния интерфейс, заложени в 802.11n (и е обратно съвместим):

- по-широва честотна лента (до 160 MHz),
- повече MIMO потоци (до 8),
- OFDM и QAM-256 модулация на всеки канал.

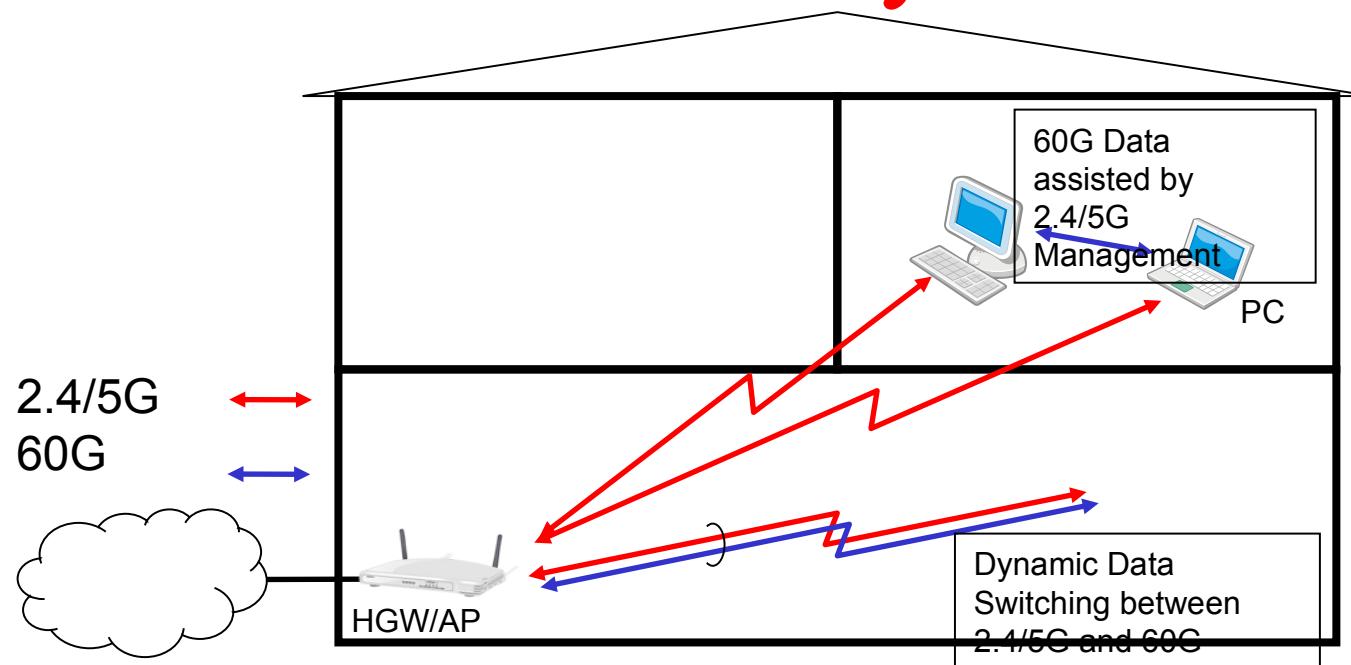
2018 г. - 802.11ac Wave 2, в бъдеще - 802.11ax

Wave 2 предстои да бъде сертифициран от IEEE. Новата технология е **MU-MIMO**.

Позволява да се създадат устройства за достъп (**access point – AP**), които “говорят” с множество клиентски устройства едновременно. Преди това **SU-MIMO** APs обслужваха потоците последователно.

802.11ac ще бъде наследен от **802.11ax**. Ключова технология при него е **OFDMA** (orthogonal frequency-division multiple access). Освен че множество клиентски устройства споделят едно и също AP (като 802.11ac), но и един и същ Wi-Fi канал по едно и също време.

Gigabit Wi-Fi: 802.11ad. Подобрение - 802.11ay.



802.11ad - 60 GHz обхват. По-малко покритие (отразява се от стени и хора), но “по-чист” ефир. Скорост около **7 Gbps**, широка приложимост – от file transfer до HD Video.

802.11ay - подобрение на 802.11ad, трябва да вдигне скоростта в пъти - до **20-30 Gbps** в радиус **10-30 м**. С някои “хватки” - 11ay-to-11ay, сливане на канали, MIMO и др., може да стигне 200 Gbps на 300 м. Забравяте за жичния Етернет.

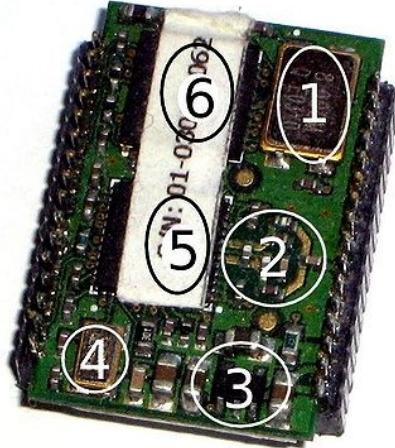
IEEE 802.15. Bluetooth, и др. към Internet of Things (IoT)

IEEE 802.15. Task Group	Пояснение
1 (WPAN/Bluetooth)	Безжичен RS-232. ISM 2.4 GHz. V. 1.2: 1 Mbit/s; V. 2.0 + EDR: 3 Mbit/s; V. 3.0 + HS: 24 Mbit/s. Class 1: ~100 м; Class 2: ~10 м; Class 3: ~1 м
2 (Coexistence)	Взаимодействие на WPAN с други ISM WLANs.
3 (High Rate WPAN)	Високоскоростни (11 to 55 Mbit/s) WPANs.
4 (Low Rate WPAN - WHANs)	С дълготрайни батерии (месеци-години). Примери: ZigBee и 6LoWPAN
5 (Mesh Networking)	Нискоскоростни и високоскоростни.
6 Body Area Network (BAN)	BAN: ниска мощност, нискочестотни мрежи на късо разстояние.
7 Visible Light Communications (VLC)	Видима светлина 400 THz (780 nm) и 800 THz (375 nm). Флуоресцентни лампи - 10 kbit/s; LEDs - до 500 Mbit/s; RONJA - 10 Mbit/s).

Bluetooth handsfree устройство



ZigBee



В “mesh network” за интелигентен контрол на
устройства в индустрията, сензори, медицината,
противопожарна и охранителна техника, в дома и др.

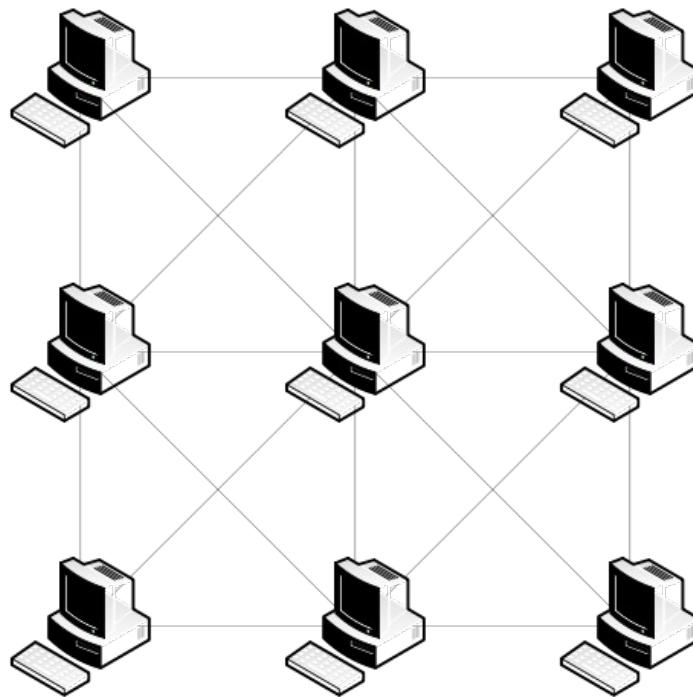
6LoWPAN

6lowpan, IPv6 over LoW Power wireless Area Networks.

Работната група на IETF дефинира енкапсулация и компресиране на заглавната част (RFC4944), за да могат по IEEE 802.15.4 мрежи да се изпращат IPv6 пакети.

Ще намери приложение в Smart Grid – интелигентно управление и измерване на електрически уреди. В момента основен приоритет в САЩ. Един от основните фактори за въвеждане на IPv6.

Mesh networking



Mesh networking – всеки възел в мрежата си е самостоятелен маршрутизатор (рутер). Гарантира непрекъсваемост на връзката чрез заобикаляне на прекъснати или блокирани пътища.

RONJA



RONJA (Reasonable Optical Near Joint Access) е устройство, излъчващо в открито небе. Изобретено е в Чехия. Предава данни със скорост 10 Mbit/s full duplex Ethernet point-to-point (точка-точка).

4G: WiMAX vs. LTE

4G – 4-то поколение клетъчни брзнични комуникации.

1981 аналогови (1G); 1992 цифрови (2G)

2002 3G мултимедия, “spread spectrum”, поне 200 kbit/s

4G е изцяло IP решение: IP телефония, свръх широколентов достъп до Internet, онлайн игри, мултимедия по поръчка. **Най-вече IPv6**.

4G - IMT-Advanced (International Mobile Telecommunications Advanced), дефиниран от ITU-R. \approx 100 Mbit/s за мобилен достъп и \approx 1 Gbit/s за постационарен.

4G: LTE

- **LTE Advanced** (Long-term-evolution Advanced) не покри изискванията на ITU за 4G скорост 1 Gbps (само до 600 Mbps).
- Но ITU допусна да се нарича 4G технология, защото дава над двойно увеличение на скоростта спрямо 3G.



5G



- 10-ки Mbps за 10-ки хиляди потребители
- 100 Mbps в градска среда
- по 1 Gbps за всеки работещ в офис среда
- няколко хиляди едновременни връзки с безжични сензори

5G

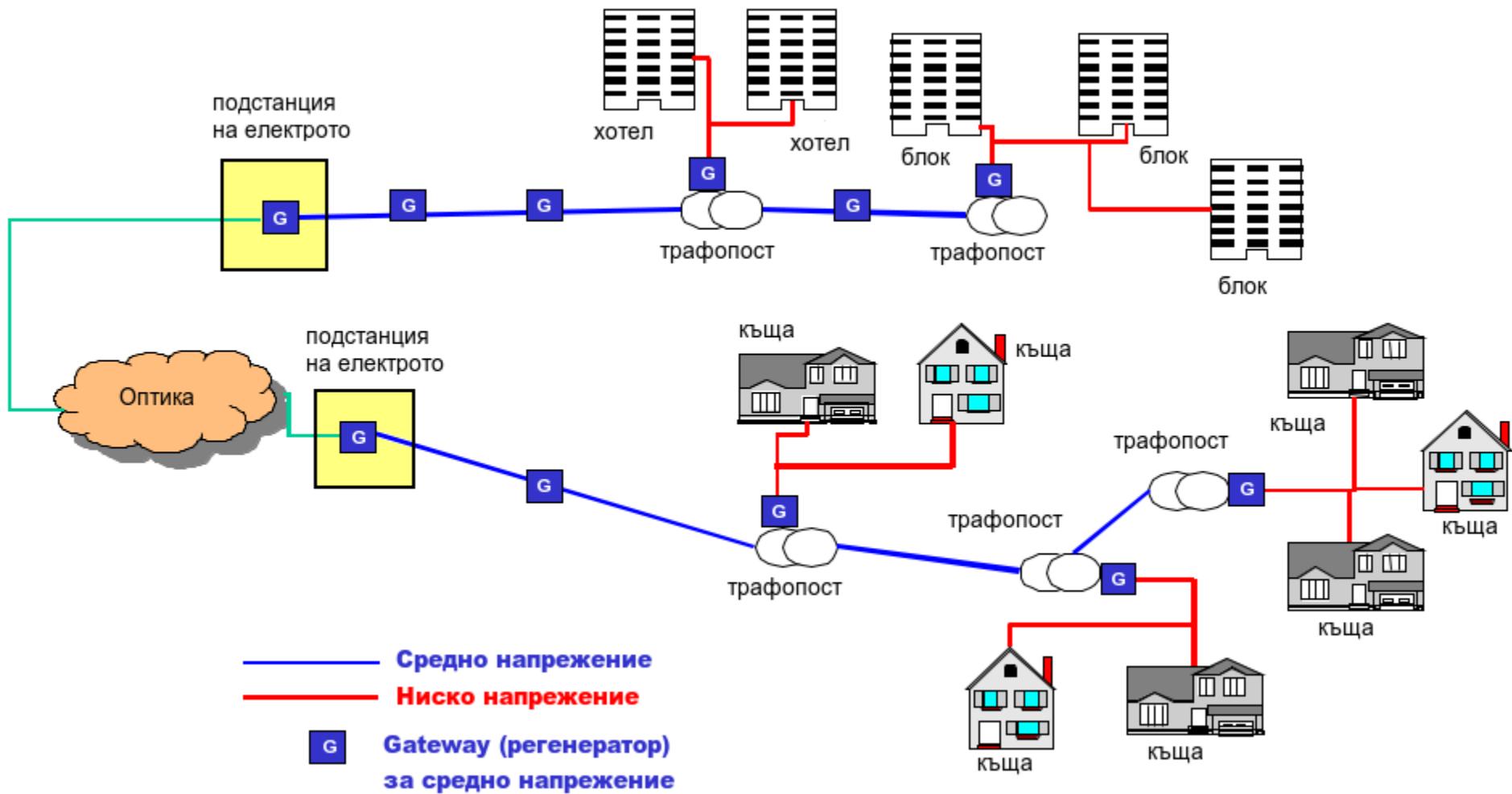
- A- Gbps скорости в движение и по-висока интелигентност;
- B- **MIMO**;
- C- интелигентни антенни системи;
- D- software-defined networking (**SDN**);
- E- Network Functions Virtualization (**NFV**);
- F- Internet of Things (**IoT**) и **cloud computing**;
- G- Софтуерно дефинирани протоколи за настройка на радиочестотната система и :
- H- **Random Linear Network Coding**.

Power Line Communications

Power Line Communication (**PLC**) се развиват благодарение на технологии като **OFDM** модулацията, които позволяват по **електрозахранващите мрежи** със средно и ниско напрежение да се пренасят данни, видео и звук със скорости **до 200 Mbps**.

Зависи от много фактори (кабели, устройства по електрическата мрежа, съединения) и затова **гарантираната скорост** от производителя е **20 Mbps**.

Топология на PLC мрежа



Топология на PLC мрежа

В подстанция на ЕРП влиза FO или друга стандартна мрежова свързаност и се прави конверсията към мрежата със средно напрежение с помощта на **gateway** (регенератор) за средно напрежение.

Такъв **gateway** заедно с филтри за шумоизолация и съединители, освен в подстанциите, се слага на всеки 400 метра кабел за ток със средно напрежение, както и в трафопостовете.

От трафопоста започва клиентската част на мрежата.

В контакти на крайния клиент се слагат адаптери.

Примерно крайно устройство

- до 200 Mbit/s.

HomePlug AV2 – Gbit/s

скорости;

Wi-Fi Alliance и HomePlug
Powerline Alliance в
колаборация за Connected
Smart Home.

IEEE 1901-2010 е Broadband
over Power Line (BPL)
стандарт. На физически
слой достига 500 Mbit/s.



Android телефон - Wi-Fi hotspot (за сведение)

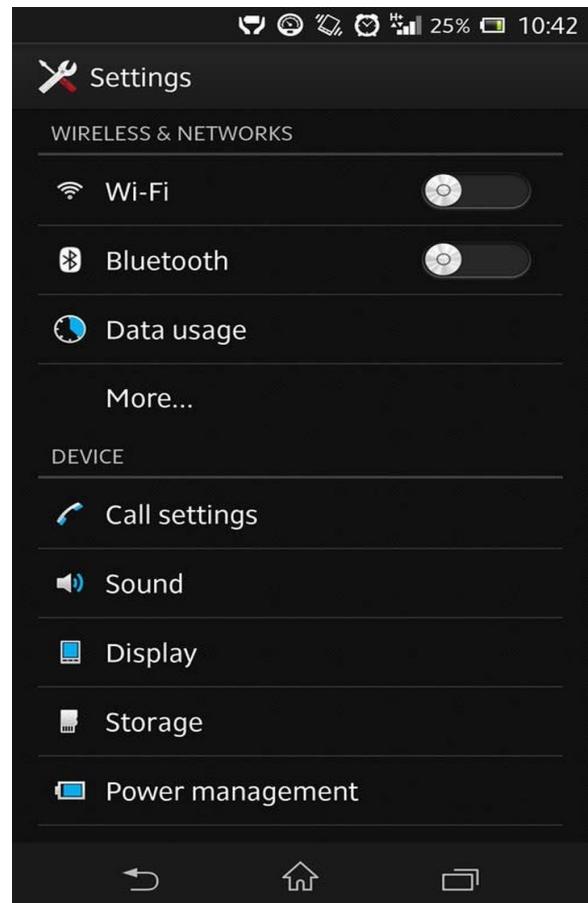
За връзка към

Интернет използвате

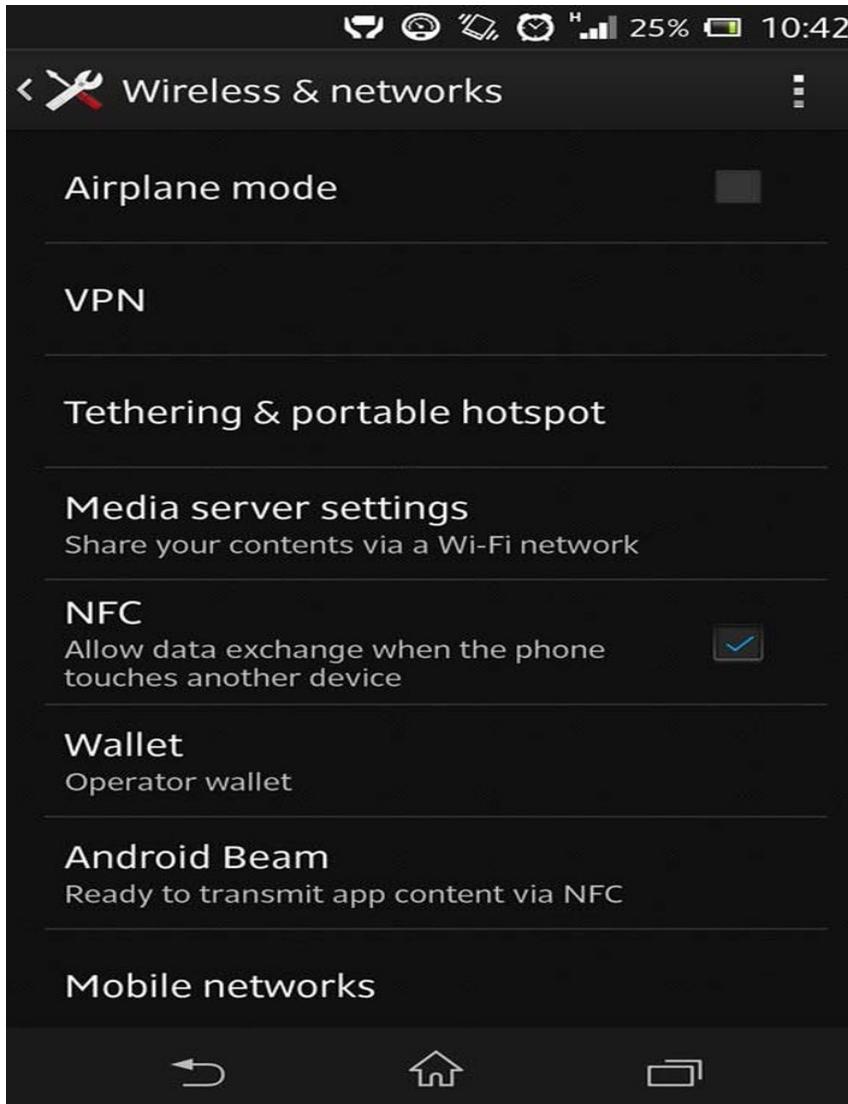
3G/4G мрежата:

1. Избирате меню

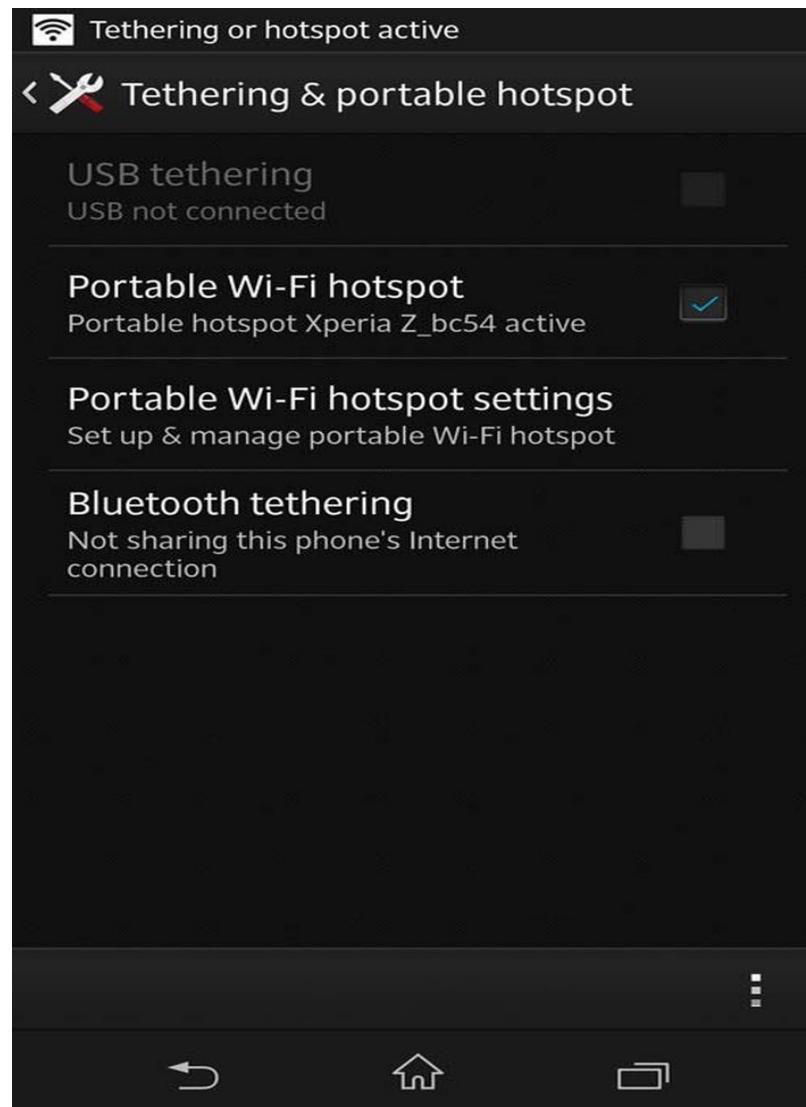
Settings



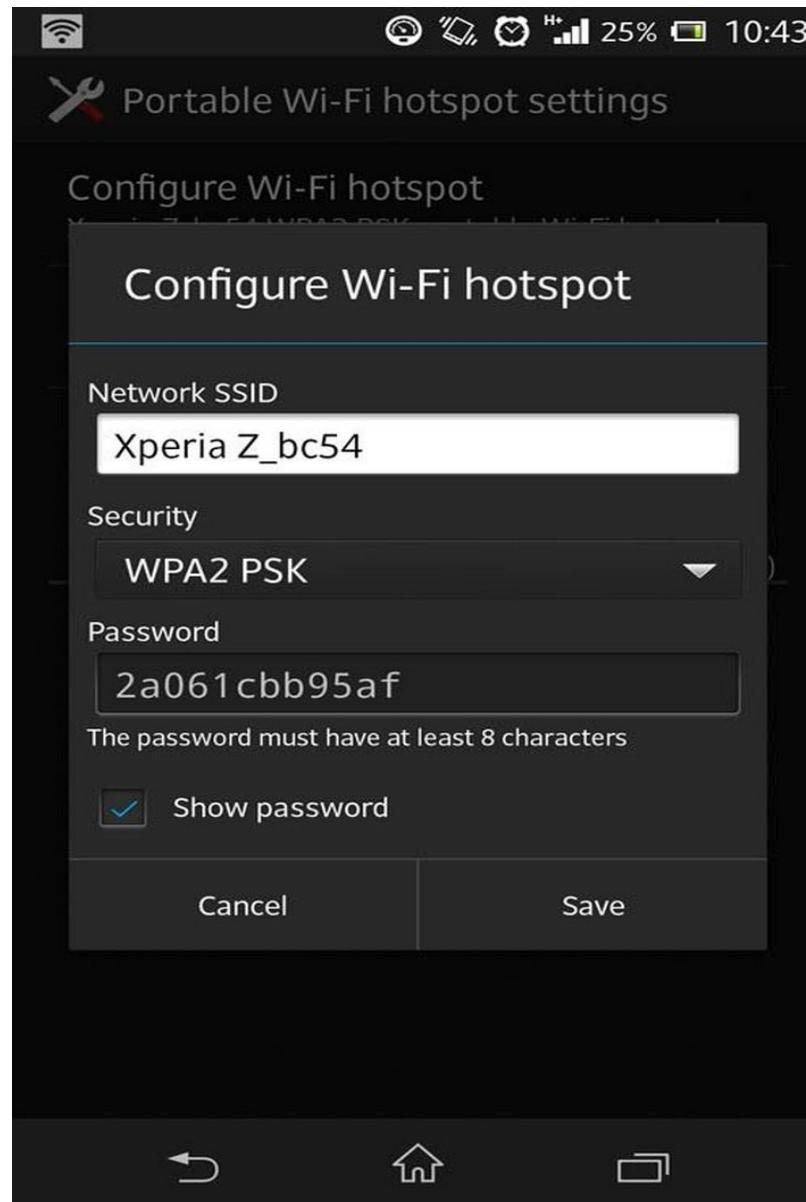
2. Избирайте Wireless & Networks и Tethering & portable hotspot



3. Кликнете Portable Wi-Fi hotspot



4. Въведете име на Wi-Fi мрежата и парола



5. На вашия компьютер/таблет:



5. Канално ниво.

**Кадри, предаване, грешки,
номерация, прозорци**

Какво ще научим

- основните функции на каналния слой;
- надеждно и ненадеждно предаване;
- нормиране на кадъра (frame);
- откриване на грешки в кадрите;
- протоколи HDLC и PPP(оE);
- MPLS – протокол на 2.5 слой.

Основни функции

Каналното ниво има **три основни функции**:

- да осигури подходящ интерфейс на по-горното мрежово ниво,
- да открива грешки по време на предаването и
- да управлява информационния обмен.

Данните за каналното ниво представляват последователност от **кадри** (frame).

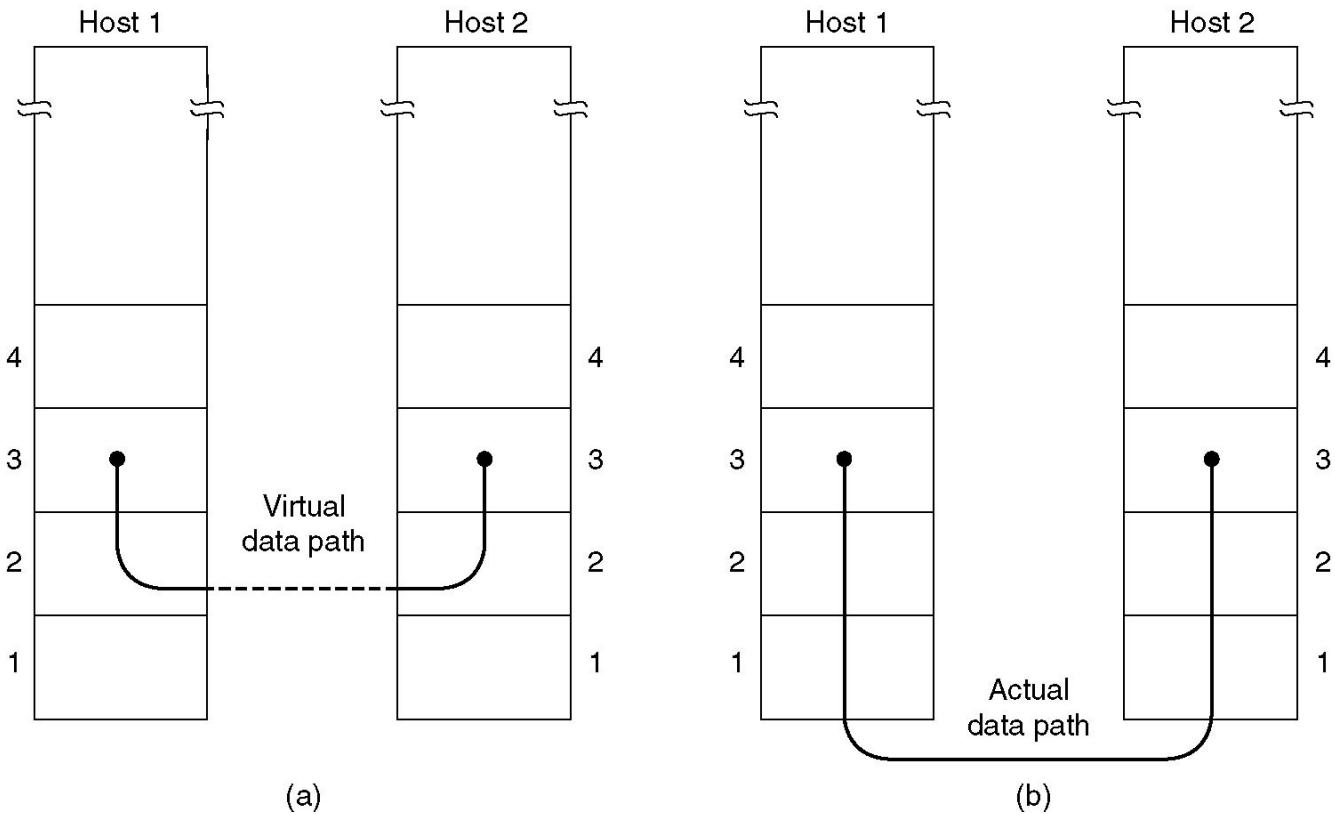
Каналите са три вида - **симплексни, полуудуплексни и дуплексни**.

Дуплексните канали позволяват едновременно предаване в двете посоки.

Полудуплексните канали позволяват предаване и в двете посоки, но в даден момент може да се предава само в една посока.

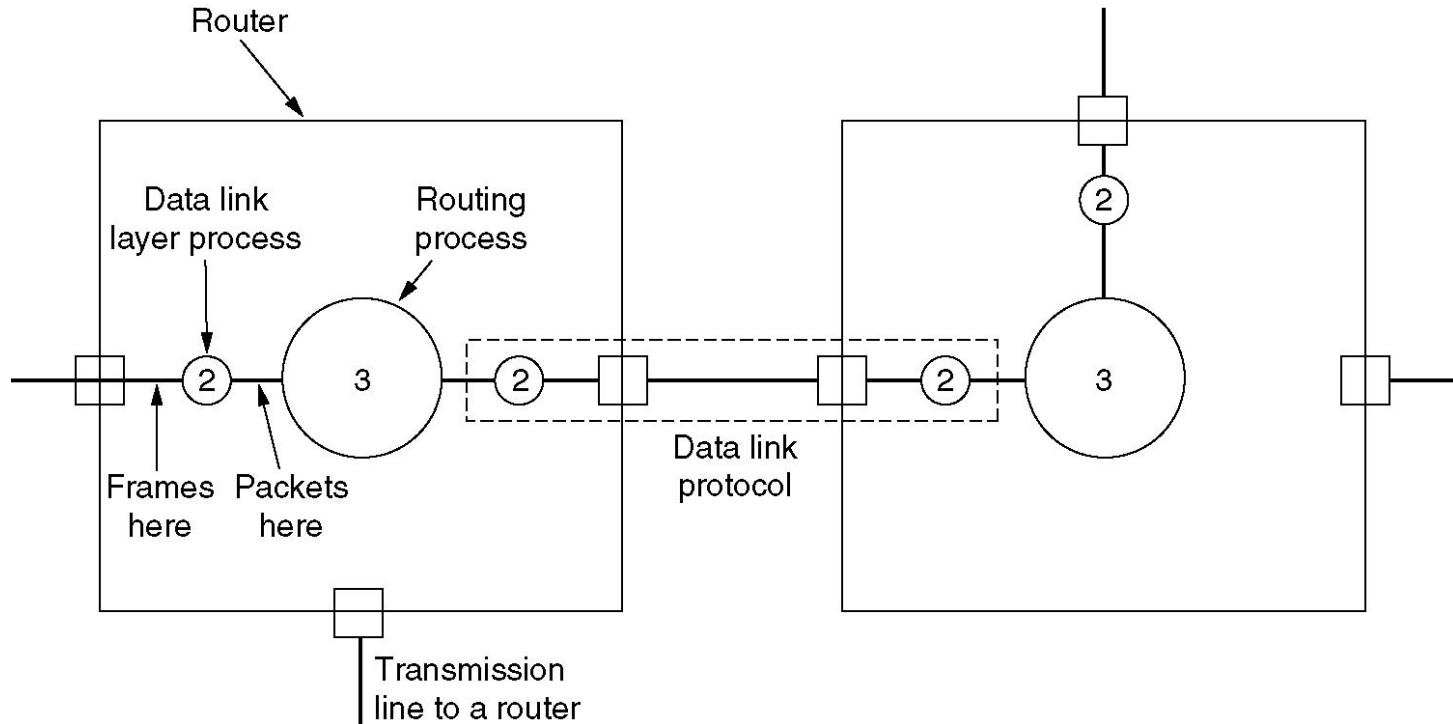
Симплексните канали позволяват предаване само в една посока.

Основни функции



- (a) Логическа комуникация.
(b) Действителна комуникация.

Основни функции



Ролята на каналния слой между две съседни машини - възли.

Основни услуги

Най-общата услуга - прехвърляне на данни (надеждно или **best effort**, но **изчистено от грешки**) между мрежовото ниво на източника и мрежовото ниво на получателя (всъщност самото предаване се извършва от физическото ниво, но това остава невидимо за мрежовото ниво).

Основните варианти на тази услуга са:

- непотвърдено, без установяване на сесия (**Unacknowledged connectionless service**),
- потвърдено, без установяване на сесия (**Acknowledged connectionless service**) и
- потвърдено, с установяване на сесия (**Acknowledged connection-oriented service**).

Основни услуги

Непотвърденото, без установяване на сесия

Източникът изпраща независими кадри към получателя, без получателя да ги потвърждава. Няма установяване на сесия между двете машини.

Ако един кадър се загуби поради шум в линията, каналното ниво не прави опит да възстанови този кадър. Това обслужване е подходящо при канали с много малка честота на грешките, което позволява функциите по възстановяване на загубената информация да се поемат от по-горни нива в йерархията.

Основни услуги

Такова обслужване се реализира в повечето LAN.

То също се използва когато навременното получаване на кадрите е по-важно от тяхната достоверност **видео, глас в реално време.**

При **потвърденото, без установяване на сесия** отново не се установява сесия между източника и получателя, но получаването на всеки кадър се потвърждава самостоятелно от получателя. Това дава възможност за повторно изпращане на непотвърдените кадри.

Основни услуги

Потвърждаването на получената информация е функция на транспортното ниво, но там то се отнася до последователности от сегменти.

Потвърждаването на каналното ниво има смисъл при ненадеждна комуникационна среда, каквато е безжичната, тъй като повторно ще се предават само непотвърдените кадри.

Основни услуги. Connection Oriented.

Потвърденото, с установяване на сесия има три фази.

Първата фаза се установява сесия и се заделят необходимите ресурси (локални буфери, броячи и т.н.).

Втората фаза се изпращат кадрите.

Третата фаза се освобождават ангажираните ресурси.

Гарантира се не само успешното предаване на кадъра, но и последователността в която се предават кадрите.

Управление на потока (Flow Control)

Друг проблем, който е свързан с управлението на обмена на канално ниво е източникът да изпраща кадри по-бързо, отколкото те могат да бъдат приети от получателя.

За целта се въвеждат механизми за управление на потока от кадри, който осигурява обратна информация на източника за темпа на предаване.

Обикновено механизмите по управление на обмена се изпълняват в транспортния слой над цели масиви от данни, обхващащи последователност от кадри.

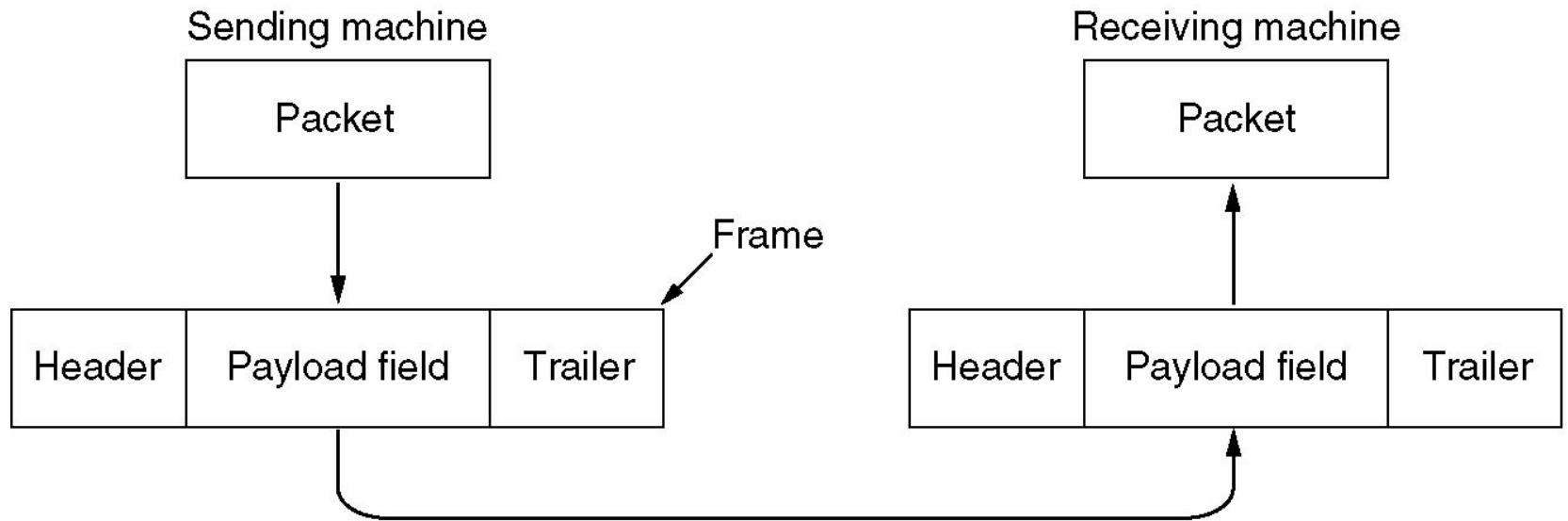
Формиране на кадри

Каналното ниво взима пакетите, които му се подават от мрежовото ниво и ги опакова в кадри.

Всеки кадър се състои от заглавна част (**header**), поле за данни (**data** или **payload**), което съдържа мрежовия пакет и опашка (**trailer**). Дължината на кадъра обикновено е ограничена отгоре.

Физическото ниво възприема информацията от каналното ниво като поток от битове, без да се интересува от нейната структура.

Формиране на кадри



Прехвърляне на данни между мрежовите нива на източник и получател (две съседни машини - възли). Пакети и кадри.

Формиране на кадри

Получателят идентифицира в потока от битове кадрите и въз основа на служебната информация в тях ги **контролира за грешки**.

За целта опашката на кадъра съдържа **контролна сума** (обикновено 2 байта), която се изчислява върху останалата част от кадъра преди той да бъде предаден.

Когато кадърът пристигне при получателя, контролната сума се преизчислява и ако тя е различна от предадената контролна сума, то получателят отхвърля кадъра и евентуално изпраща съобщение за грешка към източника.

Формиране на кадри

Разделянето на потока от битове на кадри не е тривиална задача.

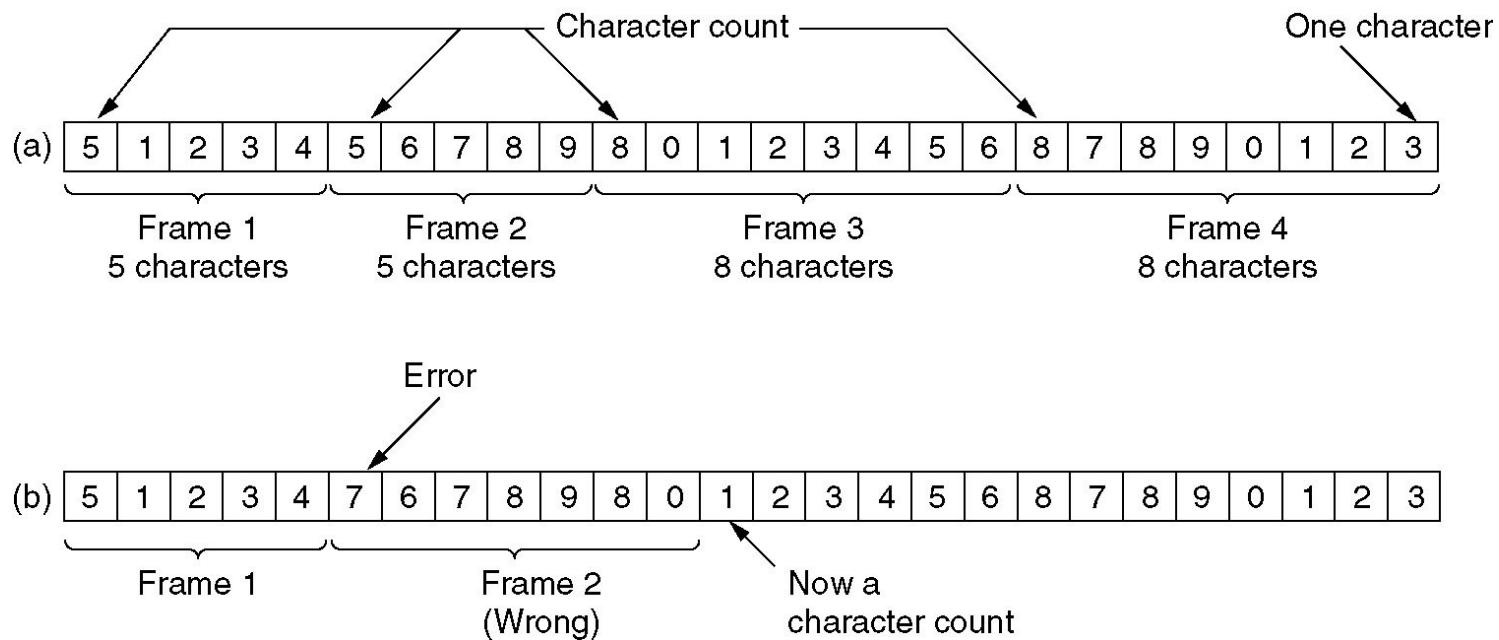
Един начин е между всеки два кадъра да се въведе времеви интервал. Този подход е твърде несигурен, тъй като времевите интервали могат да се променят по време на предаването.

По настоящем основно се използват три метода.

При първия метод е **броене на отделните символи**. В заглавието на кадъра се указва броя на символите в целия кадър.

Основният проблем на този метод е, че **броят на символите може да бъде сгрешен по време на предаването**, при което получателят ще загуби синхронизация и няма да може да определи началото на следващия кадър. Затова **не се използва**.

Броене на символи



Поток от четири кадъра: 5, 5, 8, 8 символа. (a) Без грешки. (b)
Грешка: число 5 във втори става 7. Губи се синхронизация.

Формиране на кадри

Втори метод в началото и края на кадъра се вмъкват специални служебни символи - **STX** (start of text) за начало на кадър и **ETX** (end of text) за край на кадър, които маркират границите на кадъра. Техниката е известна като **вмъкване на символи (byte stuffing, character stuffing)**.

Възможно е служебните символи да се срещат като битови последователности в оригиналните данни. За решение на този проблем се въвежда друг служебен символ **ESC** (escape), който се вмъква преди всяко срещане на служебен символ (STX, ETX, ESC) в данните. Например, ако потокът, предаван от мрежовия слой на източника е **A STX ESC B**, той ще се преобразува в **A ESC STX ESC ESC B**.

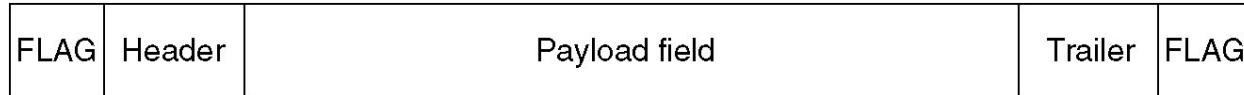
Формиране на кадри

Каналното ниво на получателя ще премахне символите ESC (като при два последователни ESC, единият се запазва), преди да предаде данните на мрежовото ниво на получателя.

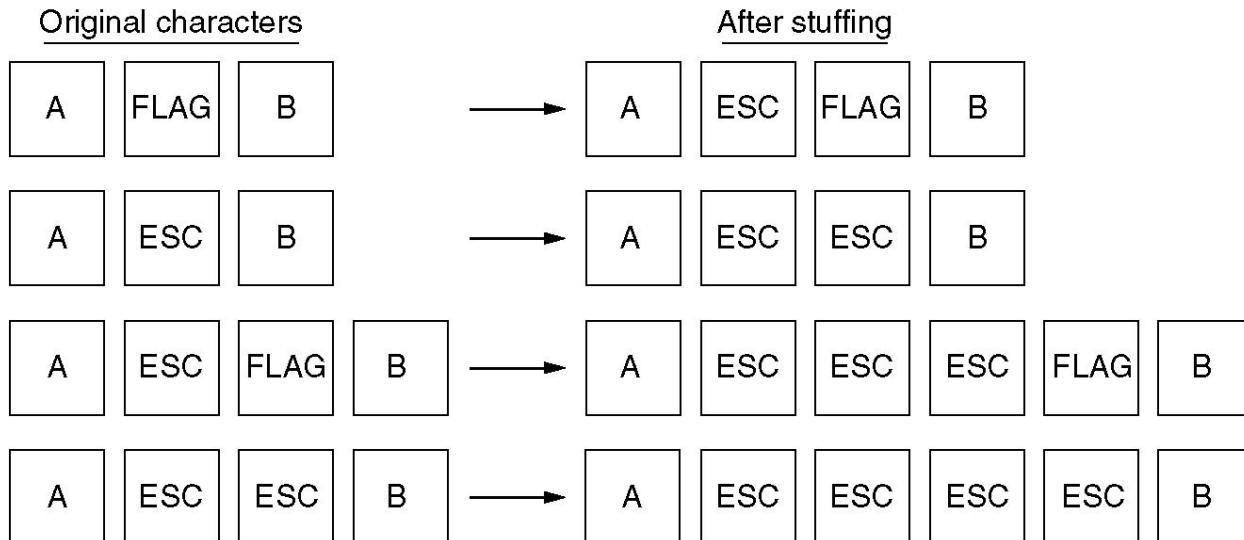
При по-новите протоколи се използва един и същ символ за маркиране на началото и края на кадъра - **флаг**.

Недостатъкът на този метод е, че той се обвързва с 8-битови символи, кодирани в ASCII.

Вмъкване на символи



(a)



(b)

(a) кадър, ограничен от флагови байтове.

(b) Последователност от байтове преди и след вмъкване.

Формиране на кадри

С развитието на мрежите стана възможно кадрите да съдържат произволно цяло число битове. За такива кадри се използва **третия метод**, при който началото и края на всеки кадър се маркира с битовата последователност **01111110**, наречена **флагов байт**.

За да се предотврати погрешното определяне на граница на кадър, ако тази последователност от битове се срещне в данните на кадъра, след всеки 5 единици в данните източникът добавя по една нула. Техниката се нарича **вмъкване на битове (bit stuffing)**.

Каналното ниво на получателя премахва нулата след всеки 5 единици в данните, преди да ги подаде на мрежовото ниво.

За постигане на допълнителна сигурност при много протоколи броенето на символи се комбинира с някой от другите два метода.

Флагов байт

(a) 011011111111111111110010

(c) 011011111111111111110010

Bit stuffing

- (a) Оригинални данни
 - (b) Как данните изглеждат по линията
 - (c) Данните, съхранени в паметта на приемника след destuffing

Процедури за надеждна работа на канала

Функциите на каналния слой се реализират в **адаптер**, предимно **хардуерно**: специализирани интегрални схеми за управление (**ASIC**) и програмен код, “прогорен” в EEPROM или записан във Flash памети (**firmware**).

В адаптера е реализиран **буфер**, в който се записват кадрите, докато изчакват да бъдат предадени нататък.

Кадърът преседява в буфера, докато не не се увери, че отсрещната страна го е получила.

Да приемем, че **източник A** изпраща кадър към **B**, но той изобщо не стига до там. Пет причини за това:

- 1) Адаптер **A** дефектен, не излъчва правilen сигнал;
- 2) “Счупен” канал – жица и т.н.;
- 3) **B** не съществува;
- 4) **B** няма свободен буфер;
- 5) Кадърът постъпва в буфера на **B**.

Процедури за надеждна работа на канала

A може да получи отговор единствено при 5). При изпращане на кадъра *A* включва брояч на време - таймер. Чака отговор до определено време – timeout.

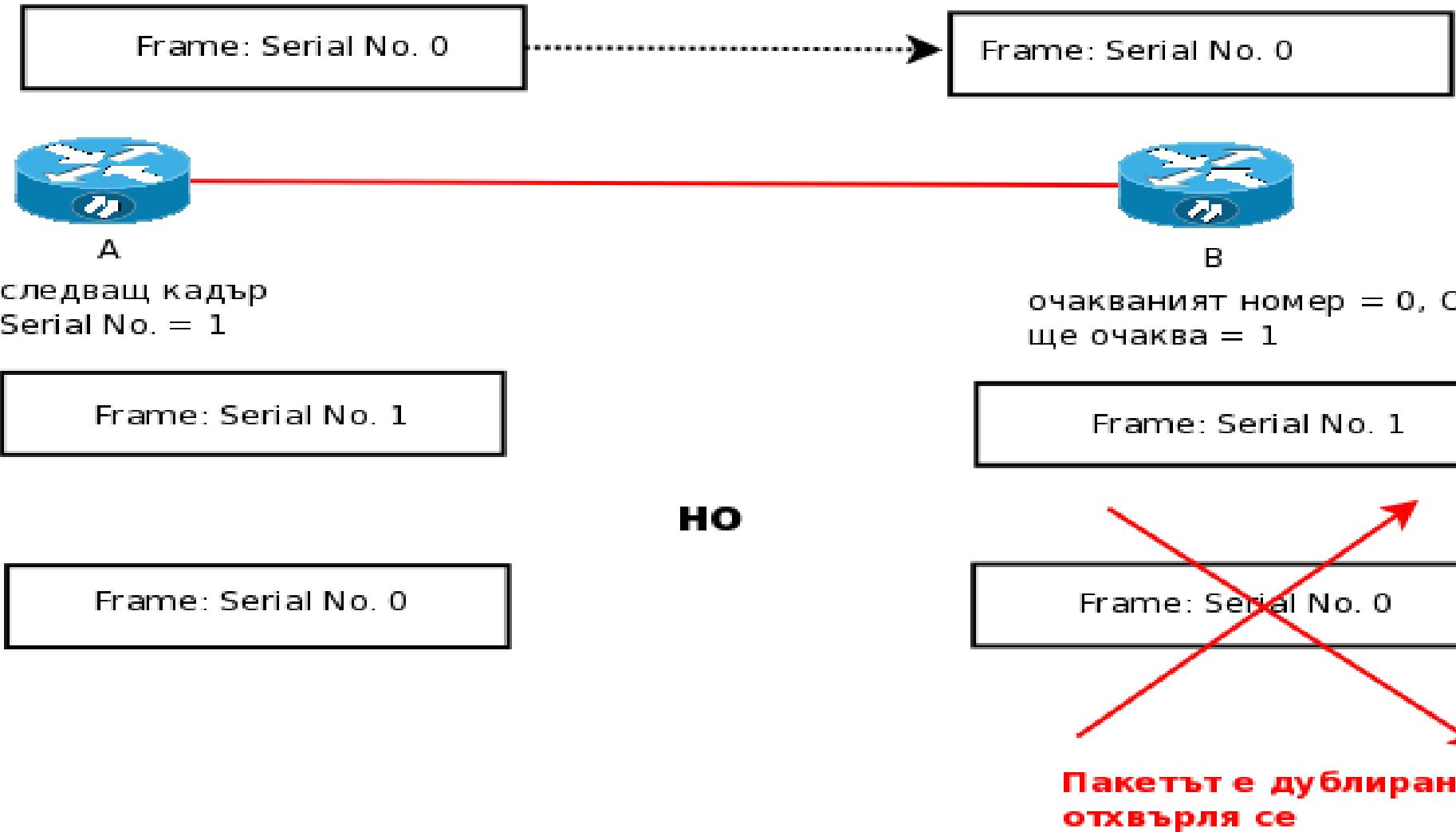
timeout трябва да е по-голямо от времето за предаване на кадъра, обработката му в приемника и получаване на потвърждение.

Ако кадърът не се потвърди в рамките на това време, то *A* предава кадърът отново.

Възможно е *A* да изпрати кадър към *B*, този кадър да се получи в *B*, но потвърждението да се изгуби.

Процедури за надеждна работа на канала. Пореден номер.

Serial No. = 0 or 1 (1-bit)



Откриване на грешки в кадрите

Горните методи си имат недостатъци. Затова...

CRC (*cyclic redundancy check* — проверка на цикличния остатък)

Алгоритъм за проверка за грешки при предаване и съхранение на данни чрез използване на **контролна сума** (*контролно число, CRC сума*).

Устройството-източник изчислява CRC-сумата на данните, които следва да бъдат проверявани и я изпраща или записва със самите данни.

Устройството-получател извършва същото изчисление след прочитане на данните и контролната сума, и установява тяхната автентичност чрез сравнение на записаната CRC сума и новоизчислената CRC сума.

Видове CRC-та

CRC-16-CCITT = $x^{16} + x^{12} + x^5 + 1$ (Bluetooth, XMODEM, HDLC, PPP)

CRC-32-IEEE 802.3 = $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

CRC-64-ISO = $x^{64} + x^4 + x^3 + x + 1$ (HDLC — ISO 3309)

Тези кодове са разработени отдавна, оптимизирани и вкарани в хардуерни схеми.

CRC се изчислява в движение и се слага в края на кадъра като FCS (Frame Control Sum)

Modulo 2 Аритметика

Изпълнява се цифра по цифра върху двоични числа. Няма “преноси” и “заеми”.

Събиране

Използва се **exclusive OR (XOR)** функцията:

A	B	A xor B
0	0	0
0	1	1
1	0	1
1	1	0

Пример:

$$\begin{array}{r} (X) \ 10110100 \\ (Y) \ 00101010 \\ + \\ \hline (Z) \ 10011110 \end{array}$$

Modulo 2 Аритметика (Изваждане)

Дава същите резултати като събиране:

$$(X) \ 10110100$$

$$(Z) \ 10011110 -$$

$$(Y) \ 00101010$$

$$X + Y = Z, \Rightarrow Y = Z - X.$$

От примера следва и: $Y = Z + X$.

Modulo 2 Аритметика (Деление)

Подобно на аритметическото деление на двоични числа. Пак използваме Modulo 2 изваждане.

10001 **остатък** 100

10011|100100111

10011

10111

10011

100

Имаме $X/Y = Y/X$. Напр.:

1 **остатък** 1011

11001|10010

11001

1011

1 **остатък** 1011

10010|11001

10010

1011

Пример на CRC изчисление

Подател и получател се уговарят за генератор на контролната сума, **полином $G(x)$** . Най-старшия и най-младшия бит трябва да са 1.

За да изчислим контролната сума на **кадър с m бита**, полинома **$M(x)$** , кадърът трябва да е по-дълъг от полинома на генератора.

Идеята е към края на кадъра се да се прибави контролна сума, така че полиномът, който представя **“checksummed”** кадъра, да е делим на $G(x)$.

Когато получателят приеме **“checksummed”** кадъра, той се опитва да го раздели на $G(x)$. Ако се получи остатък, значи има грешка.

Пример на CRC изчисление

Алгоритъмът за изчисляване на контролната сума е следния:

1. Нека r е степента на $G(x)$. Прикрепяме r нулеви бита към “младшия” край на кадъра. Така той вече съдържа $m + r$

Бита и съответства на полинома $x^r M(x)$.

2. Делим низа от битове, съответстващ на $G(x)$, на битовия низ, съответстващ на $x^r M(x)$ с помощта на “сума по модул 2” (modulo 2) делене.

3. Изваждаме **остатъка** (който винаги е $< r$ бита) от битовия низ, съответстващ на $x^r M(x)$ с помощта на **modulo 2 изваждане**. Резултатът е **checksummed frame**, който ще се предаде, т.е полинома $T(x)$.

В следващия пример имаме кадър 1101011011 и генератор:

$$G(x) = x^4 + x + 1$$

Пример на CRC изчисление

Алгоритъмът за изчисляване на контролната сума е следния:

1. Нека r е степента на $G(x)$. Прикрепяме r нулеви бита към “младшия” край на кадъра. Така той вече съдържа $m + r$

Бита и съответства на полинома $x^r M(x)$.

2. Делим низа от битове, съответстващ на $G(x)$, на битовия низ, съответстващ на $x^r M(x)$ с помощта на “сума по модул 2” (modulo 2) делене.

3. Изваждаме **остатъка** (който винаги е $< r$ бита) от битовия низ, съответстващ на $x^r M(x)$ с помощта на **modulo 2 изваждане**. Резултатът е **checksummed frame**, който ще се предаде, т.е полинома $T(x)$.

В следващия пример имаме кадър 1101011011 и генератор:

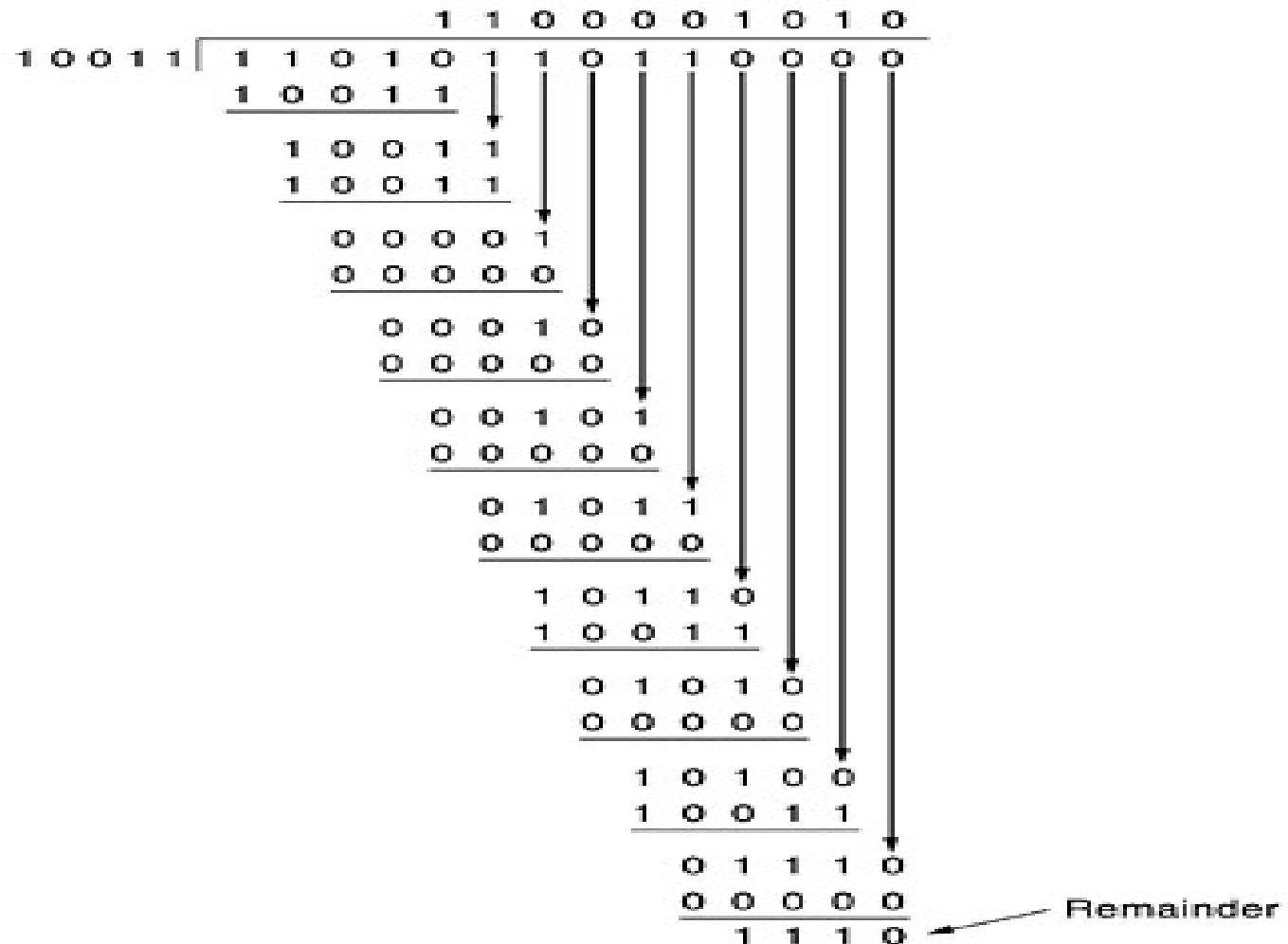
$$G(x) = x^4 + x + 1$$

Пример на CRC изчисление

Frame : 1 1 0 1 0 1 1 0 1 1

Generator: 1 0 0 1 1

Message after 4 zero bits are appended: 1 1 0 1 0 1 1 0 1 1 0 0 0 0



Transmitted frame: 1 1 0 1 0 1 1 0 1 1 1 1 0

Протоколи с прозорци (Sliding Window Protocols)

Пълзгащият се прозорец (*Sliding window*) се използва за по-ефективно предаване от протоколите със сесии (*connection oriented*):

- на 2 слой - Point-to-Point protocol (**PPP**);
- на 4 слой **TCP**.

Прозорецът се прилага при двупосочко предаване (*full duplex*). На 2 слой – два типа кадри:

1. Data
2. ACK (**потвърждение** - поредният номер на последния получен без грешка кадър)

Sliding Window Protocols

Предавател и приемник поддържат ``прозорец" на потвържденията:

- предавател – стойността на очакваното потвърждение когато получи потвърждение от приемника, прозорецът „напредва“;
- приемник – стойността на номера на очаквания кадър.

Когато получи очакваният кадър, приемникът „премества наред“ прозореца.

Stop-And-Wait (1-bit Window)

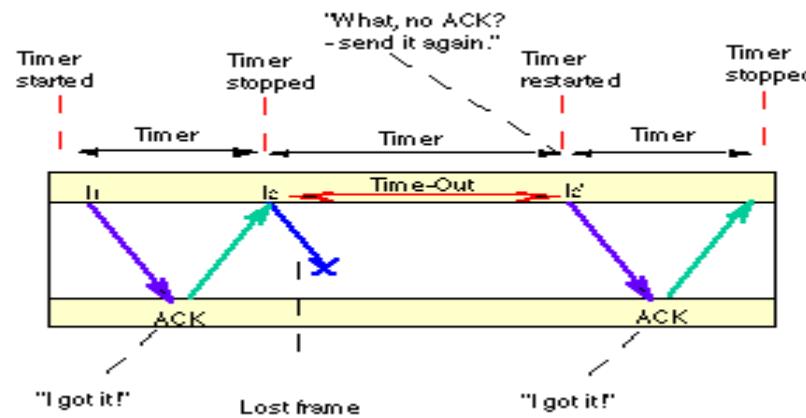
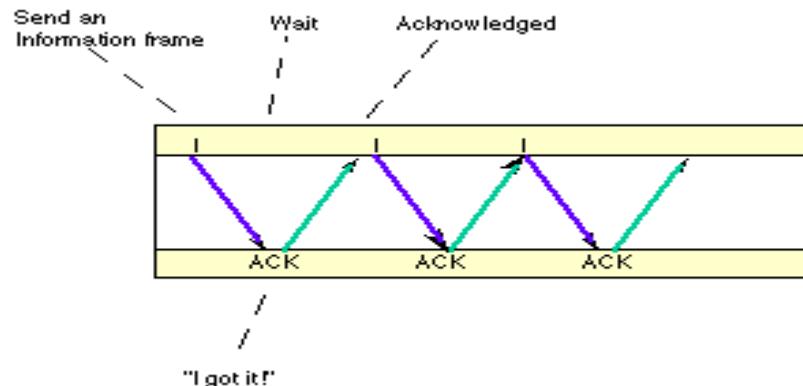
Протоколът с 1-битов пореден номер се нарича още Stop-And-Wait (“спри и чакай”).

- Предавателят изпраща един кадър;
- чака потвърждение за един RTT (round trip time) - времето, необходимо на сигнала за отиване до приемника и връщане обратно;
- след получаване на потвърждение изпраща следващ кадър.

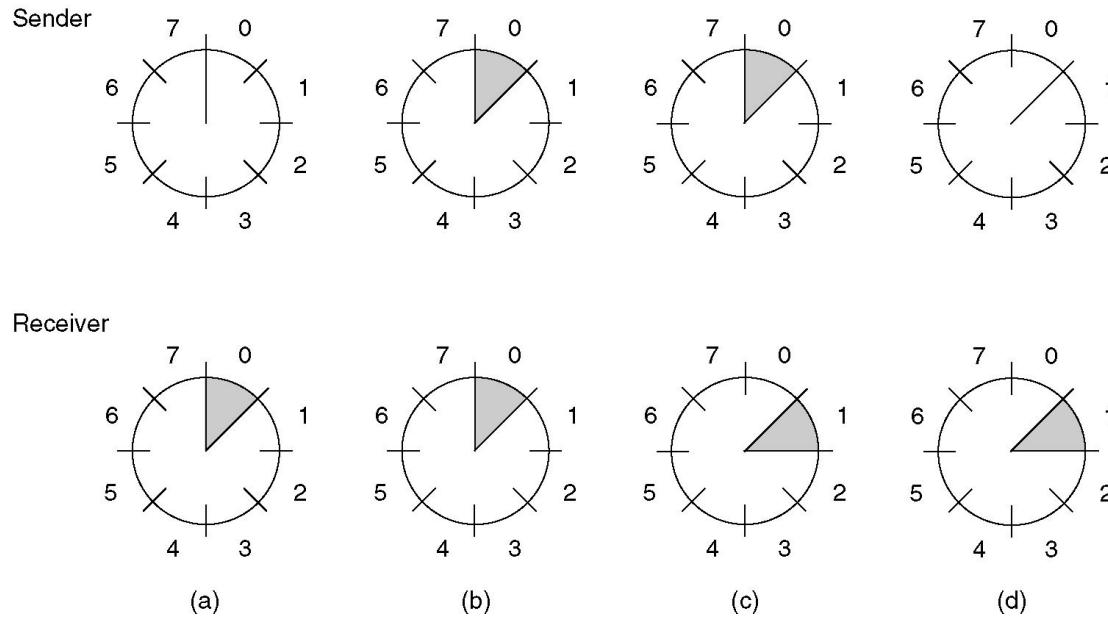
Не е ефективен. Само един кадър се предава в даден момент.

Чакането е толкова по-голямо, колкото по-бавна линията – напр. сателитна връзка.

Stop and Wait (примери: OK, загуба)



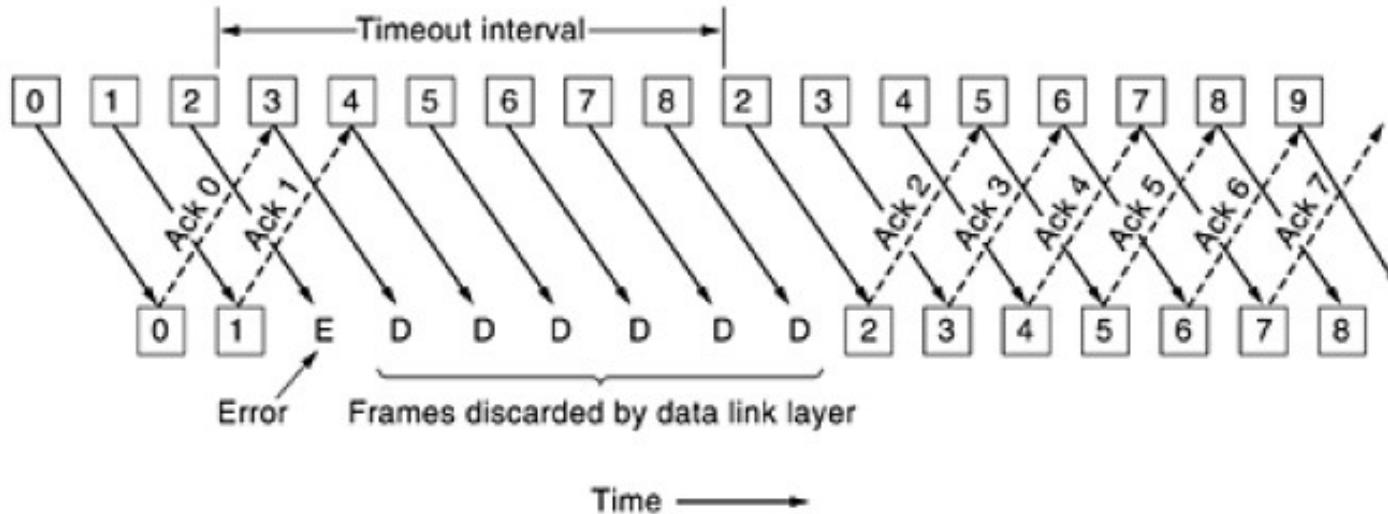
Sliding Window Protocols



Прозорец с размер 1 и с 3-битов пореден номер.

- (a) Отначало.
- (b) След изпращане на първи кадър.
- (c) След получаване на първи кадър.
- (d) След получаване на потвърждение.

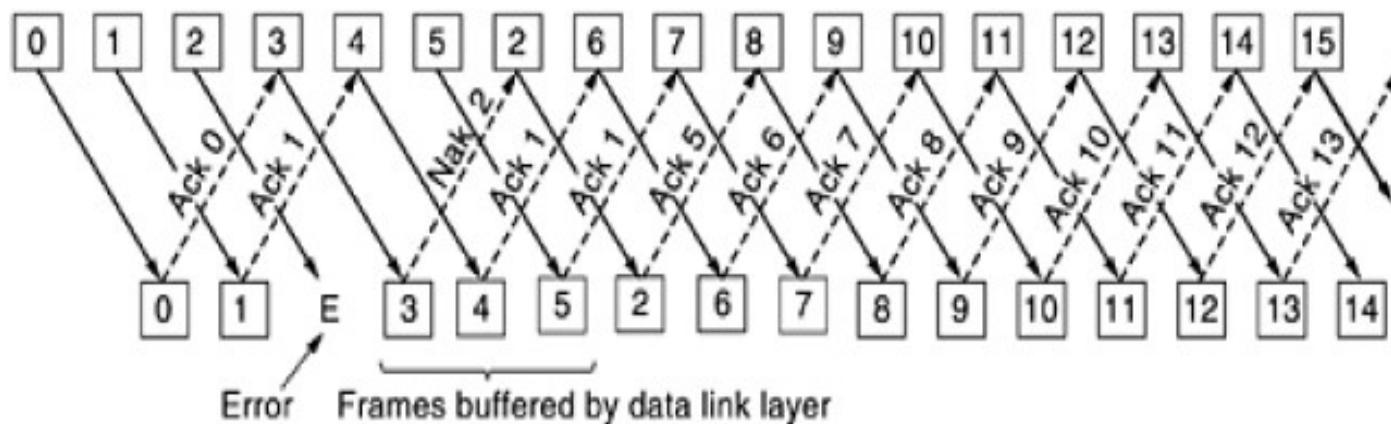
При грешка в прозореца. Go-Back-n.



Ако липсва и един кадър, напр. 2, приемникът изхвърля всички следващи до изчерпване на прозореца.

Предавателят трябва да ги предаде повторно. Губи се пропускателна способност.

При грешка в прозореца. Selective Repeat.



Повторно се изпращат само изгубените и/или повредени кадри.

Приемникът буферира всички кадри след изгубения/повредения.

Когато предавателят забележи проблема, (**няма ACK** за определен time-out), кадърът се предава наново.

High-Level Data Link Control

Първият протокол на канално ниво, който се използва в IBM е **SDLC** (*synchronous data link control*).

По-късно организацията по стандартизация ISO разработва на базата на SDLC протокола **HDLC** (*high-level data link control*).

И двата протокола са **битово-ориентирани** и използват **вмъкване на битове** за правилно идентифициране на кадрите.

Форматът на кадъра в HDLC е следния:

Bits	8	8	8	≥ 0	16	8
	0 1 1 1 1 1 0	Address	Control	Data	Checksum	0 1 1 1 1 1 0

HDLC

В началото и в края на кадъра са **флаговете** за маркиране на границите на кадъра.

Полето *Address* се използва при многоточкови канали (multipoint) и чрез него се идентифицира получателя на кадъра.

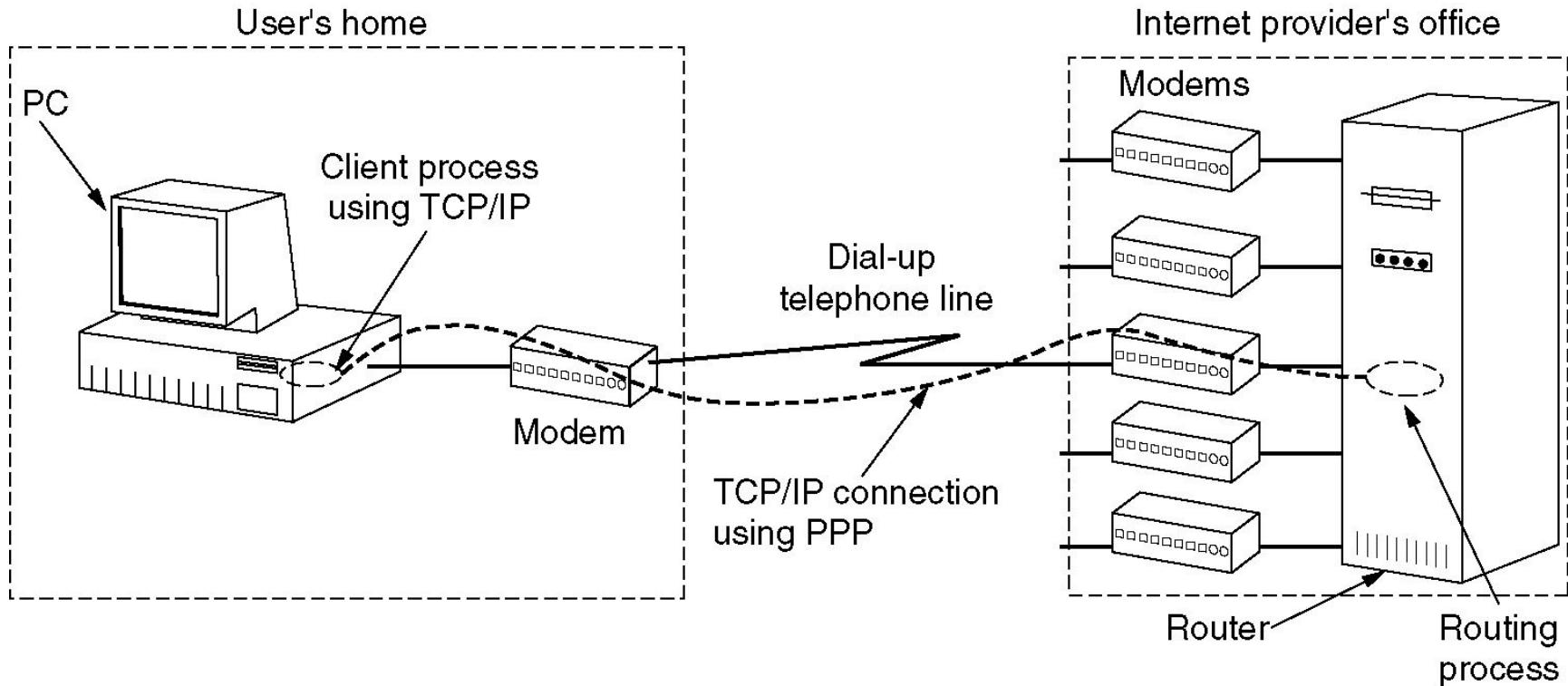
Полето *Control* се използва за номериране на кадрите, за потвърждения и др.

Полето *Data* съдържа данните на кадъра. По принцип има неограничена дължина.

Полето *Checksum* е контролната сума на кадъра (използват се циклични кодове).

Минималната дължина на кадъра, без да се включват флаговете за начало и край е **32 бита**.

PPP (Point-to-Point Protocol)



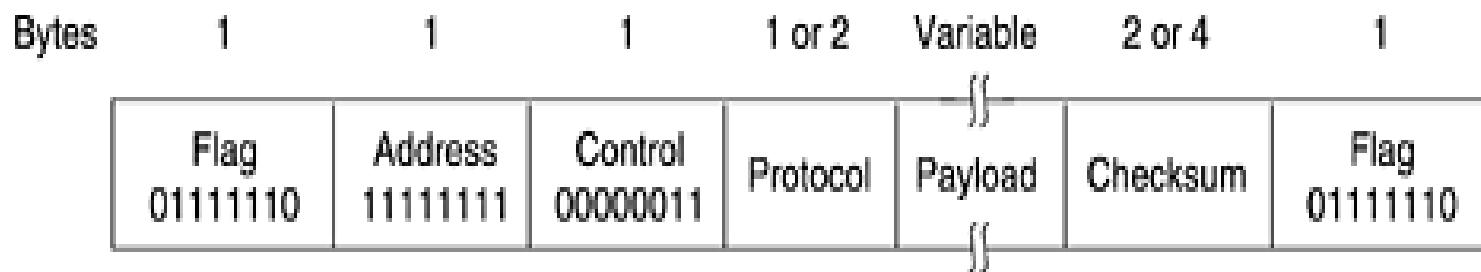
Свързване към internet по PPP.

Протокол PPP

Протоколът PPP е протокол за двуточкова връзка. Този протокол се използва за свързване на домашни компютри до доставчици на Интернет услуги по телефонна линия.

Протоколът PPP е байтово-ориентиран и за идентифициране на кадрите се използва техниката вмъкване на байтове.

Форматът на кадъра е наследен от HDLC:



Протокол PPP

При PPP няма индивидуални адреси на станциите, затова полето *Address* съдържа 11111111, което означава адресите на всички станции.

Полето *Control* съдържа 00000011, което означава *unnumbered*-кадър. С други думи, PPP не осигурява надеждно предаване чрез номера на кадрите и потвърждения.

Полето *Protocol* съдържа идентификатор на протокол, който указва как да се интерпретира полето *Payload*, в което се помества съответния пакет.

Максималната дължина на *Payload* е 1500 байта.

Протокол PPP

Дълчините на полетата *Protocol* и *Checksum* се договарят при установяването на съединение. След установяване на съединение, двете страни се договарят за мрежовите протоколи, които ще се използват. След това започват да се предават кадрите с данни, като полето *Protocol* съдържа идентификатор на един от уговорените мрежови протоколи, а *Payload* съдържа съответната дейтаграма.

PPP фази

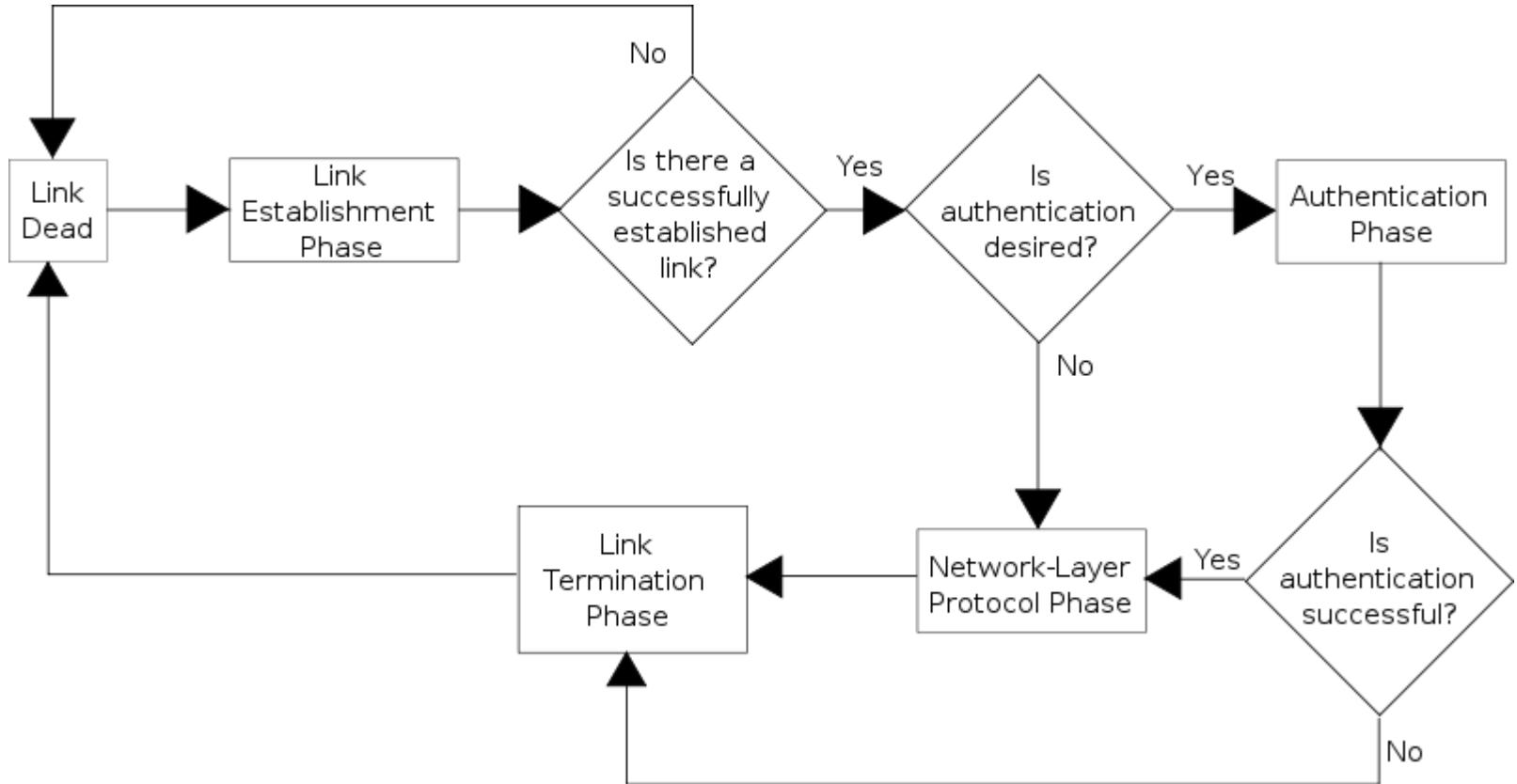


Схема на установяване на връзката.

LCP

Line Control Protocol (**LCP**):

автоматично конфигуриране на срещуположните интерфейси:

дължина на кадъра, ESC символи;

Проверка на линията за грешки с произволни числа (**magic numbers**). Ако линията е дадена накъсо, възелът получава LCP съобщение със своя си **magic number**, вместо да получи **magic number** на съседа;

Компресия.

Последвани евентуално от **аутентикация**.

Аутентикация

Съседите си обменят съобщения за аутентикация.

Имаме два варианта:

Password Authentication Protocol (**PAP**) и
Challenge Handshake Authentication Protocol
(**CHAP**).

PAP

PAP предава пароли в явен ASCII текст по мрежата, затова е несигурен.

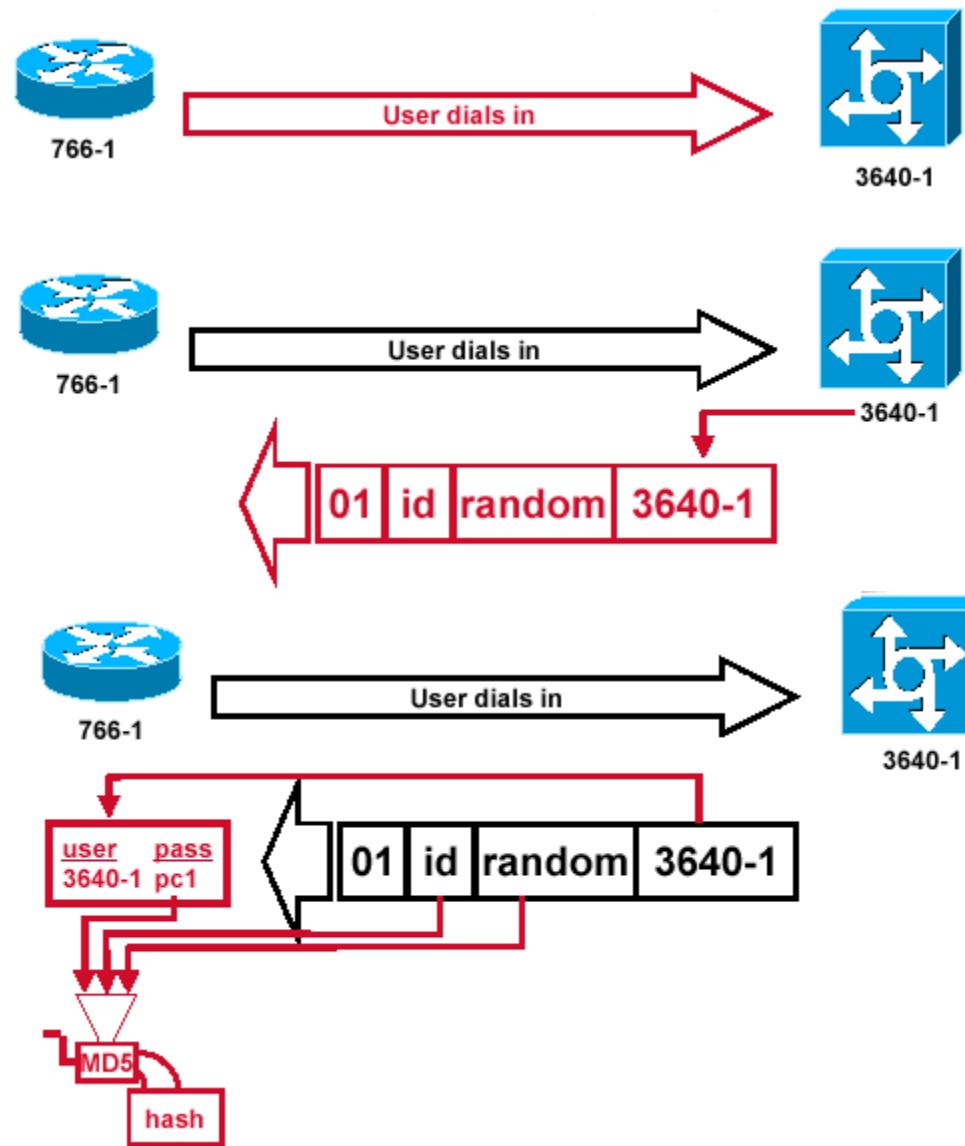
- * Клиент изпраща username и password
- * Сървърът връща:
 - authentication-ack (ако е OK) или
 - authentication-nak (в противен случай).

CHAP

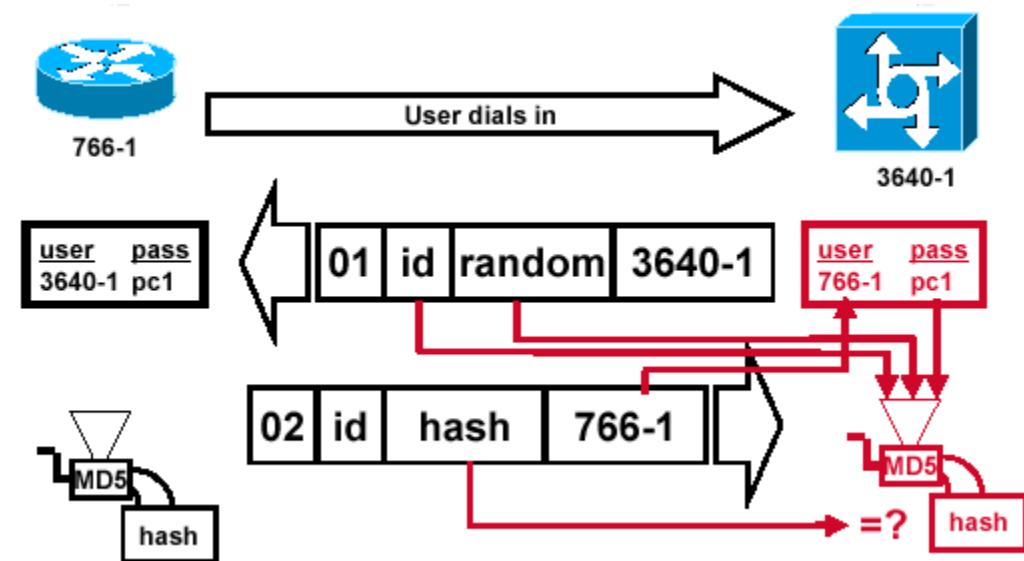
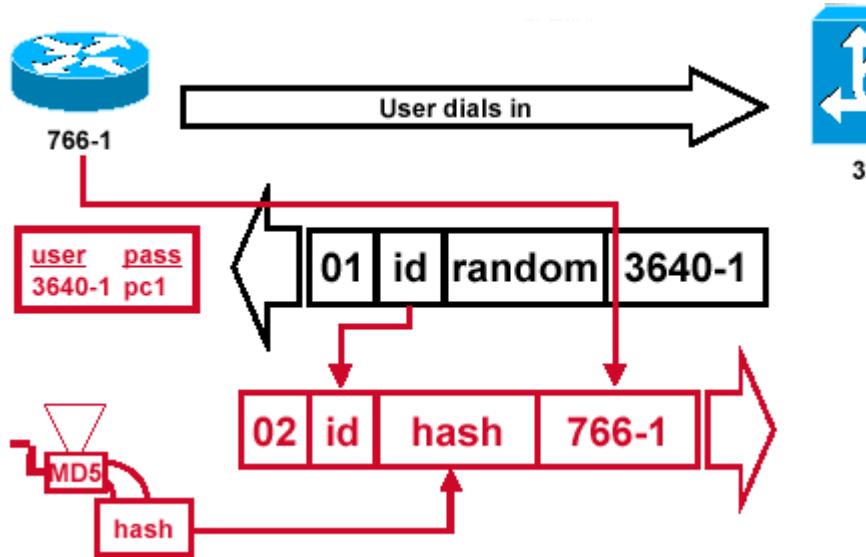
CHAP периодично проверява идентичността на клиента чрез **three-way handshake**. При установяване на сесията и през произволни интервали от време след това. Проверката се базира на **споделена** “тайна” (напр. Паролата на потребителя).

1. **Сървърът** изпраща "**challenge**" съобщение към клиента.
2. **Клиентът** отговаря с число, изчислено с помощта на еднопосочна хеш функция, напр. **MD5 checksum hash**.
3. **Сървърът** сравнява този хеш със своя. Ако съвпадат, следва **acknowledge**; в противен случай връзката се прекъсва.
4. През произволни интервали сървърът изпраща ново предизвикателство: стъпки 1-3 се повтарят.

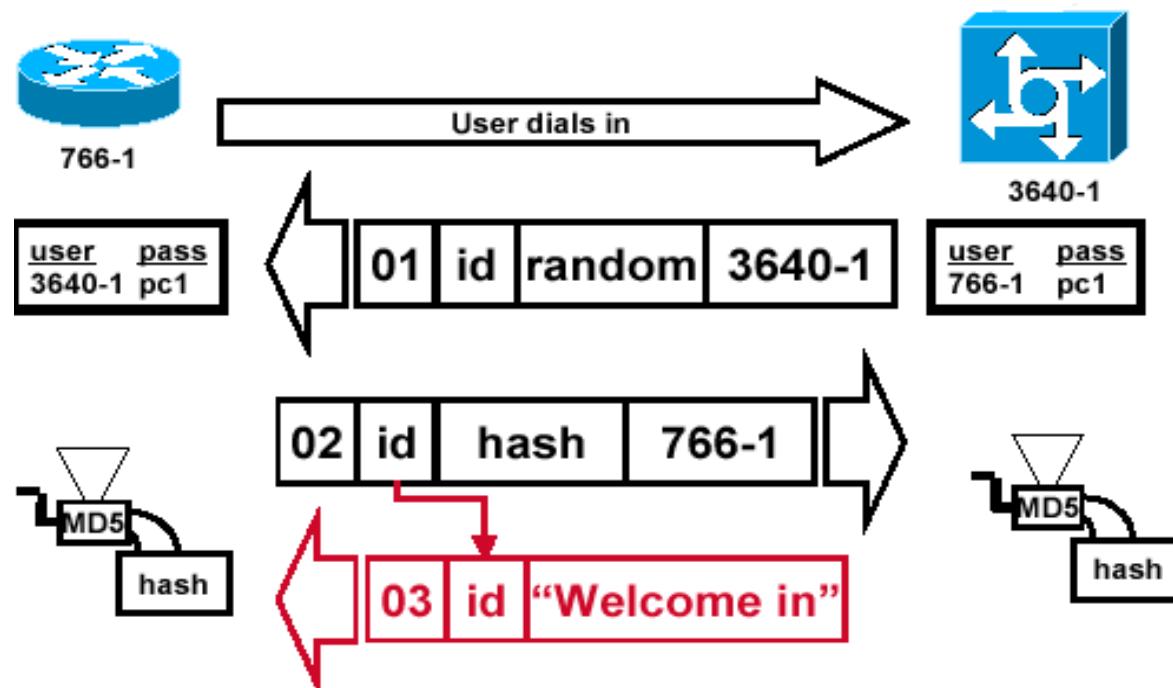
CHAP. Етапи.



CHAP. Етапи.



CHAP. Етапи.



Network Control Protocol

Network Control Protocol (NCP) се стартира след LCP.

Уговаря опции за протокола от мрежовия слой, над PPP. NCP са:

- Internet Protocol Control Protocol (**IPCP**) за IP,
- Internetes Packet Exchange Control Protocol (**IPXCP**) за IPX и
- AppleTalk Control Protocol за AppleTalk и

IPv6 Control Protocol (IPV6CP) за предаване на IPv6 пакети по PPP линии.

Развитие на PPP – PPPoE

PPPoE, Point-to-Point Protocol over Ethernet опакова PPP кадри вътре в Ethernet кадри.

Използва се при свързвания към Интернет чрез LANs, WLANs или Metro Ethernet мрежи.

Разработена е от UUNET, Redback Networks и RouterWare, стандартизирана е в RFC (Request for Comment) 2516.

Чрез PPPoE потребителите виртуално “набират номера” на отдалечен сървър на провайдера през Ethernet и установяват “point to point” връзка.

PPPoE - стадии

PPPoE се установява на два точно определени стадия:

PPPoE discovery

Традиционните PPP връзки се установяват между две крайни точки, които са предварително изградени.

Но Ethernet мрежите са multi-access, така че преди обмен на PPP контролни пакети за установяване на връзката върху Ethernet, двете страни ще трябва да си научат MAC адресите, за да бъдат закодирани в контролните пакети.

Също така се установява **Session Id**, която се използва при обмена на пакети.

PPP session

След като са известни MAC адресите и е установена сесията, двете страни имат всичката информация за изграждане на “point-to-point” връзка по Ethernet и обмен на пакети.

PPPoE Frame

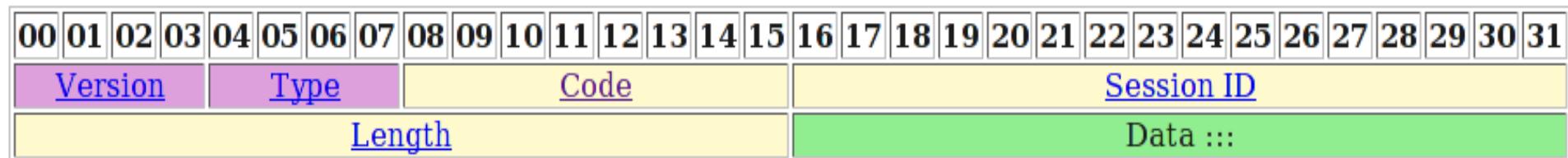
Вмъкването на PPP “заглавие” води до намаляване на полето за данни от **1500 на 1492 байта.**

Намалява ефективната скорост:

$$1492:1500 = \mathbf{0.995}$$



PPPoE header:



MPLS

Multiprotocol Label Switching (MPLS) е механизъм за реализация на високопризводителни телекомуникационни мрежи.

Разработен е от IETF (Internet Engineering Task Force).

MPLS работи на OSI "**Слой 2.5**".

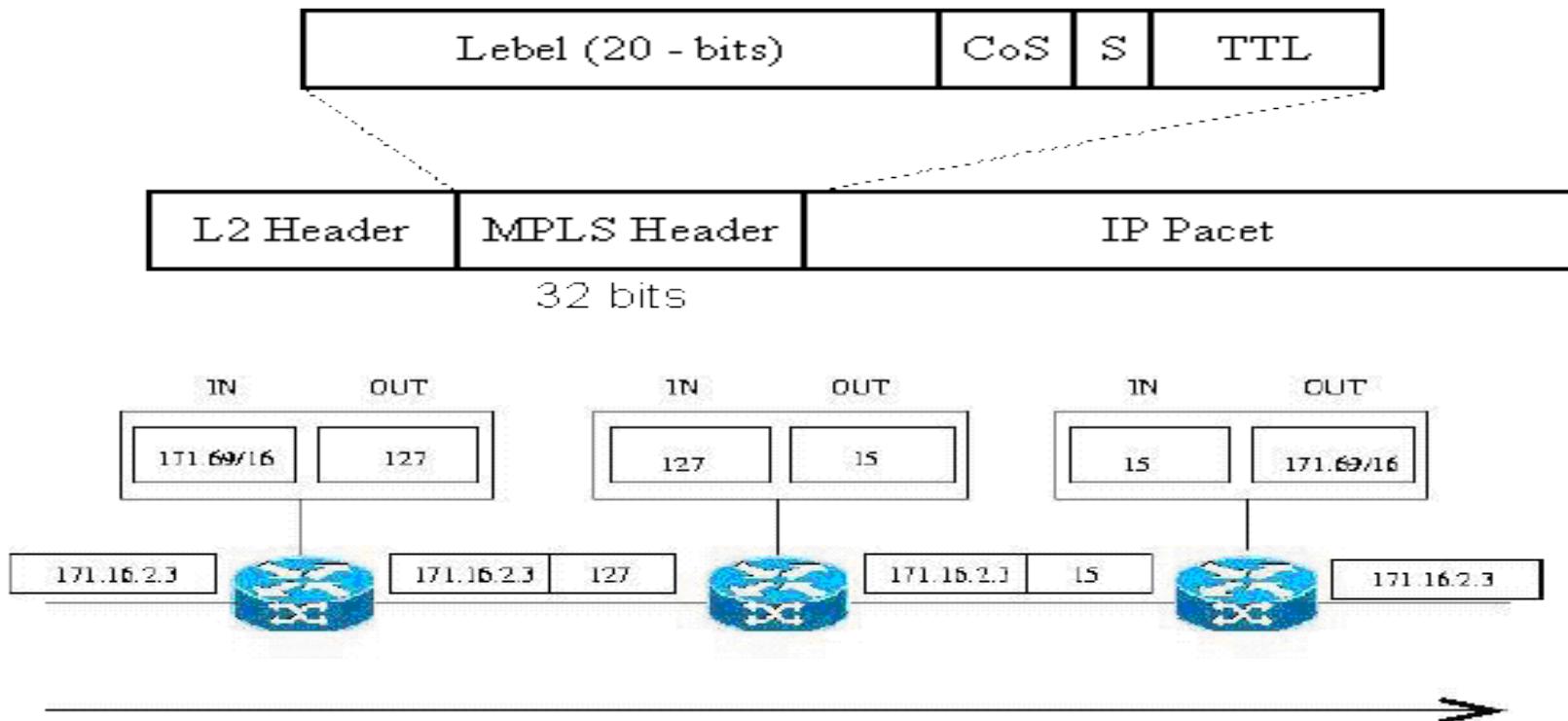
Multiprotocol:

Пренася всякакви видове трафик: **IPv4** и **IPv6**, **Ethernet** и др.

Label Switching:

Данните се направляват от възел на възел с помощта на **етикети**.

MPLS. Layer 2.5.



Фигура 3: Препращане на пакети чрез етикети в MPLS

Етикетът съответства на Forwarding Equivalence Class – FEC;
Прави се проверка в информационната база с етикети (LIB), за да се определи:

- следващия участък от връзката;
- коя връзка да се използва и как да се подреди пакета в опашката.

Как работи MPLS

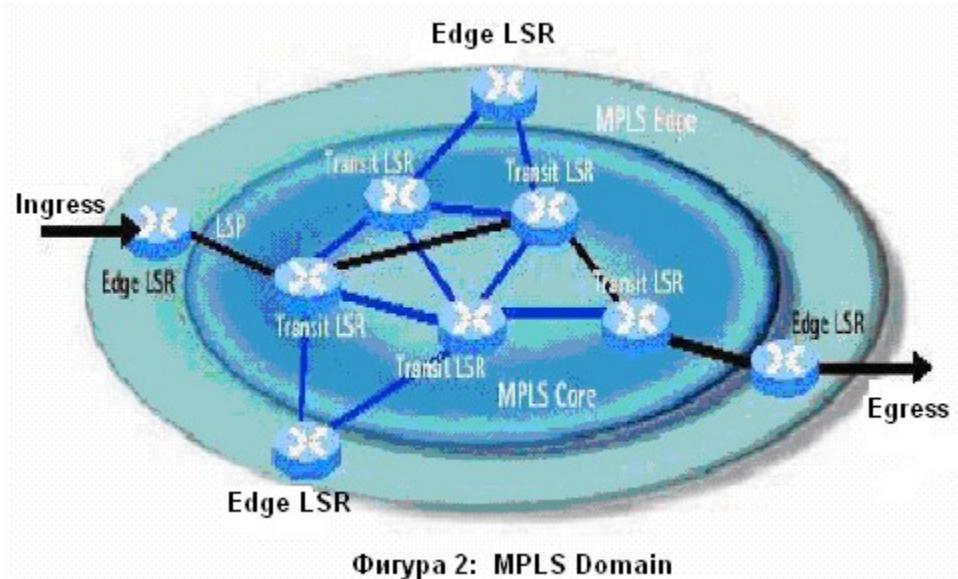
В MPLS маршрутизаторът препраща пакета през MPLS домейн. Възлите по пътя не взимат никакви маршрутизиращи решения. Използват **етикета** в пакета за определяне на **следващата стъпка** по пътя.

MPLS домейнът (domain) е подобно на **AS** (autonomous system – автономна система), в IP маршрутизацията, т.е. група от свързани рутери, които са под единен административен и управленски контрол.

MPLS domain се разделя на MPLS ядро (**core**) и MPLS периферия (**edge**).

Възлите в **core** са **LSRs** (Label Switch Routers), а възлите в **edge** - Label Edge Routers (**LER**).

MPLS domain



Когато IP пакет преминава през MPLS domain, той преминава през предварително зададен път, зависещ от FEC, Label Switched Path – **LSP**.

FEC действа, като филтър: кои IP пакети по кои LSPs да бъдат препратени.

MPLS и Ethernet

Митовете за MPLS <http://delian.blogspot.com/2006/11/mpls.html>

- QoS в IP – в IP имаме повече приоритети (64 с DSCP, срещу 8 ако използваме Exp за CoS);
- Layer3 VPN - L3 VPN се прави и с GRE тунели, и с IPSec, и с чист Ethernet. и т.н. и т.н.

MPLS не може да се мери с “чиста” Ethernet мрежа.

Ethernet е по-евтин, същата функционалност, по-висок капацитет и по-висока съвместимост.

Ethernet е достатъчна само заради бързодействието.

Канално ниво в локалните мрежи

Методи на достъп до съобщителната среда в Ethernet.

Управление на канала в Ethernet.

Превключватели и мостове.

Виртуални локални мрежи и протокол Spanning Tree.

Какво ще научим

- ✓ Втори слой в мрежовата архитектура по отношение на локалните мрежи. Методи на достъп до преносната среда.
- ✓ Логическа и физическа топология на локална мрежа
- ✓ История на възникване на метода на достъп CSMA/CD
- ✓ Ethernet – технологичната конвергенция в Internet
- ✓ Формат на кадъра в Ethernet. MAC адрес.
- ✓ MTU и производителност на мрежата
- ✓ Жична преносна среда в Ethernet. 10/100/1000 Mbps, 10/40/100 Gbps и по-високи скорости
- ✓ От хъбове към суичове. Технология на превключването.
- ✓ Протокол Spanning Tree. Виртуални локални мрежи (VLANs).
- ✓ Ethernet в глобалните мрежи

LANs - мрежите с общодостъпно предаване

Мрежите с общодостъпно предаване се характеризират с общ комуникационен канал, който се споделя от всички машини, включени в мрежата.

Всеки изпратен кадър минава през общия канал и достига до всички машини в мрежата. Адресно поле в кадъра посочва за кой е предназначен този кадър.

Когато една машина получи кадър, тя проверява дали той е предназначен за нея. Ако това е така, кадърът се приема и обработва, в противен случай се отхвърля.

Мрежи с общодостъпно предаване

При мрежите с общодостъпно предаване основен проблем е да се определи кой да започне да използва канала, дали да има състезание или поредност.

Протоколите, които разрешават този проблем се отнасят към подниво на каналния слой, наречено **подниво за достъп до средата** (medium access control - MAC). Наричат се още протоколи за множествен достъп (**Multiple Access**)

Регионалните мрежи използват връзки "точка-точка" (point-to-point), докато общодостъпни многоточкови (**multipoint**) канали се използват най-вече при локалните мрежи.

Мрежи с общодостъпно предаване

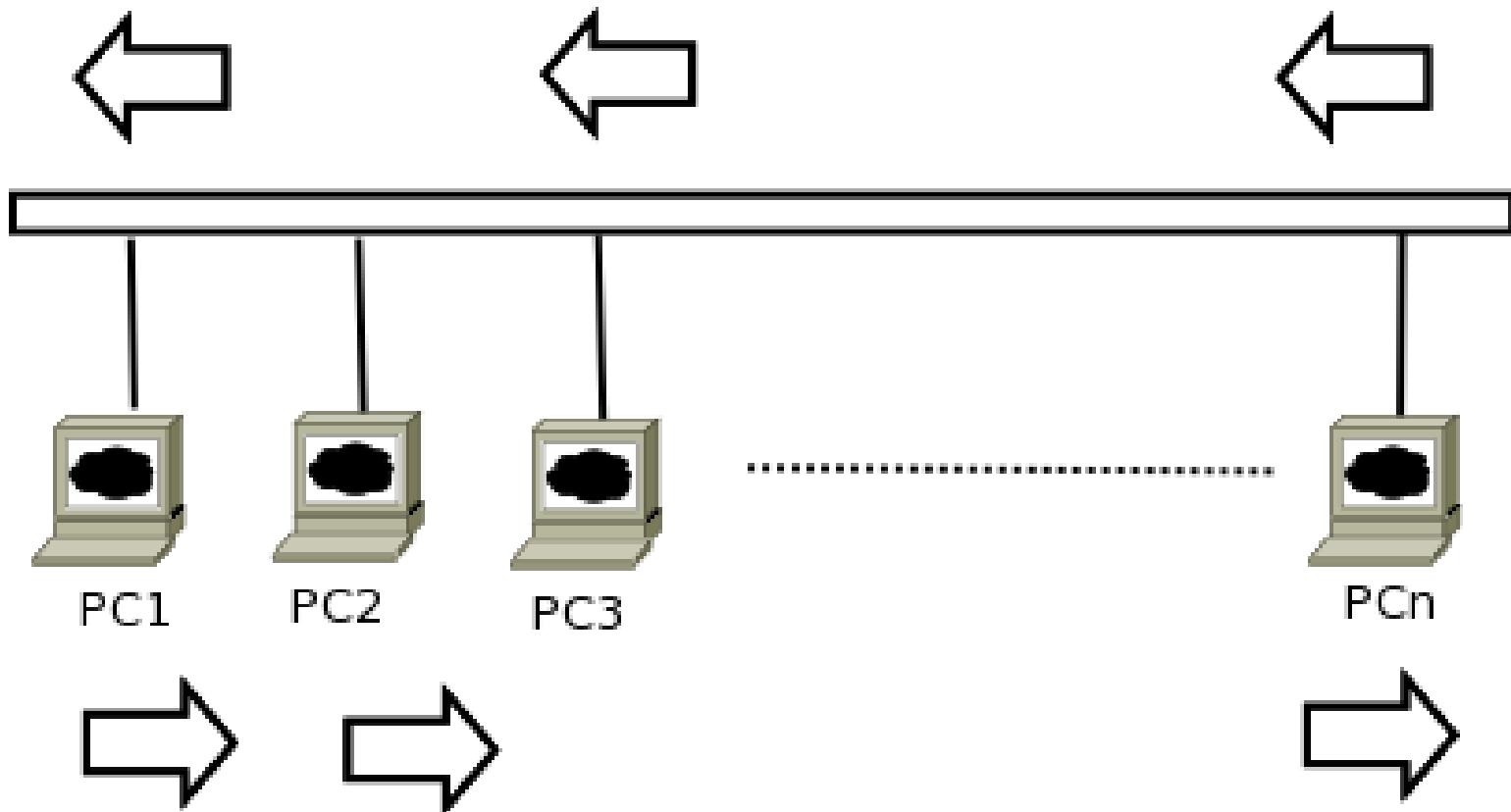
Протоколите (процедурите) за достъп до канала се делят на две основни групи:

- детерминирани и
- състезателни

От първите най-известни са **Token Ring** (разработка на IBM) и **FDDI**. Те могат да се сравнят с кръгово кръстовище, регулирано със светофари.

Поради сложността им бяха изместени изцяло от състезателните. По-нататък ще се занимаваме с тях.

Локална мрежа Token Ring



“Чиста” ALOHA

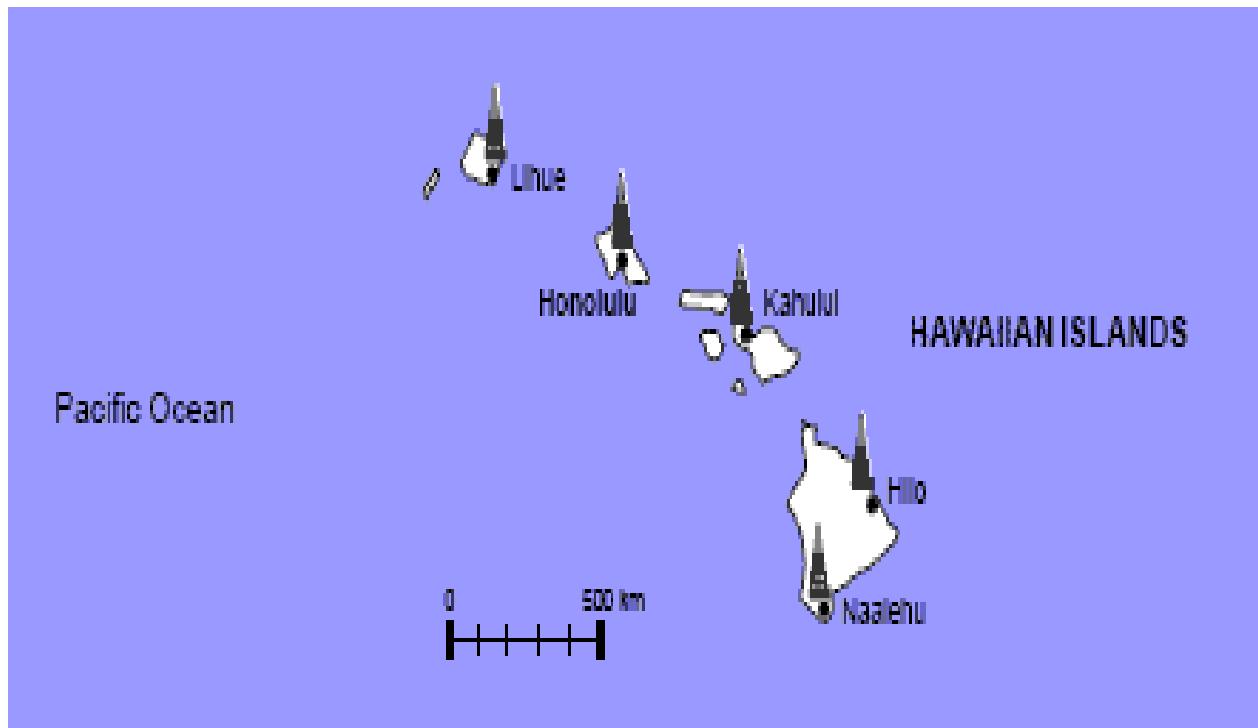
Идва от мрежата в Университета в Хонолулу –
Хавайските острови.

Множество радиостанции, расположени на
различните острови.

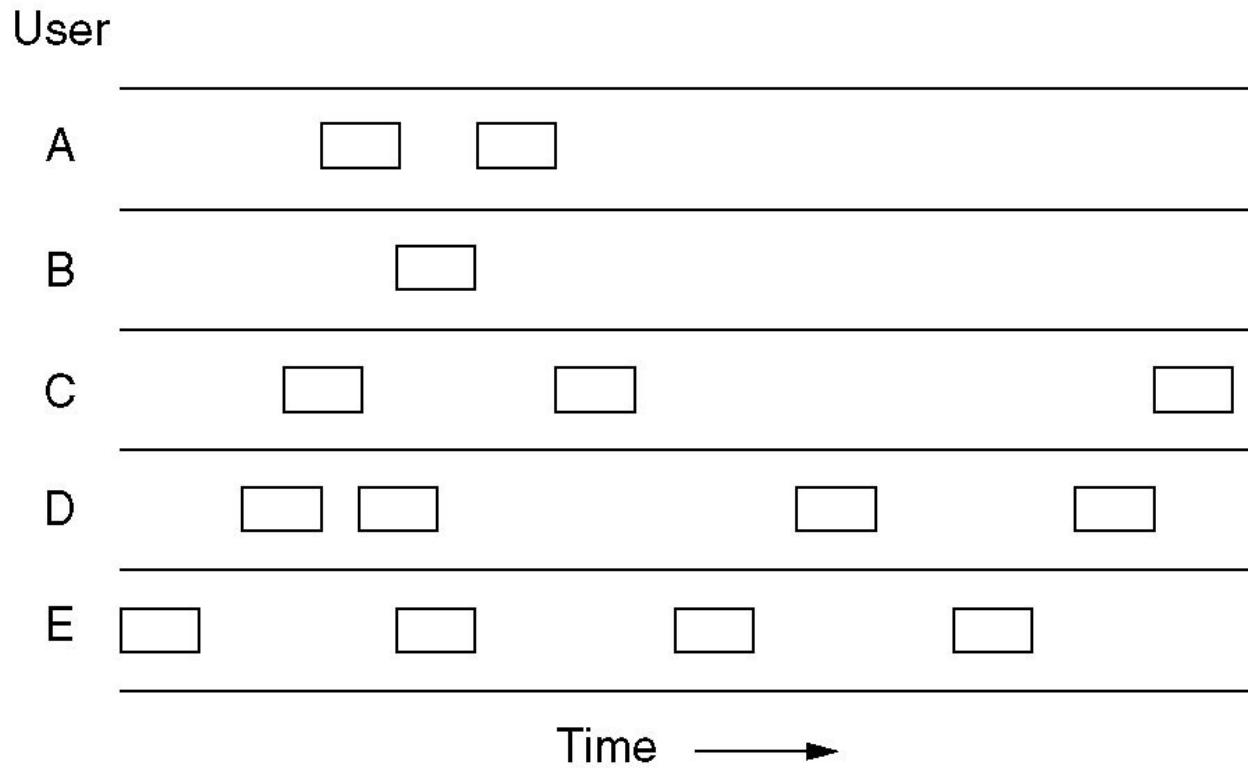
Всяка предава, “когато си поиска”, без да се
съобразява с другите.

Aloha си е **Multiple Access (МА)** и
Съответства на “нерегулируемо кръстовище”
Тъй като всички работят на една и съща честота,
едновременното предаване на две или повече
станции води до т. нар. **колизии (jamming)**,
предизвикани от интерференция на сигналите.

ALOHA

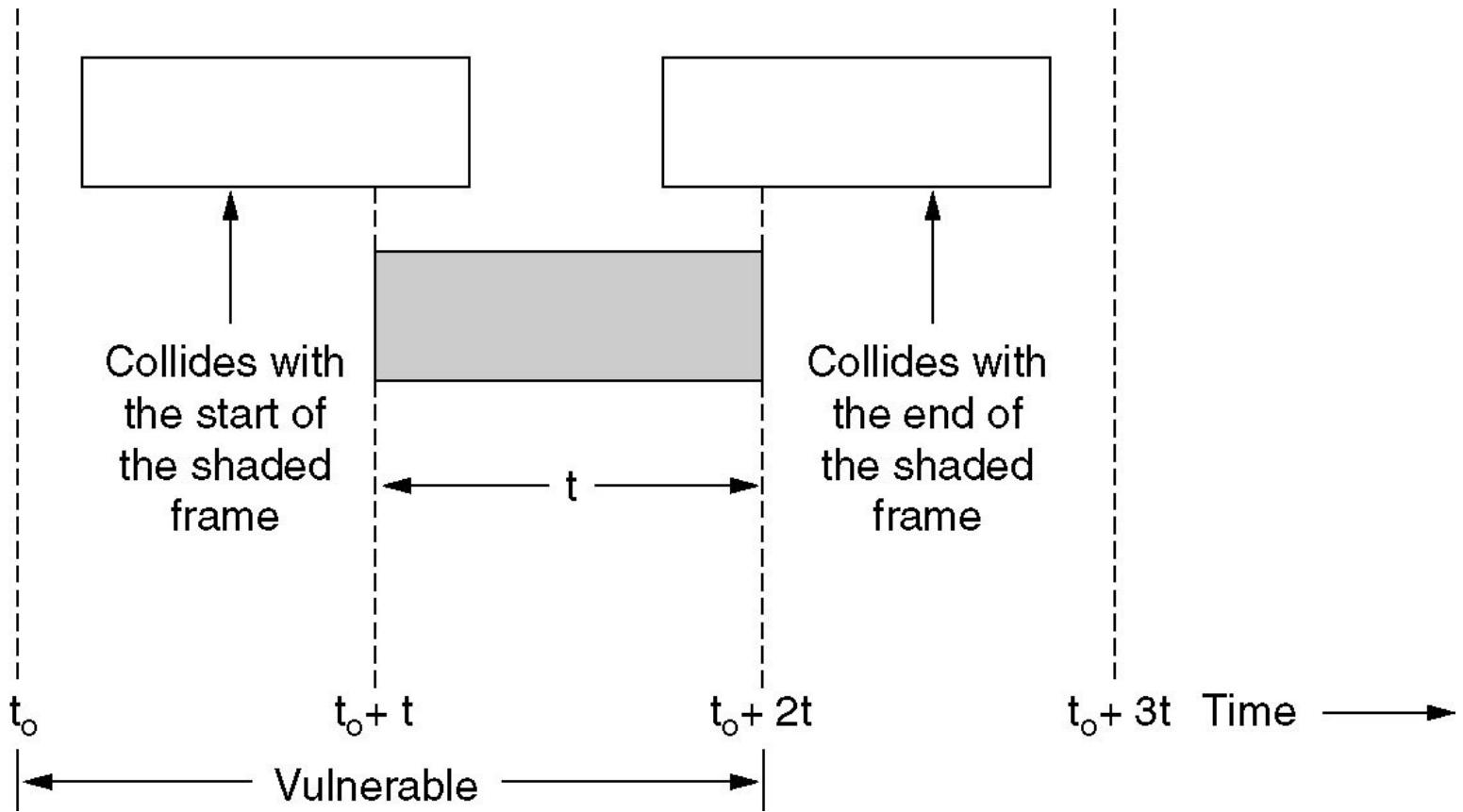


Чиста ALOHA (за сведение)



Кадрите се предават в произволно време.

Чиста ALOHA. Колизии. (за сведение)

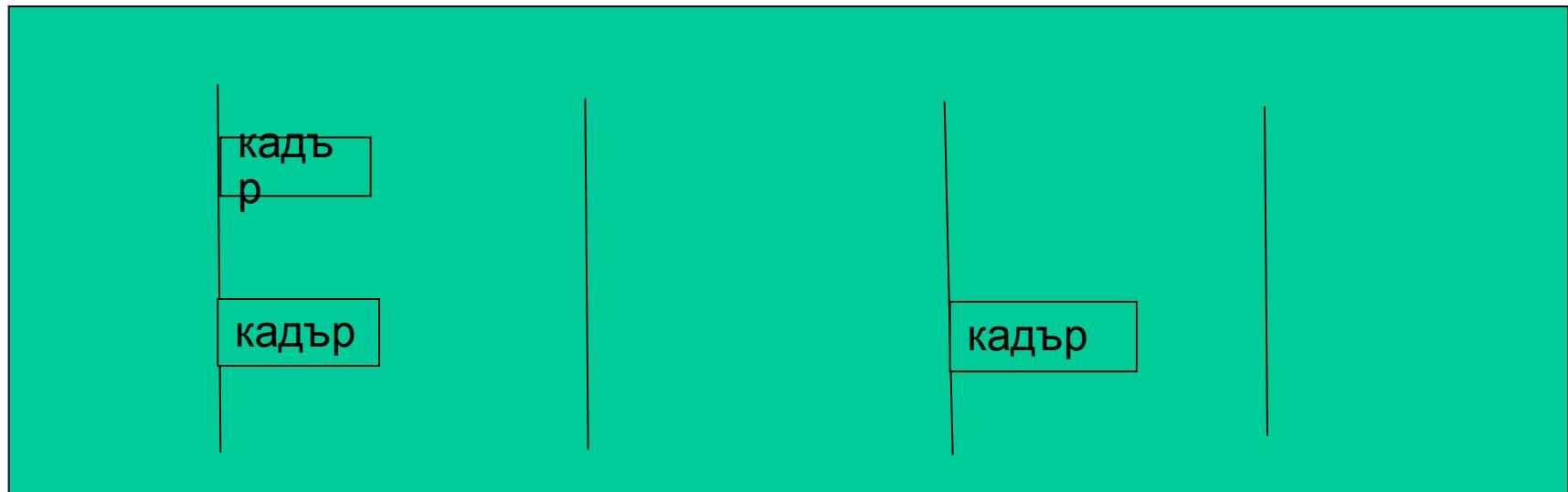


Колизии с началото и края на долния кадър.

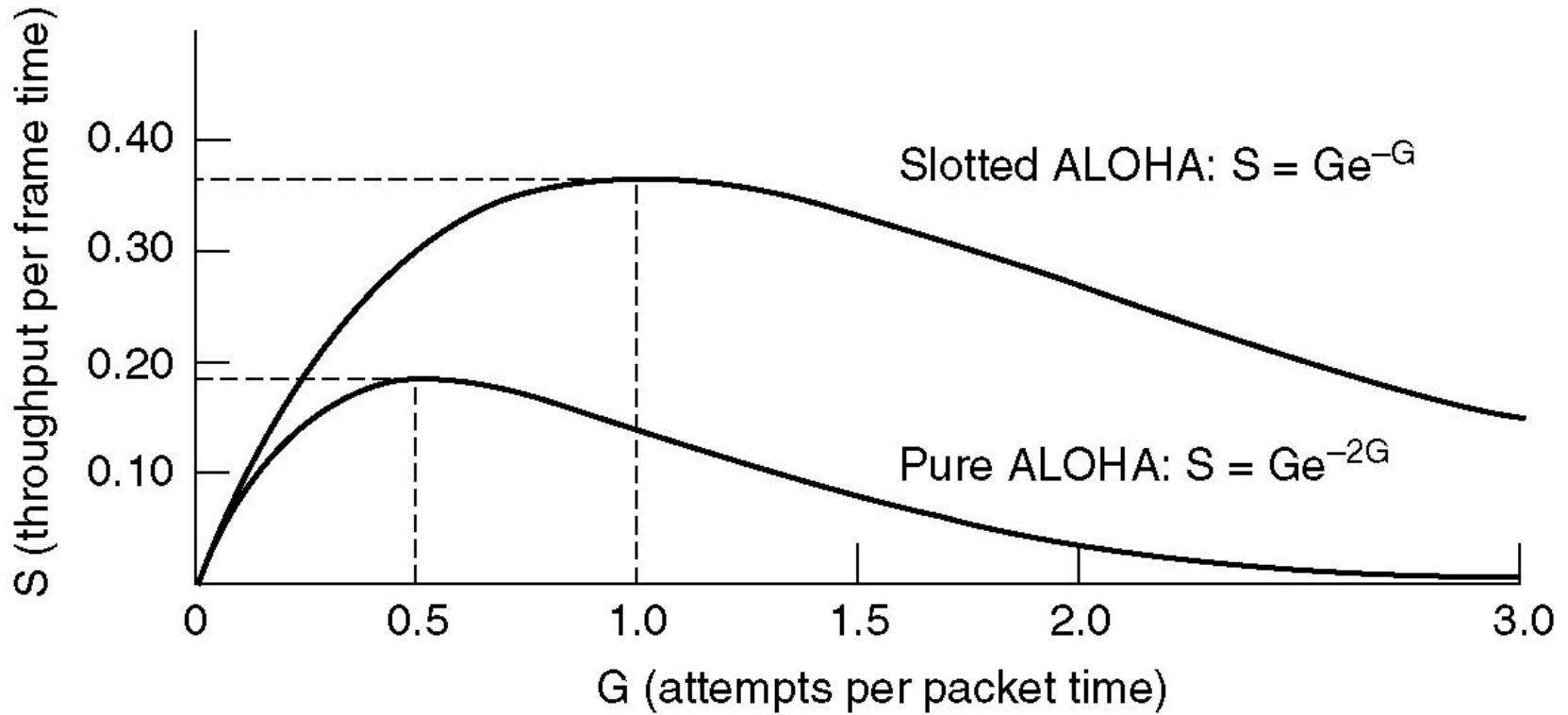
Slotted ALOHA

Предава само в началото на синхронизирани отрезъци от време -
“slot times”

Колизиите се ограничават само във времето на предаване на един
кадър



Pure vs. Slotted ALOHA



Пропускателна способност спрямо ниво на трафика

Carrier Sense Multiple Access (CSMA)



Можем да го сравним със знака „Пропусни движещите се по пътя с предимство!“

Протоколите, които прослушват носещата, се наричат **carrier sense multiple access** (множествен достъп с откриване на носещата – МДОН).

Предложени са от **Kleinrock и Tobagi** (1975), които са анализирали техни варианти.

Един от тях се нарича **1-persistent CSMA** (1 настойчив).

Протоколът се нарича **1-persistent**, защото станцията започва да предава с вероятност 1, ако има свободен канал.

Nonpersistent CSMA (за сведение)

Този протокол не е толкова “лаком”. Станцията прослушва канала, ако никой не предава, започва тя.

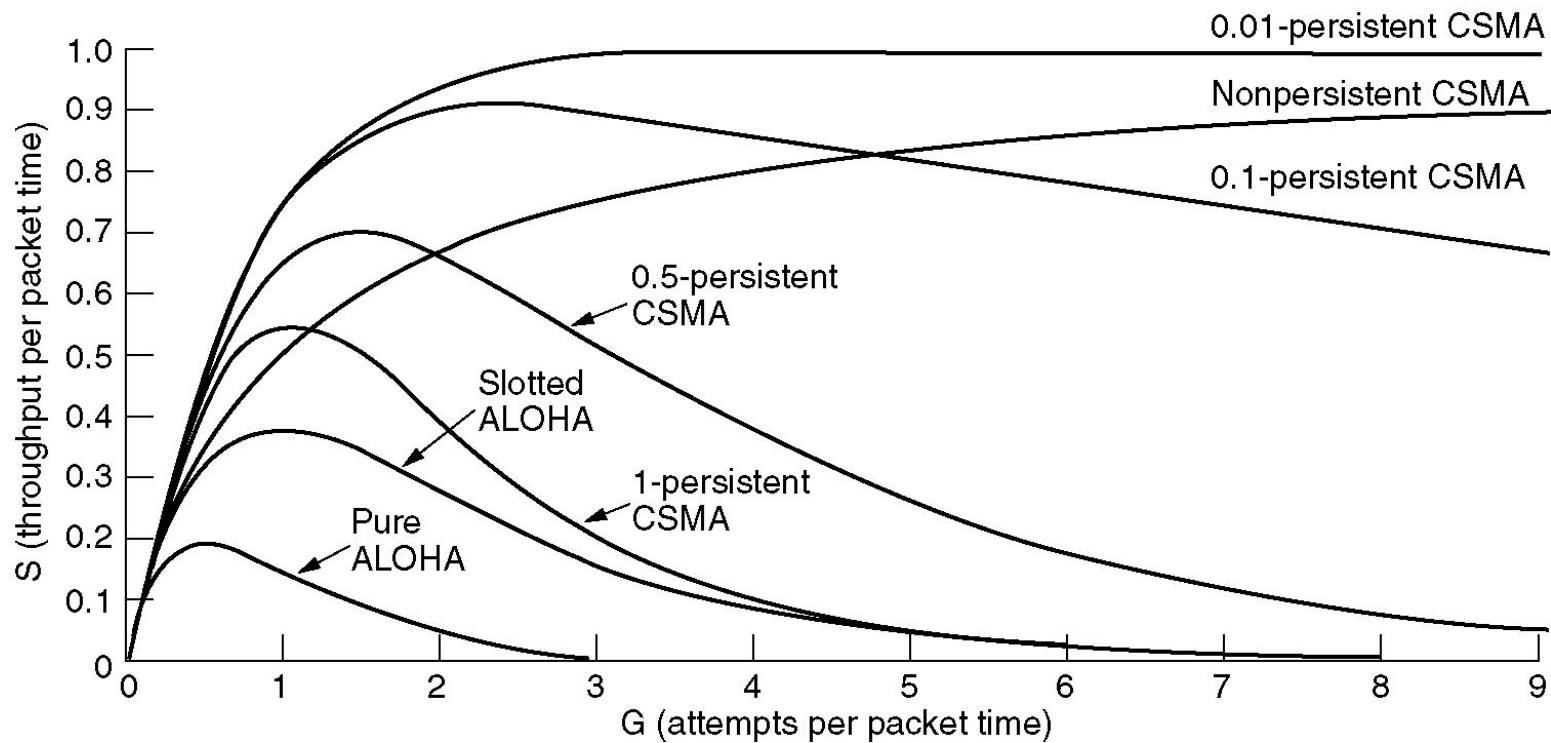
Ако каналът е зает, станцията не продължава да прослушва, а изчаква произволен период от време, след което повтаря алгоритъма.

Постига се по-добро оползотворяване на канала от 1-persistent CSMA.

p-persistent CSMA се отнася към канали с времеделене (time slot).

Ако каналът е свободен готовата станция започва да предава с вероятност p . С вероятност $q = 1 - p$ отлага за следващия слот. Ако и той е свободен, или предава, или отлага с вероятност p или q .

Persistent и Nonpersistent CSMA (за сведение)



Използване на канала спрямо натоварването

CSMA плюс Collision Detection



Наподобява пътен знак номер Б2 “Спри! Пропусни движещите се по пътя с предимство”.

В споделената комуникационна среда (шина) станцията, която иска "да каже" нещо прослушва средата. Когато е свободна (никой не "приказва"), изпраща фрейм с данни. Но възможно е точно в същия момент друга да започне да предава фрейм. Двете станции няма как да се чуят, защото сигналът има време на разпространение.

При такава ситуация настъпва **колизия**.

...CSMA/CD

Затова двете станции продължават да прослушват канала за колизии за период от време, равен на времето на разпространение на сигнала от единия край на комуникационната линия до другия и обратно.

Ако се разпознае колизия, станцията веднага прекъсва предаването и изпраща сигнал за интерференция (**JAM signal**), така че всички станции да разпознаят колизията.

Предаващата станция изчаква да мине интервал от време (**backoff**), изчислен на случаен принцип с помощта на *random generator*, преди да се опита да предава повторно.

Така се гарантира, че участниците в колизията ще предприемат повторно предаване в различни моменти от времето и колизията няма да се повтори.

Този протокол е **CSMA/CD (CSMA with Collision Detection)** и се прилага в LAN Ethernet.

...CSMA/CD

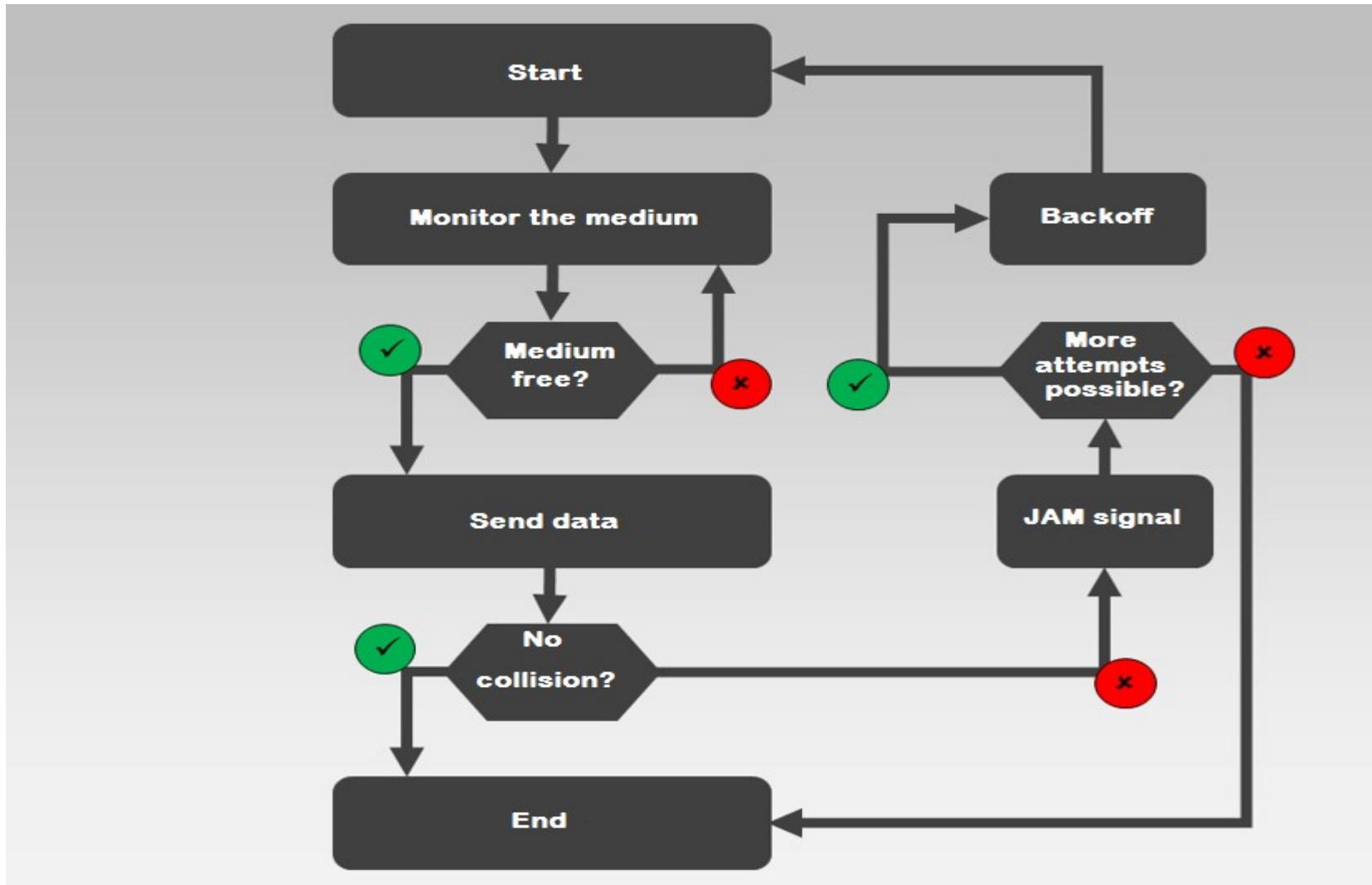
Разпознаването на колизията зависи от времето на разпространение на сигнала от единият край на кабела до другия и обратно - 2τ .

В най-лошият случай една станция не може да е сигурна, че е “захванала” канала, докато не е предавала за 2τ , без да е чула колизия.

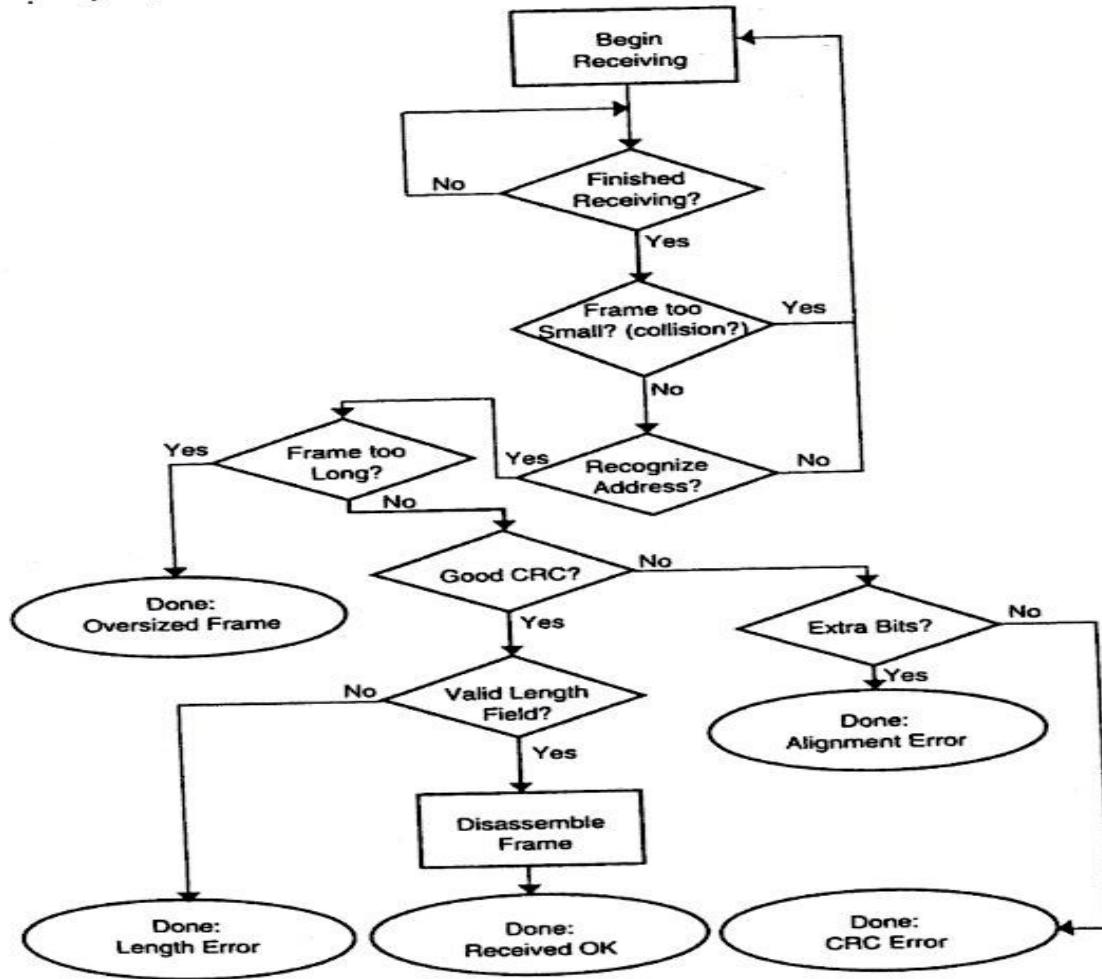
Приема се $\tau \approx 4.8 \text{ } \mu\text{sec}$, времето за разпространение на сигнала по 1-km коаксиален кабел.

За време 2τ се предават първите **64 байта** от фрейма, т. нар. **Collision Frame**.

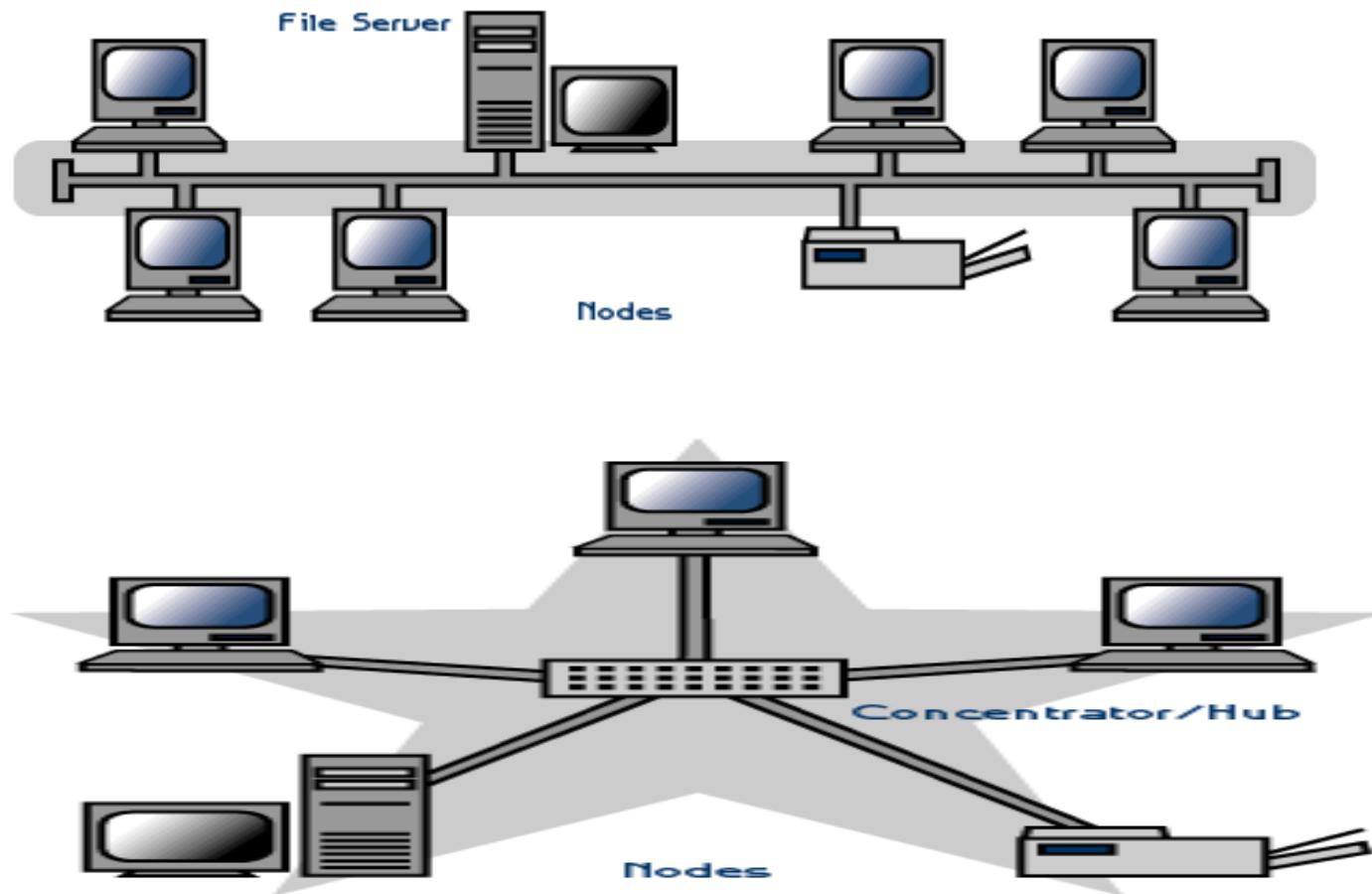
CSMA/CD. Предаване.



Приемане на Ethernet кадри



Ethernet. Логическа шина.



Robert M. "Bob" Metcalfe. Една жива
легенда.

Откривателят на Ethernet



ART: DALE STEPHANOS

Най-разпространената LAN Ethernet

Описана в стандарта IEEE (Institute of Electrical and Electronic Engineers) 802.3, издаден през 1970-те години.

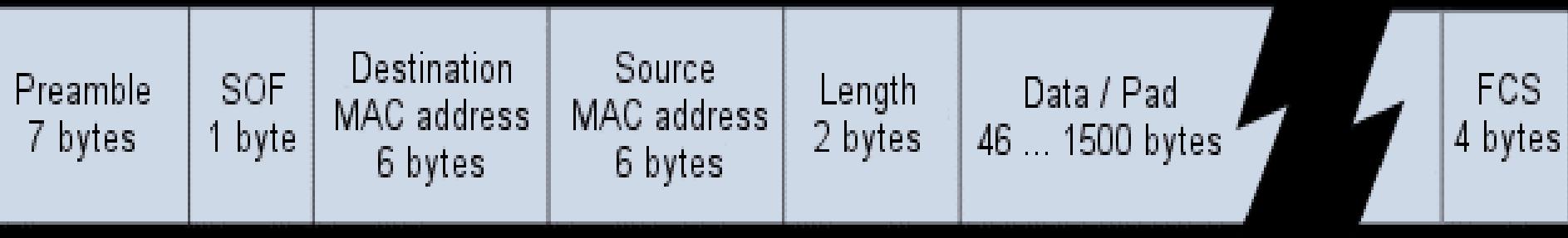
Един персонален компютър се свързва в Ethernet мрежа с помощта на NIC (Network Interface Card) (или Ethernet контролер, който го има на всяка дънна платка), която изпраща и приема кадри (frames).

Ethernet вече не е само LAN технология.

Благодарение на FO и мощните лазерни излъчватели, покриващи стотици километри, е MAN/WAN технология.

Технологична конвергенция в Интернет.

802.3 Кадър (Novell raw)



Preamble = 56 бита 0-и и 1-ци.

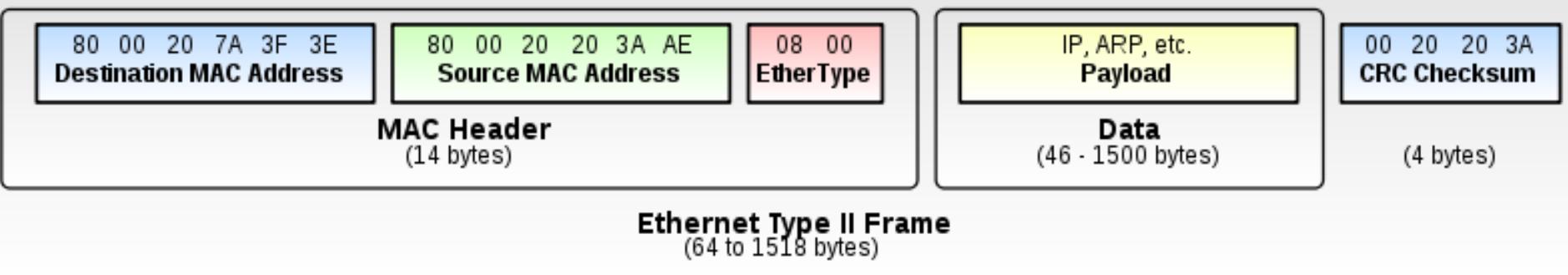
SOF = Start of frame: "10101011"

Data / Pad = ако няма достатъчно данни (payload), полето за данни се допълва, за да имаме минимален размер на кадъра

FCS = Frame check sequence – CRC

Днес се използва **Ethernet II frame**, **DIX** frame (DEC, Intel и Xerox); директно от Internet Protocol.

Ethernet II кадър (DIX)



Destination address съдържа адресът на получателя на кадъра
Source address - адресът на изпращача на кадъра.

Най-младшият бит на най-старшия байт на адреса на получателя е 0 за нормален адрес и 1 за [групов](#) адрес. При групов адрес, кадърът е предназначен за група станции ([multicast](#)). Адрес на получател, състоящ се [само от 1](#) означава, че кадърът е предназначен за всички станции ([broadcast](#)).

Полето *EtherType*: 0x0800 кадърът носи IPv4 дейтаграма; 0x0806 - ARP, 0x8100 - IEEE 802.1Q и 0x86DD - IPv6.

Формат на кадрите в Ethernet

Данните се съдържат в полето *Data* и максималната им дължина е **1500 байта**. Това е т. нар. **payload**.

Освен максимална дължина на кадъра има и **минимална дължина** на кадъра.

В стандарта 802.3 минималната дължина на кадъра е **64 байта**.

Зашото времето за разпознаване на колизия (конфликт) е времето за предаване на 64 байта.

Полето *Pad* за запълване на кадъра до 64 байта.

Полето *Checksum* е контролна suma, която се използва за откриване на грешки при предаването.

Maximum Transmission Unit (MTU)

В компютърните мрежи **МТУ** в протокол на даден слой е максималната дължина на полето за данни (в байтове), който може да понесе дадения слой. Т.e максималния **payload**.

По-голям МТУ означава по-висока ефективност:

- един пакет носи **повече потребителски данни**;
- **по-малко служебна информация (overhead)**.

Но, **по-големите пакети окупират за по-голям период бавните линии**. Например, 1500-байтов Ethernet кадър “захваща” за цяла секунда 14.4k modemна линия. Затова се налага фрагментиране.

Ефективност и нетна скорост

$$\text{Efficiency} = \frac{\text{Payload size}}{\text{Frame size}}$$

Максимална ефективност се постига с
максимален payload:

$$\frac{1500}{1538} = 97.53\%$$

за untagged ethernet кадри и е $\frac{1500}{1542} = 97.28\%$
за 802.1Q VLAN tagging.

Net bit rate: Net bit rate = Efficiency × Wire bit rate

Максималната нетна скорост за 100BASE-TX
Ethernet без 802.1Q is **97.53 Mbit/s.**

MTU. Jumbo Frames.

jumbo frames са Ethernet кадри с дължина по-голяма от 1500 байта payload (MTU). Приема се, че jumbo frames носят до 9000 bytes.

Много, не и всички, Gigabit Ethernet суичове и карти поддържат jumbo frames, но всички Fast Ethernet поддържат само стандартните 1500 байта.

Дължина на Ethernet кадъра от 1518 байта е избрана въз основа на оценка на надеждността и скоростта на канала.

От друга страна, ако увеличим размера, по-големи обеми от данни ще се предадат с по-малко усилия:

- по-малко CPU цикли;
- по-малко прекъсвания;
- CPU се съредоточава върху потребителските данни.

Jumbo Frames.Super Jumbo Frames

9000 байта като предпочитан размер на jumbo frames е резултат от споразумение между Joint Engineering Team of Internet2 и правителствените мрежи в САЩ.

Super jumbo frames (**SJFs**) са кадри с дължина над 9000 байта.

С растежа на скоростта на линията пропорционално би трябвало да **расте** и **payload**. Това обаче зависи от възможностите на логическите схеми, обработващи пакетите.

Колкото и да са трудни преговорите в тази насока, възможно е да се достигне дължина от 64000 байта.

Шестнадесетични числа (Hexadecimal)

Ед на шестнадесетична цифра:

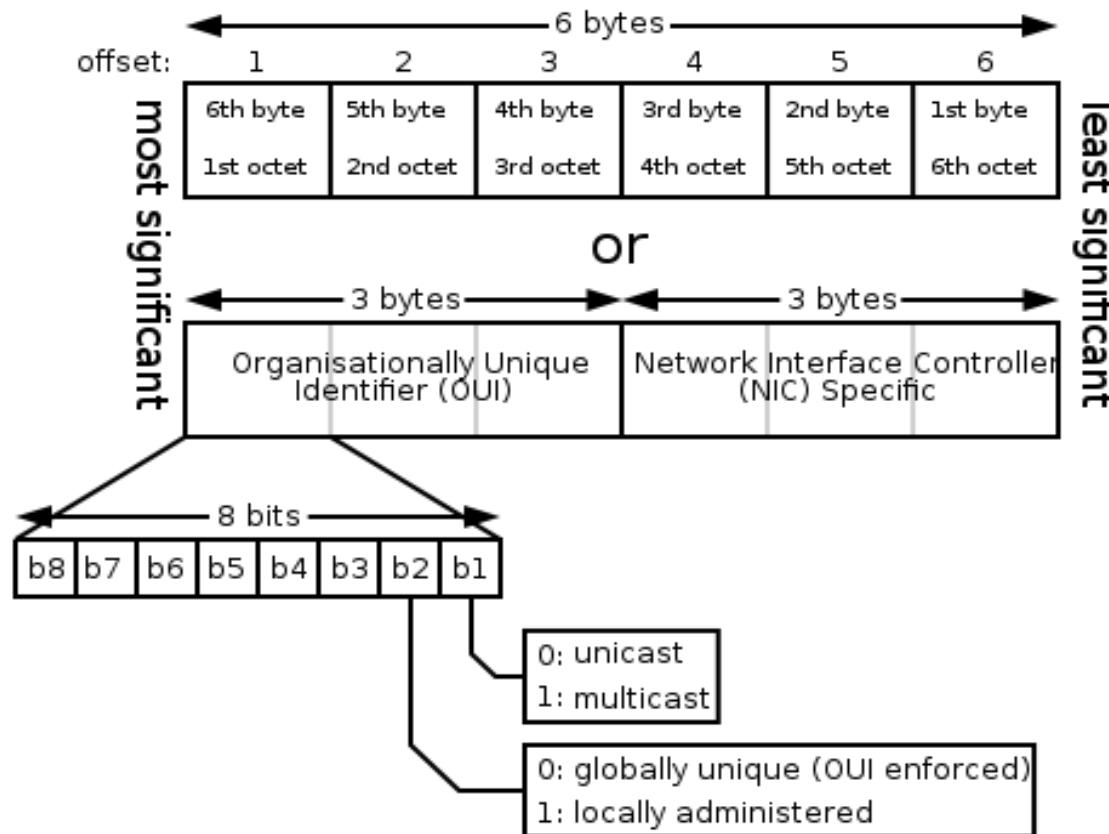
– 4 двоични разряда:

0_{hex}	$=$	0_{dec}	$=$	0_{oct}	0	0	0	0
1_{hex}	$=$	1_{dec}	$=$	1_{oct}	0	0	0	1
2_{hex}	$=$	2_{dec}	$=$	2_{oct}	0	0	1	0
3_{hex}	$=$	3_{dec}	$=$	3_{oct}	0	0	1	1
4_{hex}	$=$	4_{dec}	$=$	4_{oct}	0	1	0	0
5_{hex}	$=$	5_{dec}	$=$	5_{oct}	0	1	0	1
6_{hex}	$=$	6_{dec}	$=$	6_{oct}	0	1	1	0
7_{hex}	$=$	7_{dec}	$=$	7_{oct}	0	1	1	1
8_{hex}	$=$	8_{dec}	$=$	10_{oct}	1	0	0	0
9_{hex}	$=$	9_{dec}	$=$	11_{oct}	1	0	0	1
A_{hex}	$=$	10_{dec}	$=$	12_{oct}	1	0	1	0
B_{hex}	$=$	11_{dec}	$=$	13_{oct}	1	0	1	1
C_{hex}	$=$	12_{dec}	$=$	14_{oct}	1	1	0	0
D_{hex}	$=$	13_{dec}	$=$	15_{oct}	1	1	0	1
E_{hex}	$=$	14_{dec}	$=$	16_{oct}	1	1	1	0
F_{hex}	$=$	15_{dec}	$=$	17_{oct}	1	1	1	1

Шестнадесетични числа към десетични

Decimal	Hex	Decimal	Hex	Decimal	Hex
1	1	11	B	30	1E
2	2	12	C	40	28
3	3	13	D	50	32
4	4	14	E	60	3C
5	5	15	F	70	46
6	6	16	10	80	50
7	7	17	11	90	5A
8	8	18	12	100	64
9	9	19	13	500	1F4
10	A	20	14	1000	3E8

Формат на MAC адрес



Формат на МАС адрес

Media Access Control адресът (МАС адрес), Ethernet Hardware Address (ЕНА) или хардуерен адрес, адрес на адаптера или физически адрес е квазиуникален идентификатор, присвоен на мрежов адаптер или NIC от производителя. В този случай МАС адресът съдържа закодиран идентификатора на производителя.

IEEE дефинира три схеми за формулиране на МАС адрес: **MAC-48**, **EUI-48** и **EUI-64**. Търговски марки на IEEE са "EUI-48" и "EUI-64" (EUI - Extended Unique Identifier). Разликата между EUI-48 и MAC-48 е чисто семантична (но не и синтаксическа): MAC-48 се използва за мрежов хардуер, а EUI-48 идентифицира други устройства и софтуер.

Записва се с **шестнадесетични** цифри.

MAC spoofing

Макар че е смятан за перманентен и глобално уникален, днес е възможно да се смени MAC адреса (т.е не е “прогорен”) - MAC spoofing.

Оригиналният IEEE 802 MAC произлиза от Xerox Ethernet. Съдържа 2^{48} или $281,474,976,710,656$ възможни адреси.

Според IEEE MAC-48 пространството няма да се изчерпи до 2100 г.

Адресите могат да бъдат “[универсално администрирани](#)” или “[локално администрирани](#)“.

Формат на MAC адрес

Универсално администриран е присвоен от производителя, още “прогорен” - "burned-in addresses" (BIA). Първите три октета показват организацията, издала идентификатора - Organizationally Unique Identifier (OUI).

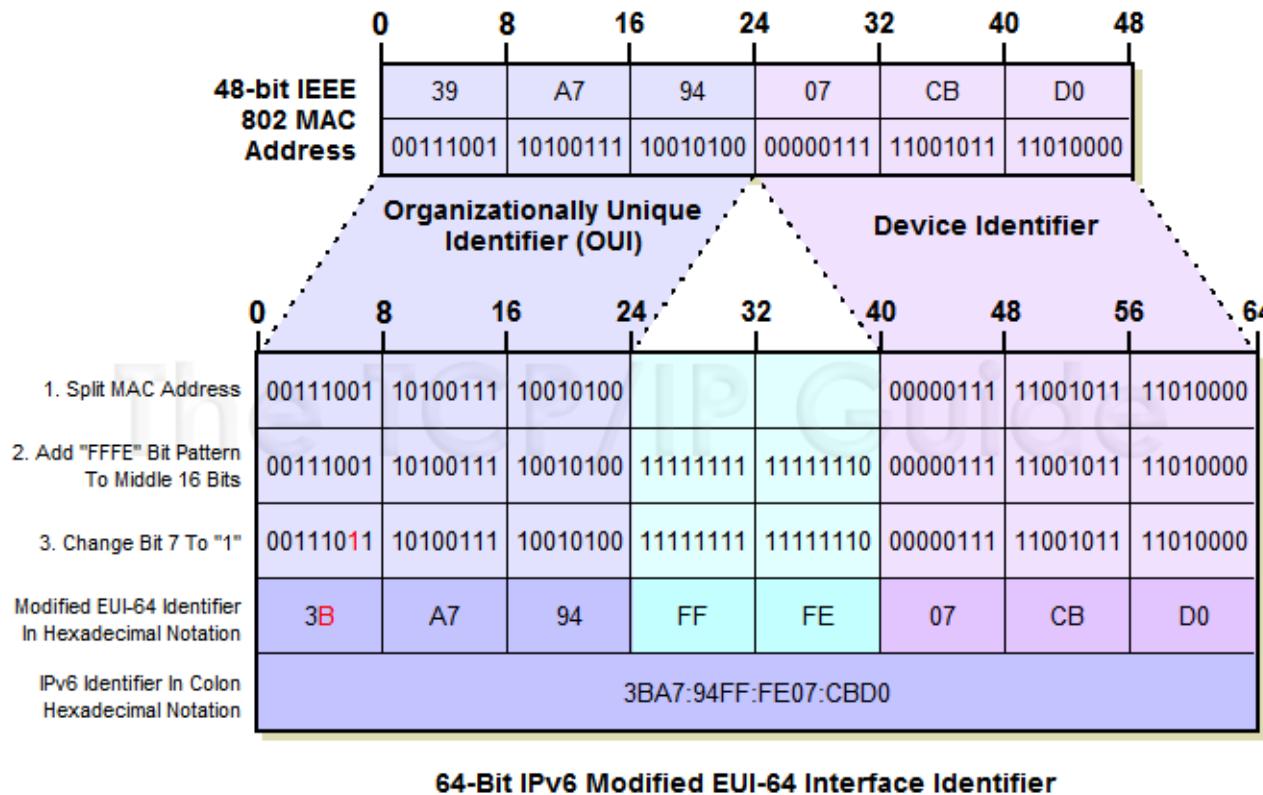
Следващите три октета (MAC-48 и EUI-48) или пет (EUI-64) се дават от самата организация.

Локално администриран се присвоява от мрежовия администратор, отменяйки “прогорения”. Те нямат OUI.

Разпознават се по bit 2 (2^1) в най-старшия октет на MAC-а. Ако е 0, адресът е универсален. Ако е 1, адресът е локален. Т.е е 0 на всички OUI-та.

Ако най-младшият бит – bit 1 (2^0) е 0, кадърът е предназначен за конкретна NIC - unicast. Ако е 1, кадърът трябва да достигне няколко (група) NIC-ве. Нарича се групов - multicast.

EUI-64 формат



EUI-64 формат

EUI-64 се използват:

- * FireWire
- * IPv6 (младшите 64 бита в unicast мрежов адрес или [link-local](#) адрес)

Преобразуване на 48-бит MAC адрес в IPv6 модифициран EUI-64 идентификатор:

1. Вземаме 24-бит OUI частта и я поставяме в най-левите 24 бита на interface ID. А 24-бит локална част слагаме в най-десните 24 бита на interface ID.
2. В оставащите в средата 16 бита на interface ID поставяме стойността “11111111 11111110” (“FFFE” hex).
3. Така адресът ни е в EUI-64 формат. Променяме [“universal/local”](#) бита (бит 7 отляво) от 0 на 1.

И получаваме модифицирания [EUI-64 interface ID](#).

Ethernet кабели и топологии (за сведение)

Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

100BASE-TX: Използва 2 чифта по Category 5 ([IEEE 802.3u](#)).

100BASE-FX: 100 Mbit/s Ethernet по FO.

1000BASE-T: 1 Gbit/s over Category 5e copper cabling ([802.3ab](#)).

1000BASE-SX: 1 Gbit/s по MM FO.

1000BASE-LX: 1 Gbit/s по SM FO (големи разстояния).

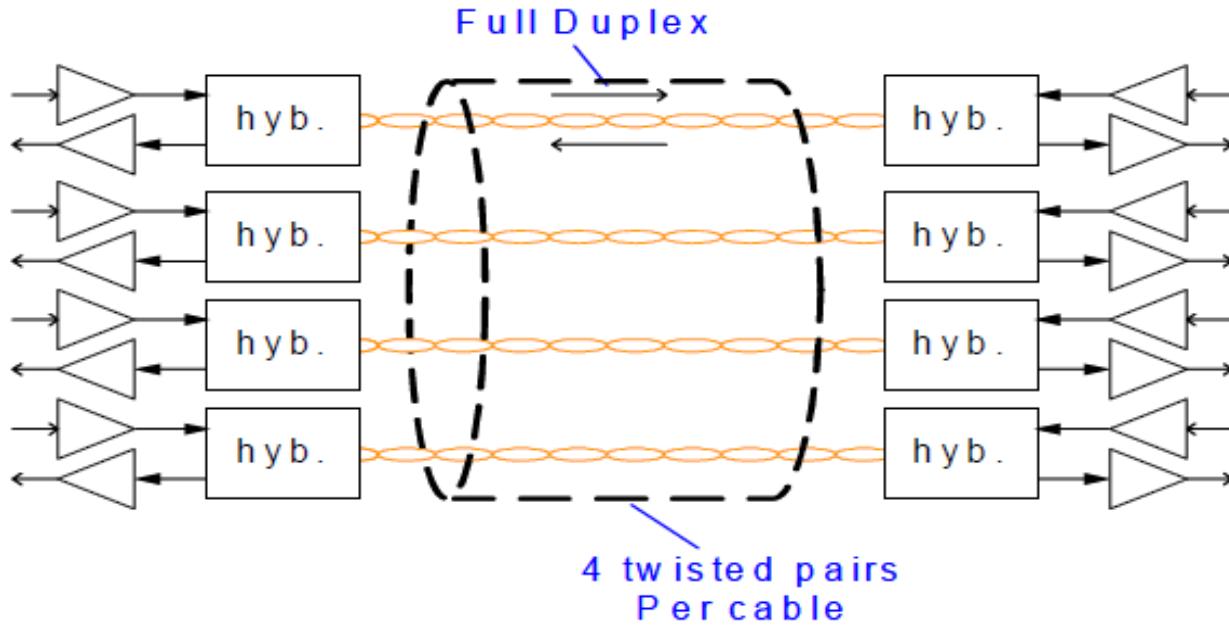
10GBASE-LX4: WDM - 240 m i 300 m по MM FO. 10 km по SM FO ([802.3ae](#)).

10GBASE-LR и **10GBASE-ER:** 10 km и 40 km по SM FO.

10GBASE-SW, 10GBASE-LW и **10GBASE-EW:** Върху WAN PHY

10GBASE-T: меден кабел Категория 6а ([802.3an](#))

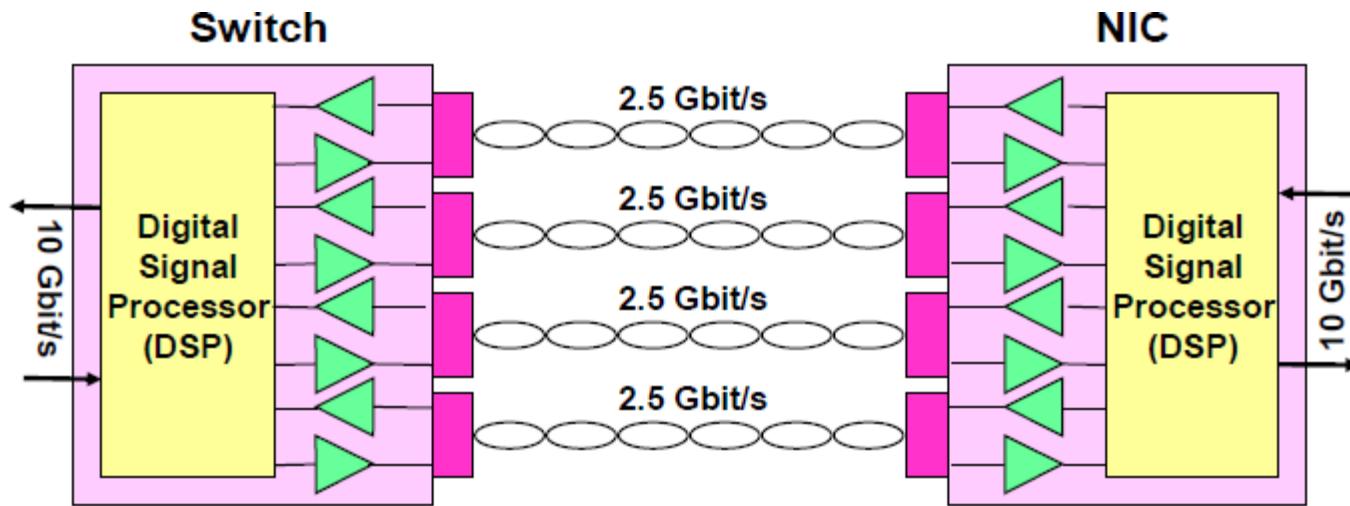
1000Base-T (за сведение)



10BASE-T и **100BASE-T** предава по два от чифтовете.

1000BASE-T Twisted-pair cabling (Cat-5, Cat-5e, Cat-6, or Cat-7) 100 meters използва и 4-те чифта.

10GBase-T (за сведение)



10GBASE-T предава и по 4-те чифта - 100 м SFTP
кабел (Cat. 6a).

2.5 Gbit/s на чифт.

40/100 Gigabit Ethernet (за сведение)

PHY	40 Gigabit Ethernet	100 Gigabit Ethernet
at least 1 m over a backplane	40GBASE-KR4	
approximately 7 m over copper cable	40GBASE-CR4	100GBASE-CR10
at least 100 m over OM3 MMF	40GBASE-SR4	100GBASE-SR10
at least 125 m over OM4 MMF ^[7]	40GBASE-SR4	100GBASE-SR10
at least 10 km over SMF	40GBASE-LR4	100GBASE-LR4
at least 40 km over SMF		100GBASE-ER4

40 Gigabit Ethernet (40GbE) и 100 Gigabit Ethernet (100GbE) са разработени от IEEE P802.3ba.

Ethernet кадрите се предават по множество 10 Gb/s или 25 Gb/s ленти.

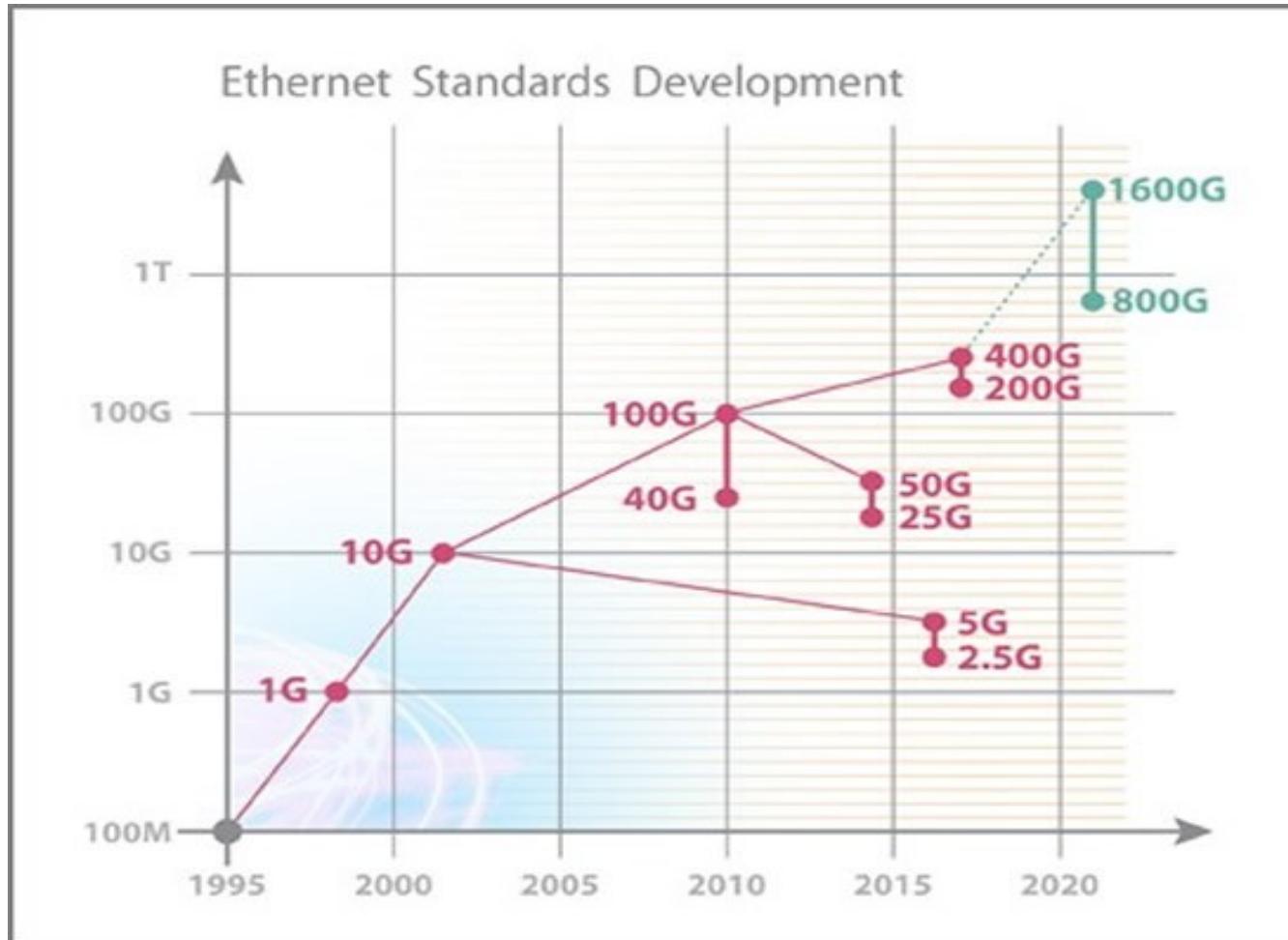
200, 400-Gigabit и нагоре към Terabit Ethernet (за сведение)

Новият стандарт **IEEE Std 802.3bs-2017** за 400G и 200G Ethernet е само за оптическа среда с множество паралелни влакна **4 * 100-Gigabit** интерфейси или **8 * 50 Gbps, 16 * 25 Gbps.** Очакват се **800 Gbps** и **1600 Gbps** Ethernet.

Terabit Ethernet е голямо предизвикателство за компютърните технологии.

Изиска подобреие на **PCI Express** стандарта.

Развитие на Етернет стандартите



Ethernet кабели и топологии



Ethernet кабели и топологии

В началото в Ethernet се използва **коаксиален кабел** и скоростта на предаването е достигала 10 Mb/s.

По-нататък се въвежда използването на **хъбове (hub)**. При окабеляване 100Base-T4 каналните станции се свързват към хъба чрез четири усукани двойки **UTP Category 3**.

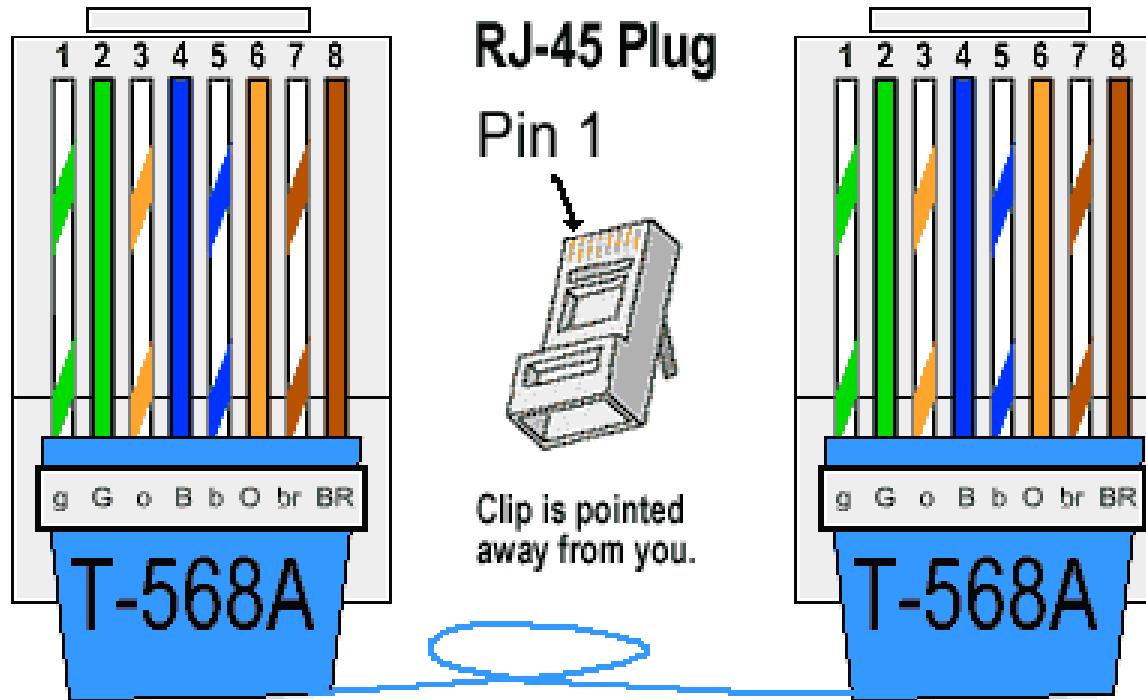
100Base-TX чрез две усукани двойки (**UTP Category 5**). По една от усуканите двойки се предава към хъба, а по другата се приема от него (при 100Base-T4 останалите две усукани двойки се превключват по посока на предаването). Скоростта на предаване достига 100 Mb/s.

Ethernet кабели и топологии (за сведение)

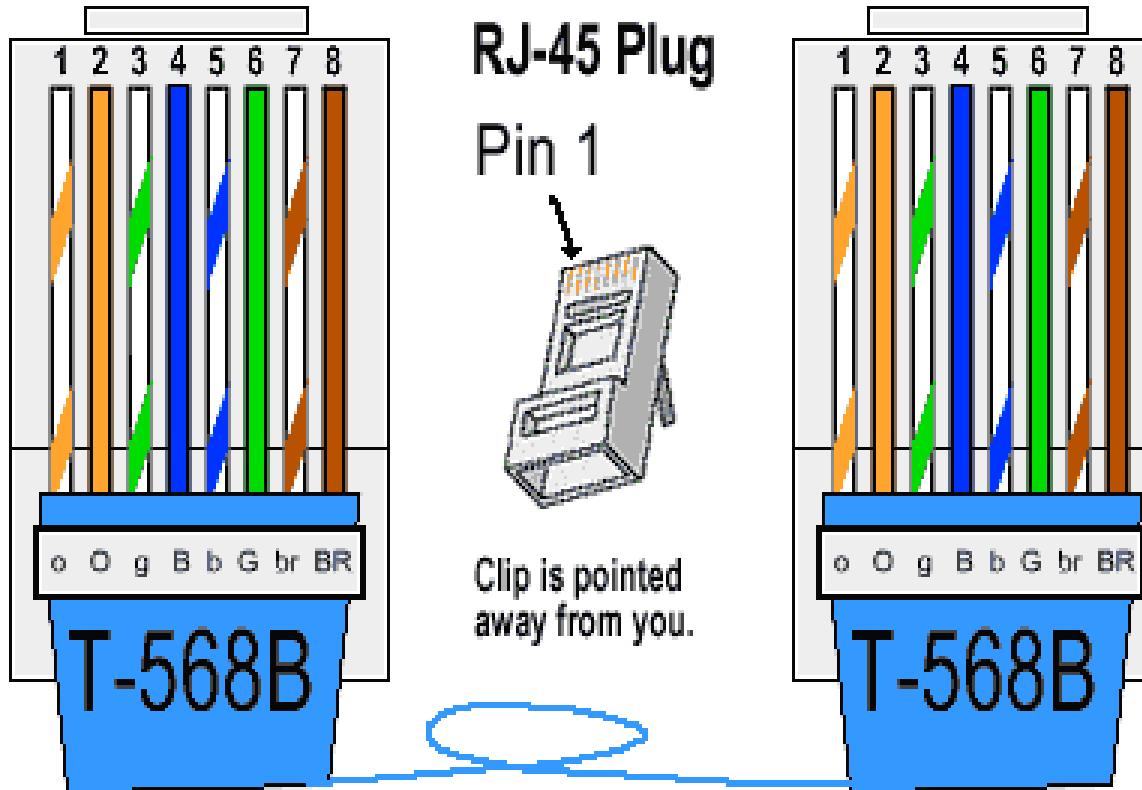
Станциите се свързват към хъба в **прав кабел**, т.е. предаващата двойка на всяка станция съответства на предаващата двойка на хъба и съответно приемащата двойка на всяка станция съответства на приемащата двойка на хъба.

При свързване на два хъба чрез усукана двойка, обаче, се използва **кръстосан (cross) кабел**, т.е. предаващата двойка на единия хъб се свързва с приемащата двойка на другия хъб и обратно.

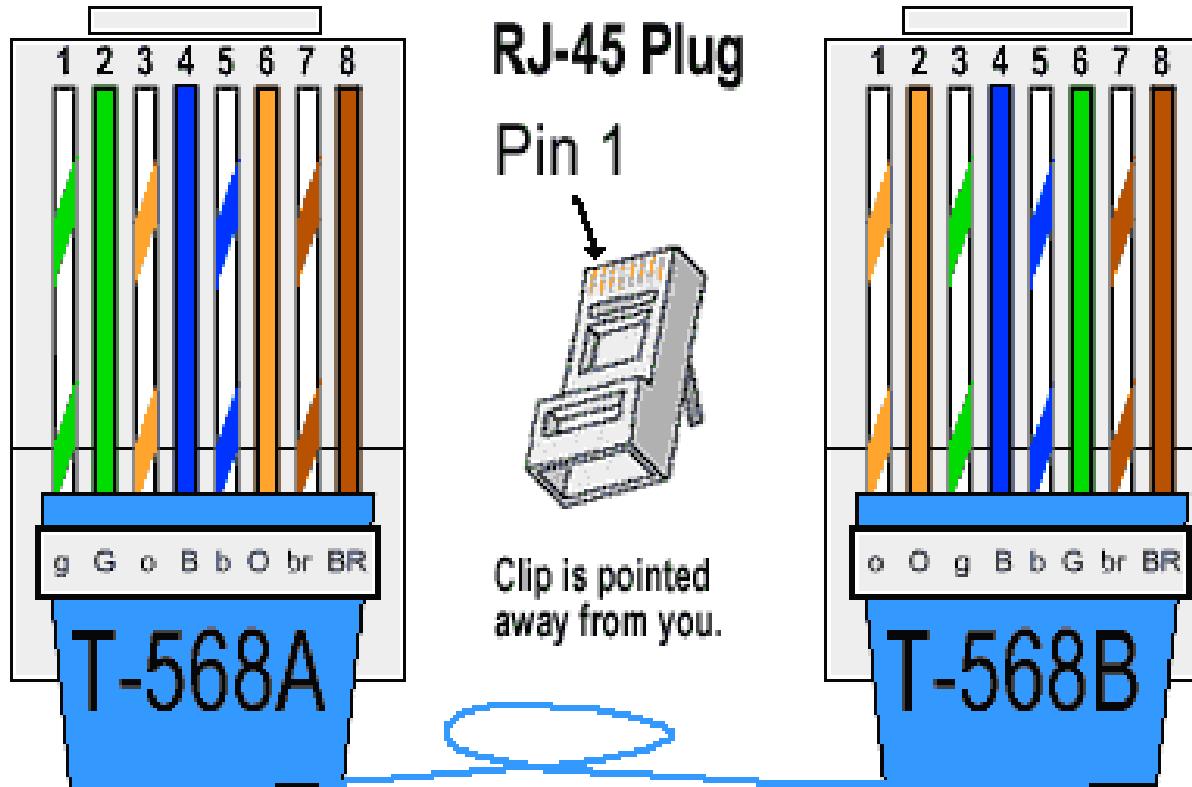
Прав (Straight-Through) кабел (за сведение)



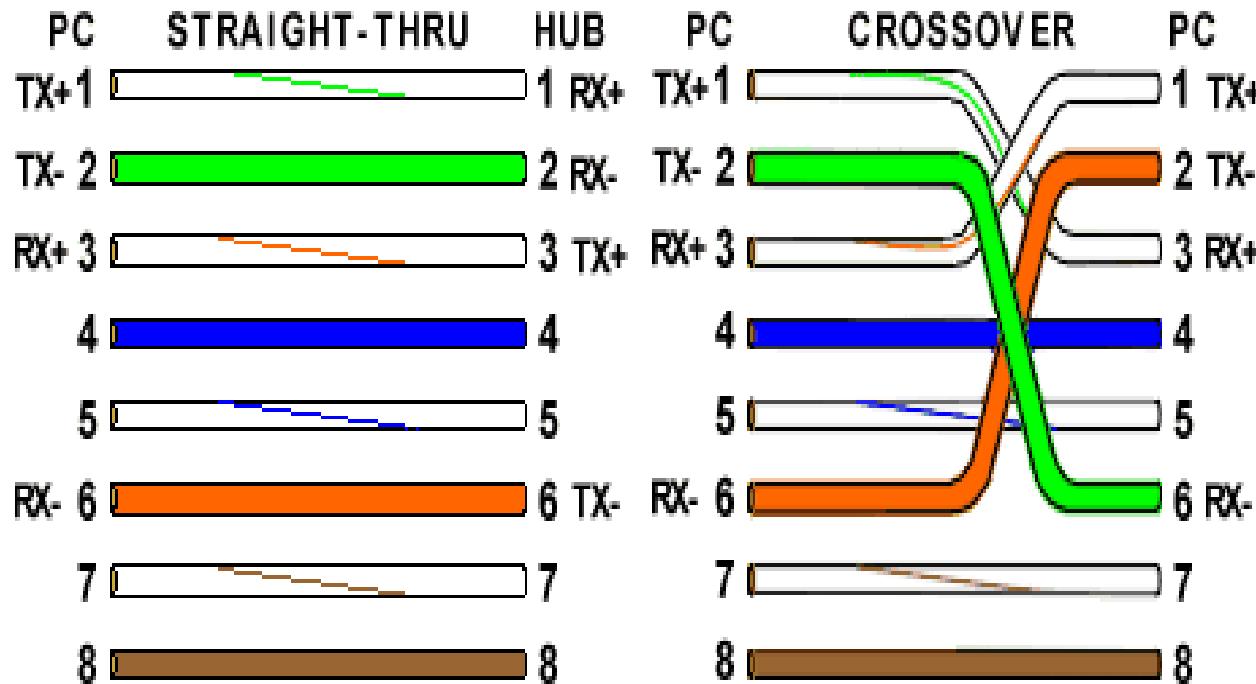
Прав (Straight-Through) кабел (за сведение)



Кръстосан (Crossover) кабел (за сведение)



Straight vs. Cross (теория - за сведение)



Хъб и повторител

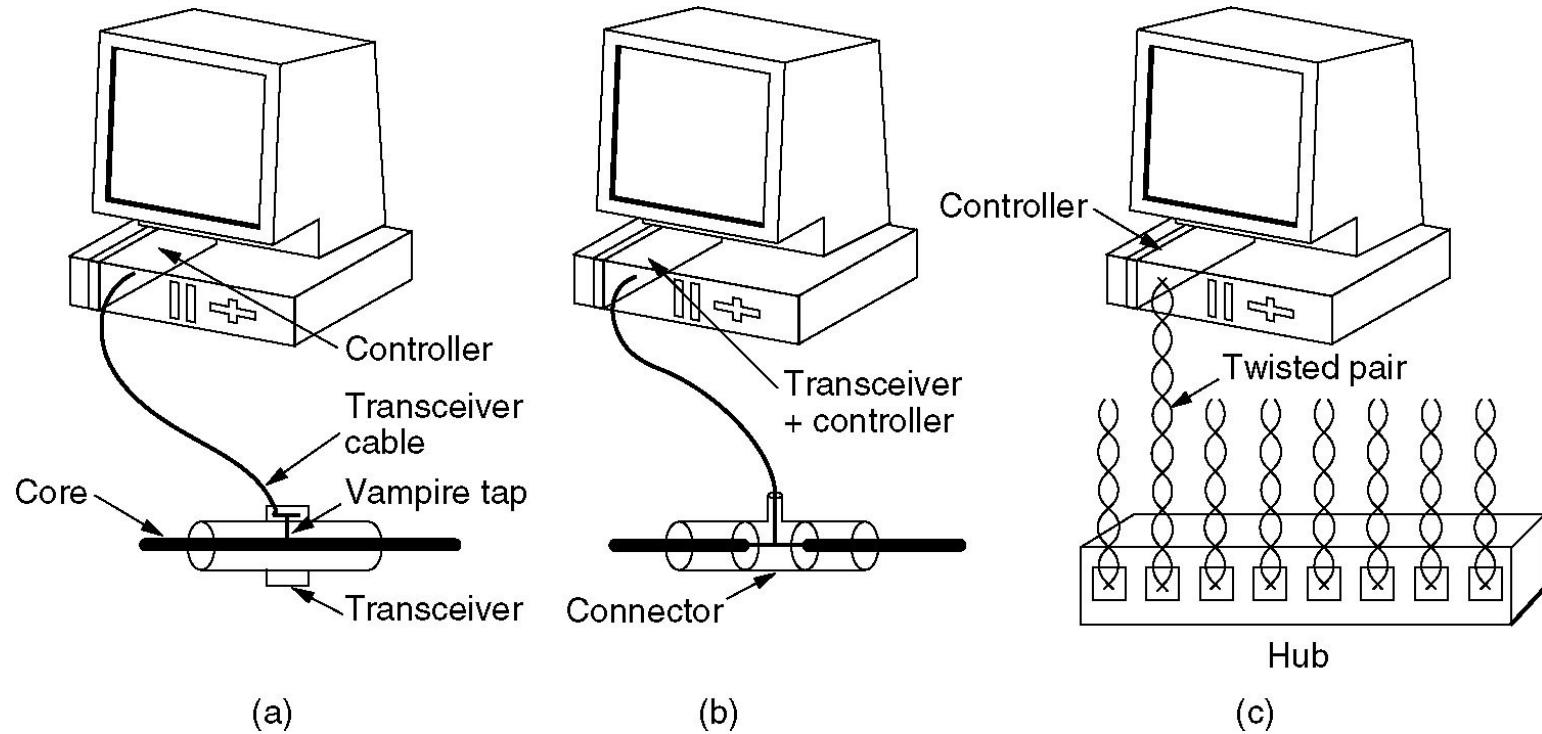
Ако хъбът получи кадър по някоя линия, той изпраща този кадър по всички останали линии. Хъбът не знае адресите на каналните станции.

Хъбът е пример за устройство, чрез което се препредават кадри от един кабел към друг. Той **работи на физическо ниво**.

Друго подобно устройство на физическо ниво е **повторителят (repeater)**.

Той приема сигнал на единния си порт, усилва го и предава сигналът на другия си порт. По този начин може да се увеличи максималната дължина на кабела в една локална мрежа

Коаксиални кабели и хъб



Три вида Ethernet cabling.

(a) 10Base5, **(b)** 10Base2, **(c)** 10Base-T.

Полу-, пълен дуплекс, колизии, хъбове, суичове

Колизии са възможни в условията на предаване от типа полуудуплекс (**half-duplex**). Шосе с една единствена лента с двупосочко движение.

Такъв вид комуникационна среда е коаксиалният кабел - "класическият" Етернет на скорост **10 Mbps**. Или Етернет, базирана на **хъбове** и кабели тип усукана двойка.

И коаксиалният кабел и хъбът са **един единствен колизионен домейн** и един бродкаст домейн.

При пълен дуплекс (**full-duplex**) - шосе с по една лента за всяка посока колизии (челни удари) не трябва да имаме.

Такъв е Етернета, базиран на комутатори (**суичове**) и кабели тип усукана двойка (за всяка посока отделен чифт/ове) и FO (за всяка посока отделно влакно или **λ**).

Bridge и switch

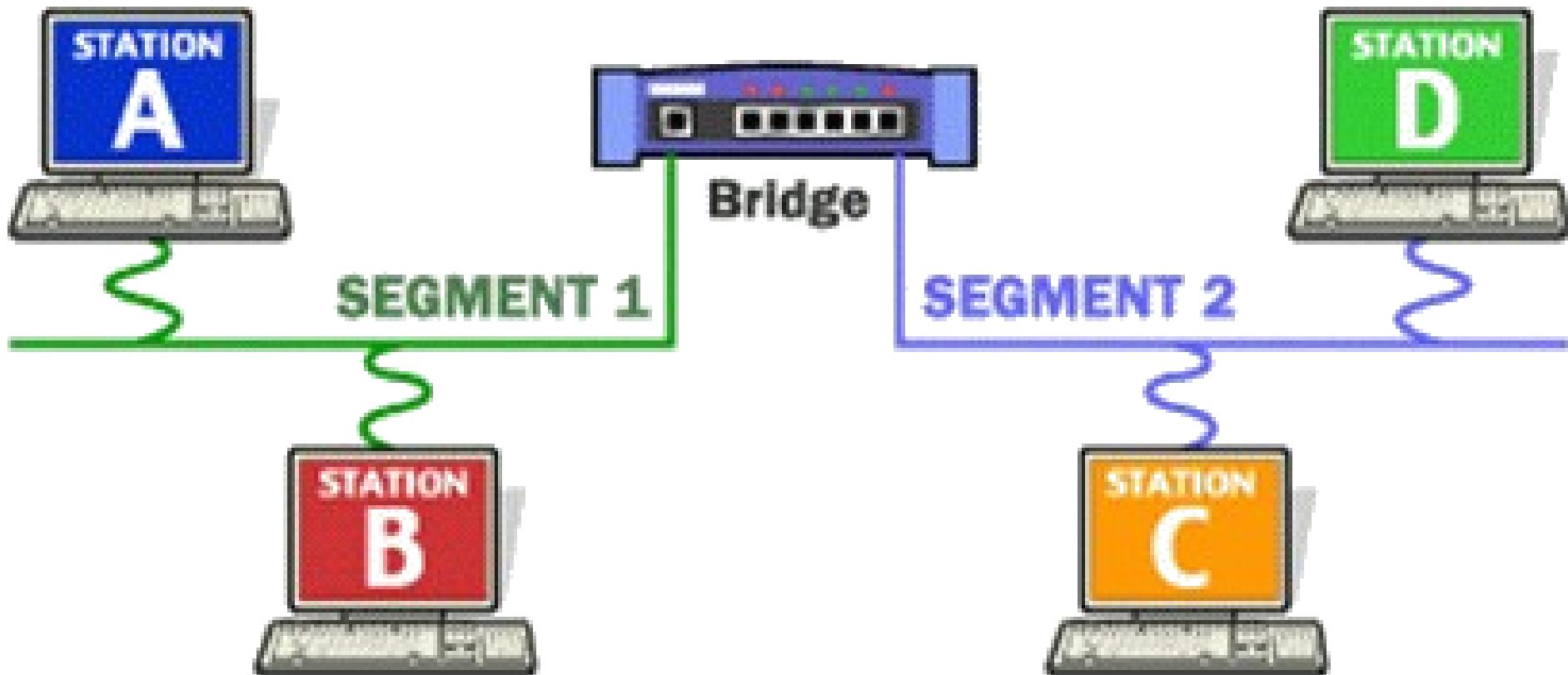
Мостът (bridge) работи на **канално ниво** и служи за свързване на две локални мрежи. За разлика от повторителите и хъбовете, мостът анализира получените кадри.

Той прочита адреса на получателя и по него определя към коя изходна линия да изпрати кадъра (за целта се поддържа специална таблица).

Мостът предава кадъра само към определената от него изходна линия, а не по всички изходни линии.

Подобно устройство е **превключвателят (switch)** – многопортов мост. Той също прочита адресите на постъпилите в него кадри.

Bridge и switch



Bridge и switch

Всяка линия (порт) е самостоятелна и представлява отделен колизионен домейн. Това се нарича още микросегментиране.

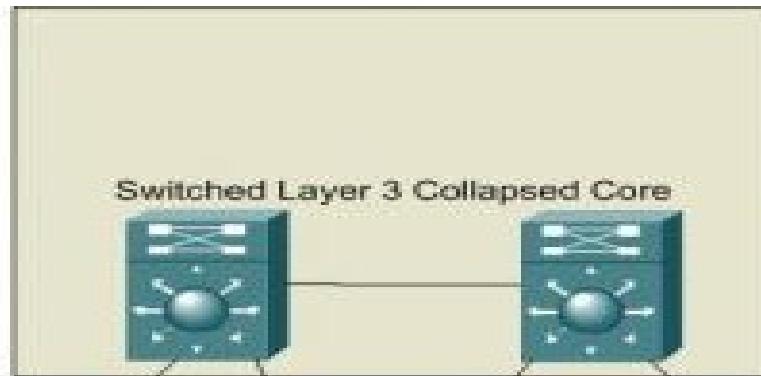
Но бродкастите се разпространяват по всички портове, т.е той е един бродкаст домейн.

При превключване между сегменти кадри не могат да бъдат изгубени поради колизии.

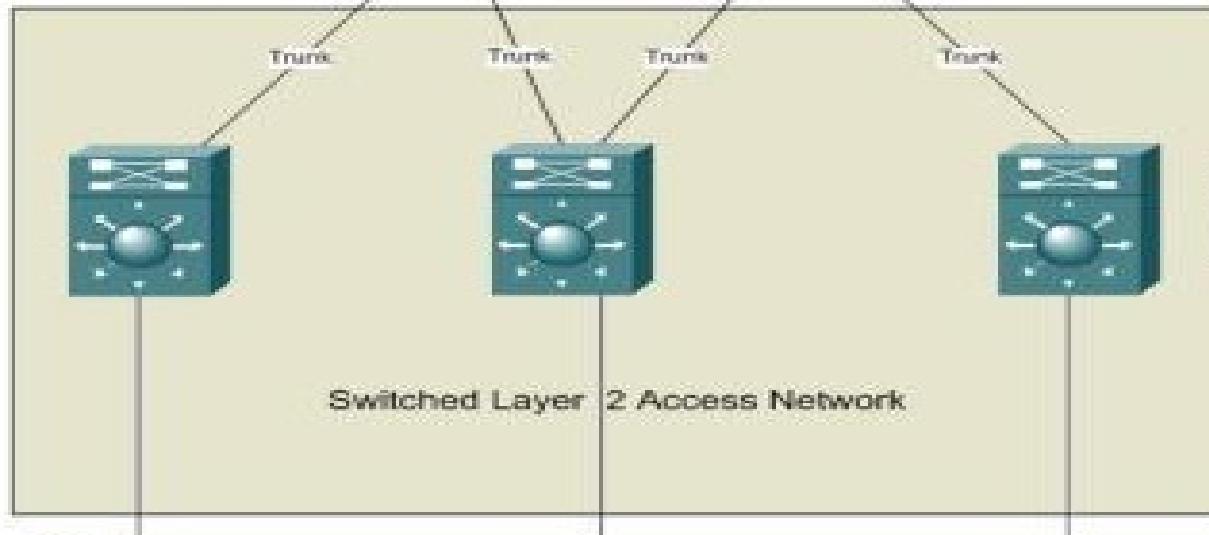
За целта превключвателя трябва да има достатъчно буферно пространство за да може да се препращат кадрите.

Switched Ethernet

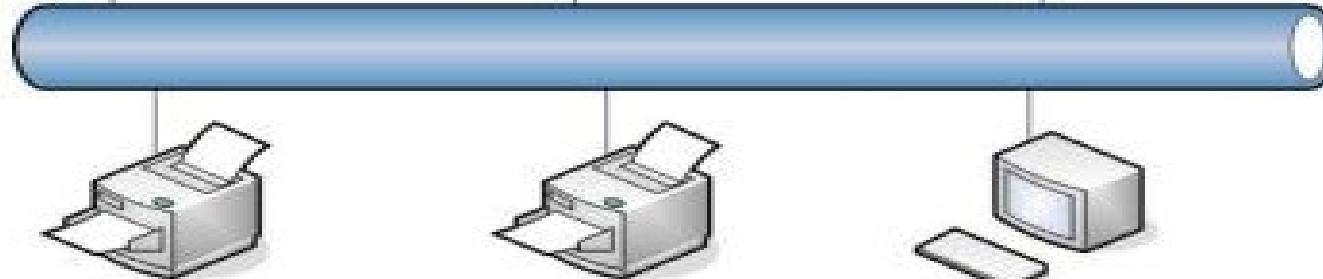
1. View ARP Cache and locate MAC address



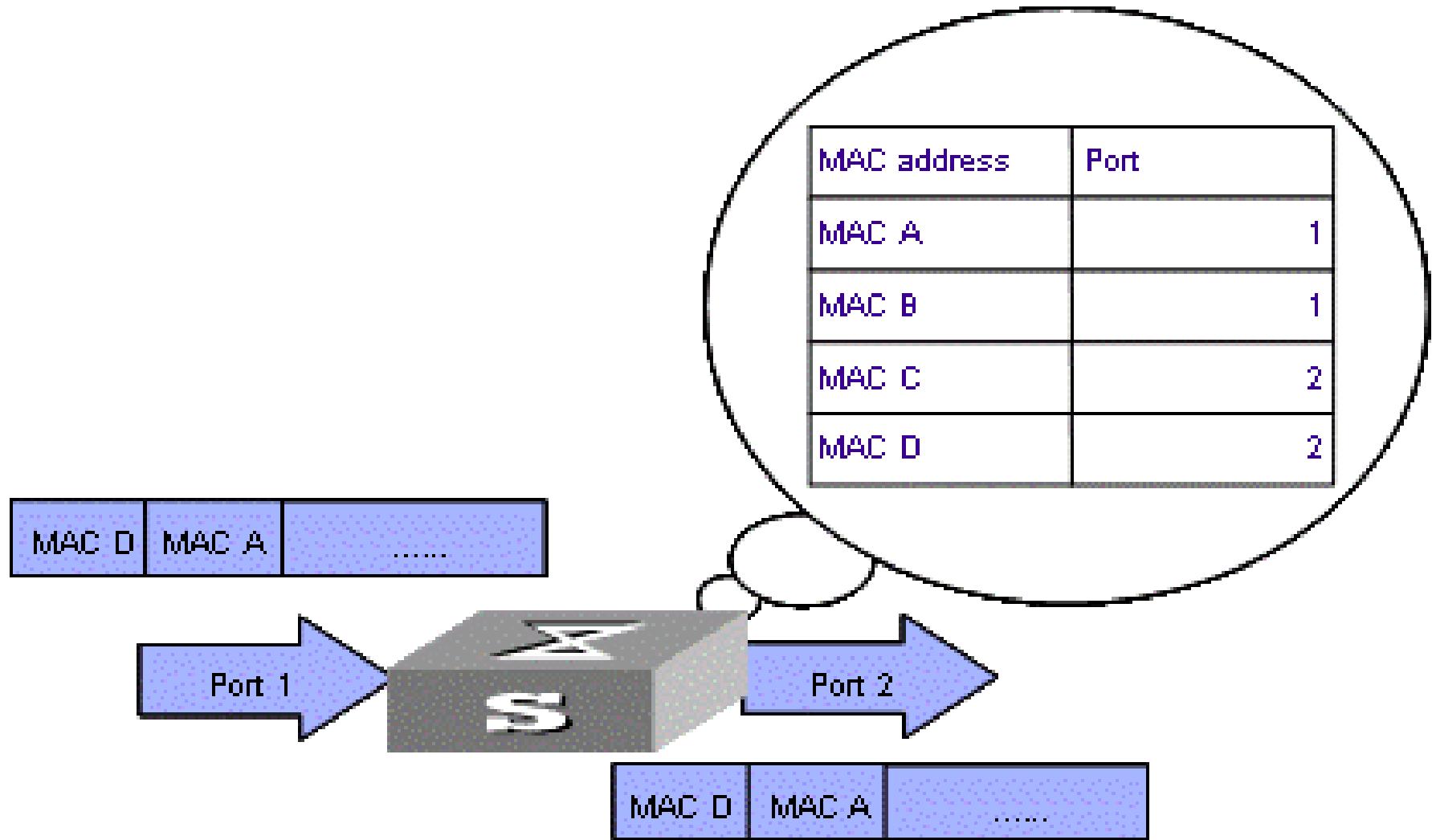
2. View MAC address table and locate the trunk bound to the source MAC



3. View MAC address table and locate interface bound to source MAC



MAC Address Table



Три режима на превключване

Пълно буфериране (**store and forward**). В буферната памет се записва целия кадър и чак след това се превключва към изходния порт. Внася се закъснение и изисква повече памет.

Cut-through – Суичът прочита адреса на получателя при получаване на кадъра. Започва прехвърлянето към изходящия порт, преди да получи пълния кадър. Така се намалява закъснението. Имаме [две форми на cut-through](#):

Fast-forward – С най-ниско закъснение, веднага превключва кадъра след приемане на адреса на получателя. Има проблеми с откриването на грешки.

Fragment-free - Филтрира кадри (фрагменти), претърпели колизии, най-често срещаните грешки. Обикновено това са кадри с дължина, по-малка от 64 байта. Т.е прочита първите 64 бита, за да определи дали това не е колизионен фрагмент, преди да започне превключването.

Spanning Tree (математика)

Spanning tree (**покриващо дърво**) е подмножество на ненасочен граф, в което всички върхове са свързани с минимален брой дъги.

Ако всички върхове са свързани в граф, то тогава съществува поне едно покриващо дърво. В един граф може да съществува повече от едно покриващо дърво.

В покриващото дърво няма зацикляне и даден връх може да бъде достигнат от всеки друг връх.

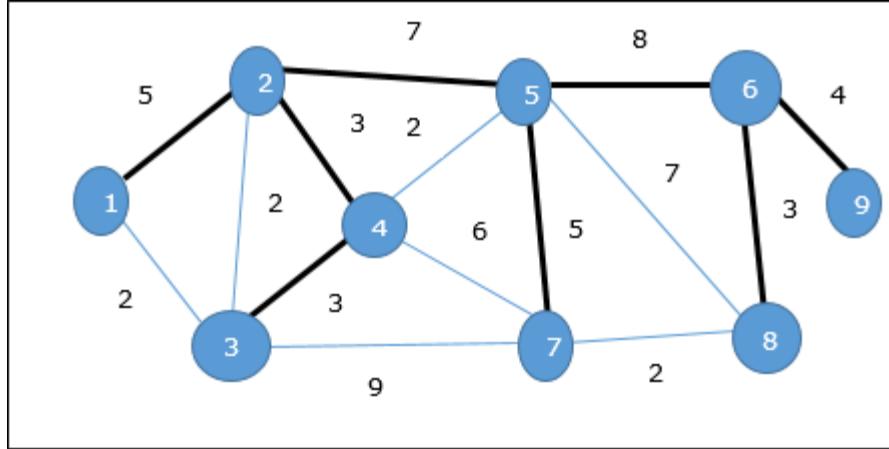
Minimum Spanning Tree (**MST**) е подмножество от дъги на свързан **мерен** ненасочен граф (с който ние ще се занимаваме), което свързва всичките върхове с минималната възможна сумарна стойност на дъгите.

В следващия слайд по Prim имаме две MST-та от един граф със стойности 38 и 23. Защо?

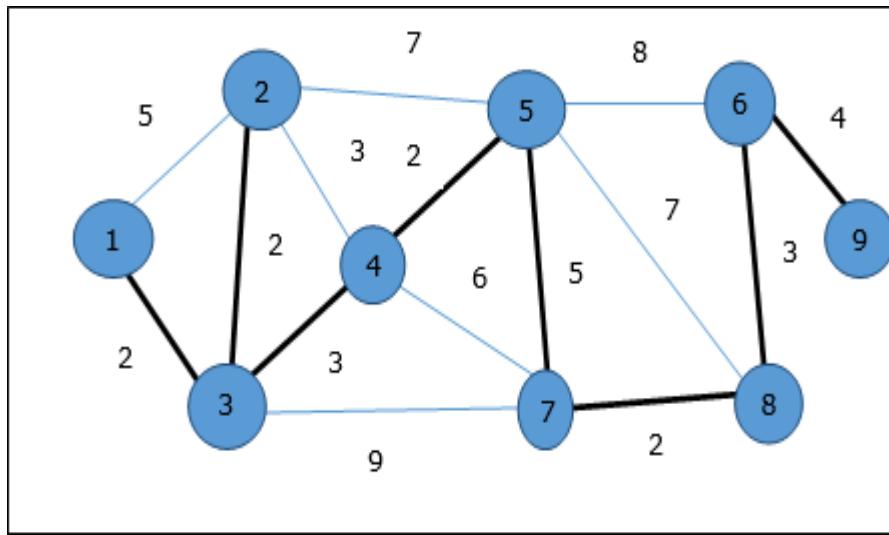
Spanning Tree

(https://www.tutorialspoint.com/design_and_analysis_of_algorithms/design_and_analysis_of_algorithms_spanning_tree.htm)

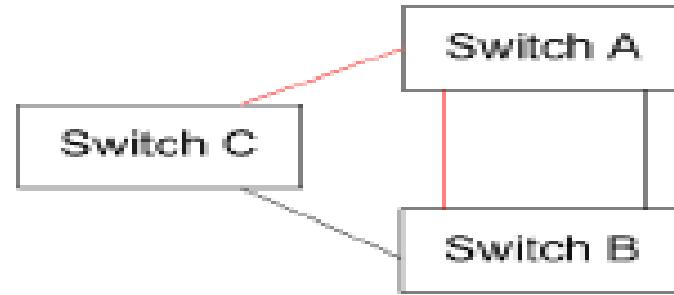
C=38



C=23



Spanning Tree. Защо в switched LAN?



Резервираност в топологията:

PROS: отклоустойчивост, по-висока производителност.

CONS: switched LAN: **broadcast storms**: задръстване на MAC таблицата и др.

Хост изпраща фрейм с несъществуващ в таблиците на съучовете Dest. MAC. Фреймът се broadcast-ва по всички портове на съучовете с изключение на входящия. Получава се “въртележка” до безкрайност между А, В и С.

Spanning Tree Protocol (STP)

Зашто на **layer 2 няма TTL** да го спре, както е при **IP** протокола на 3 слой. Решението е: **Spanning Tree Protocol (STP)**.

STP е протокол на 2 слой по модела на OSI, който гарантира **топология без зацикляне** в Switched LAN. Базира се на алгоритъма на Radia Perlman, който е работил за Digital Equipment Corporation.

Позволява да се включват резервни пътища, които автоматично да се активират при авария в основните без опасност от зацикляне.

STP се дефинира в стандартите **IEEE 802.1D** (и вариантите му Rapid STP - IEEE 802.1w, Multiple STP - IEEE 802.1s и Shortest Path Bridging - IEEE 802.1aq).

STP – стойности на дъгите

Скорост (Data rate)	(STP Cost – 802.1D-1998)	(802.1D-2004)
4 Mbit/s	250	5,000,000
10 Mbit/s	100	2,000,000
16 Mbit/s	62	1,250,000
100 Mbit/s	19	200,000
1 Gbit/s	4	20,000
2 Gbit/s	3	10,000
10 Gbit/s	2	2000

STP - алгоритъм

STP алгоритъмът изчислява път без зацикляне.

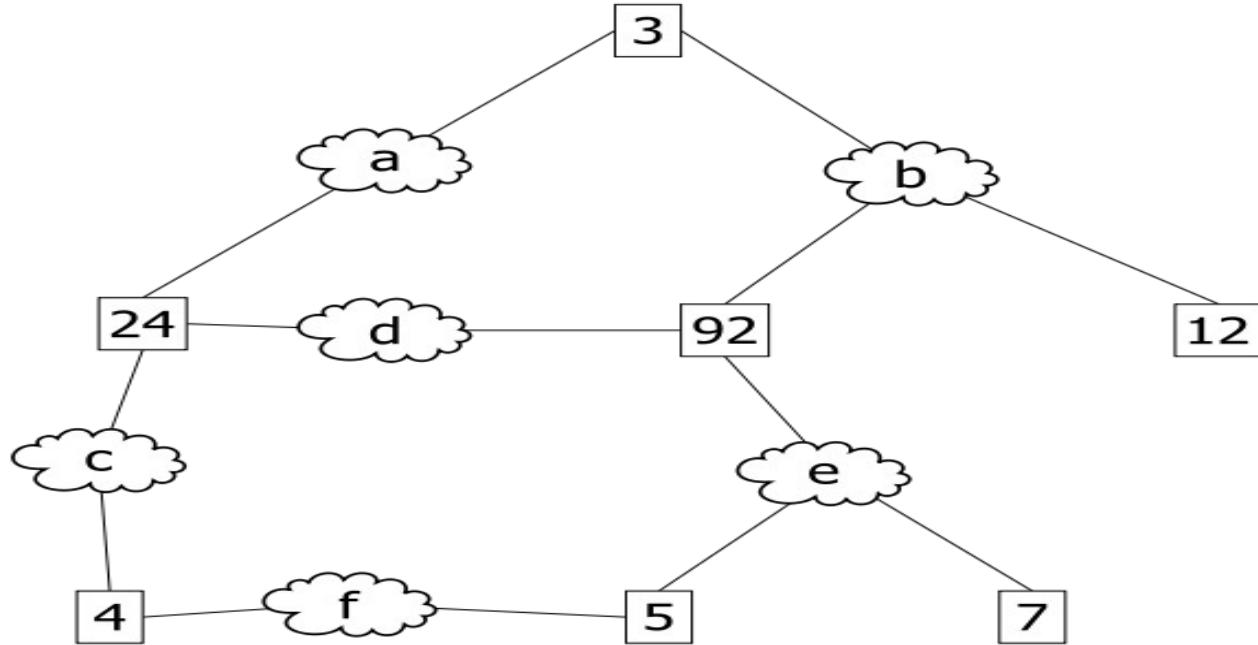
Първоначално всички портове са блокирани. Отнема около 50 s, докато започнат да превключват.

Стъпка 1 : Избор на Root Bridge – с най-нисък приоритет или най-ниско bridge ID (MAC адрес)

Стъпка 2 : Избор на Root Ports – От алтернативните пътища се избират тези с най-малка стойност до Root Bridge. RPs водят към root bridge.

Стъпка 3 : Избор на Designated Ports – Порт, който праща и получава трафик от Root Bridge – с най-ниска стойност до Root Bridge. DPs водят от root bridge към клоните на дървото.

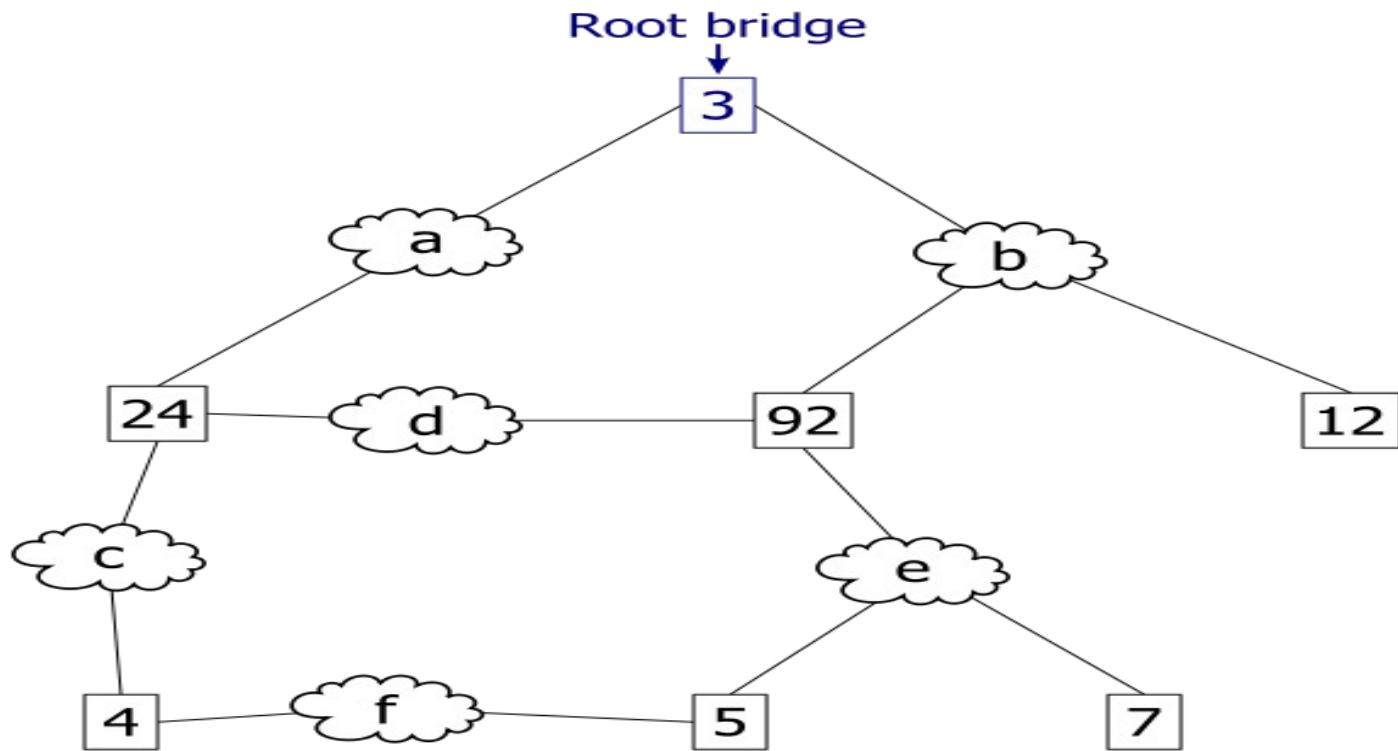
Пример



Номерираните кутийки –**bridge ID**.

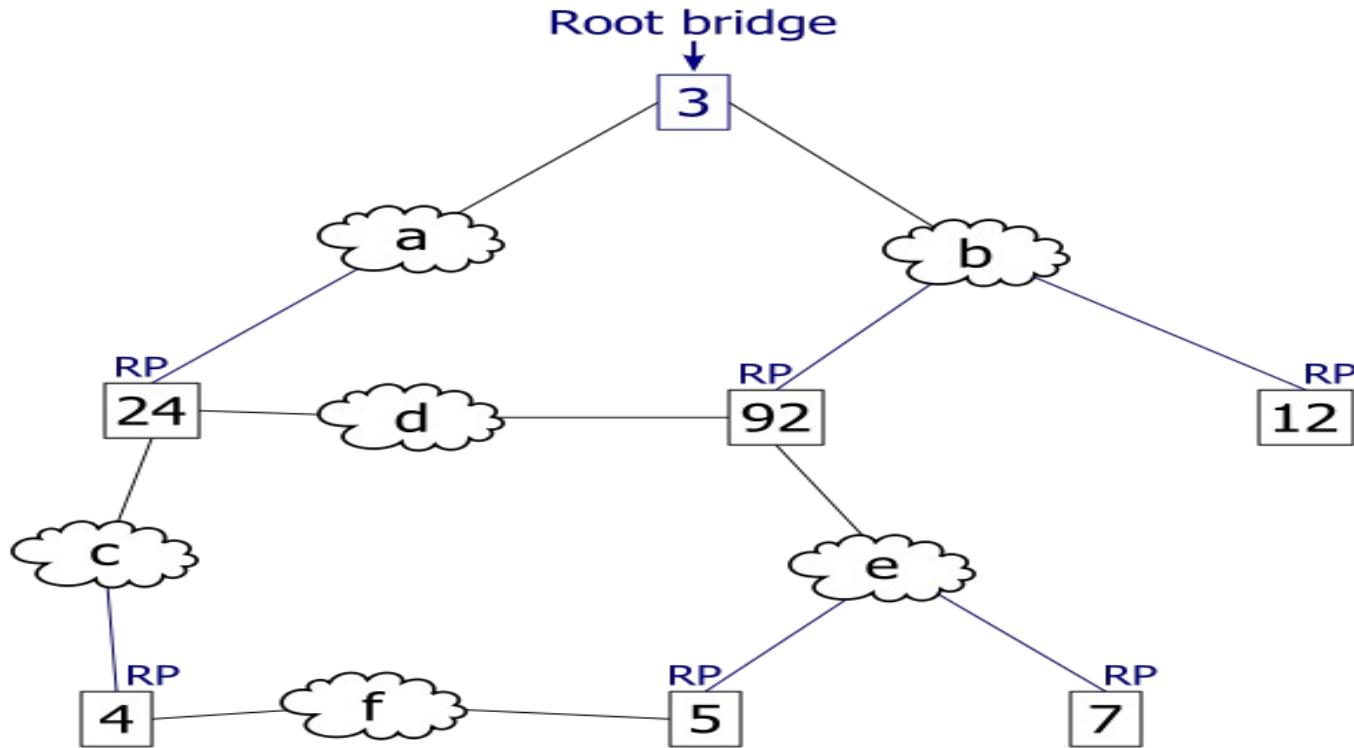
Номерираните облаци – **мрежови сегменти**.

Избор на root bridge



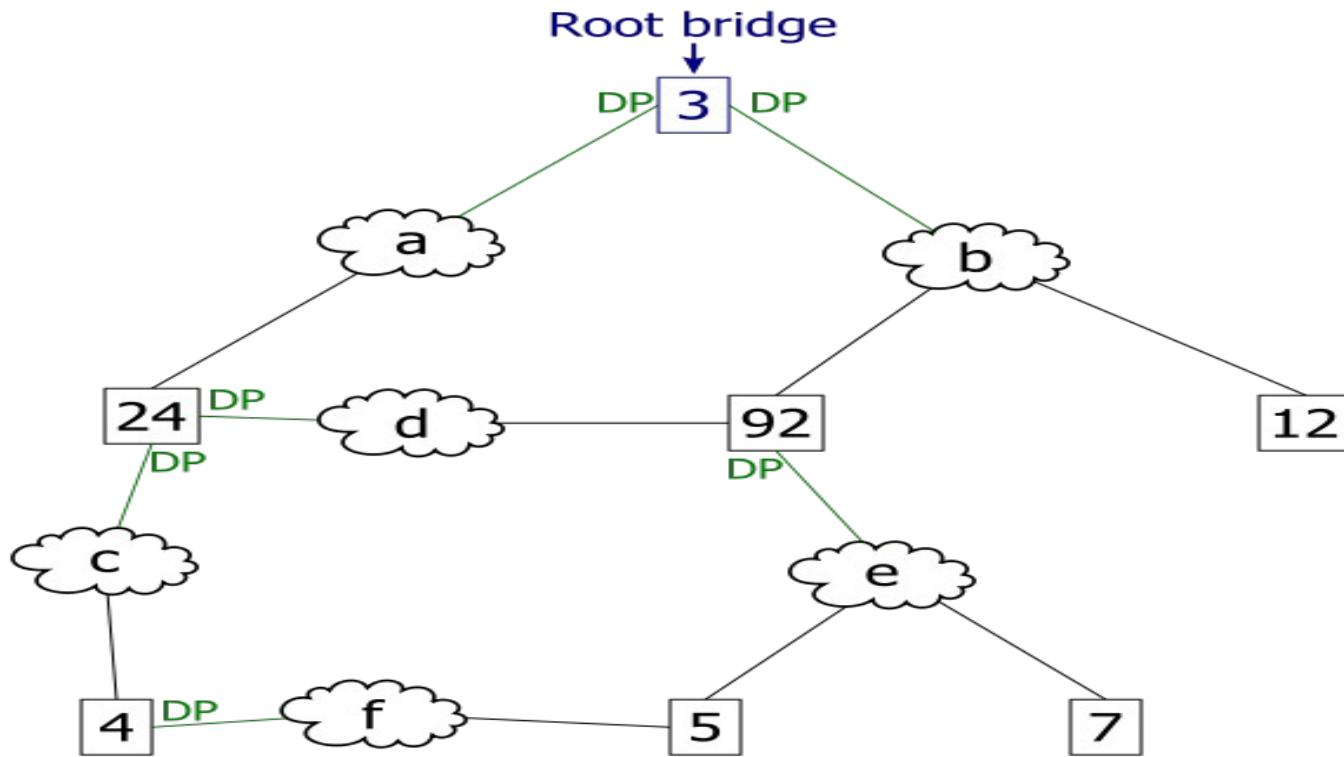
Най-малкият bridge ID е 3

Избор на root port



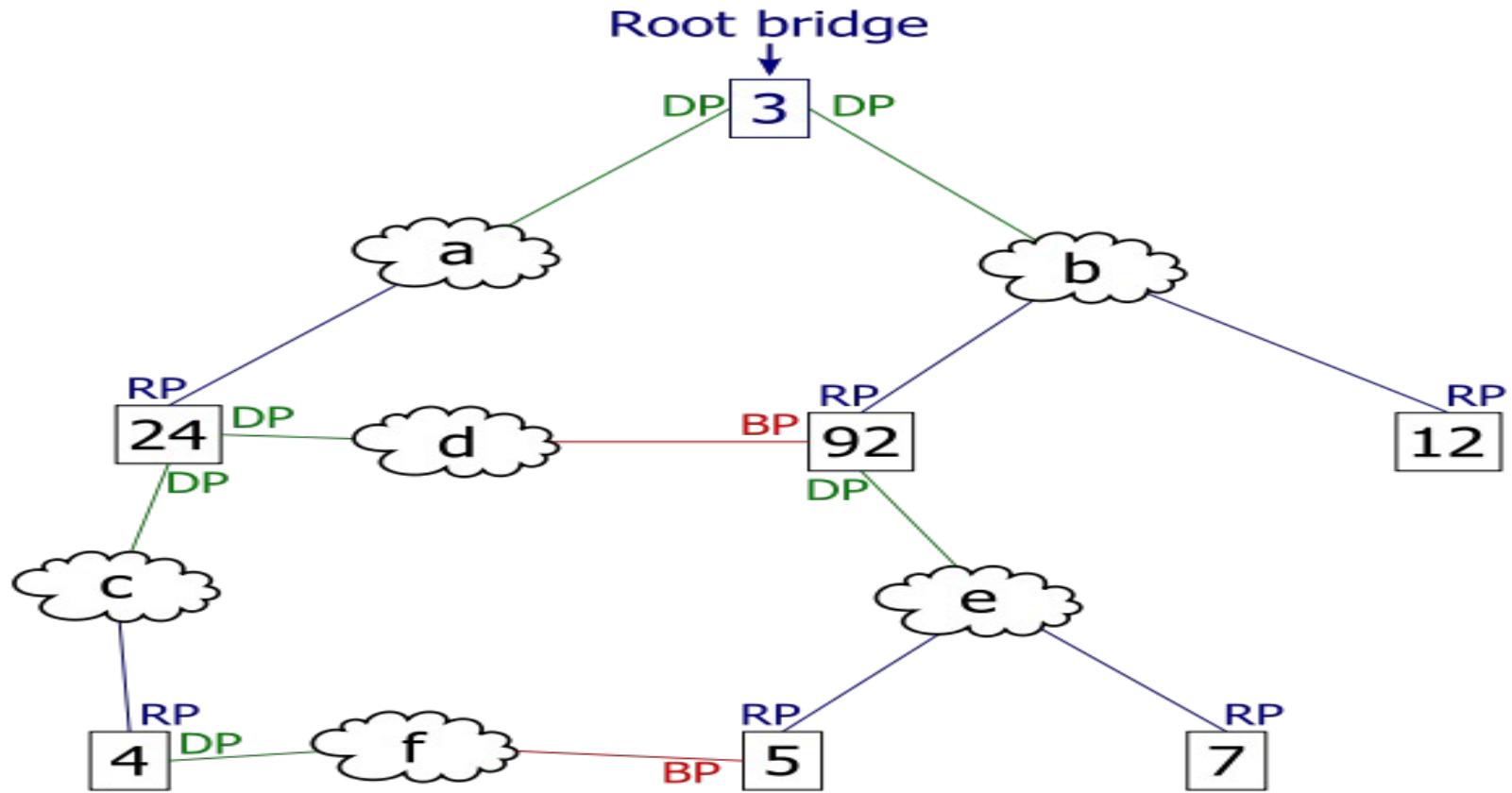
Предполагаме, че стойността на всеки сегмент е **1**. Най-късият път от bridge **4** до root bridge минава през сегмент **c**.

Избор на designated port



Най-късият (с най-малка стойност) път до root от мрежов сегмент e минава през bridge 92.

Spanning Tree - резултат



Активни портове, които не са root port или designated port са блокирани (blocked port).

Виртуални ЛМ (Virtual LANs)

VLAN е комутирана мрежа, която е логически сегментирана по някакви функции и не се влияе от физическото разположение на потребителите (по етажи, сгради и т.н.).

Един VLAN представлява един broadcast domain.

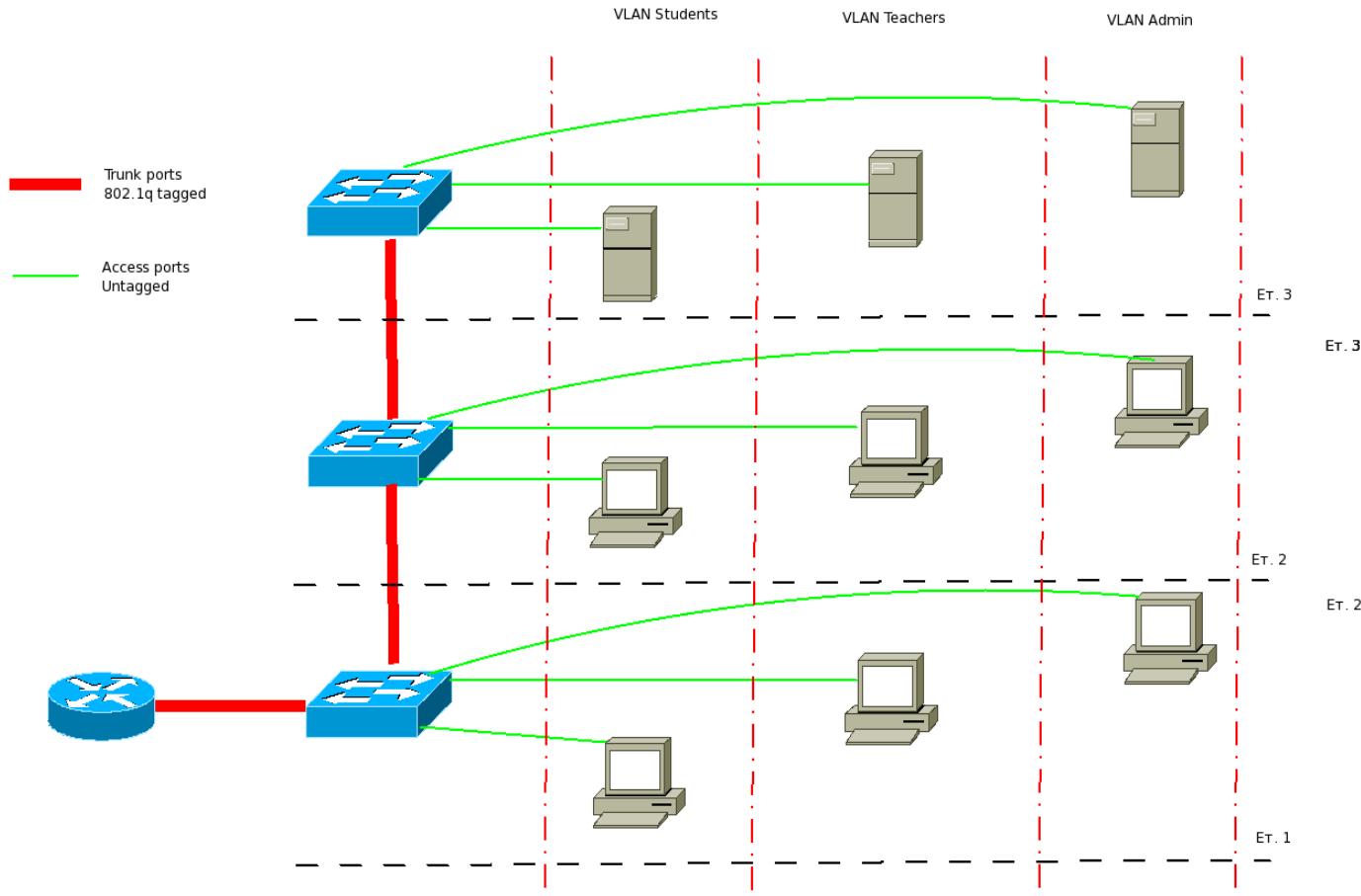
Сигурност. Потребителите на VLANi нямат достъп до машините на VLANj. Това може да стане единствено и само през рутер.

Гъвкавост. Опростява местене, добавяне, премахване на потребителски машини.

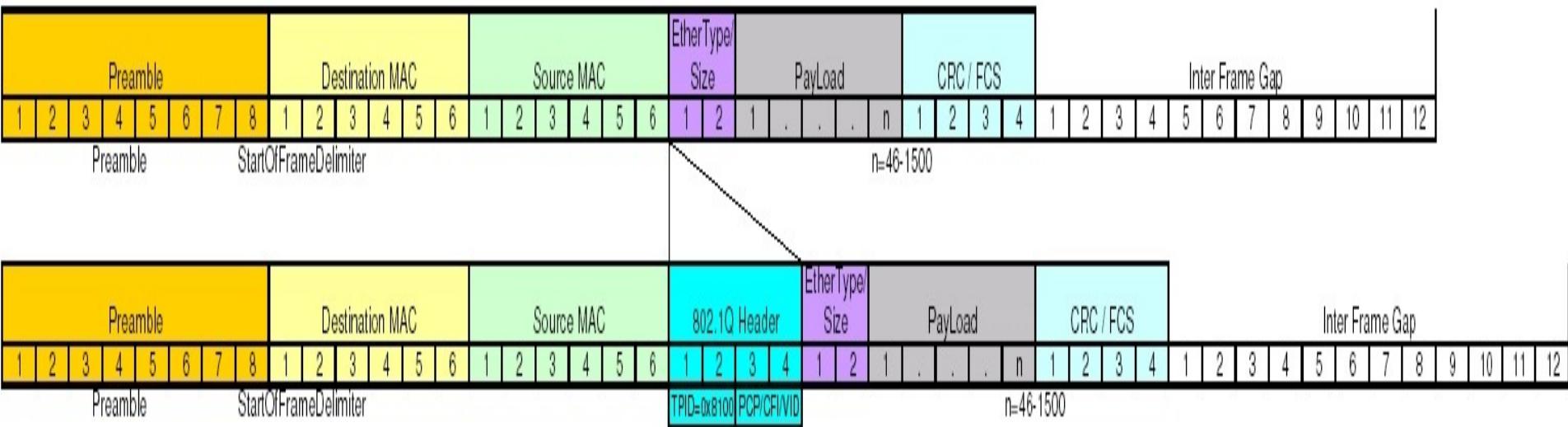
Един порт на суич може да се присвои статично или динамично към VLAN.

Trunk портове за връзка между суичове.

VLAN - пример



VLANs – 802.1Q Tag



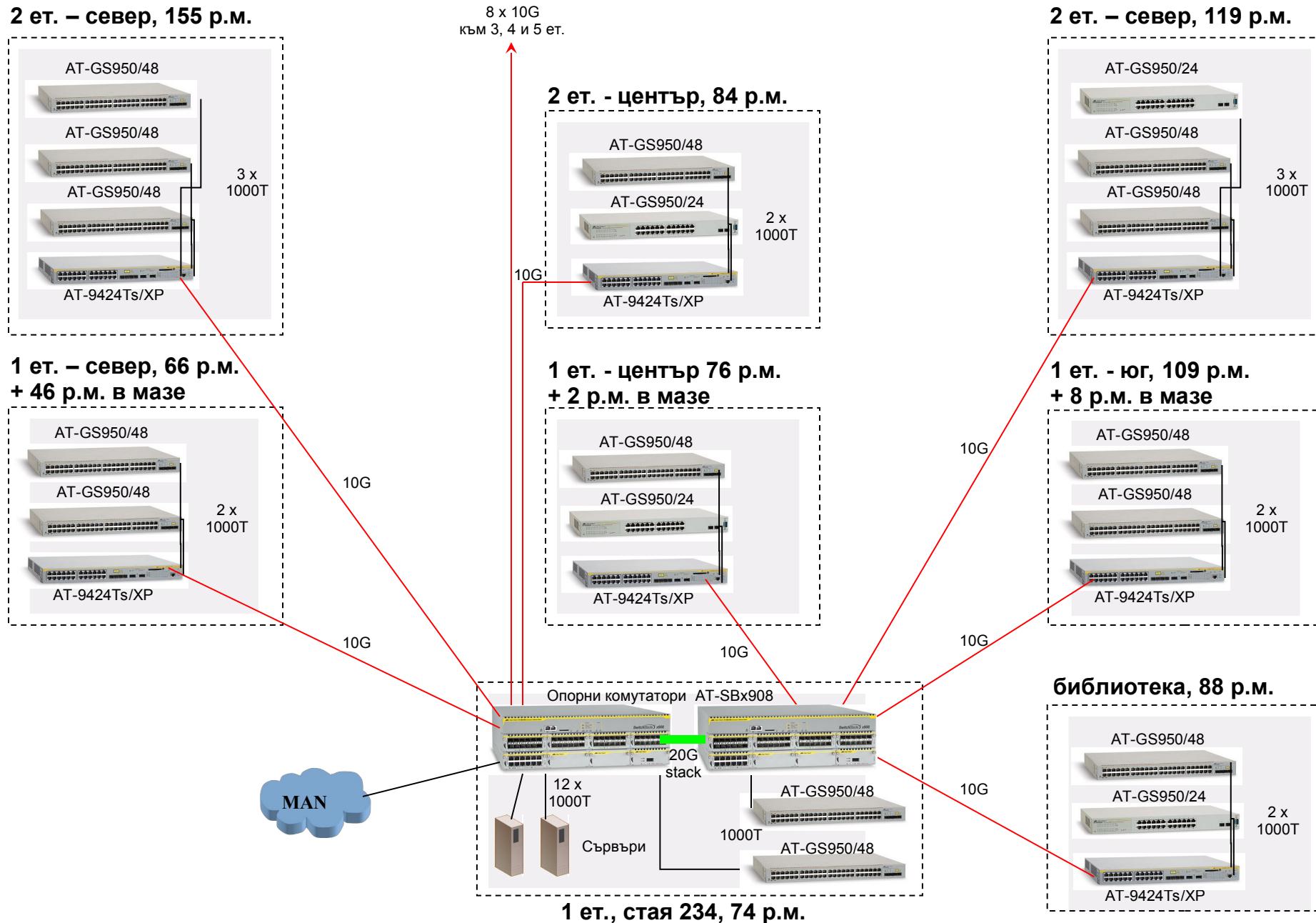
Tag Protocol Identifier (TPID): 16-битово поле: 0x8100 (IEEE 802.1Q)

Priority Code Point (PCP): 3-бита - IEEE 802.1p приоритет: 0 (най-ниско) до 7

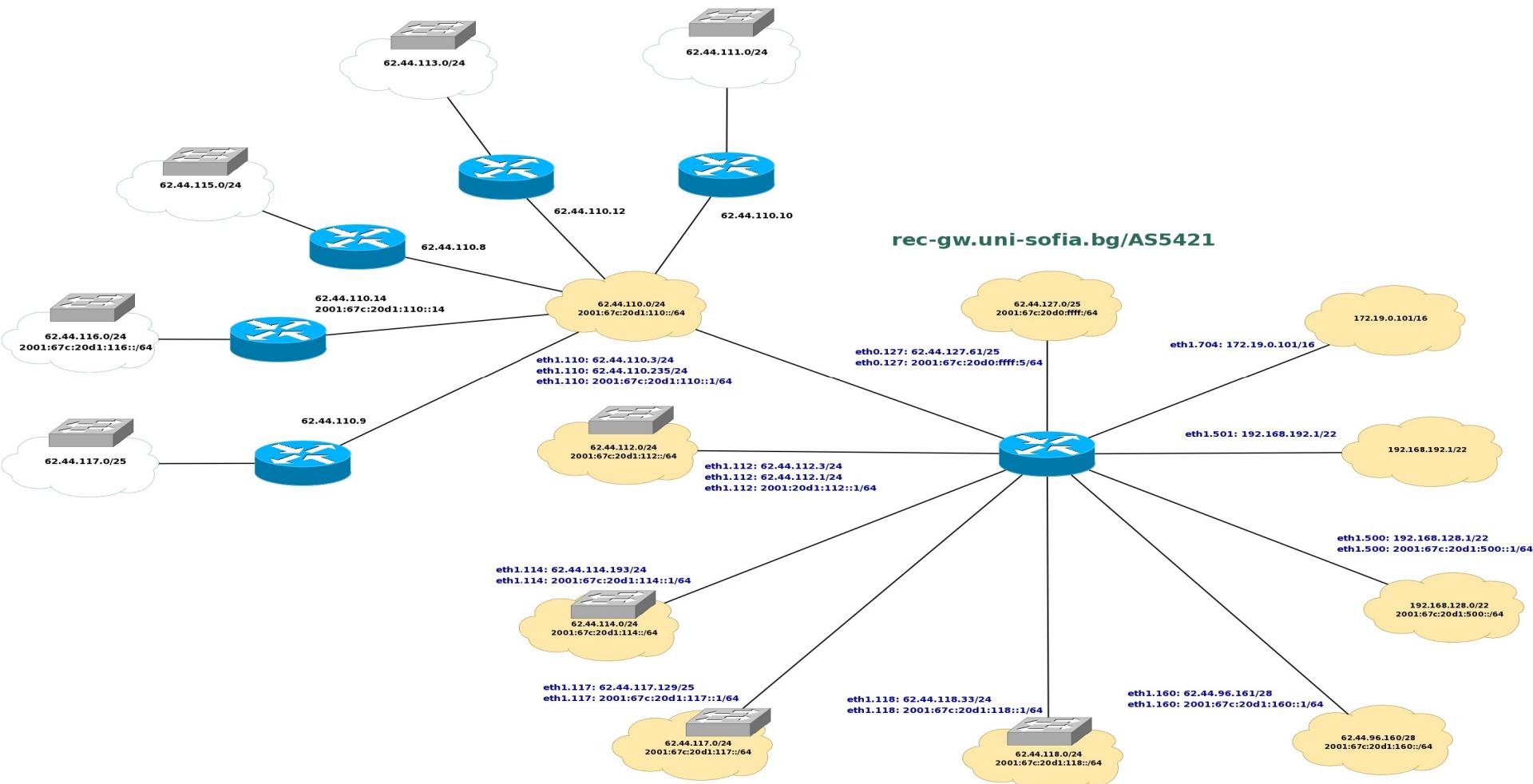
Canonical Format Indicator (CFI): 1-бит: “0” за Ethernet суичове

VLAN Identifier (VID): 12 бита.ако е “0”, кадърът не във VLAN; позволява до 4094 VLAN-а. VLAN 1 резервирана за управление.

Физическа топология на мрежа



Логическа топология на същата мрежа с VLANs



Конфигуриране на 802.1q VLAN интерфейс (като физически)

3. Конфигуриране на 802.1q VLAN интерфейс **/etc/sysconfig/network-scripts/ifcfg-eth1.100**

DEVICE=eth1.100

HWADDR=00:00:CD:4A:55:6A

BOOTPROTO=none

IPADDR=10.10.10.1

NETMASK=255.255.255.0

ONBOOT=yes

REORDER_HDR=yes

ifup eth1.100

Added VLAN with VID == 100 to IF -:eth1:-

Carrier Ethernet (за сведение)

Как Ethernet да се ползва от телеком операторите:

Ethernet over SDH/SONET.

Ethernet over MPLS. Ethernet върху IP/MPLS мрежи. Ethernet се транспортира като “псевдожици” - MPLS label switched paths (**LSPs**) вътре в MPLS “тунел”. Поддържа връзки **точка-точка** (**Virtual Private Wire Service - VPWS**) и **многоточкови** (**Virtual Private LAN service – VPLS**).

Конвенционална ("чиста") Ethernet. Прилага **802.1w** - Rapid Spanning Tree Protocol за връзки **точка-точка**.

Carrier Ethernet 2.0 (за сведение)



Боб Меткалф, сега съветник в MEF ([Metro Ethernet Forum](#)), обяви второ поколение Carrier Ethernet (**CE 2.0**).
“... възможност за опериране с **до 8 услуги** (за сравнение CE 1.0 предлага само 3),
2 от тях са разпределени в направленията E-Line, E-LAN,
E-Tree и E-Access”

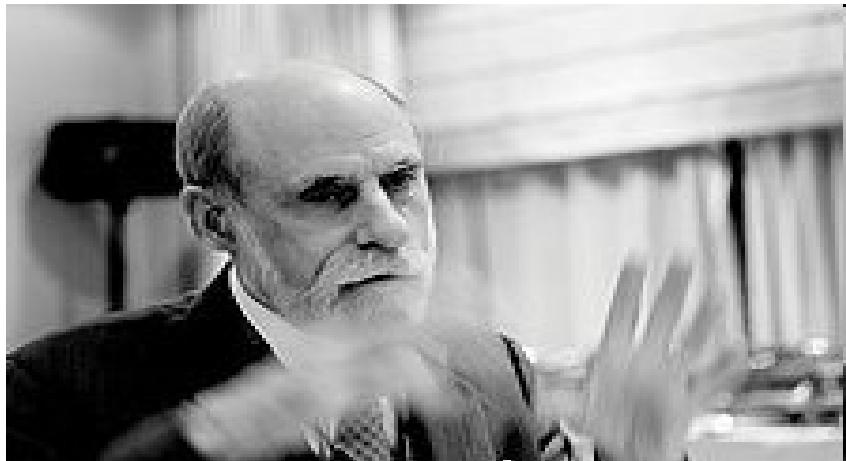
Мрежов протокол IPv4

Адресация, подмрежи и маски.
CIDR

Какво ще научим?

- Задачата на IP протокола
- Формат на IPv4 пакета
- Класове от IP адреси. Видове адреси според обхвата.
- Мрежи, подмрежи, маски, префикси
- CIDR и VLSM
- Разпределение на IP адреси в публичното пространство

IP. История.



Съществуващите към момента различни мрежови методи трябвало да се унифицират. За целта **Robert E. Kahn** от ARPANET наема **Vinton Cerf** от Stanford University.

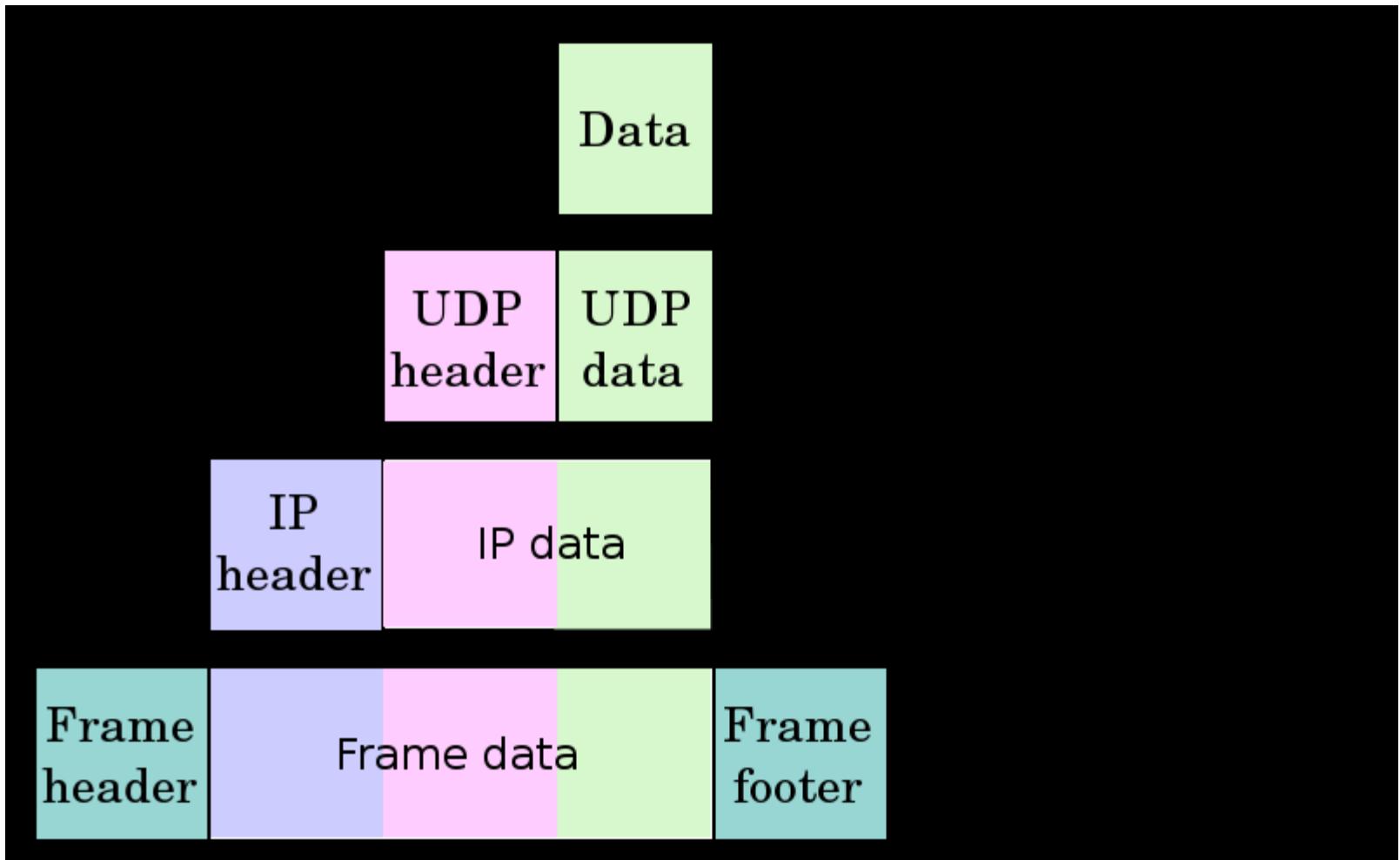
IP. История.

Към 1973 г. успяват сериозно да реформират мрежата, като различията между мрежовите протоколи се скриват под общ **internetwork protocol**, вместо мрежата да е отговорна за надеждността, както е в ARPANET, тя се прехвърля към хостовете.

През декември, 1974 г., излиза спецификацията:

RFC 675 - Specification of Internet Transmission Control Program

Мястото на IP протокола



Задачата на IP протокола

Задачата на протокола IP е да извърши успешно предаване на пакети от източника до получателя, без значение дали те са в една и съща мрежа или в различни мрежи.

Транспортното ниво взима потоци от байтове и ги разделя на **сегменти** (TCP) или **дейтаграми** (UDP), които се “обличат” като **пакети** (наричат ги още **дейтаграми**).

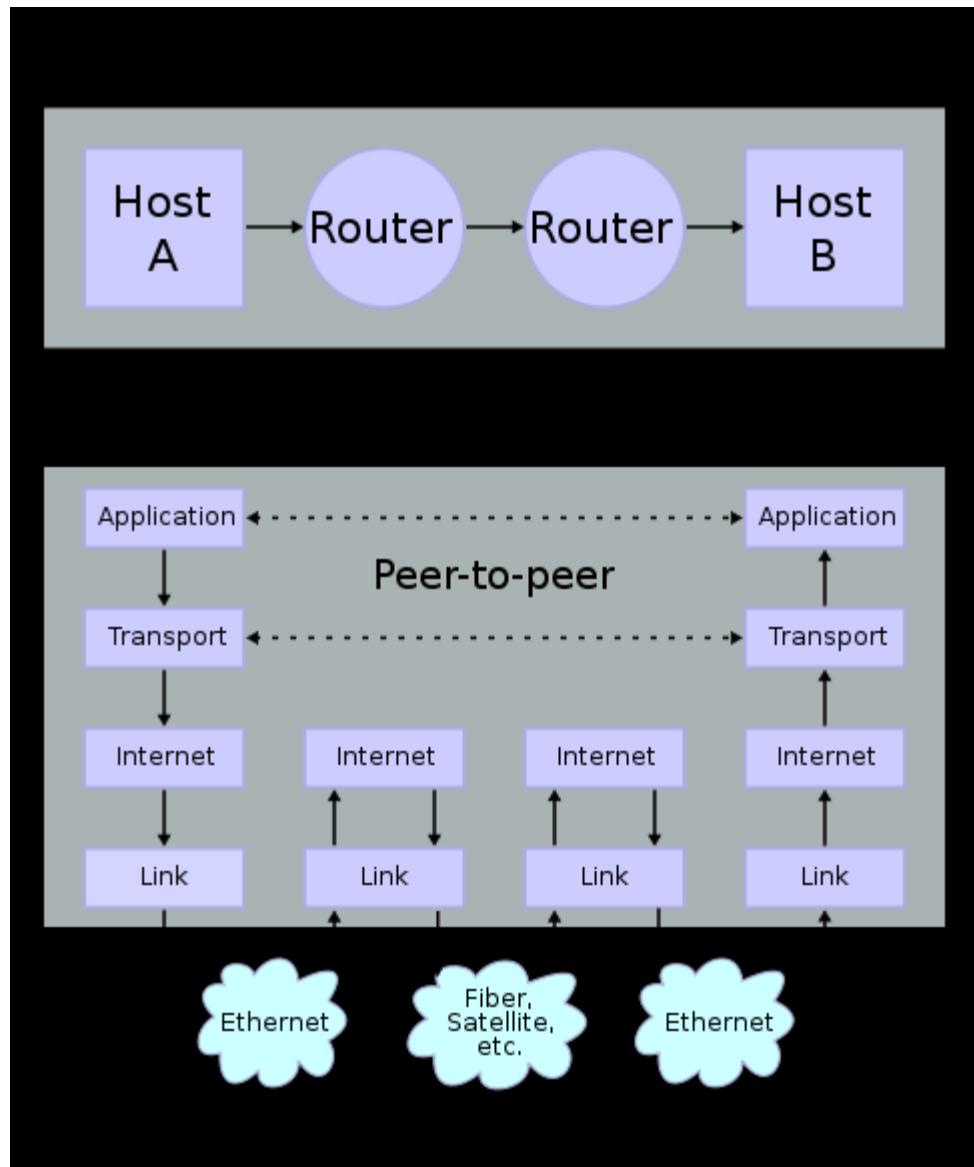
Пакетите могат на теория да достигнат 64KB, но за момента не са по-големи от 1500 байта.

Задачата на IP протокола

Всеки пакет се изпраща самостоятелно, като по пътя може да се фрагментира на по-малки единици. Когато тези единици достигнат до получателя, те се реасемблират от мрежовото ниво за получаване на оригиналния пакет.

По-нататък данните от този пакет се подават на транспортното ниво на получателя, което ги вмъква в потока от байтове на съответното приложение.

Задачата на IP протокола



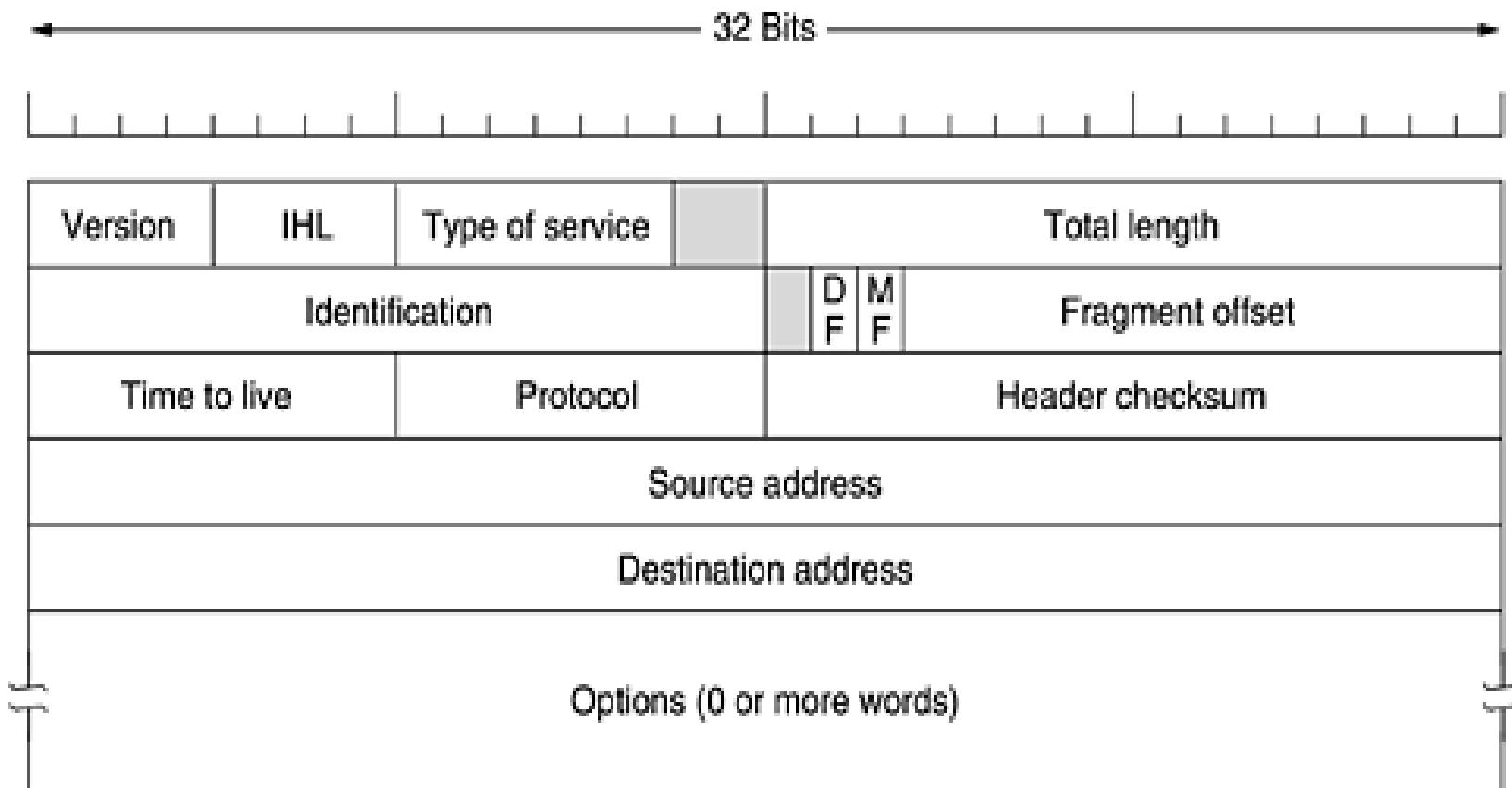
Формат на IPv4 пакета

IP пакета във версия 4 е с 32-битови адреси.

Пакетът се предава в Big-Endian формат, т.е. от старшите към младшите битове.

IP пакетът се състои от заглавна част и част за данни. Заглавната част е 20B+опции с променлива дължина и има следния формат:

Формат на IPv4 пакета



Формат на IPv4 пакета

- Полето **Version** указва версията на протокола, към който принадлежи пакета.
- Полето **IHL** указва дължината на заглавната част в 32-битови думи. То е необходимо, тъй като полето **Options** има променлива дължина.
- **Минималната стойност е 5**, което отговаря на случая когато полето **Options** е празно.
- **Максималната стойност е 15**, което ограничава заглавната част до 60B, т.e. полето за опции до 40B.

Формат на IPv4 пакета

- Полето **Type of service** показва какво обслужване очаква пакета. В днешно време се използва **DiffServ** (**Differentiated Services - QoS**) и **ECN** (**Explicit Congestion Notification** – и двете старни трябва да са съгласни да го използват).
- Полето **Total length** съдържа общата дължина на пакета (заглавна част + данни). Максималната дължина е 65535 байта.
- Полето **Identification** съдържа номер на пакета. Всички фрагменти на една и същ пакет имат еднакъв номер и по този начин получателя разбира кой фрагмент към коя дейтаграма принадлежи.

Формат на IPv4 пакета

Флагът DF (don't fragment) указва на маршрутизаторите да не фрагментират пакета.

Всички автономни системи трябва да могат да приемат фрагменти от поне 576 B. Ако размерът на фрагментите е по-голям и флагът DF е 1, то пакета може да пропусне някоя автономна система с по-малка дължина на пакета, дори тя да се намира на оптималния маршрут.

Формат на IPv4 пакета

- Флагът MF (more fragments) за всички фрагменти на пакета, освен последния е 1, а за последния е 0, т.е. дали полученият фрагмент е последен или не.
- Полето Fragment offset указва къде се намира фрагмента в оригиналната дейтаграма.
- Всички фрагменти, освен последния трябва да са с дължина кратна на 8 B.
- Fragment offset е 13 бита, максималният брой фрагменти в една дейтаграма е 8192.

Формат на IPv4 пакета

Полето **Time to live (TTL)** е брояч, който отброява времето в секунди, има дължина **8 бита**, така че максималното време за живот е **255 секунди**.

Това поле се намалява с единица на всеки **hop**, а освен това се намалява с единица и за всяка секунда престой в маршрутизатор.

При **нулиране** пакета се премахва и в обратна посока се изпраща предупредителен пакет.

Полето **Protocol** указва протокола на транспортно ниво: **TCP** (transmission control protocol), **UDP** (user datagram protocol) или някой друг.

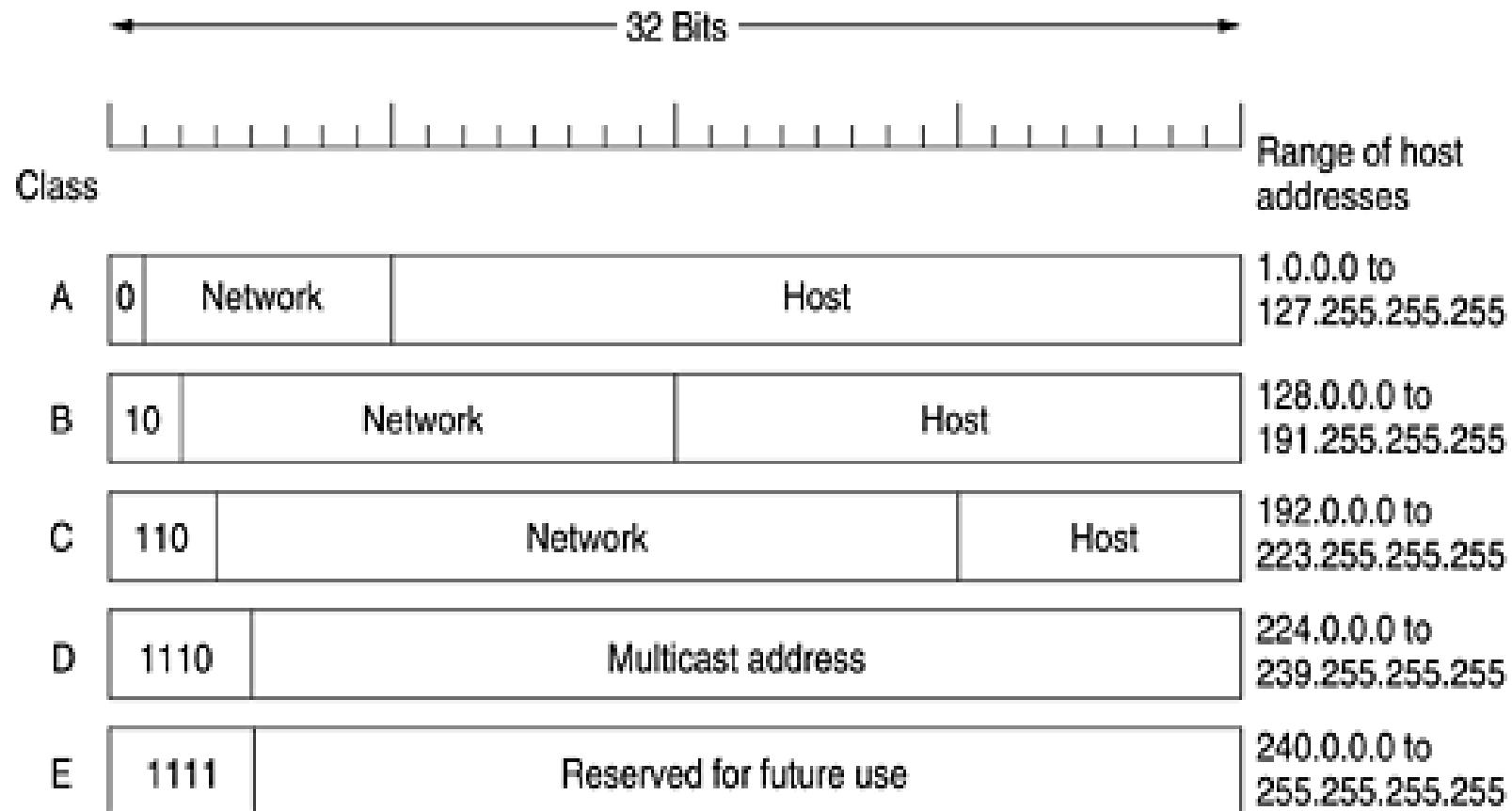
Формат на IPv4 пакета

- Полето **Header checksum** е контролна сума само на заглавната част. Тя трябва да се преизчислява на всеки hop, тъй като поне едно поле се променя - TTL.
- Полетата **Source Address** и **Destination Address** съдържат съответно адрес на източника и адрес на получателя.

Формат на IPv4 адреса

- Всеки хост и маршрутизатор в мрежата има IP-адрес.
- Всички IP-адреси са **32-битови**. Всеки IP адрес се **дели на две части** – номер на мрежа и номер на хост.
- **Номерът на мрежата (prefix)** е в лявата част на адреса, а **номерът на хоста** е останалата порция от битове в дясната част на адреса.
- В зависимост от структурата си IP-адресите се делят на следните пет класа:

Класове от IP адреси



Класове от IP адреси

Битовете в началото на адреса, които определят неговия клас, се наричат **сигнални битове**.

В **клас А** са възможни 127 мрежи, всяка с приблизително 16000000 хоста.

В **клас В** са възможни приблизително 16000 мрежи, всяка с приблизително 65000 хоста.

В **клас С** са възможни приблизително 2000000 мрежи, всяка с по 254 хоста.

Клас D е предназначен за работа с групови (**multicast**) адреси, а **клас Е** е резервиран за бъдеща употреба (научни цели и др.).

Записване на IP-адресите

За удобство IP-адресите се изписват в **точкова десетична нотация**, като всеки от четирите байта се изписва като десетично число от 0 до 255. Най-малкия IP-адрес е 0.0.0.0, а най-големия **255.255.255.255**.

Адрес, който съдържа само единици се интерпретира като **broadcast**-адрес, т.е. адресират се всички хостове в дадена мрежа.

Представяне на десетичното число 106 в двоичен формат

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
128 (2^7)	64 (2^6)	32 (2^5)	16 (2^4)	8 (2^3)	4 (2^2)	2 (2^1)	1 (2^0)

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
0	1	1	0	1	0	1	0

Представяне на десетичното число 106 в двоичен формат (обяснение)

$106 < 2^{**}7 = 128 \rightarrow 0$

$106 > 64 (2^{**}6) \rightarrow 1$

$106 - 64 = 42 > 2^{**}5=32 \rightarrow 1$

$42 - 32 = 10 < 2^{**}4=16 \rightarrow 0$

$42 - 32 = 10 > 2^{**}3=8 \rightarrow 1$

$10 - 8 = 2 < 2^{**}2=4 \rightarrow 0$

$10 - 8 = 2 = 2^{**}1=2 \rightarrow 1$

$2-2 = 0 < 2^{**}0=1 \rightarrow 0$

Мрежи и подмрежи

Голям недостатък на IP-адресацията е, че половината адреси са от **клас А** и се разпределят само между **127** автономни системи, въпреки че всяка от тях може да съдържа **милионы** хостове.

Всяка мрежа трябва да има уникален номер и всички хостове в дадена мрежа трябва да имат един и същ номер на мрежата.

Това води до проблеми при нарастване на броя на мрежите.

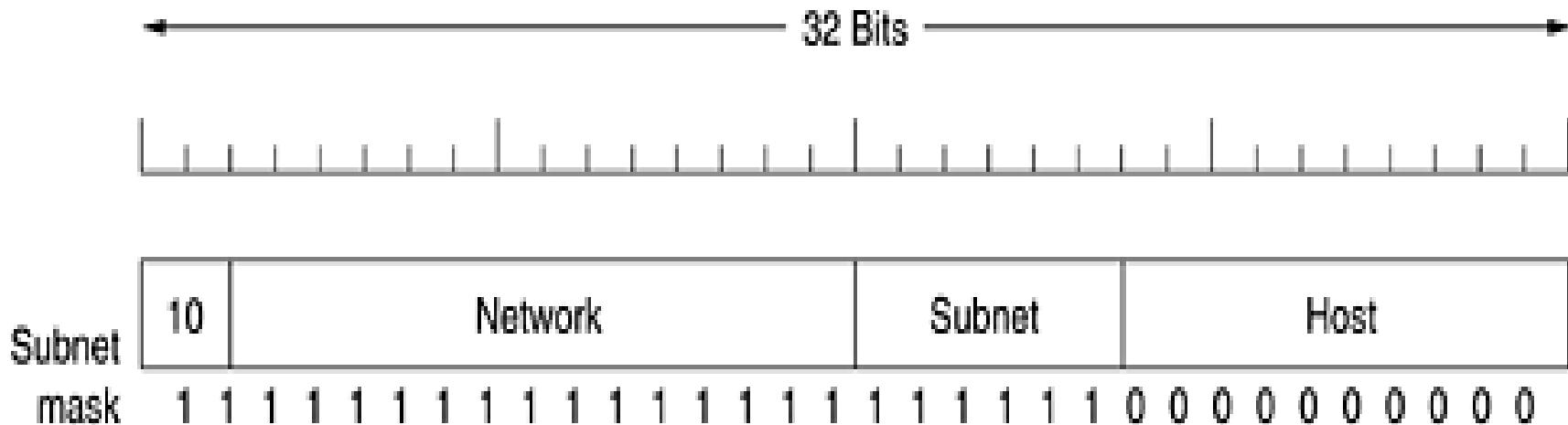
Мрежи и подмрежи

Решението на проблема е да се разреши разделянето на една мрежа на **подмрежи**. За целта полето за мрежов номер се разширява надясно, като се отнемат битове от номера на хост.

Например за един адрес от клас В вместо 16 бита за номер на мрежата и 16 бита за номер на хост се използват 22 бита за номер на мрежа, като десните 6 от тях са за номер на подмрежа и 10 бита за номер на хост.

Мрежи и подмрежи

За реализация на подмрежите маршрутизаторите се нуждаят от **подмрежова маска** (**Subnet Mask - SM**), която определя границата между номера на мрежата + номера на подмрежата и номера на хоста. В долния пример имаме мрежовата маска на една разцепена клас В мрежа:



Мрежи и подмрежи

При разделяне на една мрежа на подмрежи взимаме “назаем” (**borrow**) битове от хост частта на адресите.

Получава се следното:

N S H

Броят на подмрежите е: 2^S

Броят на хостовете в подмрежата ще е: $2^H - 2$
(нулевият адрес остава за **номер на подмрежата**, а последният – за **broadcast**)

Изписане на маската. Префикси.

SM има същия формат като IPv4 адреса:
старшите битове, които не принадлежат на хост
частта са = 1 и се наричат **префикс**,
а останалите (**хост частта**) са = 0.
Възможни са два начина на изписане на
мрежов адрес. Напр., следния клас C адрес:

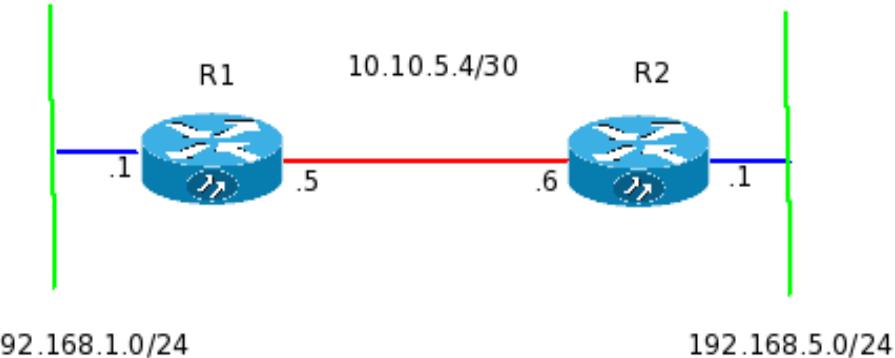
192.168.1.0 255.255.255.0

или

192.168.1.0/24

Второто означение се нарича 24-битов префикс
или просто префикс. **По-нататък ще
използваме него.**

Ролята на маската



Всеки маршрутизатор(напр. **R1**) има таблица с маршрутите (**Routing Table**), покоято определя пътя на пакета.

Всеки ред съдържа **IP адреса на мрежа / префикс**, следващ възел по пътя, изходящ интерфейс и др., например:

C 192.168.1.0/24 [0] is directly connected, eth0

S 192.168.5.0/24 [1/0] via 10.10.5.6, eth1

C 10.10.5.4/30 [1/0] is directly connected, eth1

Ролята на маската

Когато пристигне IP пакет неговият адрес на получател (напр. 192.168.5.1) се преглежда. Извършва се операцията “Логическо умножение” между IP адреса на получателя и маската:

Destination IP .AND. SM (1)

Какво означава това? Всяко число, умножено по 0, дава 0. (Важи и за лог.)

Т.е операция (1) ни дава номера на мрежа / подмрежа.

Разделяне на класове и безкласово делене

Първоначално IP адресите са били само от клас A:

- Network ID: първи (най-старши) октет (байт);
- Host ID: младшите три октета.

Т.е имаме само 256 мрежи. (Подобно е положението сега с IPv6). С разрастването на Интернет това става безсмислено.

Въведени са **класовете** (**classful networking**). От петте класа (A, B, C, D и E), три (A, B и C) имат различна дължина на мрежовата част. Груповите - Клас D (multicast) идентифицират отделни хостове. Клас E са резервираны.

Classless Inter-Domain Routing

Около 1993 г. класовете A, B и C е заменено с Classless Inter-Domain Routing (CIDR).

CIDR включва:

- VLSM (variable-length subnet masking) – префикси с произволна дължина. Записва се с /брой на битове (1-ци) в префиксата например, 192.168.0.0/16. По-ефективно използване на изчерпващите се IPv4 адреси.
- събиране (aggregation) на множество последователни префикси в “супермрежи” (supernets)
- когато се прави обобщаване на маршрути към classful граница - route summarization.

CIDR и VLSM

С помощта на VLSM се извършва обобщаване в супермрежи (supernetting) – съкращаване на броя на 1-те от дясно на ляво, което е обратно на деленето на подмрежи (subnetting) - увеличаване на броя на 1-те от ляво на дясно.

Където е възможно в Интернет се анонсират супермрежите, намалявайки броя на “редовете” в глоблната таблица с маршрутите.

Например, 16 последователни Клас С (/24) ще се анонсират като един единствен /20 префикс, респ. маршрут ($2^4 = 16$). Два последователни префикса /20 - като /19 ($2^1 = 2$).

Пример: 32 * /24 мрежи

IANA е делегирала на RIPE префикс:

62.0.0.0/8

11111111.0.0.0

На молба от организация да получи 32 Клас С
(32 * /24) мрежи RIPE делегира префикс:

62.44.96.0/19

11111111.11111111.11100000.0

Отговорете си как се получават (32 * /24), $2^5=32$

Пример: 32 * /24 мрежи

Мрежовите админ-и получават:

62.44.96.0/24 ; 62.44.97.0/24 ... 62.44.127.0/24.

На ФМИ делегират префикса:

62.44.100.0/23

1111111.1111111.1111110.0

Т.е ($2^1=2$) ФМИ получава:

62.44.100.0/24 и 62.44.101.0/24

Сървър e-learning 62.44.100.150/24

Пример: Разцепване на подмрежи.

62.44.109.0/24

62.44.109.0/26 – 1-ва подмрежа

62.44.109.64/27 – 2-а подмрежа

62.44.109.128/25 – 3-та подмрежа

CIDR и VLSM

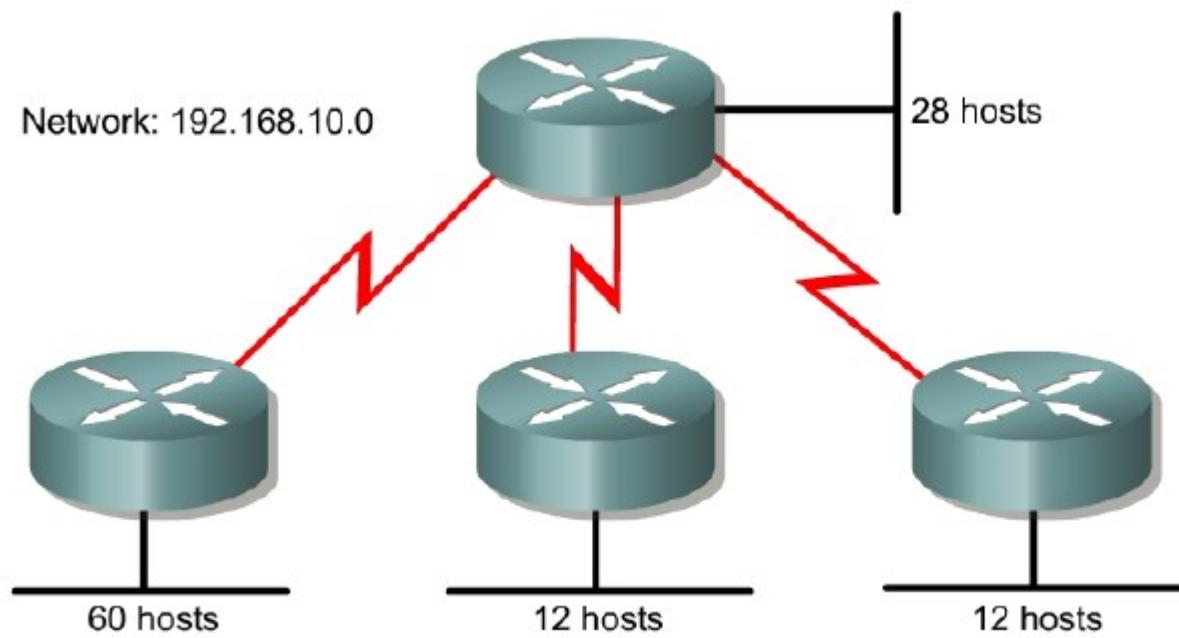
IPv4 CIDR Chart				RIPE NCC
IP Addresses	Bits	Prefix	Subnet Mask	
1	0	/32	255.255.255.255	
2	1	/31	255.255.255.254	
4	2	/30	255.255.255.252	
8	3	/29	255.255.255.248	
16	4	/28	255.255.255.240	
32	5	/27	255.255.255.224	
64	6	/26	255.255.255.192	
128	7	/25	255.255.255.128	
256	8	/24	255.255.255.0	
512	9	/23	255.255.254.0	
1 K	10	/22	255.255.252.0	
2 K	11	/21	255.255.248.0	
4 K	12	/20	255.255.240.0	
8 K	13	/19	255.255.224.0	
16 K	14	/18	255.255.192.0	
32 K	15	/17	255.255.128.0	
64 K	16	/16	255.255.0.0	
128 K	17	/15	255.254.0.0	
256 K	18	/14	255.252.0.0	
512 K	19	/13	255.248.0.0	
1 M	20	/12	255.240.0.0	
2 M	21	/11	255.224.0.0	
4 M	22	/10	255.192.0.0	
8 M	23	/9	255.128.0.0	
16 M	24	/8	255.0.0.0	
32 M	25	/7	254.0.0.0	
64 M	26	/6	252.0.0.0	
128 M	27	/5	248.0.0.0	
256 M	28	/4	240.0.0.0	
512 M	29	/3	224.0.0.0	
1024 M	30	/2	192.0.0.0	
2048 M	31	/1	128.0.0.0	
4096 M	32	/0	0.0.0.0	

K = 1.024 • M = 1.048.576

Contact Registration Services:
hostmaster@ripe.net • lir-help@ripe.net

www.ripe.net

Примерна задача



Задача. Внимание.

!!! $H = 2^h - 2$, където

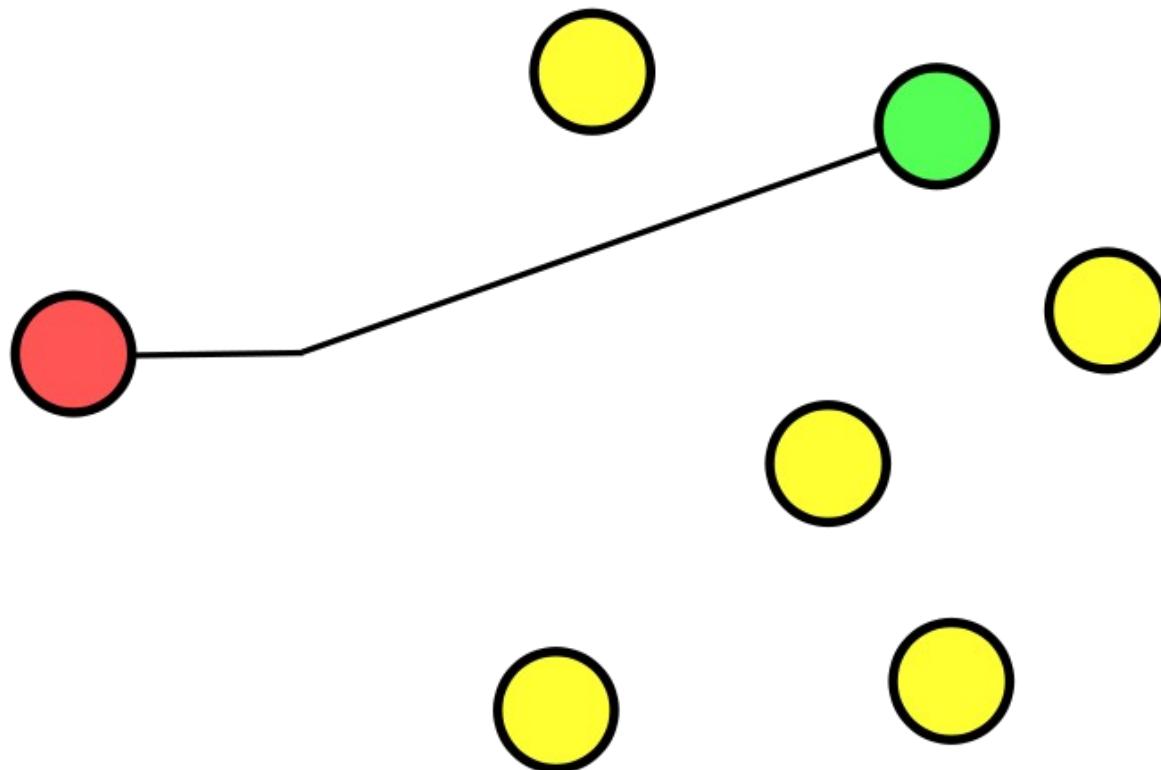
H – бр. хостове, h – бр. битове в хост
частта на IP адреса

Point-to-point мрежи. Трябват им 2 и само 2
хоста. Коя SM (префикс) ще изберем???

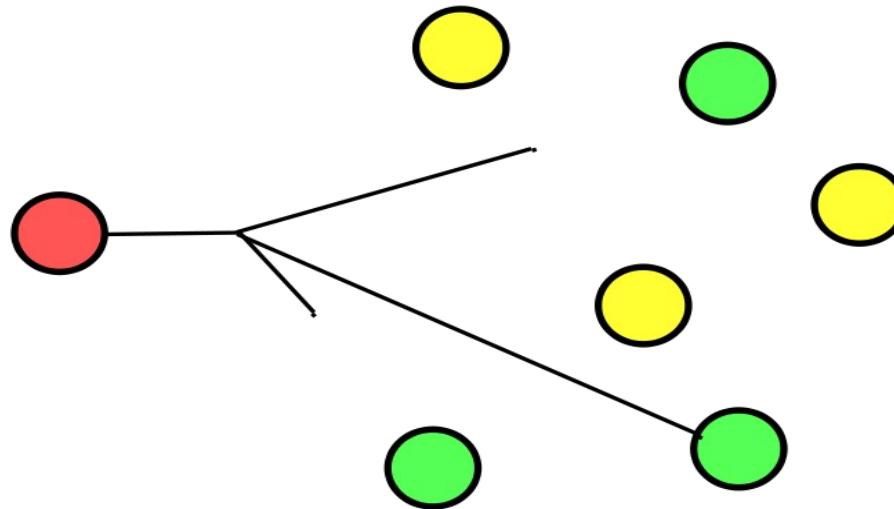
Unicast, Multicast, Anycast, Broadcast

	получател	Места в (под)мрежата
Unicast	1	1
Anycast	1	Много, но репликирани, избира най-близко
Multicast	много	много
Broadcast	всички	всички

Unicast

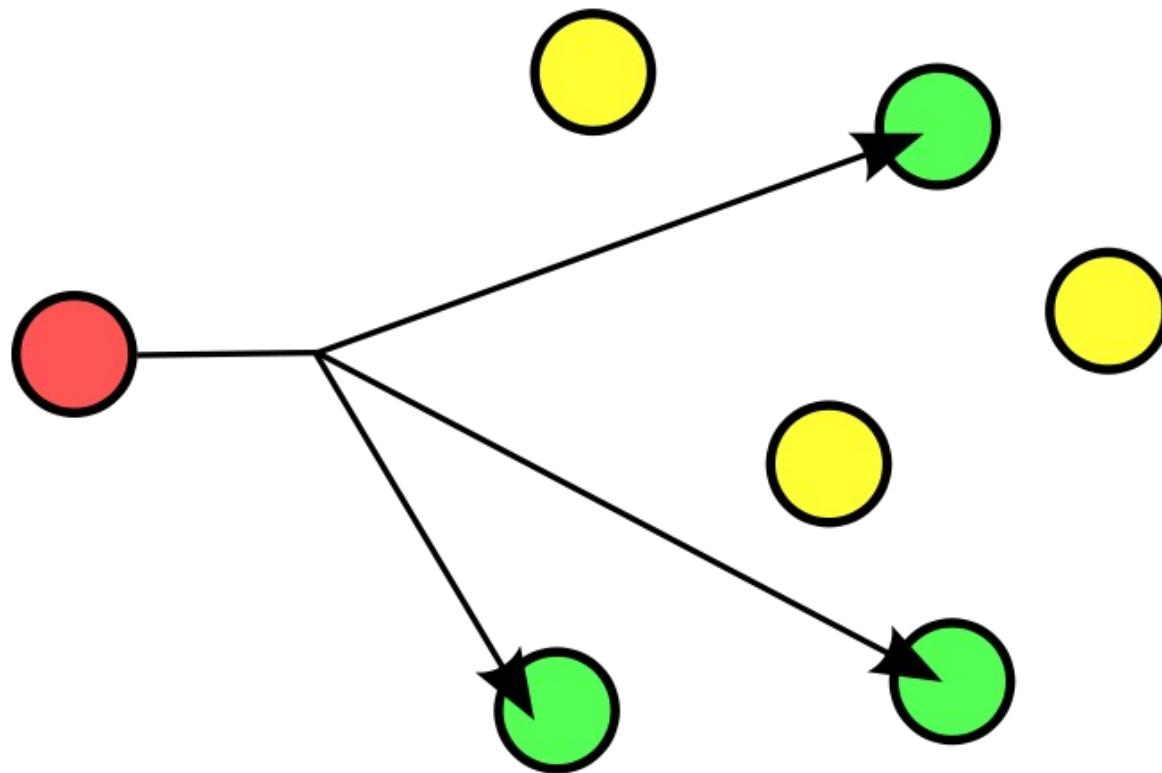


Anycast

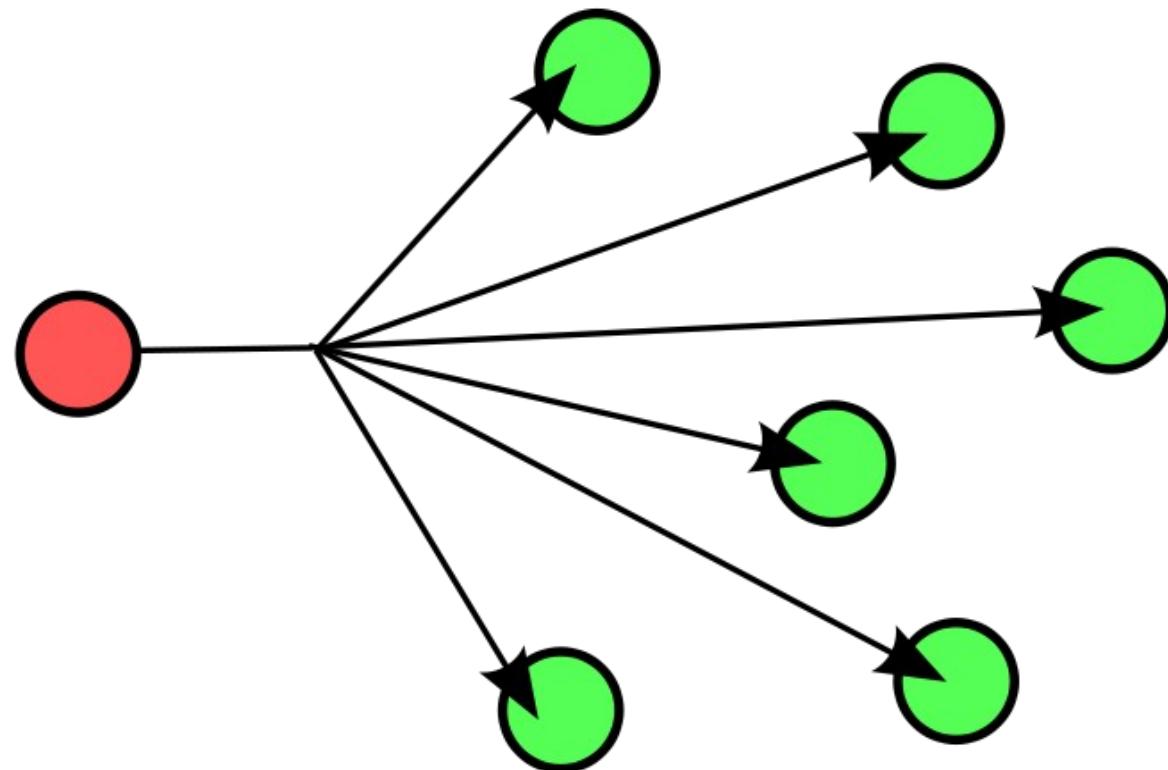


Anycast са **част от** unicast пространството.
Синтактически по нищо не се
различават.

Multicast

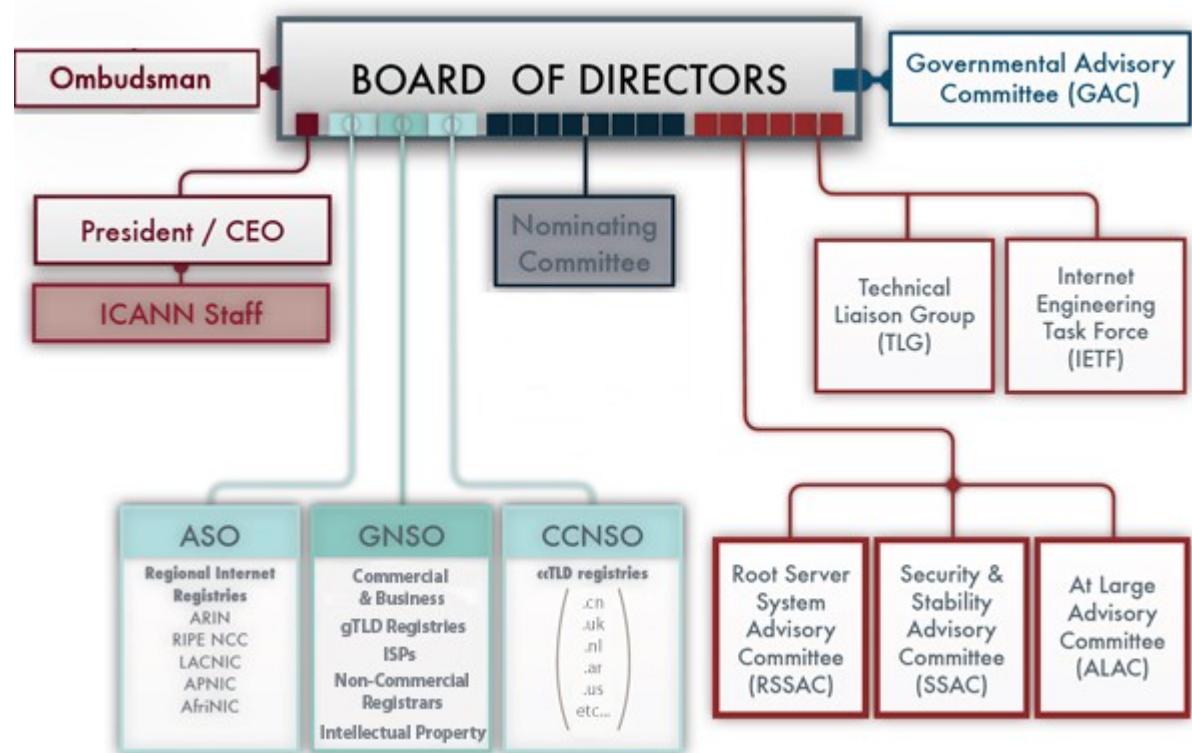


Broadcast



Раздаване на IP адреси (Address Allocation). ICANN.

Internet Corporation for Assigned Names and Numbers - ICANN (icann.org) координира процеса по разпределяне на уникалните идентификатори в Интернет.
ICANN е основана в 1998 г.



Address Allocation. IANA.

Screenshot of a Mozilla Firefox browser window showing the IANA website (<http://www.iana.org/>). The browser interface includes a toolbar at the top with icons for Applications, Places, System, and various system status indicators (USA, 8 °C, Fri Mar 19, 11:13:05, stefan). The menu bar includes File, Edit, View, History, Bookmarks, Tools, and Help. The address bar shows the URL <http://www.iana.org/>. The search bar contains the text "local internet registry". The title bar reads "IANA — Internet Assigned Numbers Authority - Mozilla Firefox". The main content area displays the IANA logo and the text "Internet Assigned Numbers Authority". Below this, a box states: "The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources. [Learn more about what we do »](#)". The page is divided into three main sections: "Domain Names", "Number Resources", and "Protocol Assignments".

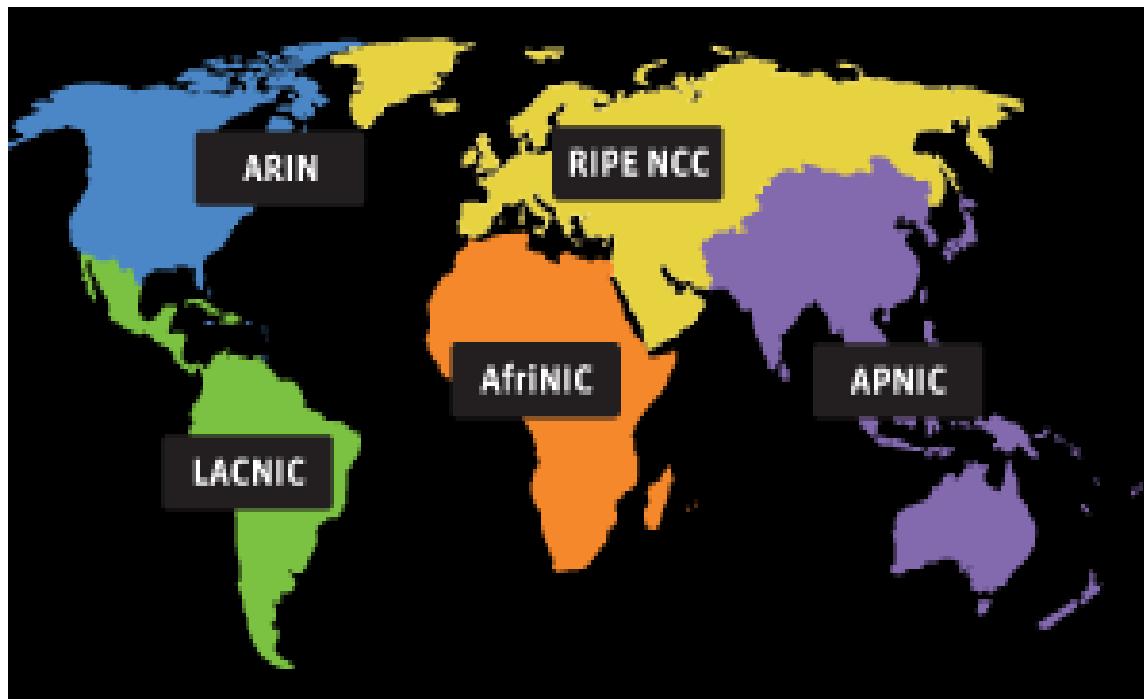
The "Domain Names" section describes IANA's management of the DNS Root Zone, ccTLDs, gTLDs, .int, and .arpa zones, with links to Root Zone Management, Database of Top Level Domains, .int Registry, .arpa Registry, IDN Practices Repository, and Interim Trust Anchor Repository.

The "Number Resources" section describes IANA's coordination of global IP and AS number space, with links to IP Addresses & AS Numbers and Think we're attacking you?

The "Protocol Assignments" section describes IANA as the central repository for protocol name and number registries, used in many Internet protocols, with links to Protocol Registries and Apply for an assignment.

At the bottom of the browser window, there is a search bar with the text "Cerf", navigation buttons for "Previous", "Next", "Highlight all", and "Match case", and a URL bar showing <http://www.iana.org/numbers/>. The status bar at the bottom right shows the Firefox icon, the title "IANA — Internet Assig...", and "Topic-9.odp - OpenOffi...".

RIRs



Address Allocation (Присвояване на IP адреси)

IP адресите се разпределят от IANA между 5-те Regional Internet Registries (RIRs).

RIRs управляват, разпределят и регистрират публичните Internet Number Resources в поверените им области.

Имаме пет регионални регистратора - RIRs:

- AfriNIC (afrinic.net)
- APNIC (apnic.net)
- ARIN (arin.net)
- LACNIC (lacnic.net)
- RIPE NCC (ripe.net)

IANA е делегирала широк обхват от Интернет ресурси на RIRs:

<http://iana.org/assignments/ipv4-address-space/ipv4-address-space.xml>

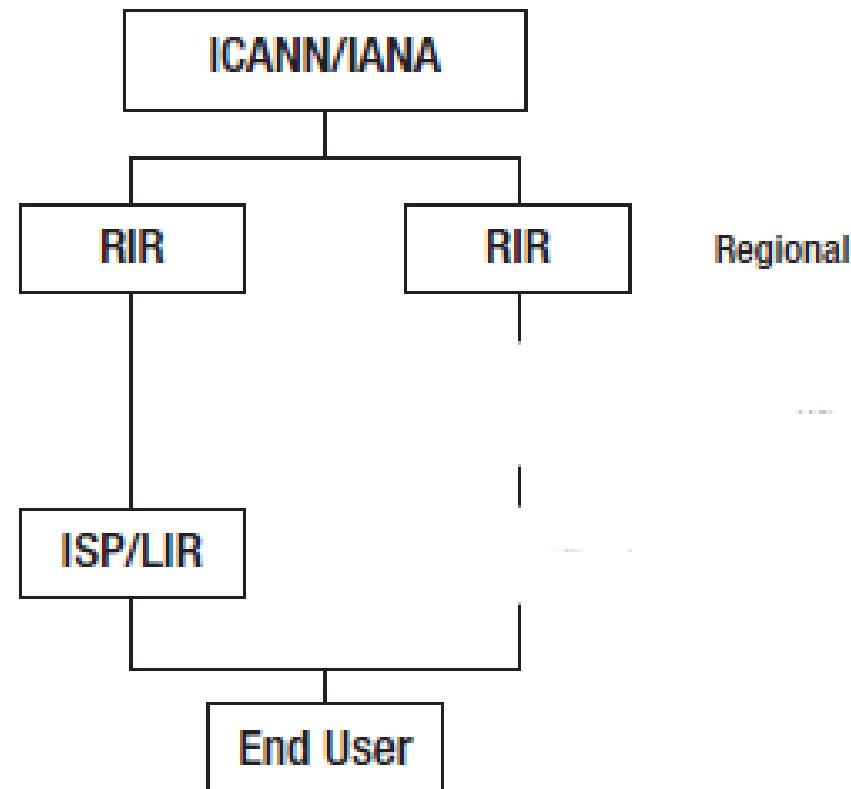
<http://iana.org/assignments/multicast-addresses/multicast-addresses.xml>

Присвояване на адреси

Всеки RIR поддържа публична база от данни **WHOIS** с информация за присвоените IP адреси.

RIRs ги присвояват на ISPs (които са LIR – Local Internet Registries), които ги раздават на своите клиенти (**PA** – Provider Assigned)...

PA vs. PI



PI присвояване на адреси

...или директно на крайни клиенти (Provider Independent - PI), които съответно се разпределят по LANs вътре в организацията.

Присвояването на адреси не е произволно. Основен принцип в маршрутизацията е, че IP адресът да показва мястото на обекта (възел, устройство) в мрежата. Т.е адрес, присвоен в една част от мрежата, няма да функционира в друга.

WHOIS 62.44.96.0/19

inetnum: 62.44.96.0 - 62.44.127.255

netname: BG-SUNET

descr: Sofia University

descr: BG-1164 Sofia

org: ORG-UoS32-RIPE

country: BG

...

status: ASSIGNED PI

(**inetnum** – съдържа подробности за алокацията или присвояването на IPv4 адресно пространство)

Големи български LIRs

<http://www.ripe.net/membership/indices/>

Е показан списък на RIPE NCC Local Internet Registries.

Големи български LIRs са:

- * Bulgarian Telecommunications Company Plc.
- * Global Communication Net Plc
- * Eurocom Cable Management Bulgaria Ltd
- * ITD Network SA
- * Neterra Ltd.
- * Spectrum NET Jsc
- * NetArt Group s.r.o. <Registry Based in CZ>
- * Equant Inc. <Registry Based in EU>
- * AT&T Global Network Services Nederland B.V. <Reg. in EU>
- * Interoute Communications Limited <Registry Based in GB>

Примерни задачи

- Имате префиксите 62.44.120.0/24; 62.44.121.0/24 и 62.44.123.0/24. Как ще ги представите с една супермрежа?
- Колко хоста могат да получат адреси в IP мрежа 172.19.18.0/29?
- Какъв е максималния брой подмрежи за IP мрежа 201.36.5.0/24, като във всяка подмрежа да могат да получат адреси 15 хоста? Каква е маската?

Специални IP адреси. NAT.

Преобразуване на IP адреси
във физически. ARP vs.
RARP. DHCP. ICMP.

Какво ще научим?

- Кои са специалните IP адреси. Частните адреси и NAT. Stateful и Stateless NAT.
- (R)ARP – Съответстващо IP – MAC
- Динамично раздаване на IP адреси. DHCP.
- Протокол за тестване на мрежовата свързаност ICMP

Специални IP адреси

В рамките на IPv4 адресното пространство има адресни сегменти, които са отделени за **частно** (локално) използване.

RFC 6890 прави "карта" на адресните сегменти (IPv4 и IPv6) за специално използване.

Обновена е от RFC 8190

Терминът "global", който поражда двойственост:

- allocation (разпределяне) или
- routing/reachability
(маршрутизация/достижимост).

Тук е заменен с "globally reachable".

Специални IP адреси

127.0.0.0/8 - Internet host **loopback address**.

Пакет се зацикля вътре в хоста. И не се появява никъде в мрежата.

169.254.0.0/16 – това е "**link local**" блок.

Хостовете получават такива адреси по “auto-configuration”, например не може да се намери DHCP сървър.

Частни IP адреси

Те [не се маршрутизират глобално](#), а само локално, за локални (частни) цели.

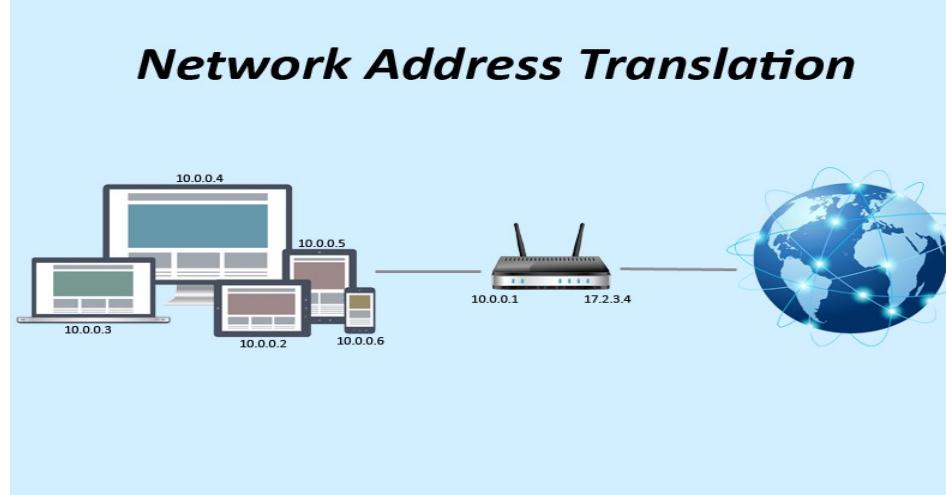
[RFC3330](#) (първото указване е в [RFC1918](#)) указва кои от адресните пространства се използват за частни цели:

10.0.0.0/8 т.е 10.0.0.0 – 10.255.255.255

172.16.0.0/12 т.е 172.16.0.0 - 172.31.255.255

192.168.0.0/16 т.е 192.168.0.0 - 192.168.255.255

NAT (Network Address Translation)



NAT е процес, при който рутер или др. компютър има интерфейс с публичен IP адрес към външната мрежа и един или повече интерфейси към вътрешната мрежа(и), на които са присвоени частни IP адреси.

Целта е да се пестят публични IP адреси.
Компютрите от вътрешната мрежа(и) се виждат от “вънния свят” с публичния адрес.

Statefull NAT (SNAT). Port Address Translation (PAT).

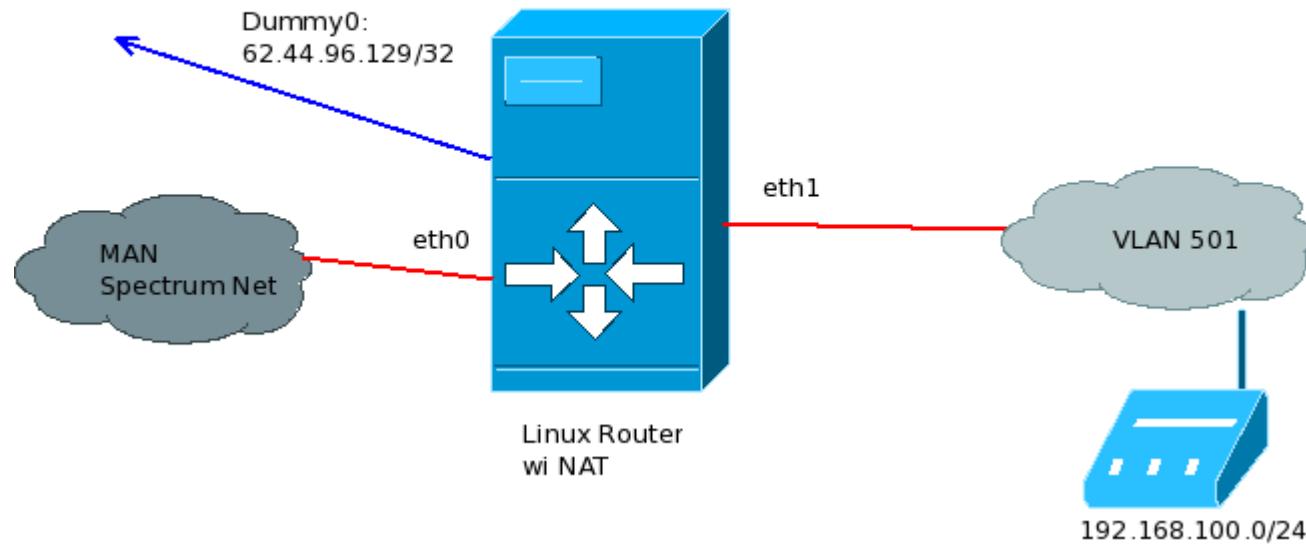
SNAT поддържа в паметта на рутера (или сървъра) специално алокирани за целта страници, съдържащи таблици на съответствие между публични и частни адреси на съответните компютри във вътрешната мрежа.

SNAT в [Linux ядрата 2.6](#) и нагоре тези таблици в паметта се наричат [connection tracking tables](#).

PAT е най-разпространеният вариант на SNAT. Компютрите от вътрешната мрежа се виждат “навън” с публичния IP адрес на NAT устройството. Единственото, което ги отличава е номера на порта на процеса, който генерира заявка или отговор.

Голяма безжична мрежа зад NAT

ТОПОЛОГИЯ НА БЕЗЖИЧНА МРЕЖА



Безжична мрежа зад NAT (dummy0)

Публичният IP адрес за NAT е добре да не бъде директно обвързан с физически интерфейс, който може да бъде променен след ремонт на компютъра.

Затова се създава се **dummy** интерфейс.

/etc/sysconfig/network-scripts/ifcfg-dummy0:

DEVICE=dummy0

IPADDR=62.44.96.129

NETMASK=255.255.255.255

ONBOOT=yes

ifup dummy0

Безжична мрежа зад NAT (Конфигуриране)

Чрез инструмента `iptables` и едноимената услуга.

Указва се правилото за NAT (като root):

```
# iptables -t nat -A POSTROUTING  
-s 192.168.100.0/24 -d 0.0.0.0/0  
-o eth0 -j SNAT --to 62.44.96.129
```

Всички изходящи от `192.168.100.0/24` (WiFi потребители) пакети през интерфейса `eth0` се маскират към публичния адрес `62.44.96.129` (`dummy0`).

Безжична мрежа зад NAT (connection tracking tables)

```
# service iptables save  
# chkconfig iptables on
```

ip_conntrack: table full, dropping packet

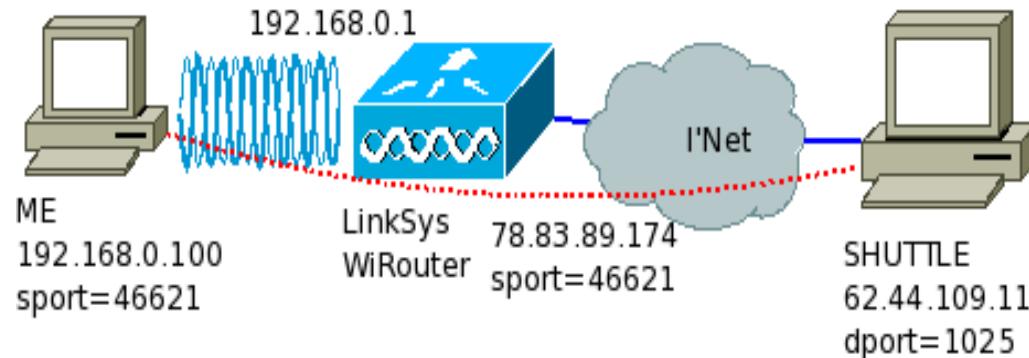
Затова във файла [`/etc/sysctl.conf`](#) се описват следните променливи на ядрото:

```
net.ipv4.ip_conntrack_max = 2000000000
```

```
net.ipv4.netfilter.ip_conntrack_max =  
2000000000
```

```
# sysctl -p
```

Установена TCP сесия по SSH. Conntrack таблица.



В примера с установена SSH сесия илюстрираме
Conntrack таблица,resp. **PAT**.

source port (sport) е номера на комуникацията, свързана с приложението – инициатор на “разговора” (**сесия**).

destination port (dport) е номера на комуникацията, свързана с приложението – дестинация, работещо върху отдалечения хост.

conntrack таблица

```
[root@shuttle]#less /proc/net/ip_conntrack
```

```
tcp      6 432000 ESTABLISHED src=78.83.89.174  
dst=62.44.109.11 sport=46621 dport=1025 packets=243  
bytes=20821 src=62.44.109.11 dst=78.83.89.174  
sport=1025 dport=46621 packets=156 bytes=28980  
[ASSURED] mark=0 secmark=0 use=2
```

```
[root@me]# less /proc/net/nf_conntrack
```

```
ipv4      2  tcp      6 431761 ESTABLISHED  
src=192.168.0.100 dst=62.44.109.11 sport=46621  
dport=1025 packets=262 bytes=22097 src=62.44.109.11  
dst=192.168.0.100 sport=1025 dport=46621  
packets=167 bytes=30432 [ASSURED] mark=0 secmark=0  
use=2
```

Stateless NAT

Stateless NAT (dumb NAT) е най-простата форма на NAT. Целта е ценен ресурс да не се вижда директно с публичен адрес. Само пренаписва адреси, преминаващи през маршрутизатора:

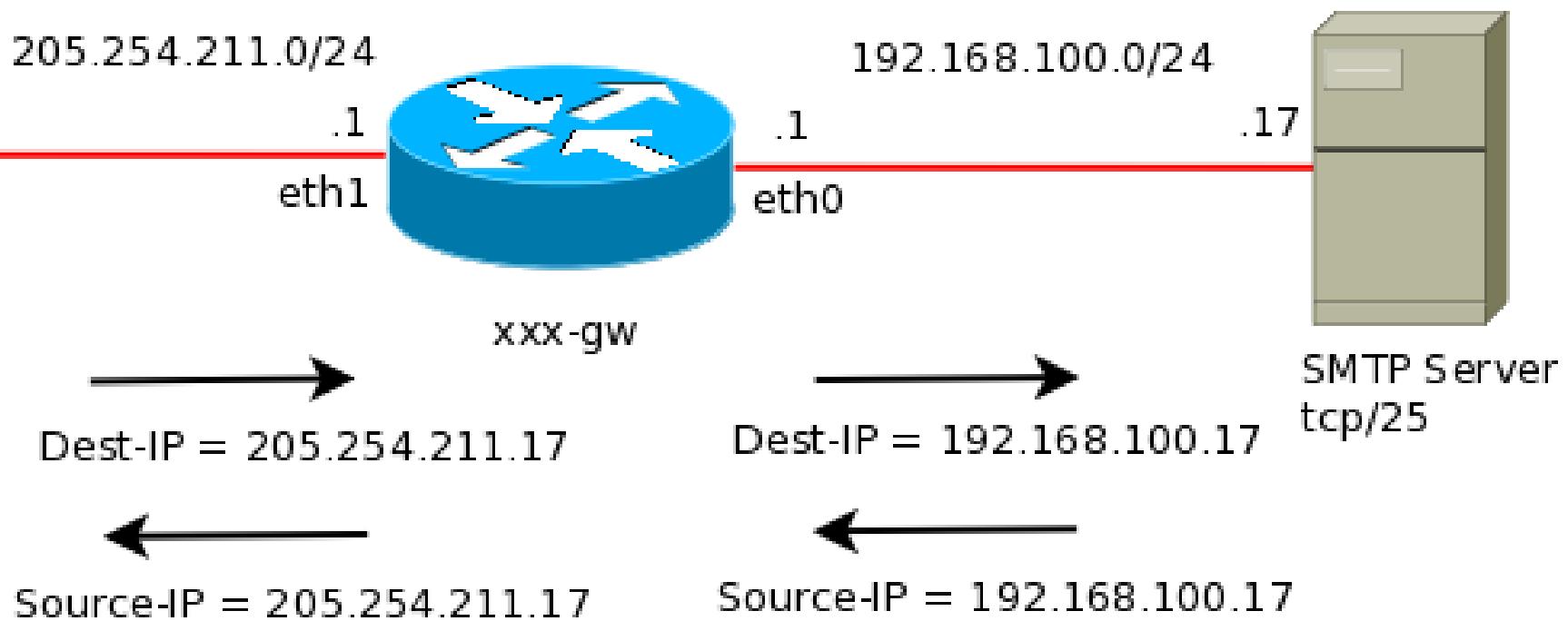
- **входящи** пакети - **destination address**:

```
[root@xxx-gw] # ip route add nat  
205.254.211.17 via 192.168.100.17
```

- **изходящи** пакети - **source address**:

```
[root@xxx-gw] # ip rule add nat  
205.254.211.17 from 192.168.100.17
```

Stateless NAT



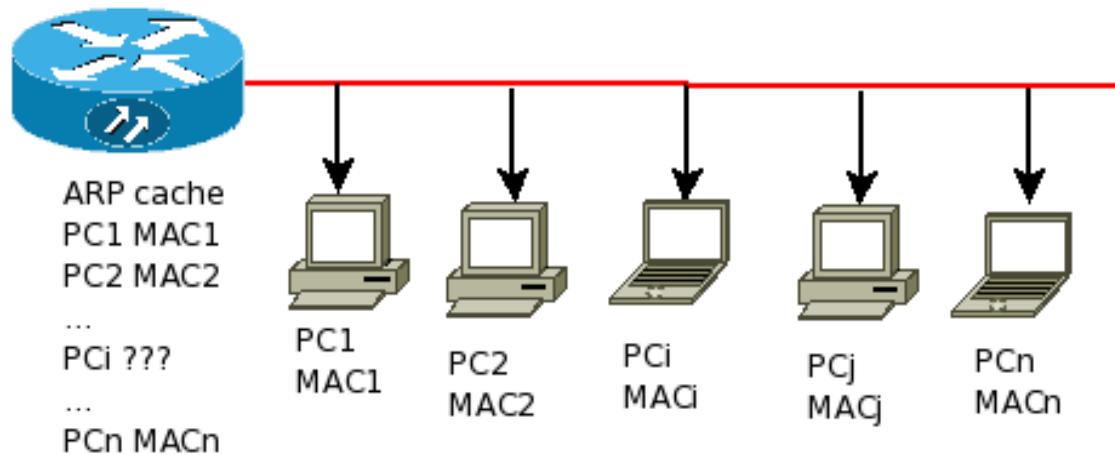
ARP (Address Resolution Protocol)

За глобална адресация в Internet се използват 32-битови IP-адреси.

В същото време хостовете, свързани към локална мрежа Ethernet, притежават уникални 48-битови MAC (физически) адреси.

При опаковането в Ethernet кадър на IP пакет, който се отправя към крайна дестинация, например, IP адресът на хоста-получател е известен, но в полето “адрес на получателя” на Ethernet кадъра трябва да се запише Ethernet адреса на съответния хост. Иначе пакетът няма да пристигне.

ARP



За установяване на съответствието между **IP** адреса и **Ethernet** адреса на хостовете в локалната мрежа се използва протокол за право преобразуване на адресите **ARP** (**address resolution protocol**).

ARP cache

```
[root@shuttle ~]# arp -e
```

Address	Hwtype	Hwaddress	Flags	Mask	Iface
loz-gw.uni-sofia.bg	ether	00:0D:56:B9:75:6D	C		eth0

```
[stefan@laptop ~]$ arp -e
```

Address	HWtype	Hwaddress	Flags	Mask	Iface
192.168.0.1	ether	00:22:6b:06:d5:ad	C		wlan0

Complete entry - **C** flag.

Permanent entries - **M** flag.

Published entries - **P** flag.

Как работи ARP

Когато даден хост трябва да изпрати пакет (дейтаграма) към машина от локалната мрежа, чийто IP адрес е известен, но не е известен Ethernet адреса, мрежовият слой разпространява в локалната мрежа ARP **пакет-заявка**.

Този пакет-заявка е от тип **broadcast**, т.е. предава се до всички машини. В полетата “Ethernet адрес на подателя” и “IP адрес на подателя” (т.е **Source IP, MAC**) са записани съответните адреси на хоста, който изпраща ARP заявката.

ARP пакет

+	Bits 0 - 7	8 - 15	16 - 31
0	Hardware type (HTYPE)		Protocol type (PTYPE)
32	Hardware length (HLEN)	Protocol length (PLEN)	Operation (OPER)
64	Sender hardware address (SHA) (first 32 bits)		
96	Sender hardware address (SHA) (last 16 bits)		Sender protocol address (SPA) (first 16 bits)
128	Sender protocol address (SPA) (last 16 bits)		Target hardware address (THA) (first 16 bits)
160	Target hardware address (THA) (last 32 bits)		
192	Target protocol address (TPA)		

Как работи ARP

В полето “Данни” е записано ARP съобщение от вида “**who is X.X.X.X tell Y.Y.Y.Y**”, където X.X.X.X и Y.Y.Y.Y са IP адреси съответно на получателя и на подателя.

Всички машини от локалната мрежа игнорират заявката с изключение на хоста, чийто адрес съвпада с **X.X.X.X**.

Хост **X.X.X.X** изпраща **ARP пакет-отговор** само на подателя, тъй като вече знае неговия Ethernet адрес от получената заявка.

Как работи ARP

В полето “Данни” на **пакета-отговор** е записано ARP съобщение от вида “**X.X.X.X is hh:hh:hh:hh:hh:hh**”, където hh:hh:hh:hh:hh:hh е Ethernet адреса (в 16-ен код) на хоста, изпращащ пакета-отговор.

Обикновено хоста, който изпраща ARP заявката, запомня (кешира) получените 48-битови Ethernet адреси, за да могат да се използват при следващо предаване.

Как работи ARP

При определяне на Ethernet адреса на получателя на даден пакет първо се проверява дали този адрес не е вече кеширан

Ако не е, се изпраща ARP заявка. Хостът може да използва и адреси, записани в конфигурационен файл.

Освен това всеки хост при първоначалното си стартиране уведомява чрез broadcast съобщение от вида “I am X.X.X.X and my Ethernet address is hh:hh:hh:hh:hh”, X.X.X.X и hh:hh:hh:hh:hh са съответно IP адреса и Ethernet адреса.

Как работи ARP

Всички останали хостове в локалната мрежа ще запишат тази информация в своите кешове.

Чрез ARP могат да се определят физическите адреси само на хостове, които са включени в локалната мрежа и имат IP адреси от IP мрежата (подмрежата) на изпраща.

Пакетите, чийто получател е хост от друга IP мрежа (подмрежа), се изпращат към маршрутизатора, включен в локалната мрежа.

Как работи ARP

Неговият Ethernet адрес се получава чрез ARP заявка, ако не е кеширан.

Този маршрутизатор избира маршрут и препраща пакета към неговия получател.

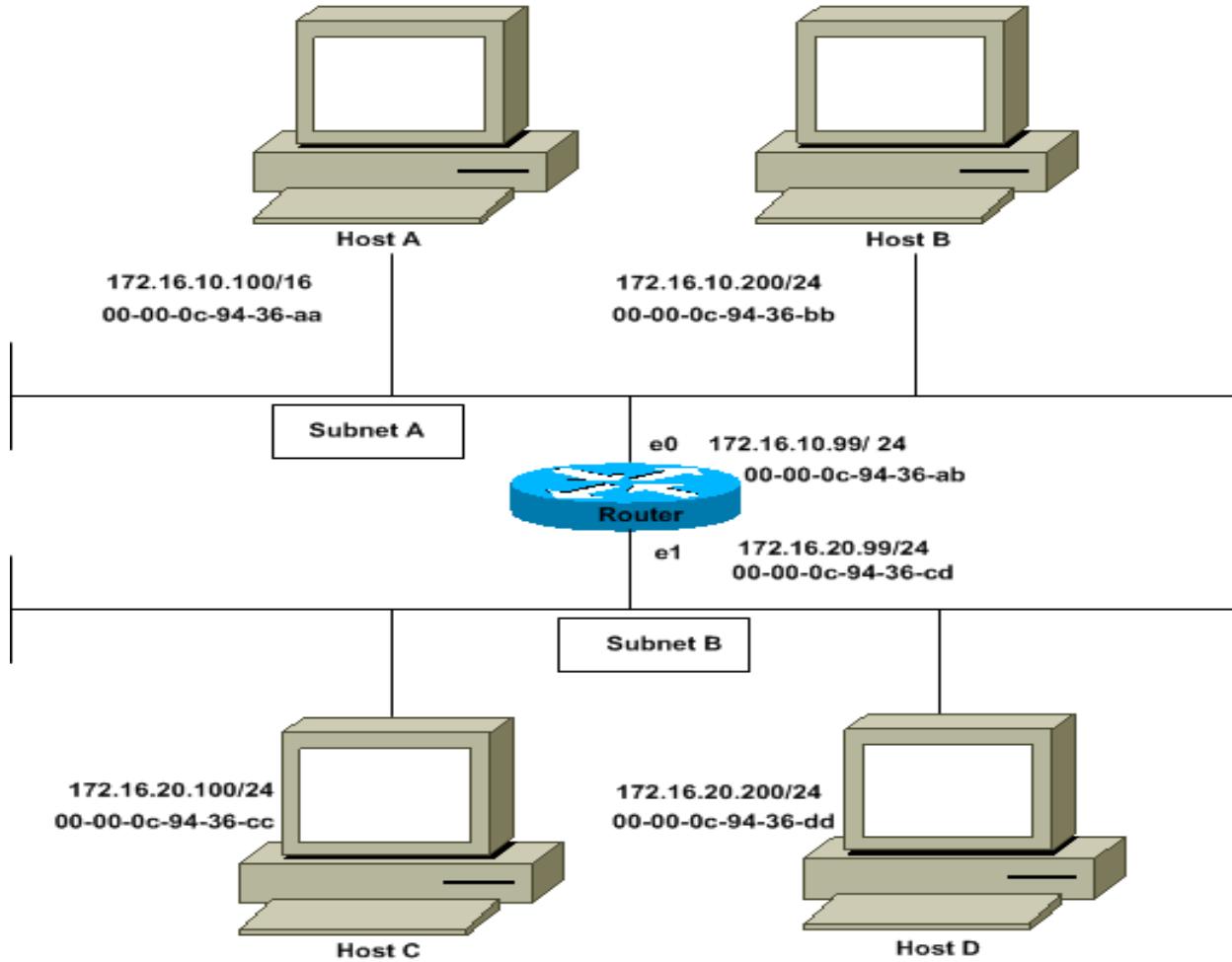
Proxy ARP

Proxy ARP е метод, чрез който хост отговаря на ARP заявки за IP адреси, които не са конфигурирани на интерфейса му.

“Проксирането” на ARP заявки за сметка на друг хост препраща целия LAN трафик, предназначен за този хост, към прокси.

Прихванатият трафик се “превключва” към другия интерфейс на проксито (**обикновено маршрутизатор**) или се препраща през серийна връзка (напр., **dialup** или **VPN тунел**), за да достигне хоста получател.

Proxy ARP



Reverse ARP

Reverse Address Resolution Protocol (**RARP**) - RFC 903, е излизащ от употреба протокол.

Клиентски компютър – хост, заявява (broadcast-ва) IPv4 адреса си от мрежата, като за целта подава MAC адреса си.

Заменен е от Bootstrap Protocol (BOOTP) и модерния Dynamic Host Configuration Protocol (DHCP), които са с по-богати характеристики от RARP.

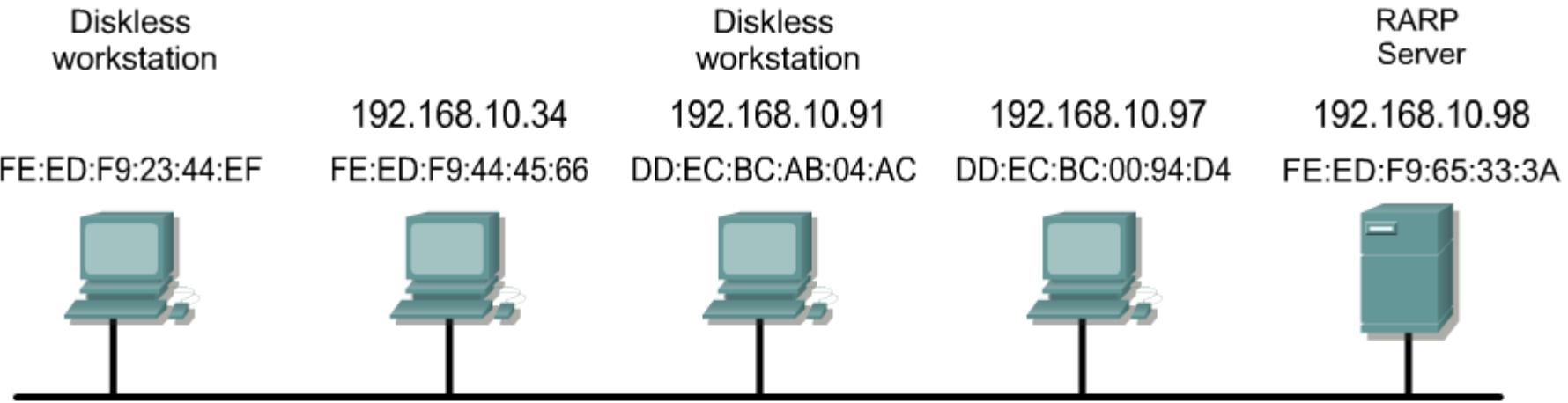
RARP

IP адресът на хоста е записан в конфигурационен файл, който се намира на твърдия диск на машина (**RARP сървър**) в мрежата.

Този сървър съхранява съответствието между Ethernet и IP адреси на станциите в мрежата.

При първоначално зареждане на операционната система файлът се прочита от твърдия диск на сървъра и хостът научава своя IP адрес.

Този протокол се прилага при машини, които не притежават собствени твърди дискове (**diskless**).



Frame header	2	0800 ₁₆
Source MAC	48	32
FE:ED:F9:65:33:3A		FE:ED:F9:23
Destination MAC	44:EF	192.168
FE:ED:F9:23:44:EF	10.36	FE:ED
Field Type		F9:65:33:3A
0X8035 (Ethernet)		192.168.10.98

DHCP

Dynamic Host Configuration Protocol (DHCP) се използва за автоматично (**динамично**) конфигуриране на свързаността на даден хост към IP мрежата.

За разлика от твърдото (**ръчно** или **статично**) конфигуриране.

DHCP “раздава” не само IP адреси, но и всички други параметри на връзката – **Default Gateway** (изхода навън по подразбиране, DNS сървър/и, име на домейн и т.н.)

DHCP улеснява процеса на добавяне на машина в мрежата, местене и т.н.

DHCP

Днешната версия на DHCP за IPv4 е стандартизирана в RFC 2131 (1997 г.).

DHCP за IPv6 (DHCPv6) е дефинирана в RFC 3315 (2003 г.), обновявана с девет RFC-та до 2015 г.

DHCP е протокол от типа клиент-сървър.

DHCP-конфигуриран клиент веднага след включването се свързва към мрежата и изпраща broadcast заявка, искайки необходимата информация от DHCP сървър.

DHCP

DHCP сървърът разполага с **пул от IP адреси** и необходимата информация за **конфигуриране на клиента**: GW, SM, домейн, DNS сървър/и, NTP, WINS и др.

При получаване на валидна заявка сървърът присвоява **IP адрес**, време за отдаване на адреса (**lease time** – през което алокацията е валидна) и др. (гореспоменати) IP конфиг. параметри.

Раздаване на IP адреси (allocation)

DHCP сървърите раздават (алокират) IP адреси по 3 начина:

Динамична алокация: Обхват от IP адреси се дават за DHCP и всеки клиент си заявява IP адрес от DHCP сървъра при включване. Времето на отдаване (lease) е дефинирано, така че сървърът може да преотдаде адреса на друга машина.

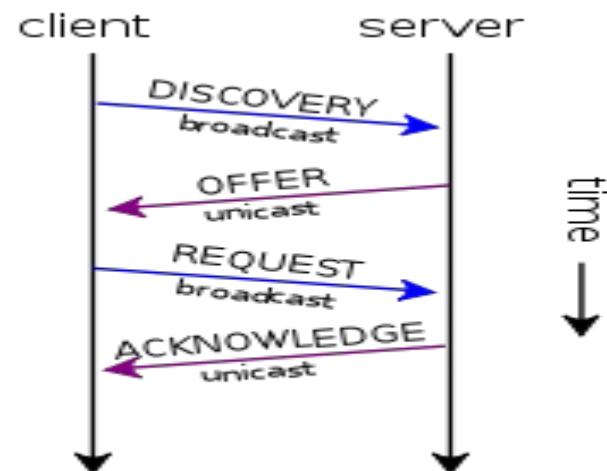
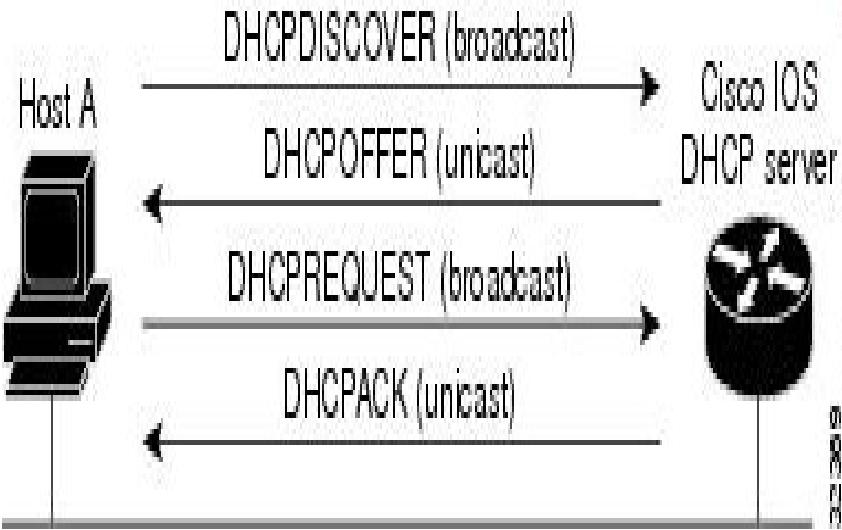
Автоматична алокация: Подобн е на динамичната, но даден IP адрес е резервиран за даден клиент.

Раздаване на IP адреси (allocation)

Статична алокация: DHCP раздава IP адреси на базата на таблица **MAC адрес/IP адрес**, ръчно попълнена от администратора. Само клиенти, чиито MAC адреси присъстват в тази таблица, ще получат IP адреси.

Нарича се още *Static DHCP Assignment* (от DD-WRT, Linux-базиран фърмуер, Linksys), *fixed-address* (от *dhcpd*), *DHCP reservation* или *Static DHCP* (от Cisco/Linksys) или *IP reservation*, *MAC/IP binding* (други производителни).

Фази на DHCP процеса



DHCP discovery

DHCP сървър:

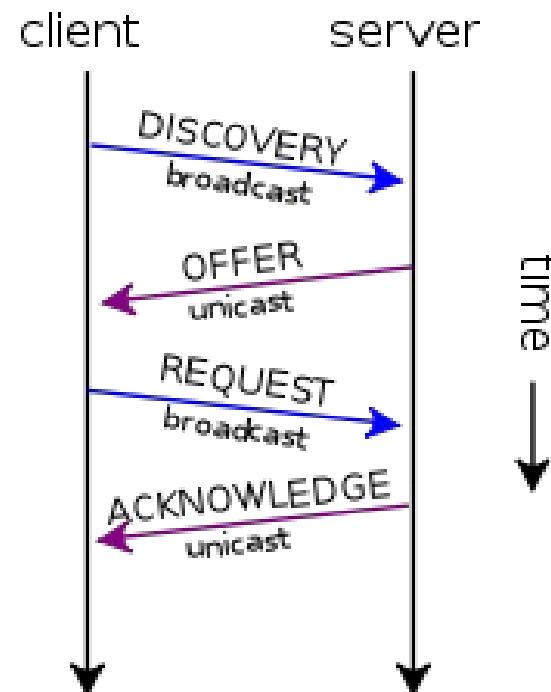
62.44.109.140

DHCP пул: 62.44.109.141 –
254/25

Последен свободен адрес:
62.44.109.151

Транзакция 654:

UDP Src=0.0.0.0 sPort=68
Dest=255.255.255.255
dPort=67



DHCP offer

UDP Src=62.44.109.140 sPort=67
Dest=255.255.255.255 dPort=68

Offer IP: 62.44.109.151

ID: 654

Lease Time: 3600 s

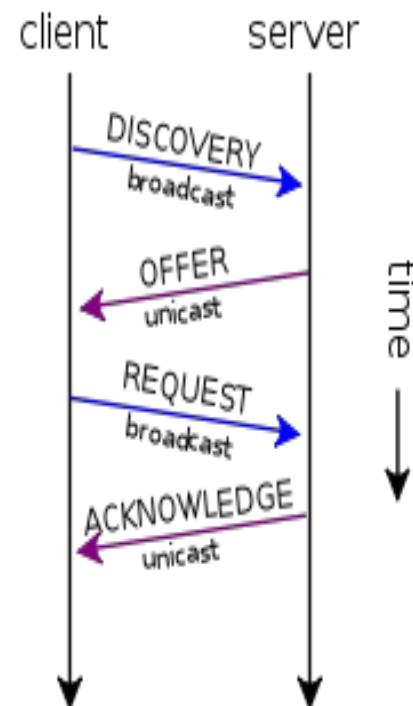
SM: 255.255.255.0

DHCP server: 62.44.109.140

Router (GW): 62.44.109.193

DNS: 62.44.109.1, 62.44.96.1

Domain: ucc.uni-sofia.bg



DHCP request

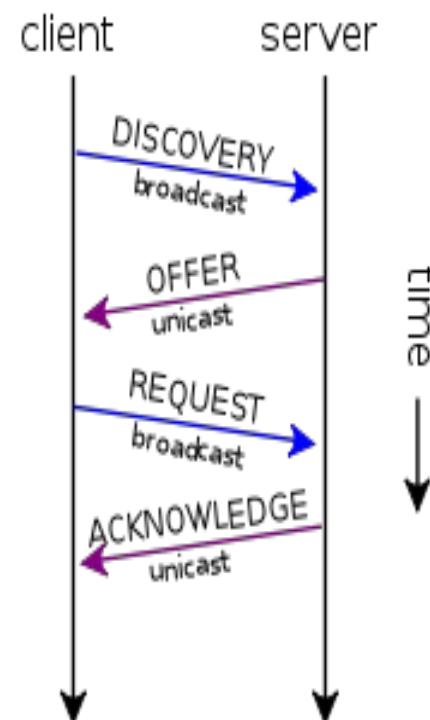
UDP Src=0.0.0.0 sPort=68
Dest=255.255.255.255
dPort=67

Requested IP:
62.44.109.151

ID: 655

DHCP server: 62.44.109.140

Lease Time: 3600 s



DHCP acknowledgement

UDP Src= 62.44.109.140 67

Dest=255.255.255.255 68

Requested IP: 62.44.109.151

ID: 655

Lease Time: 3600 s

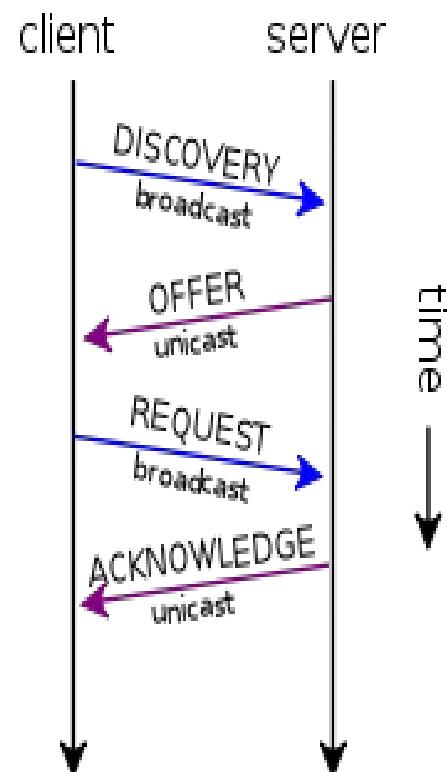
SM: 255.255.255.0

DHCP server: 62.44.109.140

Router (GW): 62.44.109.193

DNS: 62.44.109.1, 62.44.96.1

Domain: ucc.uni-sofia.bg

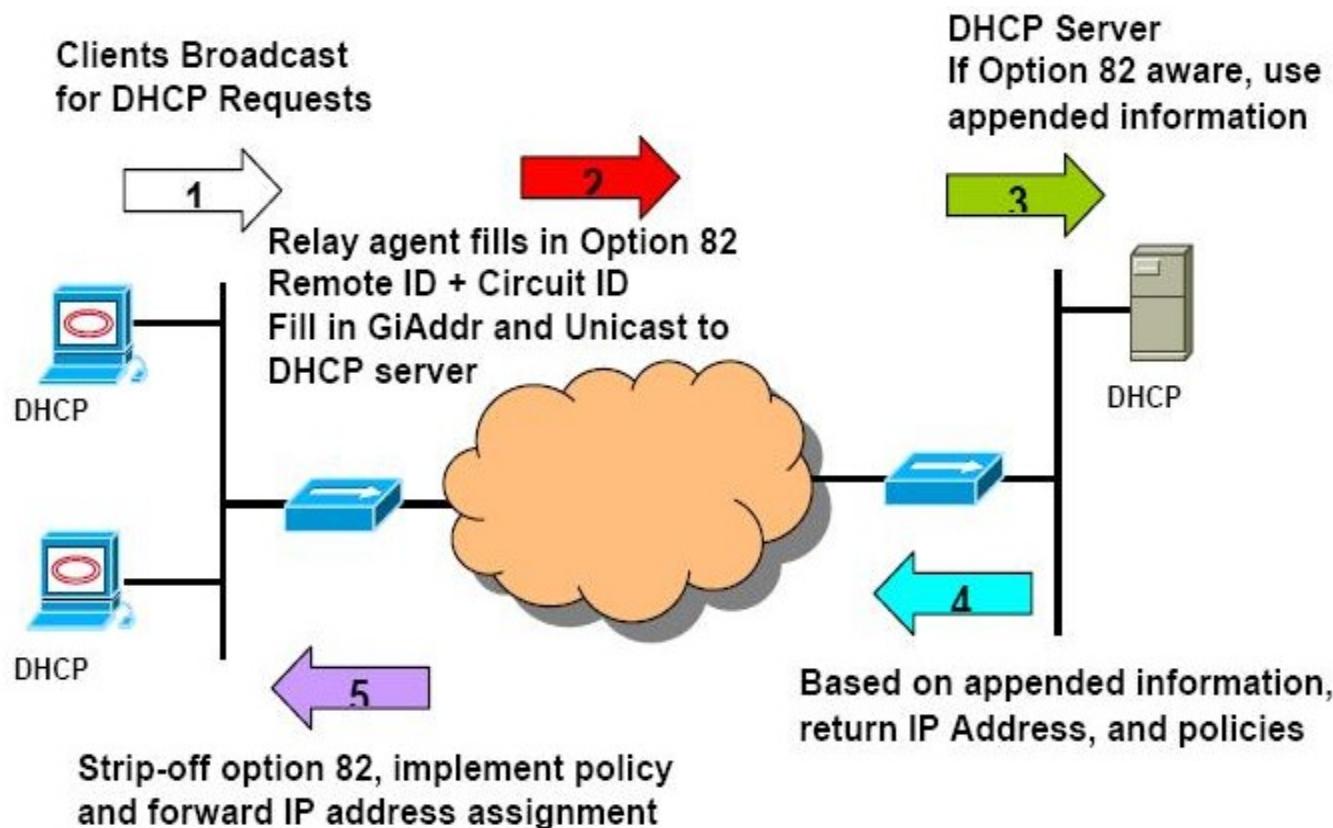


DHCP Relay

Желателно е DHCP сървър и клиенти да са **на един и същ сегмент (Ethernet и IP)**.

Когато това не е възможно, прилага се **DHCP Relay**.

DHCP Relay



DHCP Linux сървър: vim /etc/dhcpd.conf

```
subnet 172.18.0.0 netmask 255.255.254.0 {
```

```
# --- default gateway
```

```
    option routers           172.18.0.1;
```

```
    option subnet-mask       255.255.254.0;
```

```
    option nis-domain        "uni-sofia.bg";
```

```
    option domain-name       "conf.uni-sofia.bg";
```

```
    option domain-name-servers  
62.44.96.7,62.44.96.1;
```

vim /etc/dhcpd.conf (cont'd)

```
option time-offset          7200; # East European  
Standard Time  
option ntp-servers         62.44.96.44;  
# option ntp-servers        62.44.96.7, 62.44.96.1;  
# option netbios-name-servers 192.168.1.1;  
# --- Selects point-to-point node (default is hybrid). Don't  
# change this unless you understand Netbios very well  
# option netbios-node-type 2;
```

vim /etc/dhcpd.conf (cont'd)

```
host vlado {  
    option host-name "vladi";  
    hardware ethernet 00:0a:e4:b1:6e:52;  
    fixed-address 172.18.0.101;  
}  
  
range 172.18.0.2 172.18.1.254;  
}
```

ICMP

Internet Control Message Protocol (ICMP) е част от протокола IP.

Използва се от мрежовите ОС главно за откриване на грешки по мрежата и изпращане на съобщения за това.

ICMP за IPv4 е известени като ICMPv4. IPv6 има подобен, ICMPv6.

Дефиниран е в RFC 792, обновявана с 4 RFC-та до 2013 г.

IP опакова ICMP съобщението с нов IP хедър, за да го върне на изпращаца и го предава като обикновен пакет.

ICMP

Например, всеки възел в мрежата (рутер, GW), която направлява IP пакета, трябва да декрементира TTL полето на IP хедъра с 1.

Ако TTL достигне 0, ICMP съобщение **Time to live exceeded in transit message** се изпраща към източника.

ICMP съобщенията се съдържат в стандартни IP пакети, но се обработват като специални случаи.

Много мрежови средства за диагностика се базират на ICMP.

ICMP

Командата traceroute изпраща UDP дейтаграми с определени IP TTL полета и очаква ICMP Time to live exceeded in transit, също изпраща "Destination unreachable" в отговор.

Средството ping се реализира с ICMP "Echo request" и "Echo reply" съобщения.

Структура на ICMP пакет

	Bit 0 - 7	Bit 8 - 15	Bit 16 - 23	Bit 24 - 31		
IP Header (160 bits OR 20 Bytes)	Version/IHL	Type of service	Length			
	Identification			flags and offset		
	Time To Live(TTL)	Protocol	Checksum			
	Source IP address					
	Destination IP address					
	Type of message	Code	Checksum			
ICMP Payload (64+ bits OR 8+ Bytes)	Quench					
	Data (optional)					

Структура на ICMP пакет

Тип – вж. по-долу.

Код - вж. по-долу.

Checksum – контролна сума за ICMP header+data.

Данни

Linux ping 56 байта (октета) плюс 8 за хедър.

Windows "ping.exe" - 32 + 8 хедър.

ICMP съобщения

Type	Code	Description
0 - Echo Reply	0	Echo reply (used to ping)
1 and 2		<i>Reserved</i>
3 - Destination Unreachable	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation required, and DF flag set
	5	Source route failed
	6	Destination network unknown
	7	Destination host unknown
	8	Source host isolated
	9	Network administratively prohibited
	10	Host administratively prohibited
	11	Network unreachable for TOS
	12	Host unreachable for TOS
	13	Communication administratively prohibited
4 - Source Quench	0	Source quench (congestion control)

ICMP съобщения

	0	Redirect Datagram for the Network
5 - Redirect Message	1	Redirect Datagram for the Host
	2	Redirect Datagram for the TOS & network
	3	Redirect Datagram for the TOS & host
6		Alternate Host Address
7		<i>Reserved</i>
8 - Echo Request	0	Echo request
9 - Router Advertisement	0	Router Advertisement
10 - Router Solicitation	0	Router discovery/selection/solicitation
11 - Time Exceeded	0	TTL expired in transit
	1	Fragment reassembly time exceeded
	0	Pointer indicates the error
12 - Parameter Problem: Bad IP header	1	Missing a required option
	2	Bad length
13 - Timestamp	0	Timestamp
14 - Timestamp Reply	0	Timestamp reply
15 - Information Request	0	Information Request
16 - Information Reply	0	Information Reply
17 - Address Mask Request	0	Address Mask Request
18 - Address Mask Reply	0	Address Mask Reply
19		<i>Reserved for security</i>
20 through 29		<i>Reserved for robustness experiment</i>
30 - Traceroute	0	Information Request

ping

Ping е инструмент за тестване на достъпимостта на даден хост по IP мрежата.

Изпраща ICMP “echo request” пакети към целта и очаква ICMP “echo response” отговори.

Ping измерва round-trip time и регистрира загуби на пакети.

Накрая разпечатва статистика: минималното, средното, максималното и (в някои версии) стандартното отклонение от round trip time.

Mike Muuss е написал програмата през декември, 1983. Нарекъл я на звуковите импулси, издавани от локатор в подводница.

Пример на ping

```
C:\Users>ping -l 1473 www.google.com

Pinging www.l.google.com [74.125.47.99] with 1473 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 74.125.47.99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users>ping -l 1472 www.google.com

Pinging www.l.google.com [74.125.47.103] with 1472 bytes of data:

Reply from 74.125.47.103: bytes=56 (sent 1472) time=50ms TTL=240
Reply from 74.125.47.103: bytes=56 (sent 1472) time=48ms TTL=240
Reply from 74.125.47.103: bytes=56 (sent 1472) time=58ms TTL=240
Reply from 74.125.47.103: bytes=56 (sent 1472) time=58ms TTL=240

Ping statistics for 74.125.47.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 48ms, Maximum = 58ms, Average = 53ms
```

traceroute

traceroute е инструмент за определяне на маршрута на пакетите по мрежата. За IPv6 вариантът е **traceroute6**.

traceroute го има за всички Unix-подобни ОС. Подобна функционалност имат **tracepath** на модерните Linux дистрибуции и **tracert** в Microsoft Windows.

Traceroute инкрементира с 1 "time-to-live" (TTL) на всяка следваща "тройка" от изпратени пакети. Първата тройка е с TTL=1. Следващата е с TTL = 2 и т.н. Минавайки през хост, TTL на пакета се декрементира с 1 и се отправя към следващия хост. Хостът изхвърля пристигнал пакет с TTL = 1 и изпраща на подателя ICMP time exceeded (type 11).

traceroute използва тези връщани пакети, за да създаде списък от хостове, през които пакетът е минал по маршрута до дестинацията.

traceroute

Трите timestamp за всеки хост по пътя са закъснението - delay (latency) в ms за всеки пакет от тройката.

Ако пакетът не се върне в рамките на очаквания timeout, разпечатва се звездичка (asterisk).

Traceroute може и да не изброя реалните хостове. Само показва, че първият хост е на един хоп, вторият – на два, и т.н.

Просто IP не гарантира, че всички пакети ще минат по един и същ път.

Ако хост на хоп N не отговори, този хоп ще бъде пропуснат в разпечатката.

Traceroute и tcptraceroute

В съвременните Unix и Linux-базирани ОС traceroute използва по подразбиране UDP дейтаграми с номера на дестинационни портове 33434 - 33534. Но има опция да се използва ICMP echo request (type 8) както в Windows tracert.

Tcptraceroute прави същото като traceroute.

tcptraceroute изпраща TCP SYN пакети вместо UDP или ICMP ЕCHO пакети, така че по-трудно може да бъде блокиран.

traceroute

```
[root@shuttle ~]# traceroute ripe.net
traceroute to ripe.net (193.0.19.25), 30 hops max, 40 byte packets
 1  ucc-gw.ucc.uni-sofia.bg (62.44.109.5)  0.227 ms  0.237 ms  0.252 ms
 2  border-main.uni-sofia.bg (62.44.127.21)  0.590 ms  0.584 ms  0.567 ms
 3  core-su.lines.acad.bg (194.141.252.21)  1.179 ms  1.311 ms  1.448 ms
 4  istf.rti.sof.geant2.net (62.40.125.141)  1.266 ms  1.265 ms  1.232 ms
 5  so-2-3-0.rti.bud.hu.geant2.net (62.40.112.202)  15.477 ms  15.490 ms  15.468
ms
 6  bpt-b2-link.telia.net (80.239.134.1)  15.437 ms  14.885 ms  14.944 ms
 7  hbg-bb1-link.telia.net (80.91.250.130)  36.623 ms  36.597 ms  36.586 ms
 8  adm-bb1-link.telia.net (80.91.252.40)  46.064 ms adm-bb1-link.telia.net (80.
91.253.45)  44.637 ms  44.634 ms
 9  adm-b1-link.telia.net (80.91.254.221)  44.634 ms adm-b2-link.telia.net (80.9
1.254.133)  44.818 ms  44.821 ms
10  * gw.amsix.nikrtr.ripe.net (195.69.144.68)  468.713 ms *
11  gw.transit.nsrp.ripe.net (193.0.3.1)  40.922 ms  42.555 ms  40.804 ms
12  aquila.ripe.net (193.0.19.25)  43.185 ms  41.560 ms  43.088 ms
```

arping

arping е подобна на ping, но използва ARP вместо ICMP.

Затова, arping е използваема само в локалната мрежа

В някои случаи отговорът може да идва от междинна система - proxy ARP (напр. рутер).

arping

```
[root@shuttle ~]# arping 62.44.109.1
ARPING 62.44.109.1 from 62.44.109.11 eth0
Unicast reply from 62.44.109.1 [00:40:95:30:13:ED] 0.638ms
Unicast reply from 62.44.109.1 [00:40:95:30:13:ED] 0.608ms
Unicast reply from 62.44.109.1 [00:40:95:30:13:ED] 0.604ms
Unicast reply from 62.44.109.1 [00:40:95:30:13:ED] 0.610ms
Unicast reply from 62.44.109.1 [00:40:95:30:13:ED] 0.594ms
Unicast reply from 62.44.109.1 [00:40:95:30:13:ED] 0.591ms
Unicast reply from 62.44.109.1 [00:40:95:30:13:ED] 0.585ms
Unicast reply from 62.44.109.1 [00:40:95:30:13:ED] 0.591ms
Sent 8 probes (1 broadcast(s))
Received 8 response(s)
```

Мрежов протокол IPv6

Какво ще научим?

- Защо се налага преход към IPv6
- Предимства на IPv6 пред IPv4 освен дължината
- Формат на IPv6 адрес. Префикси.
- Типове IPv6 адреси. Защо няма бродкаст.
- ICMPv6 вместо ARP. Автоконфигуриране.
- Преход от IPv4 към IPv6

Предпоставки за прехода

Преходът към IPv6 е **неизбежен**.

IPv4 адресите са **изчерпани**.

IPv6 **не е обратно съвместим** с IPv4,
необходими са промени в мрежови устройства
и услуги.

Трудности при **едновременна работа** на IPv4 и
IPv6, която е наложителна в дългия преходен
период.

Подобрения в IPv6

Според RFC 4291: адресното пространство от 32-битово става 128-битово: 2^{32} (4.3×10^9) с/у 2^{128} (3.4×10^{38}).

Автоконфигуриране. RFC 4862 дефинира автоматично (plug-and-play) присвояване на адрес без помощта на DHCP сървър като в IPv4.

Header

В IPv6 е по-опростено от IPv4; с фиксирана дължина 40 байта (RFC 2460):

- 2 * 16-byte IPv6 адреса;
- 8 байта друга информация.

По-бързо и лесно обработване на пакетите.

Структура на заглавието

Version (4)	Traffic Class (8)	Flow Label (20 bits)		
Payload length (16)		Next Header (8)	Hop Limit (8)	
Source Address (128 bits)				
Destination Address (128 bits)				

traffic class (заменя IPv4 ToS);

flow label (ново QoS management);

payload length (до 64KB);

next header (заменя IPv4 protocol);

hop limit (заменя IPv4 TTL).

Поддържа IPsec

IP security (IPsec) съдържа протоколи за аутентикация на изпращаща и гарантиране на данните в IP комуникациите:

- Encapsulating Security Payload (ESP);
- Authentication Header (AH);
- Internet Key Exchange (IKE).

IPsec е част от IPv6.

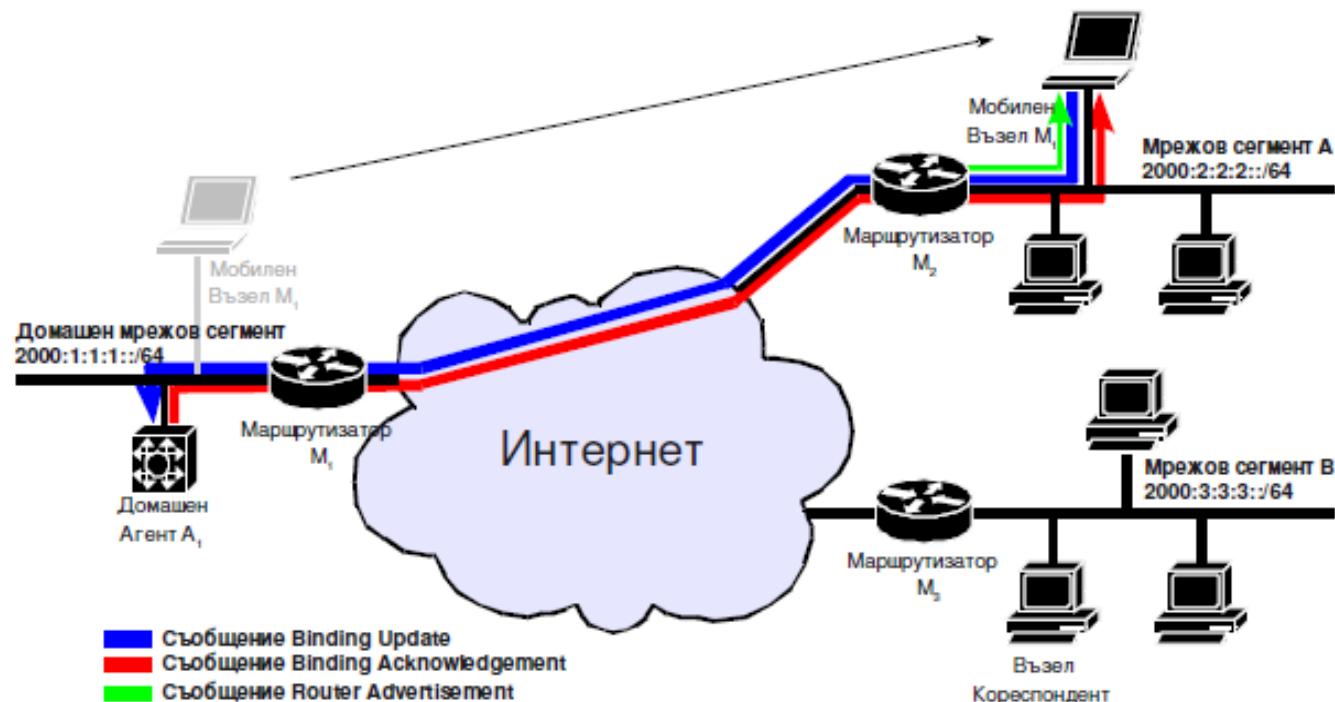
Задължителен е IPsec за защита на Mobile IPv6 и OSPFv3.

Mobile IPv6

MIPv6 поддържа roaming за мобилни възли (RFC 3775).

MIPv6 използва **Neighbor Discovery** (RFC 4861), за да реши проблема с прехвърлянето (**handover**) на мрежов слой и оптимизация на маршрута (RFC 4449).

Mobile IPv6



*Фигура 2.3: Домашният агент A_1 , получава СоA адреса на преместилия се в сегмент A
мобилния възел M_1 , чрез съобщение BU и в отговор изпраща съобщение BAC*

Quality of Service (QoS)

IP третира всички пакети еднакво – best effort.

TCP (Transmission Control Protocol) гарантира доставянето, но не контролира закъснение, честотна лента и т.п.

QoS – опции за въвеждане на политики и приоритети на трафика.

IPv4 и IPv6 сходни QoS възможности:
Differentiated Services и Integrated Services.

QoS

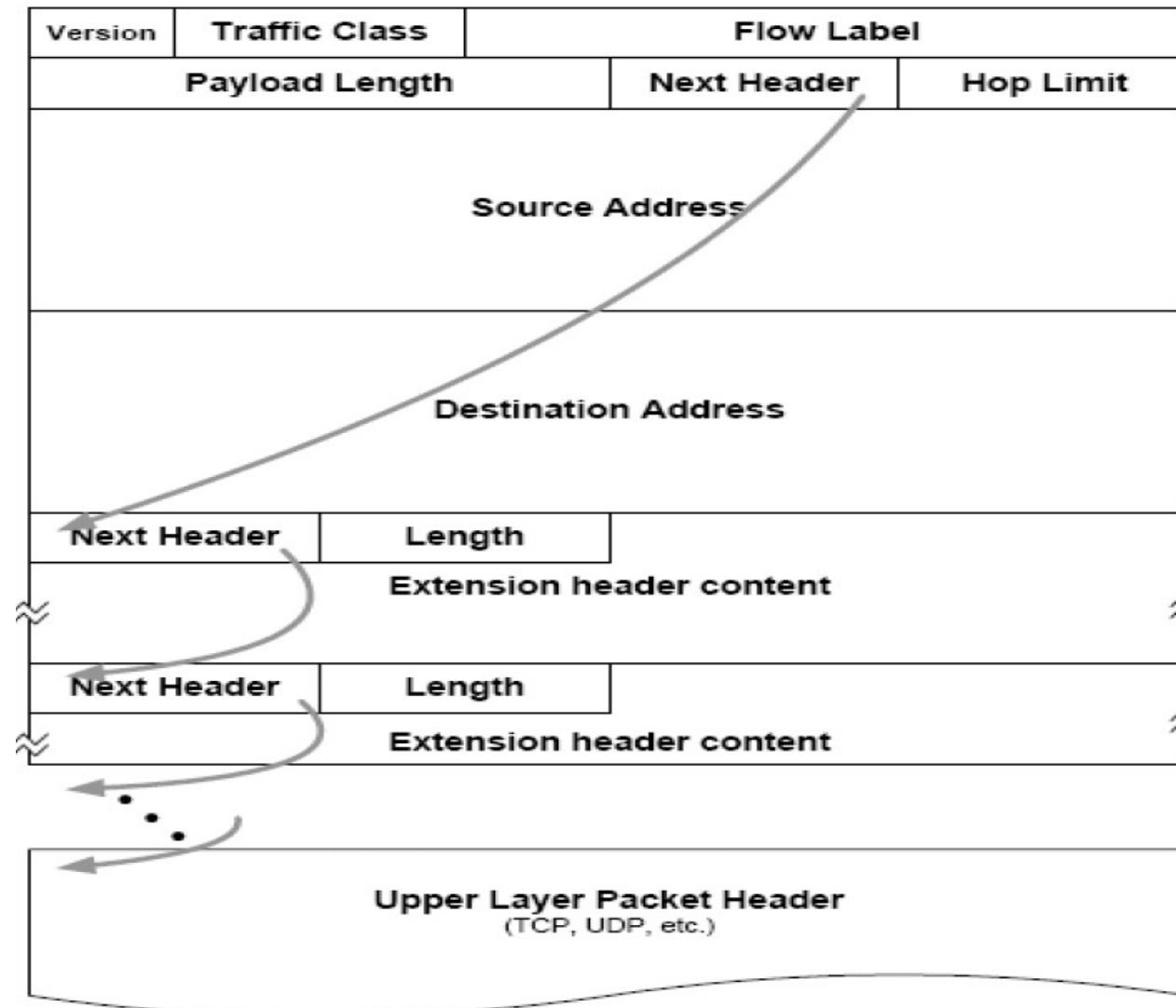
В IPv6 header има **две** полета за QoS:

- Traffic Class и
- Flow Label.

Traffic Class е разширено по-прецизно диференциране на различните типове трафик.

Новото Flow Label поле - съдържа етикет за идентифициране или приоритетизиране на определен поток от пакети като VoIP или видеоконференции, чувствителни към времето на доставяне.

IPv6 Extension Header



IPv6 Extension Header

Extension Header	Type	Remarks
Hop-by-hop Options	0	used for options that apply to intermediate routers
Routing	43	used for source routing
Fragment	44	processed only by the final recipient
Destination Options	60	used for options that apply only for the final recipient
Authentication header (AH)	51	used for IPsec integrity protection
Encapsulating Security Payload (ESP)	50	used for IPsec integrity and confidentiality protection
Mobility	135	used for managing mobile IPv6 bindings

Jumbograms

RFC 2675 дефинира IPv6 Hop-by-Hop Option - **jumbograms**, IPv6 пакет с 32-bit поле за данни (payload) $> 65\ 535$ октета.

Важи за IPv6 интерфейси, които могат да поемат кадри с такива дължини ($\geq 1\ \text{gbps}$).

16-бит поле Payload Length (в IPv6 Header) = 0

След това:

IPv6 Fragment Extension Header

В IPv6 фрагментирането на пакетите става още при източника.

В IPv4 рутерът фрагментира пакета, когато MTU на следващия канал е по-малък. Ако при дестинацията не се възстанови оригиналния пакет, сесията се разваля.

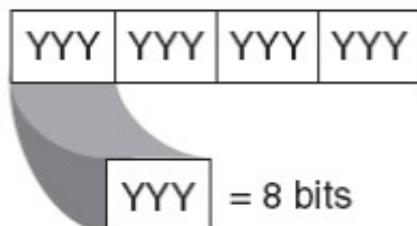
В IPv6 всеки хост използва **Path Maximum Transmission Unit (PMTU) Discovery**, за да научи размера на MTU по пътя, за да не се налага фрагментиране.

IPv4 vs. IPv6

Property	IPv4	IPv6
Address size and network size	32 bits, network size 8-30 bits	128 bits, network size 64 bits
Packet header size	20-60 bytes	40 bytes
Header-level extension	limited number of small IP options	unlimited number of IPv6 extension headers
Fragmentation	sender or any intermediate router allowed to fragment	only sender may fragment
Control protocols	mixture of non-IP (ARP), ICMP, and other protocols	all control protocols based on ICMPv6
Minimum allowed MTU	576 bytes	1280 bytes
Path MTU discovery	optional, not widely used	strongly recommended
Address assignment	usually one address per host	usually multiple addresses per interface
Address types	use of unicast, multicast, and broadcast address types	broadcast addressing no longer used, use of unicast, multicast and anycast address types
Address configuration	devices configured manually or with host configuration protocols like DHCP	devices configure themselves independently using stateless address autoconfiguration (SLAAC) or use DHCP

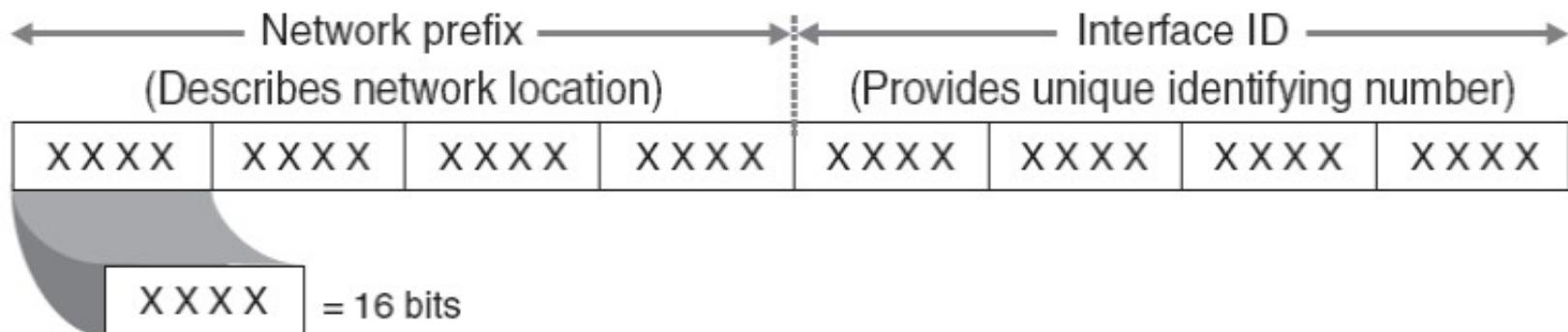
IPv4 vs. IPv6

32-bit IPv4 address



(Resulting in 4,294,967,296 unique IP addresses)

128-bit IPv6 address



(Resulting in 340,282,366,920,938,463,374,607,432,768,211,456 unique IP addresses)

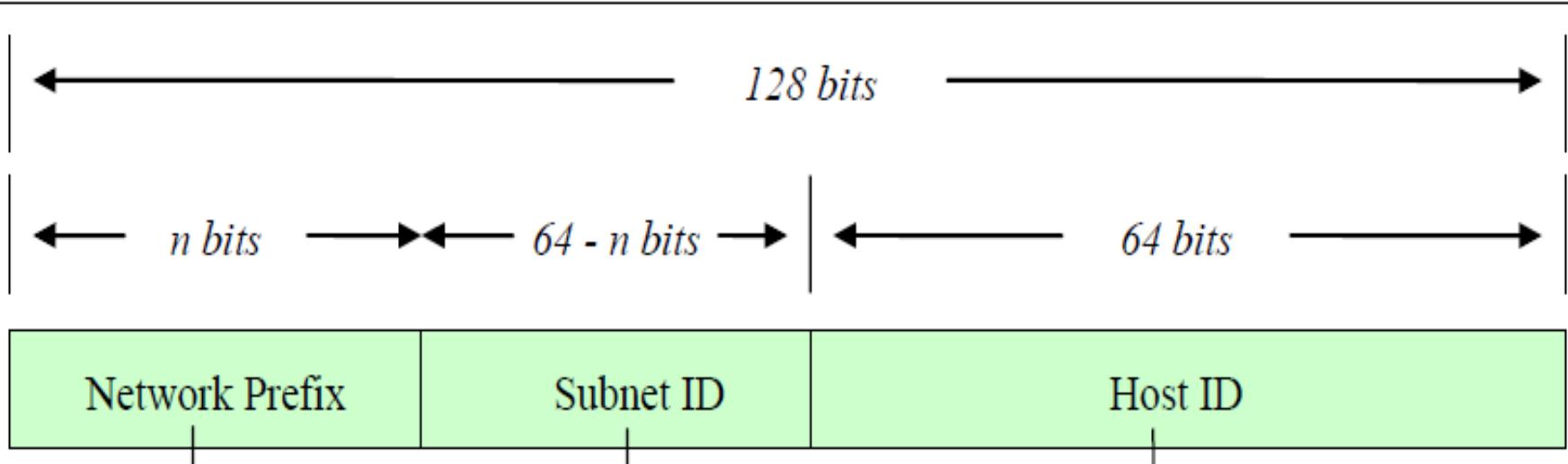
IPv6 адресиране

IPv6 адрес (пример):

2001:0db8:9095:02e5:0216:cbff:feb2:7474

8 групи с по **4** щестнадесетични числа

$$8 * 4 * 4 = 128$$



Формат на IPv6 адрес

Мрежовият префикс (**network prefix**) – идентифицира даден мрежов обект (напр. СУ, фирма и др.). Присвоява се от ISP (PA) или RIR (PI).

Идентификаторът на подмрежата (**subnet ID**) се присвоява от администратора на обекта. Един обект ≥ 1 subnet IDs. Определя на кой мрежов сегмент принадлежи даден хост.

host ID идентифицира конкретен възел в мрежата – конкретен негов интерфейс.

Префикси в IPv6

Мрежовият префикс (RFC 4291) е аналогичен на означението с “/” на SM в IPv4:

IPv6 address/prefix length

Например адрес с 32-bit мрежов префикс:

2001:0db8:9095:02e5:0216:cbff:feb2:7474/32

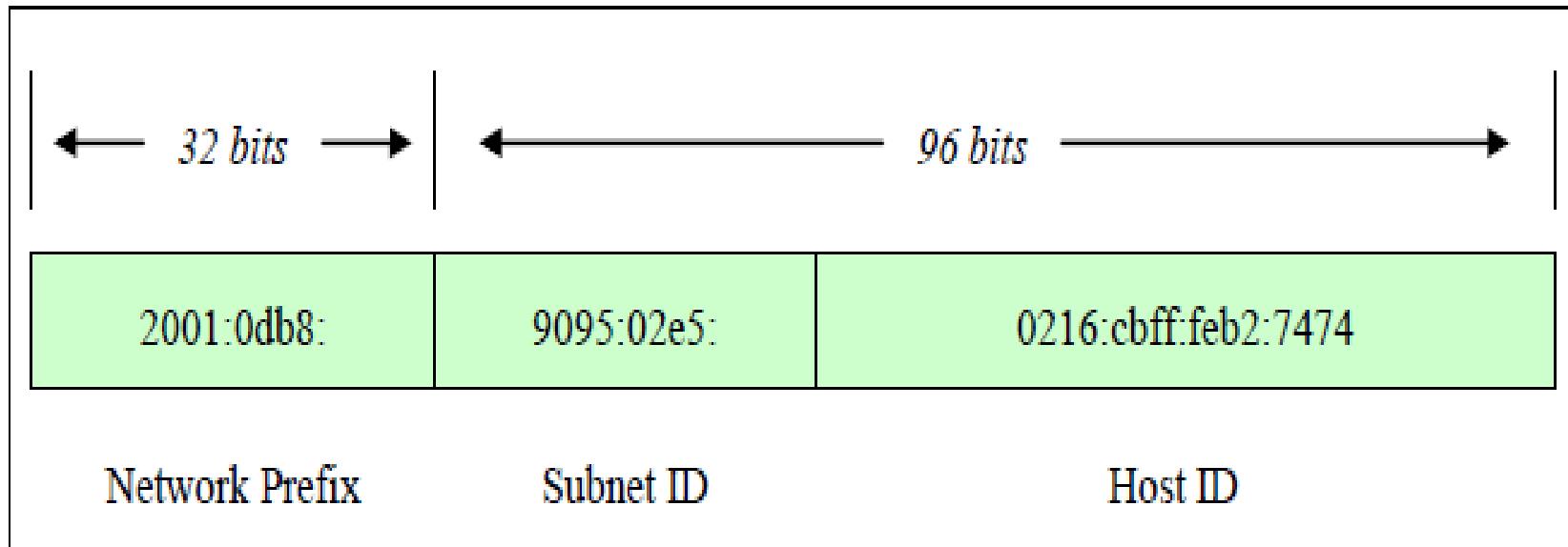
Алокация на IPv6 префикси

IPv6 (подобно на IPv4) се присвояват от RIRs и ISP.

Големите провайдери (LIRs) могат да получат префикс с минимална дължина 32 бита:

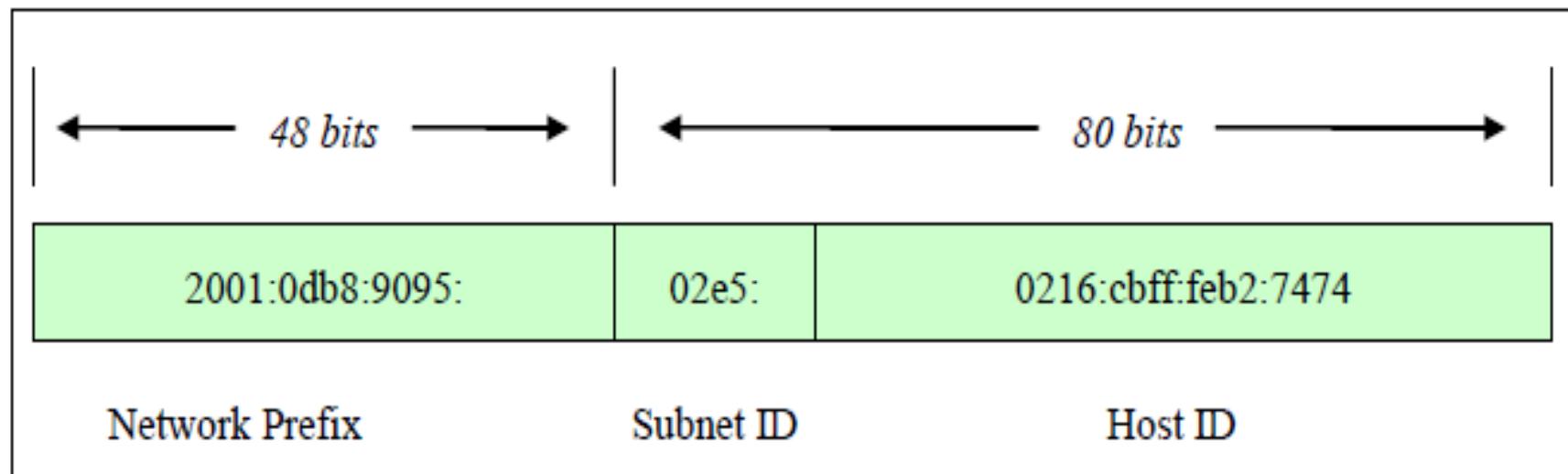
- най-старшите 32 бита са мрежовия префикс;
- останалите 96 бита са на разположение на администратора за раздаване на subnet ID-та и за host ID.

32-битов мрежов префикс

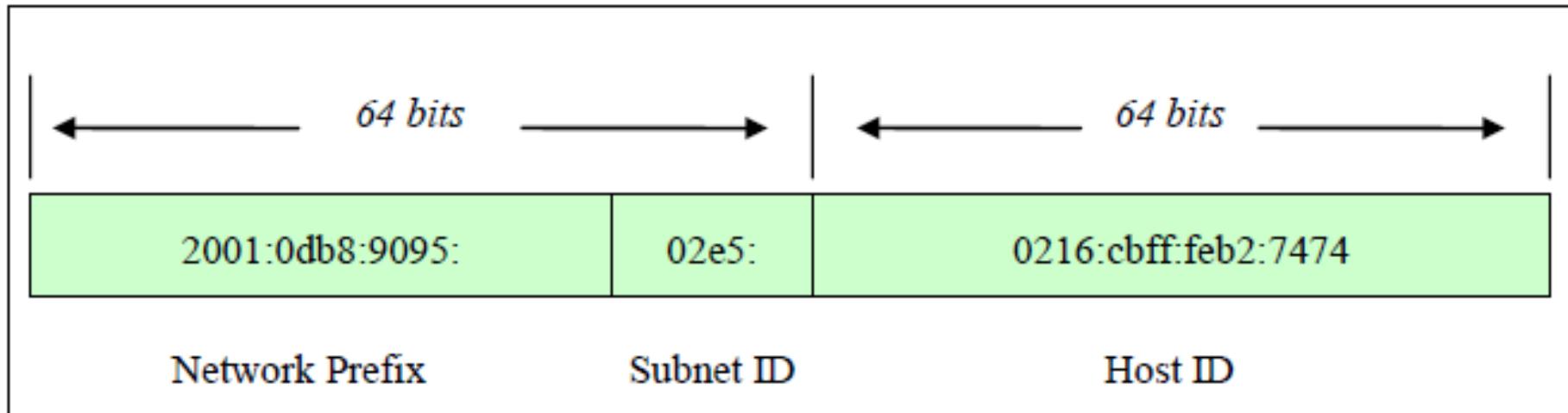


48-битов мрежов префикс

Правителствени, образователни, търговски и др. организации обикновено получават от големите ISPs (PA) или от RIRs (PI) 48-битови алокации (/48), оставяйки 80 бита за subnet ID и host ID.



64-битов мрежов префикс



Подмрежите в рамките на организация обикновено са 64 битови ([/64](#))

64 бита остават за **host ID** - 64-bit идентификатор на интерфейса.

Префикси /127 за P2P връзки

RFC 6164 стандартизира **/127** префикси за **point-to-point** връзки между рутери, за да се избегнат зацикляния, известни като **ping-pong** проблема.

(В СУ нет ползваме /126 с идеята някога да сложим допълнителни хостове за мониторинг на трафика.)

Префикси при маршрутизация

Според предписанията на [RFC 7421](#) (Analysis of the 64-bit Boundary in IPv6 Addressing):

От гледна точка на маршрутизацията може да се прилагат различни стойности на префикса, включително /128, ако създаваме хост маршрути.

Запис на IPv6 адреси

За да се улесни записването на адреси, съдържащи нули, те се компресират по определени правила.

"::" - замества една или повече 16-битови групи от нули.

"::" може да се появи само веднъж в адреса.

Например:

Запис на IPv6 адреси

2001:DB8:**0:0**:8:800:200C:417A unicast

FF01:**0:0:0:0:0:0**:101 multicast

0:0:0:0:0:0:1 loopback

0:0:0:0:0:0:0 unspecified

Се представлят:

2001:DB8:**::**8:800:200C:417A

FF01**::**101

::1

::

Запис на IPv6 адреси и префикси

ПРАВИЛНО представяне на 60-bit префикс:

2001:0DB8:0000:CD30:**0000:0000:0000:0000**/60

2001:0DB8::CD30:**0:0:0:0**/60 или

2001:0DB8:0:CD30:**::**/60

НЕПРАВИЛНО:

2001:0DB8:**::**CD30:**::**/60

Типове IPv6 адреси

Тип	Двоичен формат IPv6	IPv6 означение
Unspecified (неопределен)	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-Local unicast	1111111010	FE80::/10
Unique Local	1111 1100(1)	FC00::/7
Global Unicast	Всички останали Anycast са част от unicast пространството	

Няма Broadcast адреси

Broadcast адреси **не са дефинирани** в IPv6.

Multicast адресирането в IPv6 поема функциите и на broadcast.

Разпределение на IPv6 адресното пространство:

<http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml>

Алокации между RIRs:

<http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml>

Unicast адреси

IPv6 unicast адресите, подобно на IPv4 CIDR, имат префикси с произволни дължини.

Един възел в IPv6 мрежа може да няма знание за вътрешната структура на адреса:

128 бита

Адрес на възела

Unicast адреси. Interface ID - EUI-64 или временни

Но възелът може да е наясно с дължината на префикса n:

n bits	128-n bits
subnet prefix	interface ID

Идентификаторите на интерфейси в IPv6 трябва да са **уникални** в рамките на subnet prefix.

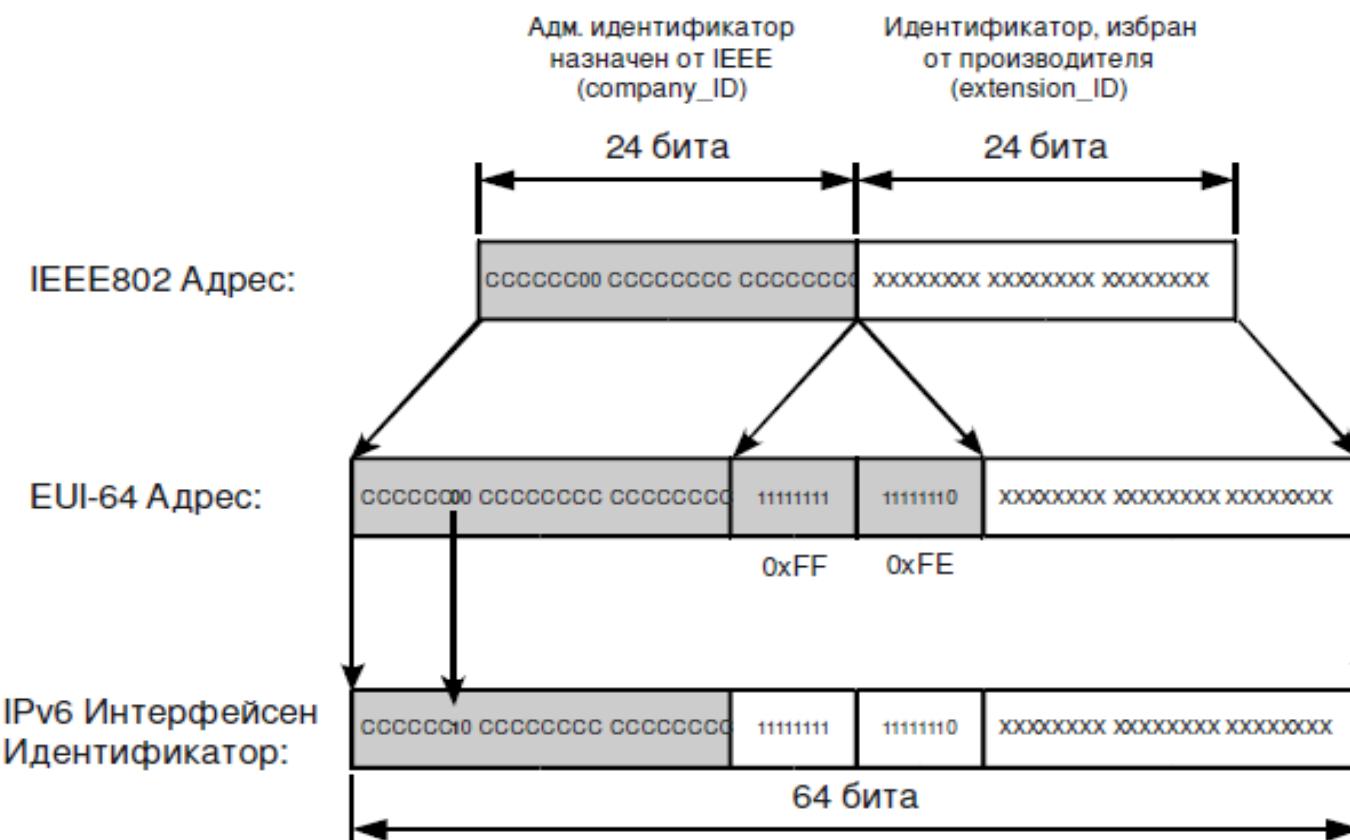
Interface ID - EUI-64 или временни

При всички унікаст адреси, с изключение на започващите с 000, Interface IDs трябва да са 64-bit. Ако са изведени от IEEE MAC адрес, трябва да са в Modified EUI-64 формат [RFC 7136]. Това обаче създава проблем с разкриване на идентичността на потребителя.

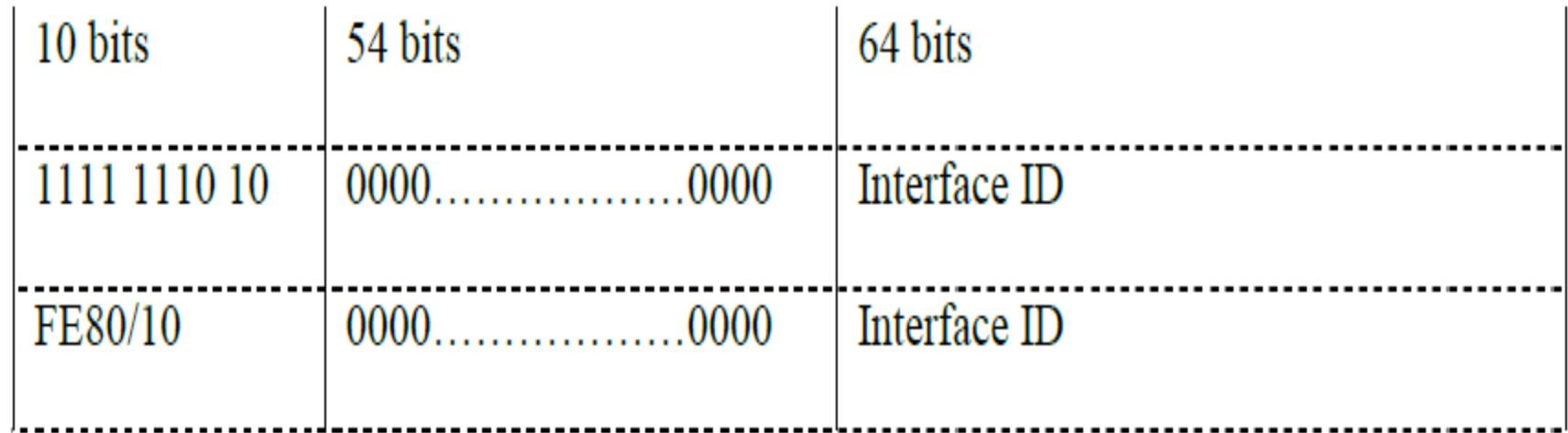
За да се редуцира тази опасност, възелът може да създаде временни адреси, чиито Interface ID-та са случајно генериирани низове от битове [RFC 4941].

По подразбиране временни адреси се прилагат в Apple OS X Lion и следващи и в Microsoft Windows Vista, Windows 2008 Server и следващи версии.

EUI-64 формат



Link-local адреси



Подобно на IPv4, по тях може да се комуникира само в рамките на физическия (**LAN**) канал, към който е свързан даден интерфейс.

На всеки IPv6 интерфейс в LAN автоматично се присвоява такъв адрес.

Пример (динамично раздададени адреси)

```
[root@shuttle ~]# ip a
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
```

Пример (динамично раздададени адреси)

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu  
1500 qdisc pfifo_fast qlen 1000  
    link/ether 00:16:17:b2:0e:96 brd  
ff:ff:ff:ff:ff:ff  
    inet 62.44.109.11/26 brd 62.44.109.63 scope  
global eth0  
        inet6 2a01:288:8003:0:216:17ff:feb2:e96/64  
scope global dynamic  
            valid_lft 2591981sec preferred_lft  
604781sec  
    inet6 fe80::216:17ff:feb2:e96/64 scope link  
        valid_lft forever preferred_lft forever
```

Пример (статично зададен адрес)

```
[root@shuttle ~]# ip a
```

```
...
```

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu  
1500 qdisc pfifo_fast qlen 1000
```

```
...
```

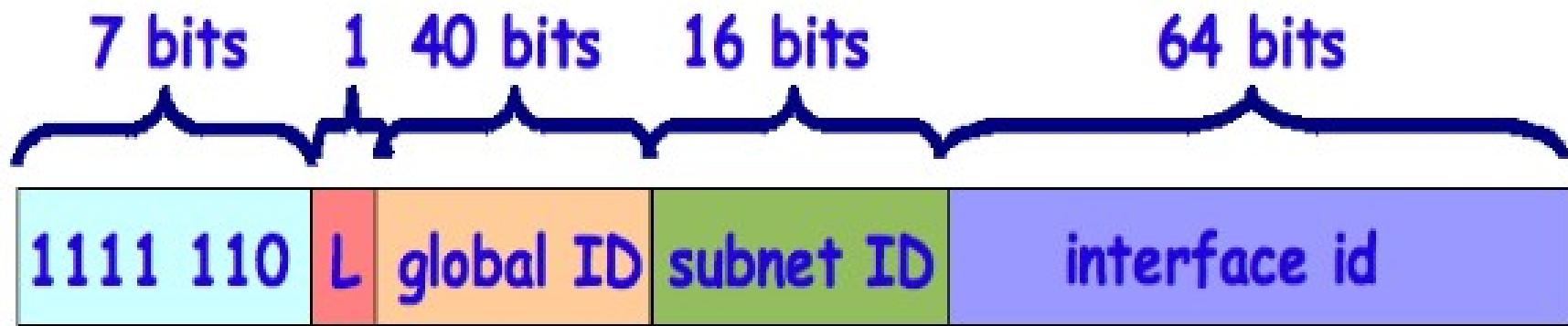
```
inet6 2001:67c:20d0:10::11/64 scope global
```

```
    valid_lft forever preferred_lft forever
```

```
inet6 fe80::216:17ff:feb2:e96/64 scope link
```

```
    valid_lft forever preferred_lft forever
```

Unique Local IPv6 Unicast Addresses (ULA) – подобни на частните IPv4. RFC 4193.



ULA (прод.)

Prefix **FC00::/7**

L =1 ако префиксът е локално присвоен.
 =0 предстои да се дефинира.

Global ID **40-bit** глобално уникален префикс,
генериран псевдо случайно.

Subnet ID **16-bit**, идентифицира подмрежата в
сайта.

Interface ID **64-bit** (генериран от MAC адреса)

ULA (прод.)

ULA адресите (**RFC 4193**) - Unique Local IPv6 Unicast Addresses (уникални локални адреси) или

локални IPv6 адреси (**Local IPv6 addresses**)

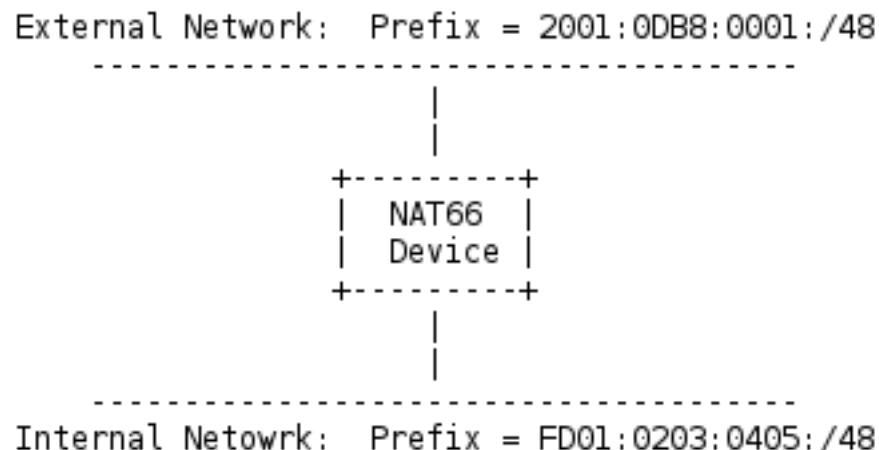
Не се маршрутизират в глобалния Internet.

Маршрутизират се само в рамките на сайт или група от сайтове.

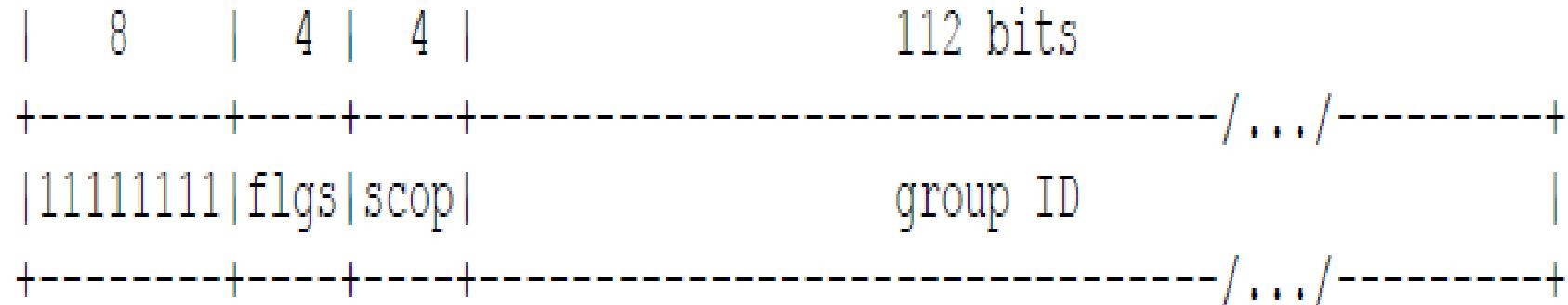
ULA (прод.)

Прилагат се при ограничаване на достъп (вътре в сайт или автономна система) до защитени ресурси и

NAT66:



IPv6 Multicast. Формат.



Въвеждането на периметър (**scope**) в IPv6 multicast ограничава разпространението на пакети само до необходимите части от мрежата: интерфейси, мрежови сегменти и префикси.

IPv6 Multicast. Scope.

Value	Scope
1	Interface Local
2	Link Local
4	Admin. Local
5	Site Local
8	Organization Local
E	Global

Някои добре известни multicast Group IDs се дефинират с различни обсези (scopes).

Например адресът на "All NTP [Network Time Protocol] Servers":

All NTP Servers

FF02::101	All NTP Servers	Link Local
FF04::101	All NTP Servers	Admin Local
FF05::101	All NTP Servers	Site Local
FF08::101	All NTP Servers	Organization Local
FF0E::101	All NTP Servers	Global

RFC 2375 съдържа списък с добре известни (well-known) IPv6 multicast адреси, категоризирани по периметър.

А актуален списък с адресите:

<http://www.iana.org/assignments/ipv6-multicast-addresses>

ICMPv6 vs. ICMPv4. Основните функции са същите: ping6...

Next Header (NH) = 58; (=1 в IPv4)

```
[root@shuttle ~]# ping6 google.com
```

```
PING google.com (2a00:1450:8004::63) 56 data  
bytes
```

```
64 bytes from 2a00:1450:8004::63: icmp_seq=0  
ttl=54 time=47.4 ms
```

```
64 bytes from 2a00:1450:8004::63: icmp_seq=1  
ttl=54 time=46.3 ms
```

```
64 bytes from 2a00:1450:8004::63: icmp_seq=2  
ttl=54 time=46.6 ms
```

...

... и traceroute6

```
[root@shuttle ~]# traceroute6 google.com
```

```
traceroute to google.com (2a00:1450:8004::63), 30 hops  
max, 40 byte packets
```

```
1 * * *  
  
2 border-lozenets.uni-sofia.bg (2a01:288:8000::a)  
1.962 ms 1.956 ms 1.946 ms  
  
3 core-su.lines.acad.bg (2001:4b58:acad:252::25)  
69.643 ms 69.663 ms 69.655 ms  
  
...  
  
14 2a00:1450:8004::63 (2a00:1450:8004::63) 46.596 ms  
47.212 ms 46.264 ms
```

Neighbor Discovery.

Новото в ICMPv6. (вече и в IPv4)

Neighbor Discovery (ND, RFC 4861) заменя (broadcast трафика) ARP в IPv4.

ND се използва от възлите в мрежата за следното:

- определяне на link-layer и MAC адреса на съседния възел, към който е насочен IPv6 пакет;
- да определи кога е настъпила промяна на link-layer адреса на съседния възел;
- да определи дали съседът е все още достъгим.

Neighbor Discovery (ND). Хост и рутер функции.

От хостовете в мрежата:

- откриване на рутери в съседство;
 - автоматично конфигуриране на IPv6 адреса, префикса, маршрути DNS и др. параметри;
- ...от рутерите:

- да се рекламират, да подават на хостовете параметрите за конфигуриране;
- да информират хостовете за по-добри next-hop адреси (т.е маршрути) до конкретни локации.

Neighbor Discovery. Съобщения.

Имаме следните пет ND съобщения:

Router Solicitation (ICMPv6 type 133)

Router Advertisement (ICMPv6 type 134)

Neighbor Solicitation (ICMPv6 type 135)

Neighbor Advertisement (ICMPv6 type 136)

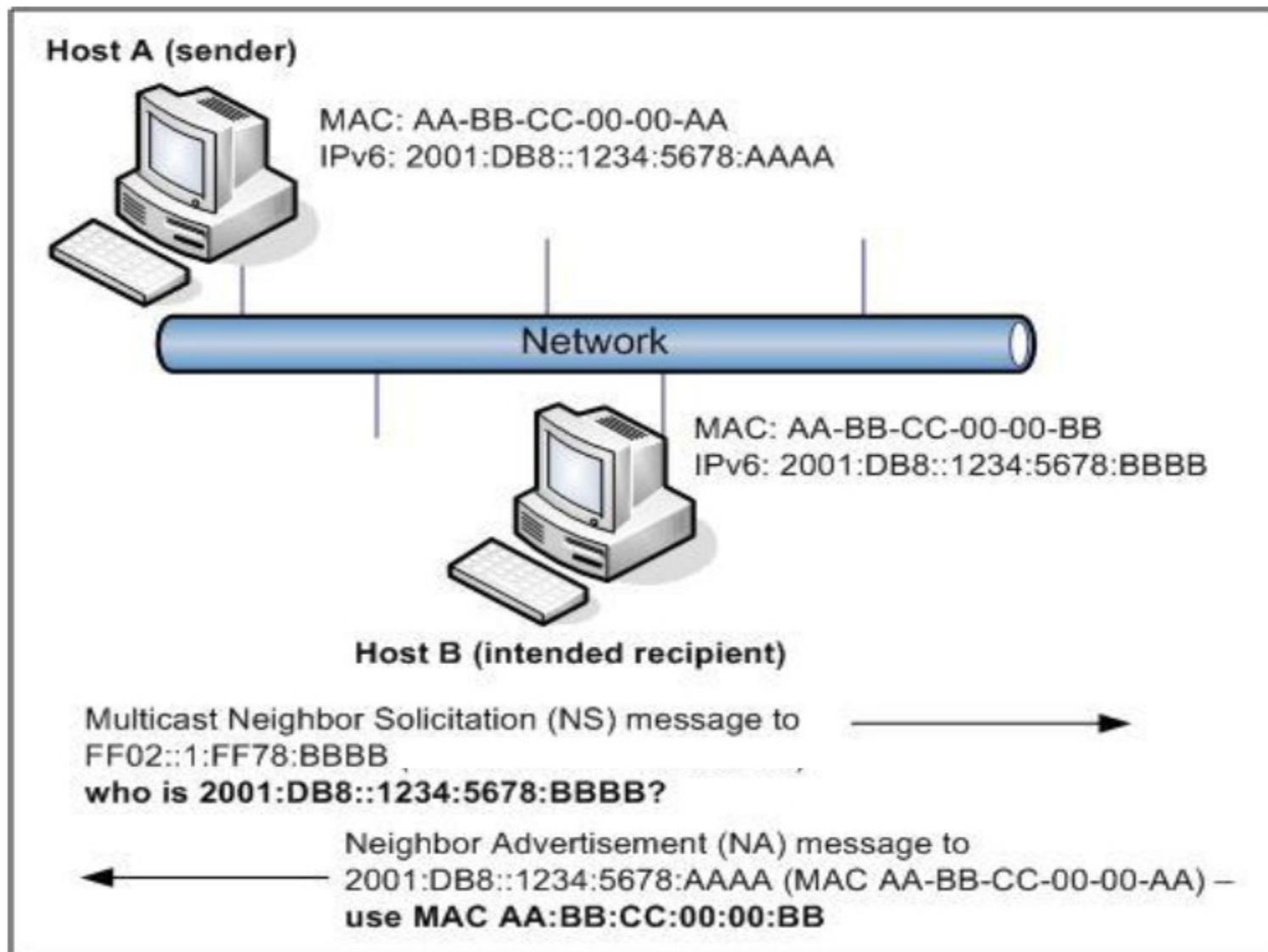
Redirect (ICMPv6 type 137) – Рутерите информират хостовете за **по-добър next-hop** до дестинацията.

ND. Откриване на съсед.

Neighbor Solicitation (NS). Възлите изпращат NS съобщения (135), за да определят адреса на 2 слой на съседа или да се уверят, че съседът е все още достъгим. NSs разпознават и дублирани адреси (**Duplicate Address Detection – DAD**).

Neighbor Advertisement (NA - 136). Отговор на NS. Възел може да изпраща самостоятелно NAs, за да съобщи за промяна на адрес.

Пример: NS/NA



Пример на ND: таблица на съседите

```
[root@shuttle ~]# ip neighbor
```

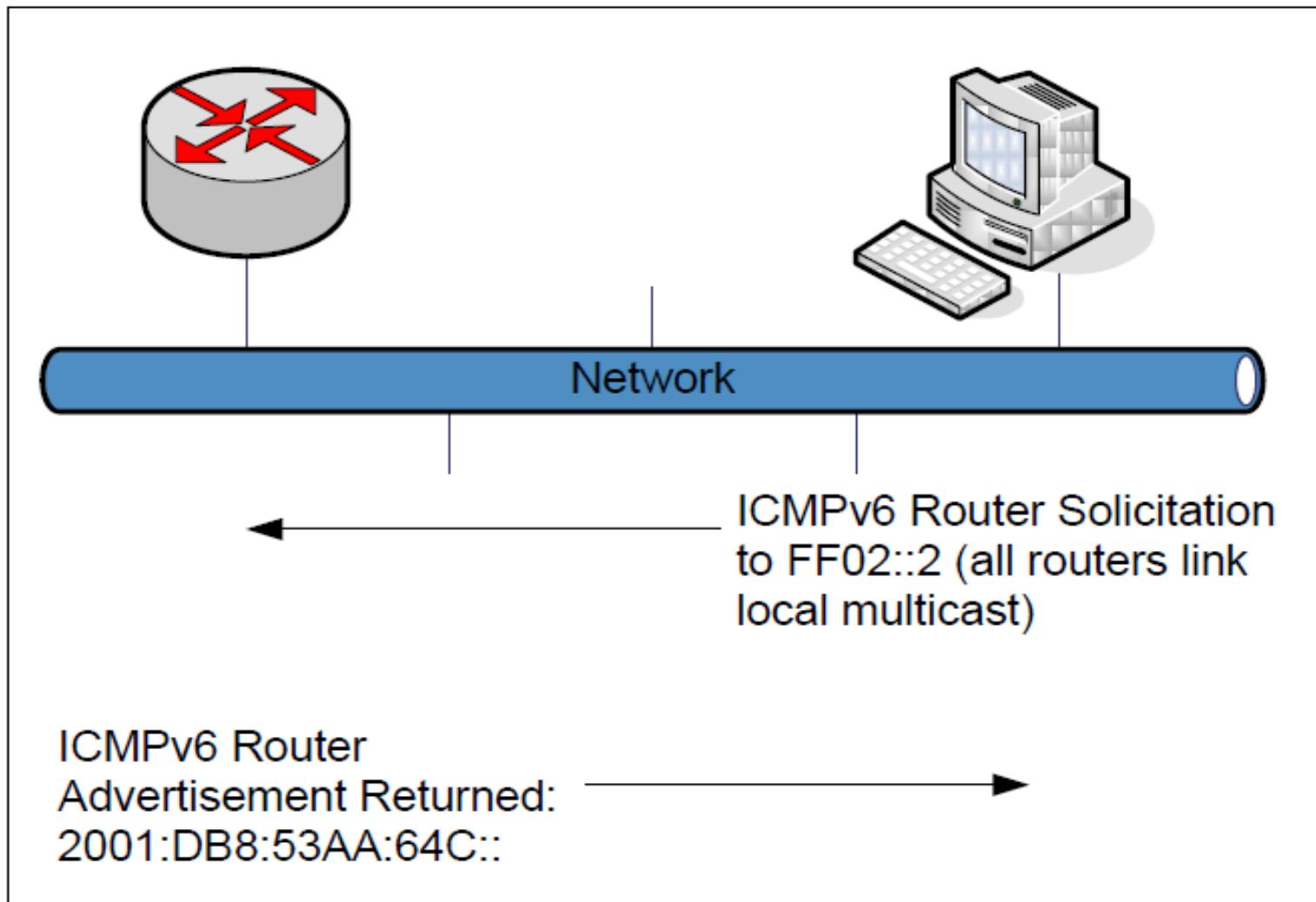
```
2001:67c:20d0:10::5 dev eth0 lladdr  
00:0d:56:b9:75:6d router STALE  
  
62.44.109.5 dev eth0 lladdr  
00:0d:56:b9:75:6d DELAY
```

ND. Откриване на рутер.

Router Solicitation (RS - 133). При активиране на интерфейс хостът изпраща RS съобщения (133), заявявайки от рутерите в мрежата да се “рекламират” - RAs.

Router Advertisement (RA- 134). Рутерите рекламират присъствието си и някои параметри периодически или веднага след RS. RA съдържа префикси на връзката, конфигурации на адреси, брой hop-ве, MTU, DNS и др.

Пример: RS/RA



Autoconfiguration

В IPv6 има и **Stateful** (с определено състояние – **DHCPv6**), но повече се прилага **Stateless** автоконфигуриране - **Stateless Address Autoconfiguration (SLAAC)**.

Дефинира се в **RFC 4862** и е базирано на **ND**.

SLAAC не изиска ръчно конфигуриране на хостове, само минимално на рутери без допълнителни сървъри.

Рутерите рекламират мрежов префикс, а хостът генерира interface ID.

Autoconfiguration. Radvd.

Ако в мрежовия сегмент няма рутер, хостът генерира само адрес на 2 слой, с който може да комуникира единствено и само във физическия мрежов сегмент.

Достатъчната конфигурация на Линукс (RedHat, CentOS, Fedora) рутер е процеса (демона) Router Advertisement Daemon (**radvd**)

Router Advertisement Daemon (radvd). Пример.

```
# less /etc/radvd.conf
```

```
...
```

```
interface enp0s20f1.125
```

```
{
```

```
    AdvSendAdvert on;
```

```
    MinRtrAdvInterval 30;
```

```
    MaxRtrAdvInterval 100;
```

```
    prefix 2001:67c:20d1:1125::/64
```

```
    /* продължава на следващия слайд */
```

radvd пример (прод.)

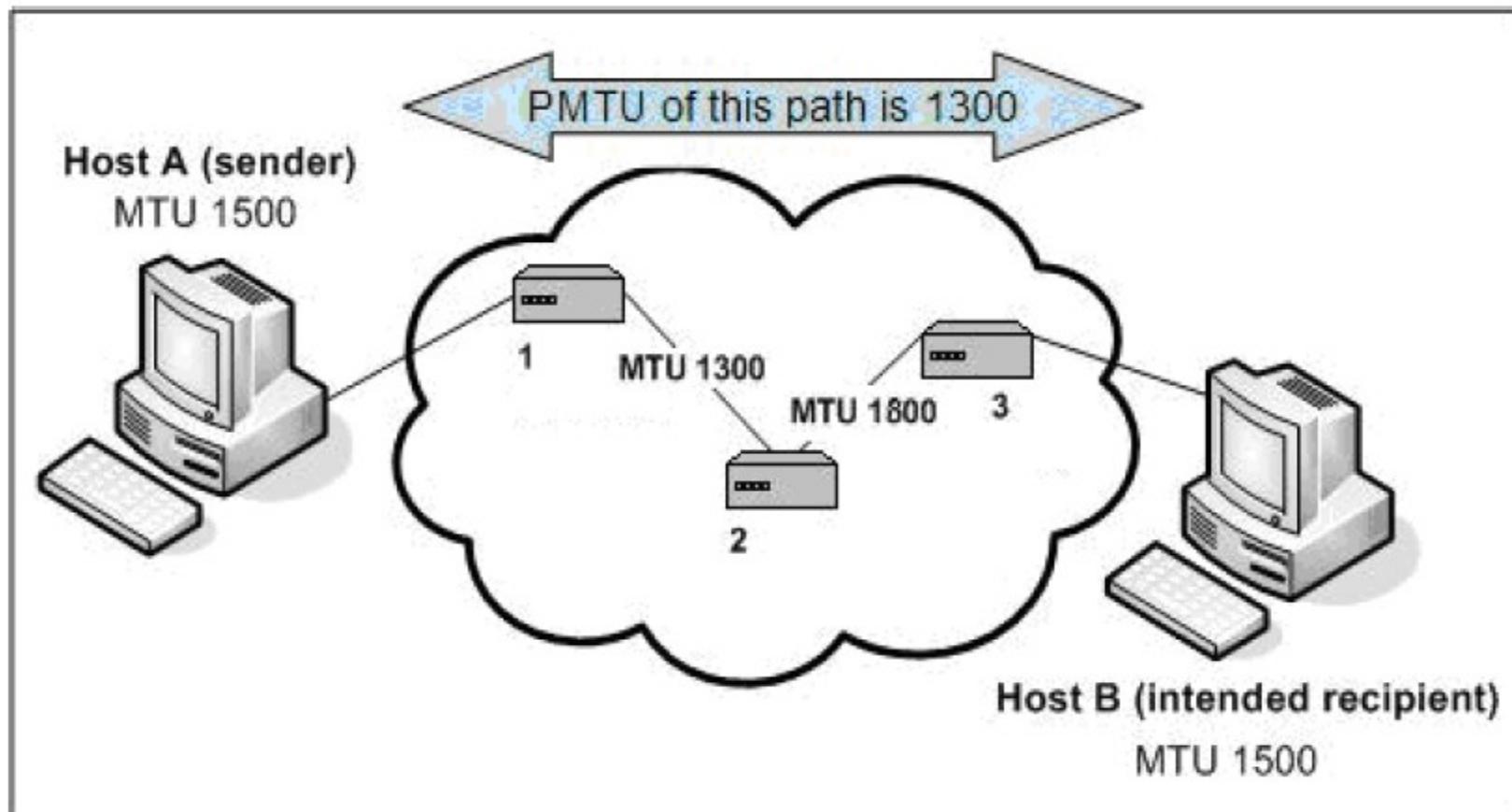
```
/* продължава от предишния слайд */

{
    AdvOnLink on;
    AdvAutonomous on;
    AdvRouterAddr off;
};

RDNSS 2001:67c:20d0:ff::143 2001:67c:20d0:ff::142
{
};

};
```

ND: Path Maximum Transmission Unit (PMTU) Discovery



Механизми за преход от IPv4 към IPv6

IPv6 не е обратно съвместим с IPv4.

Механизмите за преход трябва да осигуряват взаимодействието.

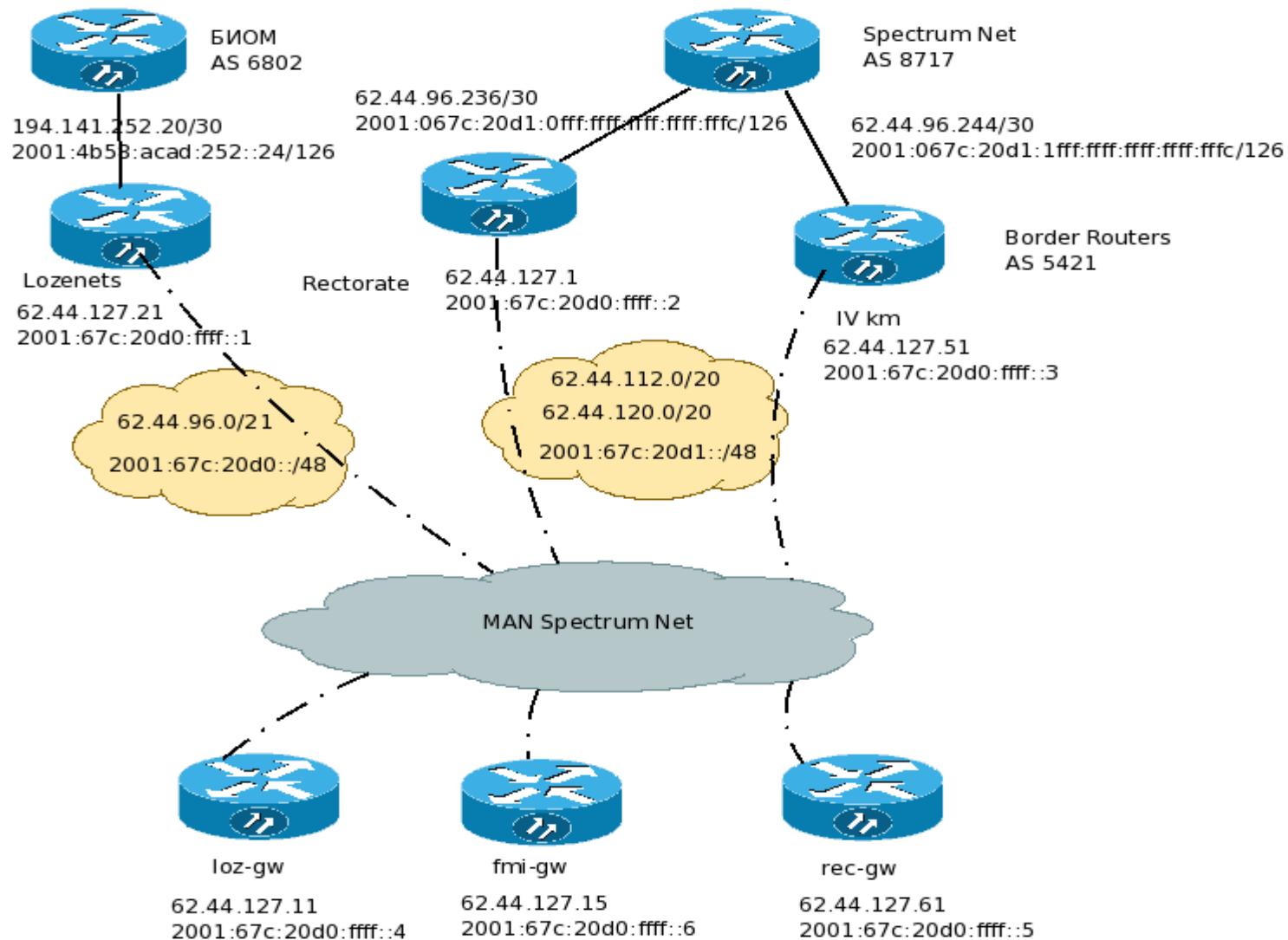
Определят се и от вида на хостовете:

- само IPv4;
- само IPv6 и
- dual stack IPv4/IPv6.

Видове механизми

- Dual stack
- Tunneling
- Translation (NAT)

Dual Stack IPv4/IPv6



Dual Stack IPv4/IPv6

За потребителите е прозрачно дали за дадена услуга ползват IPv4 или IPv6.

Постига се с оборудване, което поддържа и двата протокола:

- втора ръка сървъри за маршрутизатори, работещи под Linux с пакет за маршрутизация;
- DNS е един и същ за IPv4 и IPv6;
- присвояване на адреси по IPv4 – статично или DHCP, IPv6 – автоматично;
- Web (Apache) – “слуша” по IPv4 и IPv6.

Сървър като маршрутизатор

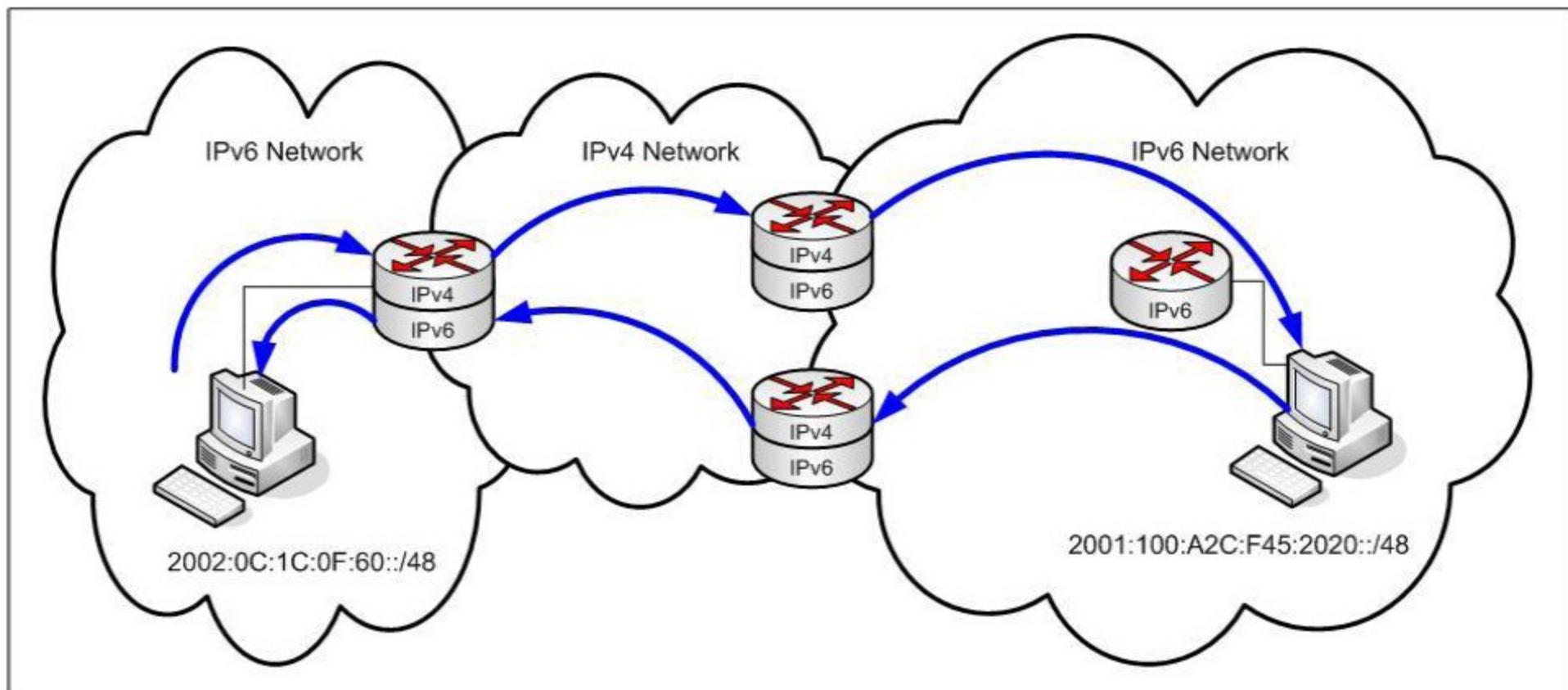


Dual stack

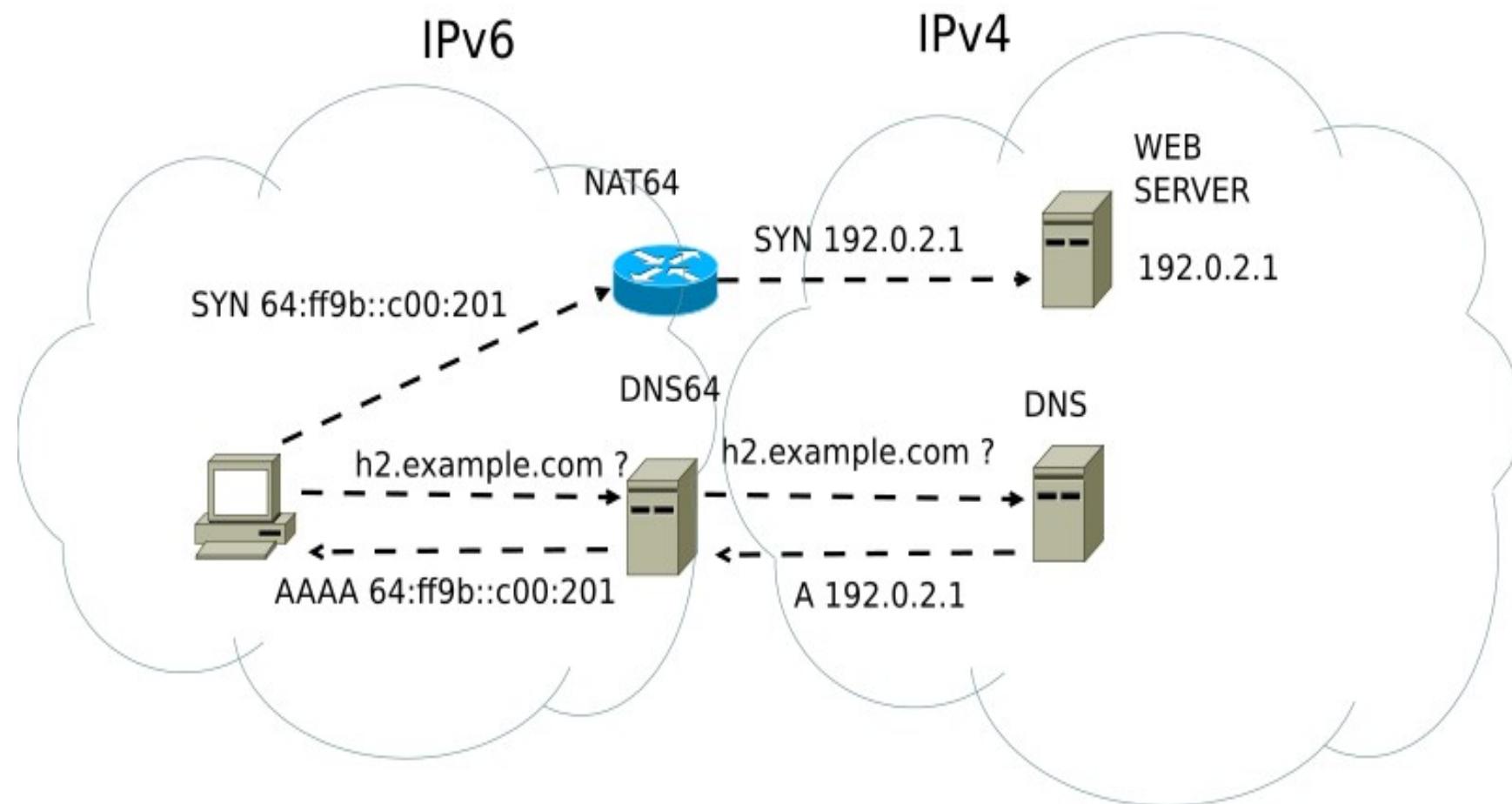
Работни станции:

- Linux – IPv4/IPv6 – автоматично;
- от Windows7/Vista нататък – IPv4/IPv6 – автоматично;
- Windows XP – IPv6 се стартира ръчно.

Tunneling IPv6 over IPv4



NAT64



ТЕМА № 1: УВОД В АРХИТЕКТУРАТА НА КОМПЮТЪРНИТЕ МРЕЖИ

Компютърните мрежи се отличават със **слоеста архитектура**. Всеки слой изпълнява функции, независими от останалите. Така промени в даден слой не засягат функциите на останалите – принципите на **машабируемостта и гъвкавостта (scalability и flexibility)** Подният слой ползва услугите, подавани от по-горния. По-горният слой осигурява услуги за по-долния, като по-горният „не се интересува“ от особеностите на по-долния - принципът на „**прозрачността**“ (**transparency**).

Седемслойният модел OSI (Open Systems Interconnection) на Международната организация по стандартизация (ISO) е теоретичен (**еталонен**) модел, който стандартизира комуникациите между отдалечени (компютърни) системи, притежаващи мрежов интерфейс, т.е **отворени системи**. OSI дефинира използваните формати на данните и протоколите за взаимодействие между системите на съответните нива (слоеве).

Протокол е набор от правила, определящи взаимодействието между системите в рамките на едно ниво от модела. Протоколът дефинира и единиците от данни (**protocol data unit - PDU**), които се предават по мрежата между идентичните слоеве на „говорещите си“ отдалечени системи.

	PDU	Слой
HOST LAYERS	DATA	APPLICATION
	DATA	PRESENTATION
	DATA	SESSION
	SEGMENT	TRANSPORT
MEDIA LAYERS	PACKET	NETWORK
	FRAME (кадър)	DATA LINK
	BITS	PHYSICAL

Всеки слой на OSI модела изпълнява конкретна задача в процеса на мрежовата комуникация и след това предава данните нагоре или надолу към следващия слой. Когато данните се предават през слоевете, всеки слой добавя пред оригиналните данни своя собствена информация под формата на заглавие – **header** (или **хедър**), която формира т.нар. служебен (или **overhead**) трафик.

На мрежовия слой (network) се прилага комутация на пакети (**packet switching**).

Слоевете се делят на две групи:

host layers – тези нива на модела OSI се реализират единствено и само в крайните устройства (възлите) на мрежата. Тези слоеве от модела OSI (слой 4-7) осигуряват връзката от приложение до приложение (взаимодействието между процеси и услуги, работещи на тези крайни устройства) и затова са реализирани всичките в крайните устройства.

media layers – чрез тези слоеве на модела OSI (слой 1-3) се реализира и в крайните, и в междинните (мрежови) устройства, като осигуряват взаимодействие между тях.

Ниво 7 от модела осигурява интерфейс към приложенията, участващи в комуникацията между възлите в межата.

Ниво 6 – това ниво има за цел да представи данните в разбираем за приемащата ги страна вид. Тук например става конвертирането на различни кодови таблици, прилагат се методи за запис на цели или с плаваща запетайка числа. Целта е приложения на различни машини и различни идеологии да могат да си комуникират безпрепятствено.

Ниво 5 – осигурява методи за установяване на нова сесия, прекратяването и, повторното ѝ отваряне ако е необходимо. Дефинирани са механизмите за Full Duplex, Half Duplex и Simplex комуникация, както и механизми за управление на потока Flow Control (те са дефинирани и в 4-то ниво, но по различен начин).

Ниво 4 – Транспортното ниво има една единствена дефинирана функционално цел. То е да осигури сигурна комуникация и прозрачен пренос за поток от данни. В OSI спецификацията са дефинирани 5 различни класа на транспорт (транспортен протокол) маркирани като TP0, TP1, TP2, TP3, TP4, като всеки по-горен включва функционалността на по-долния. Класовете на транспорт няма да бъдат разглеждани подробно. Данните се пренасят, оформени в **сегменти**.

Ниво 3 – това е първото напълно независимо от физическата среда ниво. Основното тук е, че разполагаме с адреси, които не са обвързани пряко с адресите от второто ниво, или можем да предаваме данни между различни сегменти с различни протоколи от второ ниво, и различни физически среди. На практика това е първото напълно независимо от физическата среда ниво, даващо възможност на две или повече машини да си препредават данни без значение към каква физическа мрежа са свързани. Предаването на данни на базата на тези адреси се нарича **routing** (маршрутизация), а форматирането на данните се нарича **пакет**.

Ниво 2 – Това ниво е обвързано с физическото ниво, но добавя допълнителна функционалност. Първо то добавя физически адреси на различните мрежови устройства, наречени **MAC** (Media Access Control) адреси, имащи за цел отделянето на комуникацията между отделните двойки от останалите, изльзвани по единакъв начин в една и съща споделена физическа среда. Второ, то има грижата да открие възможни грешки при предаването на данни по физическата среда, които тя не е успяла да установи и поправи. Или казано функционално:

- Разделя комуникиращите възли чрез адреси (дава възможност на приемащите данните да разпознаят дали са били за тях на базата на адресни идентификатори)
- Проверява предадените на физическо ниво данни за коректност (и дава възможност на приемащия да предприеме мерки за коригирането им)

Данните се пренасят под формата на **кадри (frames)**.

Ниво 1 – това ниво се занимава с физическата среда и физическата комуникация. В него няма физическа маршрутизация и комуникацията е или между две страни директно свързани помежду си, или между група участници, получаващи едни и същи данни „едновременно“ в даден момент. Данните се предават като потоци от **битове**.

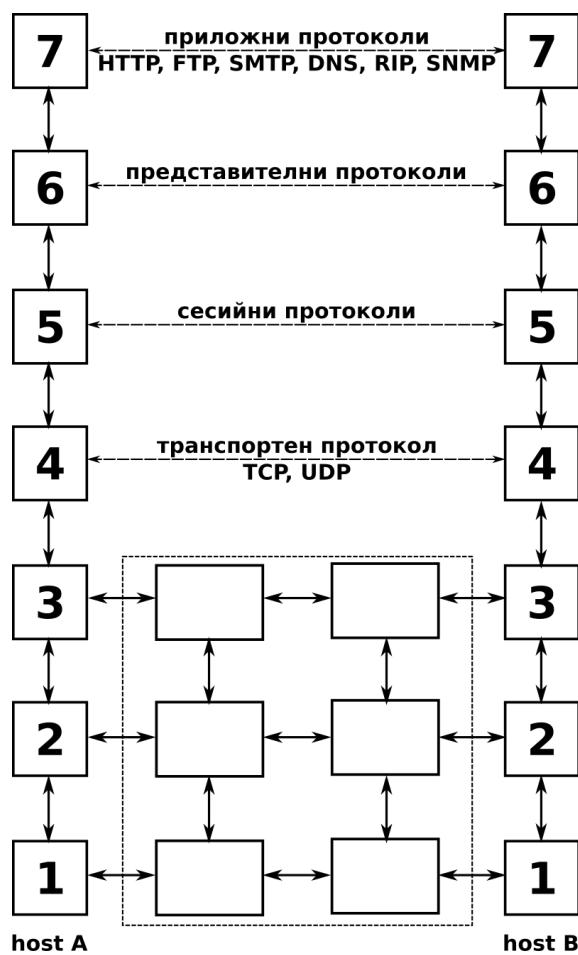
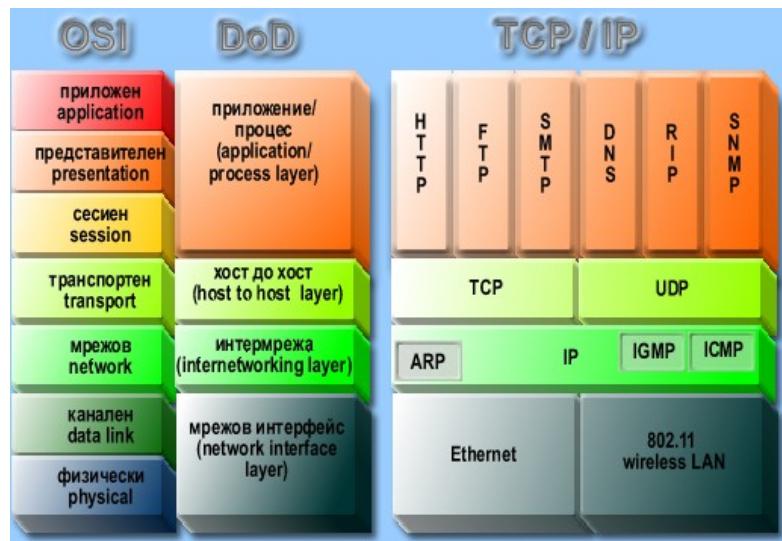
TCP/IP стек

TCP/IP (Transmission Control Protocol/Internet Protocol) е протоколен стек, който е специално разработен за големи мрежи, състоящи се от много мрежови сегменти, свързани чрез маршрутизатори (рутери - routers). TCP/IP е крайъгълният камък на Интернет комуникациите. Той се преврна в най-използваното мрежово/транспортно решение за мрежи с всякакъв размер и конфигурации.

TCP/IP е не само протоколен стек, състоящ се от протокол от мрежовия слой и протокол от транспортния слой, но и пълен комплект от протоколи, работещи в много слоеве на мрежовия модел. Понятието комплект от протоколи (*protocol suite*) е по-широко от понятието протоколен стек и включва и елементи, които не се изискват за мрежовата комуникация (например, помощни програми от приложния слой, които са част от комплекта TCP/IP). Много от протоколите, включени в комплекта, функционират като инструменти за събиране на информация и отстраняване на проблеми.

Архитектура на TCP/IP

Архитектурата на комплекта протоколи TCP/IP отговаря на четирислойния мрежови модел DoD (известен още като модел DARPA), но всеки един от четирите му слоя може да бъде съпоставен на един и няколко от слоевете на референтния OSI модел. Това е илюстрирано на схемата по-долу.



фигура 2. Действие на TCP/IP стека

Мрежов интерфейс

Мрежовият интерфейс изпраща и получава TCP/IP пакетите от мрежовата преносна среда. TCP/IP е проектиран така, че да бъде независим от методите за достъп до мрежата, формата

на кадрите и преносната среда. Следователно, може да бъде използван с различни LAN технологии, като Ethernet и 802.11 wireless LAN и лесно може да бъде адаптиран към бъдещи нови технологии.

IP протоколи

Address Resolution Protocol (ARP) - транслира логическите адреси в MAC адреси. Тази транслация е необходима, защото по-долните слоеве от модела могат да обработват само MAC адреси.

Internet Control Message Protocol (ICMP) – протокол за мрежова диагностика. Програми, които използват протокола ICMP са **ping**, **traceroute**, **nmap** и др. Функцията **Neighbor Discovery (ND)** в **ICMPv6** известват ARP при IPv6, а вече и при IPv4.

Терминология

PDU – protocol data unit: общият блок от данни на протокола – заглавие + полезни данни;

SDU – service data unit: блок от данни, преминал от по-горно към по-долното ниво и все още не капсулиран в PDU на това ниво;

MTU – maximum transmission unit: максимален размер на блока от полезни данни, който може да бъде предаден без фрагментация.

Фрагментация на пакетите

Важна особеност на протокола IP е способността му да изпълнява динамична фрагментация на пакетите при тяхното предаване в мрежи с различни стойности на MTU. Това е основна характеристика на каналния слой. Фрагментите от пакетите, предадени по мрежата се събират от IP модула на възела, получател на пакетите, но понякога това се прави и от междинните маршрутизатори по техния път.

Какво ще се случи, ако при предаване на фрагментиран пакет, един от фрагментите не достигне до получателя на пакета и времето за дефрагментация на целия пакет изтече? IP модулът на получателя ще отхвърли всички останали получени фрагменти от този пакет. IP модулът на източника няма да предприеме действия за повторно предаване на този пакет. Оставя решаването на този проблем на по-горните нива (на транспортно при TCP-базирани приложения и на приложно при UDP-базирани).

Причини за фрагментацията:

1. за намаляване на времето за повторно предаване на пакета в случай на загубване или повреждане;
2. ако се работи в режим half duplex да не може възела да заема за дълго време канала;
3. колкото е по-голям пакета (респективно MTU), толкова по-дълго е изчакването на другите пакети да бъдат изпратени (особено при последователни интерфейси).

Задачка: Изпраща се IP пакет (дейтаграма), съдържащ UDP пакет с големина 8192 байта потребителски данни. Колко фрагмента ще се предадат и какви ще са стойностите на отместването и дължината на всеки фрагмент (MTU=1480)?

Решение: Добавяме 8 байта (UDP header) към размера на IP дейтаграмата и тя става 8200 байта.

1. 1480 @0+ (MF=1);
2. 1480 @1480+ (MF=2);

3. 1480 @2960+ (MF=3);
4. 1480 @4440+ (MF=4);
5. 1480 @5920+ (MF=5);
6. 800 @7400(MF=6).

Проверка: $1480 \times 5 + 800 = 8200$

Команди ip, дефинирани от пакета iproute2:

1. *ip addr add 192.168.11.17/24 dev eth0* – добавя ip адрес към интерфейс eth0
2. *ip addr show* – показва адресите
3. *ip addr del 192.168.11.17/24 dev eth0* – премахва ip адрес
4. *ip link set eth0 up*
ip link set eth0 down
5. *ip route show* – показва маршрутизиращата таблица
6. *ip route add 10.10.20.0/24 via 192.168.11.17 dev eth0* – добавя статичен маршрут
7. *ip route del 10.10.20.0/24* – премахва статичен маршрут
8. *ip route add default via 192.168.11.50* – добавя шлюз (gateway) по подразбиране

команда ifconfig:

Тази команда е остатяла и е заменена от командата ip от пакета iproute2 (вж. по-горе). Препоръчва се избягването на наейната употреба.

1. *ifconfig eth0* – показва мрежовите настройки на определен интерфейс;
2. *ifconfig -a* – показва мрежовите настройки на всички интерфейси;
3. *ifconfig* – показва информация за всички **активни** интерфейси;
4. *ifconfig eth0 up*
5. *ifconfig eth0 down*
6. *ifconfig eth0 192.168.2.2* – присъединява мрежовия адрес 192.168.2.2 на интерфейс eth0;
7. *ifconfig eth0 255.255.255.0* – присъединява мрежова 255.255.255.0 на интерфейса eth0;
8. *ifconfig eth0 broadcast 192.168.2.255* – променя адреса за broadcast на интерфейса eth0;
9. *ifconfig eth0 mtu #####* – определя размера на максималния размер на пакета в байтове (#####), който може да бъде предаден без фрагментация. По подразбиране mtu=1500 байта;
10. *ifconfig eth0:0 172.16.25.127 alias eth0:0* и присъединява към него мрежовия адрес 172.16.25.127;
11. *ifconfig eth0 hw aa:bb:cc:dd:ee* – сменя MAC адреса на интерфейс eth0.

Повече примери за използването на командата ifconfig може да се намерят в нейната помощна страница (man ifconfig).

Deprecated command	Replacement command(s)
arp	ip n (ip neighbor)
ifconfig	ip a (ip addr), ip link, ip -s (ip -stats)
iptunnel	ip tunnel
iwconfig	iw
nameif	ip link, ifrename
netstat	ss, ip route (for netstat-r), ip -s link (for netstat -i), ip maddr (for netstat-g)
route	ip r (ip route)

Broadcast address – условен, неприсвоен на никое устройство в мрежата адрес, който се използва за изпращане на broadcast пакети (пакети, предназначени за получаване от всички възли в мрежата) в компютърната мрежа.

Първото появяване на broadcast адреси в IP мрежи е през 1982 г., Robert Gurwitz & Robert Hinden.

Видове broadcast адреси в зависимост от слоя на модела OSI:

L2 – ff:ff:ff:ff:ff:ff. Използва се за предване на служебна детайли (например при запитвания по протокола arp).

L3 – зависят от използвания протокол в мрежовия слой.

Инверсия на мрежовата маска – всички 0 в нея се установяват на 1 (нарича се wildcard маска и се прилага в рутерите на Cisco Systems при конфигуриране на протокола OSPF)

команда **ping** – средство за диагностика на мрежата. Командата измерва общото време (RTT) в милисекунди за изпращане на пакет до целта и получаване на отговор от нея по мрежата. За тази цел се използва протокола ICMP – изпращане на echo request пакет и получавае на echo reply packet. Протоколът ICMP, заедно с протокола IP осигуряват възможността за проверка за грешки, както и функционалността за тяхното докладване.

RTT – Round Trip Time – включва времето за разпространение, очакване и обработка на заявката.

```
[nick@lascar ~]$ ping google.bg
PING google.bg (216.58.208.99) 56(84) bytes of data.
64 bytes from sof01s11-in-f3.1e100.net (216.58.208.99): icmp_seq=1 ttl=57 time=1.06 ms
64 bytes from sof01s11-in-f3.1e100.net (216.58.208.99): icmp_seq=2 ttl=57 time=1.07 ms
64 bytes from sof01s11-in-f3.1e100.net (216.58.208.99): icmp_seq=3 ttl=57 time=1.07 ms
64 bytes from sof01s11-in-f3.1e100.net (216.58.208.99): icmp_seq=4 ttl=57 time=1.11 ms
64 bytes from sof01s11-in-f3.1e100.net (216.58.208.99): icmp_seq=5 ttl=57 time=1.05 ms
64 bytes from sof01s11-in-f3.1e100.net (216.58.208.99): icmp_seq=6 ttl=57 time=0.916 ms
```

```
[nick@lascar ~]$ ping 62.44.96.142
```

```
PING 62.44.96.142 (62.44.96.142) 56(84) bytes of data.
64 bytes from 62.44.96.142: icmp_seq=1 ttl=61 time=0.753 ms
64 bytes from 62.44.96.142: icmp_seq=2 ttl=61 time=0.801 ms
64 bytes from 62.44.96.142: icmp_seq=3 ttl=61 time=0.689 ms
64 bytes from 62.44.96.142: icmp_seq=4 ttl=61 time=0.641 ms
64 bytes from 62.44.96.142: icmp_seq=5 ttl=61 time=0.647 ms
64 bytes from 62.44.96.142: icmp_seq=6 ttl=61 time=0.585 ms
^C
--- 62.44.96.142 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5000ms
rtt min/avg/max/mdev = 0.585/0.686/0.801/0.072 ms
```

Когато ping-вате дестинация по име на хост, отговорите съдържат IP адреса на хоста, броят на изпратените байтове, RTT и Time to Live ([TTL](#)) на пакета. Когато ping-вате дестинация по IP address, получавате същите отговори с изключение на името на хоста (освен ако не сте въвели параметъра **-a**). Ping тества не само достъпимостта, но и верифицира дали TCP/IP стека е инсталиран правилно и дали DNS резолвинга работи правилно.

- ping localhost – проверява състоянието на TCP/IP стека на локалната машина
- ping 127.0.0.1 – същото
- ping local_IP_address – проверява състоянието на мрежовата карта
- ping gateway_IP_address – проверява състоянието на връзката до шлюза на локалната мрежа

команда **ss** – замества командата netstat. ss – socket statistics.

```
[nick@sakurajima ~]$ ss -t
State      Recv-Q Send-Q          Local Address:Port          Peer Address:Port
ESTAB      0      0              192.168.11.102:36568        208.68.163.218:xmpp-client
CLOSE-WAIT 1      0              192.168.11.102:42815        152.19.134.142:https
ESTAB      0      0              192.168.11.102:49139        88.221.211.11:http
CLOSE-WAIT 1      0              192.168.11.102:57670        157.249.32.164:http
ESTAB      0      0              192.168.11.102:48127        84.43.191.101:xmpp-client
```

Програма wireshark

3 прозореца:

- списък на събраните пакети от мрежата с кратко описание;
- дърво на протоколите, инкапсулирани в кадъра;
- дъмп на пакета в шестайсетичен или текстов вид.

Tshark – конзолна версия на wireshark.

```
tshark -R "ip.addr == 192.168.0.1" -r /tmp/capture.cap
```

```
tshark -f "udp port 1812" -i eth0 -w /tmp/capture.cap
```

- Флагът **-f** се използва за дефиниране на филтъра. Пакетите, които не удовлетворяват условието, дефинирано с **-f** флага, няма да бъдат прихванати. В горния пример се прихващат само IP пакетите, които са с UDP порт 1812 (източник или дестинация).

- Флагът -i се използва за дефиниране на интерфейса, от който се очаква да видим RADIUS пакети. На мястото на 'eth0' се поставя конкретния интерфейс.
- Флагът -w flag се използва за дефиниране на файла, където ще се запише прихватият трафик.

```
tshark -z "proto,colinfo,tcp.srcport,tcp.srcport" -r /tmp/capture.cap
```

ping abv.bg – първият пакет ползва DNS. С wireshark наблюдаваме енкапсулирането, като сме направили DNS филтриране.

ping abv.bg -s 65000 -M – със забрана на фрагментацията на пакетите

ping abv.bg -s 65000 – с wireshark се наблюдава фрагментацията на пакетите

Тема № 2: IP АДРЕСАЦИЯ

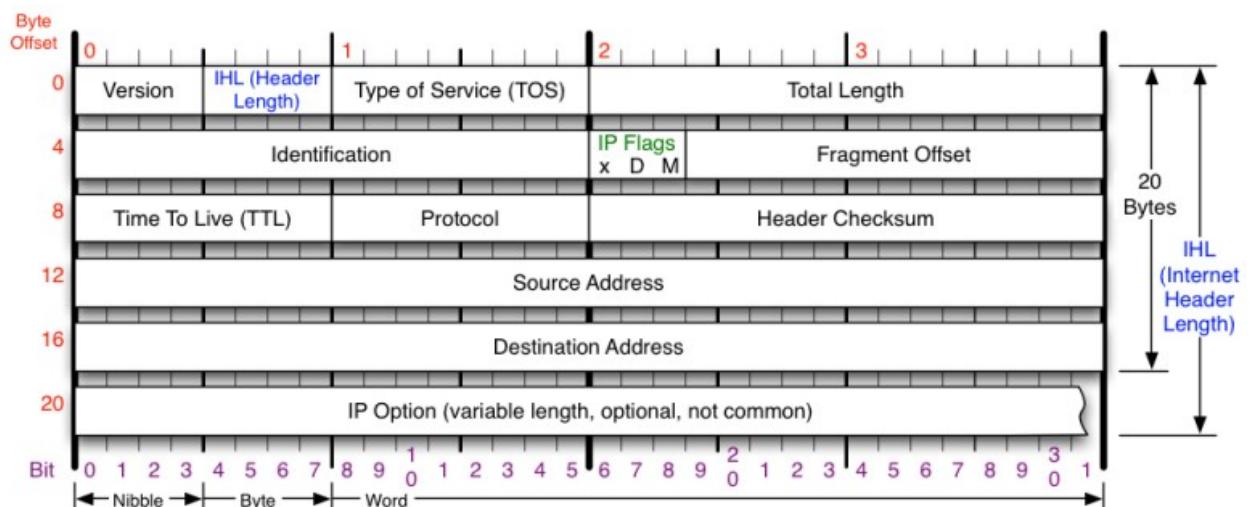
IP адресът представлява логически адрес на конкретен възел от мрежата. За да се осъществи връзка между две крайни устройства, те трябва да имат уникални адреси (в мрежата).

IP адресът се присвоява на мрежовия интерфейс на крайното устройство. Много често в сървърите се монтират повече от една мрежова карта (NIC), като всяка карта има собствен, уникален IP адрес.

NIC притежават:

- работни станции;
- сървъри;
- мрежови принтери;
- IP телефони.

Във всеки изпратен по мрежата пакет има записани в неговата заглавна част (IP header) IP адресът на изпращача и IP адресът на получателя на пакета.



Version	Protocol	Fragment Offset	IP Flags
Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.	IP Protocol ID. Including (but not limited to): 1 ICMP 17 UDP 57 SKIP 2 IGMP 47 GRE 88 EIGRP 6 TCP 50 ESP 89 OSPF 9 IGRP 51 AH 115 L2TP	Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.	x D M x 0x80 reserved (evil bit) D 0x40 Do Not Fragment M 0x20 More Fragments follow
Header Length	Total Length	Header Checksum	RFC 791
Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.	Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.	Checksum of entire IP header	Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

СТРУКТУРА НА IP АДРЕСА

IP адресът представлява серия от 32 двоични бита (0 или 1), което го прави трудно разбираем даже и ако битовете се групират в групи (4 групи) по 8 бита, наречени октети. За улесняване на разбирамостта на IP адресите, всеки октет се записва с неговото десетично представяне (точково-десетичен запис):

dec:	192	168	1	5
bin:	110000000	10101000	00000001	00000101

Структурата на 32 битовия IP адрес е описана в мрежовия протокол IPv4 – **RFC 791**; IPv6 – **RFC 2460**; **RFC 6144** – **Framework for IPv4/IPv6 Translation**. Все още 32 битовият протокол IPv4 е най-разпространеният протокол за адресация в Internet.

Всеки октет на мрежовия адрес се състои от 8 бита, като всеки бит има своята стойност. И 4-те групи от октети имат един и същ набор от стойности. Значението на най-десният бит в октета е 1, а значението на останалите битове, отляво надясно е 2, 4, 8, 16, 32, 64 и 128.

128	64	32	16	8	4	2	1
-----	----	----	----	---	---	---	---

За да определим стойността на октета, трябва да съберем стойностите на позициите, в които има двоична единица. При извършване на това събиране в сила са следните правила:

1. В събирането не участват позициите, в които има 0;
2. Ако всичките осем бита имат стойност 0 (00000000), тогава стойността на октета е 0;
3. Ако всичките осем бита имат стойност 1 (11111111), тогава стойността на октета е 255;
4. Ако стойностите на осемте бита са различни, например 00100101, тогава стойността на октета е 39 (32 + 4 + 2 + 1):

128	64	32	16	8	4	2	1
0	0	1	0	0	1	1	1
		32			4	2	1

Стойността на всеки октет се намира в диапазона от 0 до 255.

ФОРМАТ НА IP АДРЕС

Логическият IP адрес представлява йерархична система и се състои от две части – първата част от него идентифицира мрежата като цяло, а втората идентифицира конкретният възел в нея. Първата част се нарича мрежова част (net_ID), а втората – хост част (host_ID).

$$\text{net_ID} + \text{host_ID} = 32 \text{ bits}$$

10000011	01101100	01111010	11001100
8 бита	8 бита	8 бита	8 бита

131	108	122	204
8 бита	8 бита	8 бита	8 бита

Пример на IP адрес от клас C: 192.168.18.57

Първите три октета образуват мрежовата част (192.168.18), а последният октет (.57) – идентифицира възела в нея.

Такава система се нарича **йерархична адресация**, защото мрежовата част от адреса идентифицира мрежата, в която се намират всички възли (хостове). На маршрутизаторите е нужно да знаят само пътя до мрежата, но не и разположението на отделните възли в нея.

Друг пример за йерархична мрежа е телефонната мрежа:

359-2-1234567

359 – код на държавата;

2 – код на града;

1234567 – телефонен номер.

359 и 2 идентифицират мрежата (на телефонния оператор), а 1234567 е локалният номер на телефона.

При IP адресацията, в една физическа мрежа може да съществуват няколко логически мрежи.

Възлите с еднаква мрежова част (например, 192.168.18) могат да обменят информация помежду си, но не могат да обменят с други възли (с друга мрежова част, например 192.168.5), без да използват маршрутизация.

КЛАСОВЕ IP МРЕЖИ И МРЕЖОВИ МАСКИ ПО ПОДРАЗБИРАНЕ

IP мрежите се разделят на следните класове:

- A – раздават се на интерфейси на компютри;
- B – раздават се на интерфейси на компютри;
- C – раздават се на интерфейси на компютри;
- D – за групови (multicast) предавания, примерно мултимедия;
- E – за експериментални цели.

Мрежа клас А:

net_ID – само един октет;

host_ID – цели три октета.

Мрежи от клас А се дават само на големи организации. Броят на възлите в такава мрежа е 2^{24} . Мрежовата маска на мрежите от такъв клас е 255.0.0.0, а самата мрежова маска се състои от 24 бита.

Мрежа клас В:

net_ID – два октета;

host_ID – два октета.

Мрежовата маска по подразбиране се състои от 16 бита: 255.255.0.0. Броят на възлите в такива мрежи е $2^{16} = 65536$ възела. Мрежи от такъв клас обикновено се раздават на средноголеми организации.

Мрежа клас С:

net_ID – три октета (8 бита);

host_ID – един октет (24 бита).

В мрежи от такъв клас може да има $2^8 = 256$ адреса. Мрежовата маска по подразбиране е 255.255.255.0. Използват се за малки по размер мрежи.

Мрежа клас D:

1	1	1	0						2	3	4
net_ID				host_ID							

Мрежа клас Е:

1	1	1	1						2	3	4
net_ID				host_ID							

Класът на мрежата може да се определи по значението на нейния първи октет.

Клас мрежа	Мрежи	Битове в първия октет
A	1-127	<u>0</u> 0000000 – <u>0</u> 1111111
B	128-191	<u>1</u> 0000000 – <u>1</u> 0111111
C	192-223	<u>1</u> 1000000 – <u>1</u> 1011111
D	224-239	<u>1</u> 1100000 – <u>1</u> 1101111

E	240-255	<u>1111</u> 0000 – <u>1111</u> 1111
---	---------	-------------------------------------

Подчертаните битове от първия октет не се променят. Броят на мрежите от съответния клас се определя от броя на битовете, които могат да бъдат променяни в първия октет. За мрежите от клас А те са 7 бита, от което следва, че броят мрежи е $2^7 = 128$ (от 1 до 127). За клас B – $2^6 = 64$ (от 128 до 191), за клас C – $2^5 = 32$ (от 192 до 223), за клас D и E – $2^4 = 16$ (от 224 до 239 и от 240 до 255).

RFC 6890 (Special-Purpose IP Address Registries) прави "карта" на адресните сегменти (IPv4 и Ipv6) за специално използване.

10.0.0.0/8; 172.16.0.0/12 и 192.168.0.0/16 са блокове от адреси, предназначени за употреба в частни мрежи и са документирани в [RFC1918]. Както е описано в този документ (RFC 1918), адресите от тези блокове не може да бъдат използвани в публични мрежи. Тези адреси могат да бъдат използвани без да има нужда от съгласуване с IANA или някой Internet регистратор.

Класовата адресация не позволява рационалното използване на ограничения ресурс от уникални IP адреси, тъй като не позволява използването на различни мрежови маски на подмрежи. При нея се използва **фиксирания** мрежова маска, което позволява идентифицирането на класа мрежа по първия байт от адреса (но само при класовата адресация).

БЕЗКЛАСОВА IP АДРЕСАЦИЯ (CIDR – Classless Inter-Domain Routing)

При безкласовата IP адресация се използват мрежови маски с променлива дължина (VLSM – Variable Length Subnet Mask), което позволява по-рационалното управление на адресното пространство на мрежата.

Общо адреси	Битове в host_id	префикс	клас	Десетична мрежова маска
1	0	/32		255.255.255.255
2	1	/31		255.255.255.254
4	2	/30		255.255.255.252
8	3	/29		255.255.255.248
16	4	/28		255.255.255.240
32	5	/27		255.255.255.224
64	6	/26		255.255.255.192
128	7	/25		255.255.255.128
256	8	/24	1C	255.255.255.0
512	9	/23	2C	255.255.254.0
1024	10	/22	4C	255.255.252.0
2048	11	/21	8C	255.255.248.0
4096	12	/20	16C	255.255.240.0

8192	13	/19	32C	255.255.224.0
16384	14	/18	64C	255.255.192.0
32768	15	/17	128C	255.255.128.0
65536	16	/16	1B	255.255.0.0
131072	17	/15	2B	255.254.0.0
262144	18	/14	4B	255.252.0.0
524288	19	/13	8B	255.248.0.0
1048576	20	/12	16B	255.240.0.0
2097152	21	/11	32B	255.224.0.0
4194304	22	/10	64B	255.192.0.0
8388608	23	/9	128B	255.128.0.0
16777216	24	/8	1A	255.0.0.0
33554432	25	/7	2A	254.0.0.0
67108864	26	/6	4A	252.0.0.0
134217728	27	/5	8A	248.0.0.0
268435456	28	/4	16A	240.0.0.0
536870912	29	/3	32A	224.0.0.0
1073741824	30	/2	64A	192.0.0.0
2147483648	31	/1	128A	128.0.0.0
4294967296	32	/0	256A	0.0.0.0

Предназначение на мрежовата маска – **определя каква част от IP адреса се отнася за net_ID и каква част – за host_ID.**

Маската се сравнява с мрежата побитово, отляво надясно. В мрежовата маска единиците отговарят на мрежовата част, а нулите – на адреса на възела.

Изпращайки пакет по мрежата, крайното устройство сравнява мрежовата маска със своя IP адрес и IP адреса на получателя. Ако битовете на мрежовата част съвпадат, значи и двата адреса (на изпращача и на подателя) се намират в една и съща мрежа и пакета се доставя локално. Ако не съвпадат, изпращащият възел изпраща пакета на интерфейса на локалния маршрутизатор за изпращане в друга мрежа.

Брой възможни мрежови адреси – взимат се отредените за host_id битове и с тях се повдига 2 на съответната степен. Например, за host_id са отделени 6 бита, тогава възможните мрежови адреси в такава мрежа (/26) е $2^6 = 64$.

Максималният брой мрежови адреси е $2^8 = 256$. От него трябва да извадим два адреса – частта, в която host_id се състои само от 0 се използва за идентификатор на мрежата и не се присвоява на конкретен възел от мрежата.

Частта, в която host_id се състои само от единици се използва за broadcast

разпращане до всички адреси. Този адрес също не се присвоява на конкретни възли от мрежата.

По този начин възможният брой използвани адреси в една мрежа е $256 - 2 = 254$.

ПУБЛИЧНИ И ЧАСТНИ АДРЕСИ

Поради ограничения ресурс от 32-битови IP адреси съществува опасност от тяхното изчерпване. Едно от решенията за намаляване на тази опасност е резервирането на част от адресите за вътрешна употреба в отделните организации.

RFC 1918 регламентира това резервиране. Запазени са няколко диапазона адреси от мрежи, клас A, B и C.

A – запазена е една мрежа от клас A – 10.0.0.0;

B – запазени са 16 мрежи от клас B – 172.16.0.0 – 172.31.0.0;

C – запазени са 256 мрежи от клас C – 192.168.0.0 – 192.168.255.0

Частните адреси позволяват на възлите от мрежата да обменят данни помежду си без да използват **уникални** IP адреси. Частните адреси **не се маршрутизират** в Internet.

Съществуват и частни адреси за диагностика на устройствата. Наричат се **адреси за обратна връзка (loopback address)**. За такива адреси е запазена мрежата 127.0.0.0 от клас A.

ЗАДАЧИ:

Задача 1: Определете от кой клас са следните адреси:

1. 127.0.0.1 - A
2. 201.13.123.245 - C
3. 226.4.37.105 - D
4. 103.24.254.0 - A
5. 10.234.17.25 - A
6. 154.12.255.255 - B
7. 13.13.13.13 - A
8. 204.0.3.1 - C
9. 193.256.1.16 - C
10. 194.87.45.0 - C
11. 195.34.116.255 - C

12. 161.23.45.305 - nonexisted address

Кой от тези адреси може да се ползва като постоянен адрес на възел в Internet?

Всички без 1, 6, 10 и 12:

1 – loopback адрес;

10 – идентификатор на мрежа, не се присвояват на крайни устройства;

6 – broadcast адрес;

12 – такъв адрес не съществува, последният октет е извън обхвата 0-255.

Задача 2: Възел в мрежата има адрес 198.65.12.67, мрежовата маска е 255.255.255.240. Определете адреса на подмрежата. Какъв е максималният брой адреси в тази (под)мрежа?

Започва се от маската – 255.255.255.240 отговаря на префикс /28 – взети са 4 бита от host_id => имаме 16 мрежи с 16 адреса във всяка мрежа:

198.65.12.0-198.65.12.15 – Ist subnet;

198.65.12.16-198.65.12.31 – IInd subnet;

198.65.12.32-198.65.12.47 – IIIrd subnet;

198.65.12.48-198.168.12.63 – IVth subnet;

198.65.12.64-198.65.12.79 – Vth subnet

Следователно адресът 198.65.12.67 попада в петата подмрежа. Мрежовият адрес на тази мрежа е 198.65.12.64/28. Максималният брой възли в тази мрежа е $2^4 - 2 = 16 - 2 = 14$.

Сравняваме двоично само последния октет от адреса с последния октет от мрежовата маска:

67 – 01000011

240 – 11110000

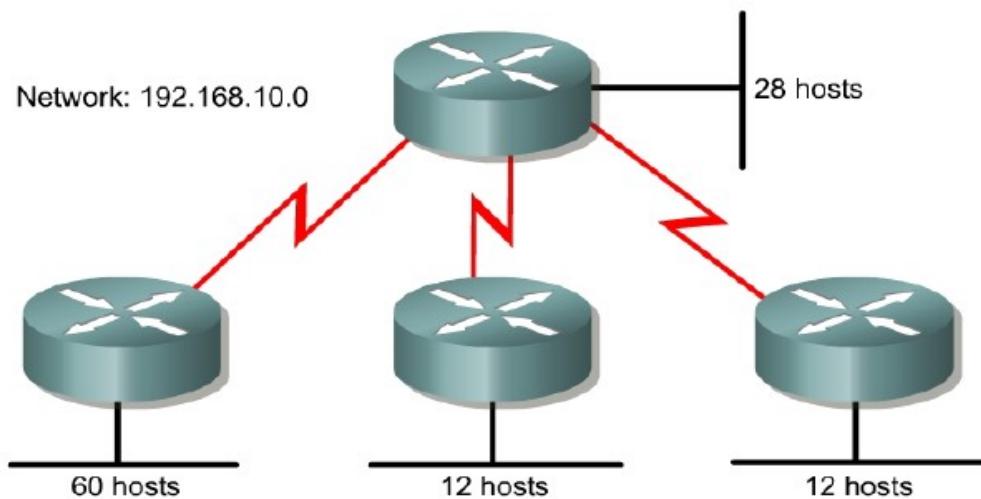
64 – 01000000

→ мрежовият адрес е 198.65.12.64/28

```
# sipcalc 108.65.12.67/28
host address:198.65.12.67
network address: 192.168.12.64
network mask: 255.255.255.240
network mask (bits): 28
network mask (hex): FFFFFFF0
```

broadcast address: 192.65.12.79
 addresses in network: 16
 network range: 192.65.12.64-192.65.12.79
 usable addresses: 192.65.12.65-192.65.12.78

Задача 3:



Имате мрежата на горната фигура. Отпуснат ви е IPv4 адресния блок 192.168.10.0/24. Как ще разпределите адресното пространство така, че да имате възможно най-оптимално използване на IP адресите?

(Заб. Тук можете да посочите различни префикси и различен брой мрежовите сегменти и хостове в тях)

Задача 4:

В Интернет пространството трябва да рекламирате префиксите 62.44.120.0/24, 62.44.121.0/24, 62.44.122.0/24 и 62.44.123.0/24. Как можете да представите тези 4 префикса само с един, за да не хабите честотна лента по линията към съседния рутер. (тук имаме супернетване, отг. е 62.44.120.0/22)

(Може да се посочи и пример с префикси 62.44.110.0/24, 62.44.111.0/24, ... 62.44.117.0/24 – 62.44.110.0/21)

Задача 5:

IP мрежата 62.44.109.0/24 е разделена на 4 подмрежи. Кой е първият (последният, бродкаст и т.н.) използваем (хост) адрес на втората (3-та, 4-та) подмрежа?

ПРОТОКОЛ IPv6

IPv6 не е обратно съвместим с IPv4, необходими са промени в мрежови устройства и услуги. Според RFC 4291: адресното пространство от 32-битово става 128-битово:

232 (4.3 x 109) с/y 2128 (3.4 x 1038). Една основна характеристика е автоконфигурирането. RFC 4862 дефинира автоматично (plug-and-play) присвояване на адрес без помощта на DHCP сървър като в IPv4.

Цели на протокола IPv6 – същите като на протокола IPv4: присъединяване на адреси към мрежовите устройства; маршрутизиране на пакетите в мрежата...

За разлика от протокола IPv4, в който се използва десетична нотация на записване на мрежовите адреси, в шестата версия на протокола IP за избягване на объркване се използва по-различна нотация. За разделител между отделните части на адреса се използва :, а не .. Също така не се използва десетичен запис на числата, а шестнадесетичен.

Структура на хедъра в IPv6

Version (4)	Traffic Class (8)	Flow Label (20 bits)				
Payload length (16)		Next Header (8)		Hop Limit (8)		
Source Address (128 bits)						
Destination Address (128 bits)						

traffic class (заменя IPv4 ToS);

flow label (ново QoS management);

payload length (до 64KB);

next header (заменя IPv4 protocol);

hop limit (заменя IPv4 TTL).

IPv6 адресиране

2001:0db8:9095:02e5:0216:cbff:feb2:7474

8 групи с по 4 шестнадесетични числа

Мрежовият префикс (RFC 4291) е аналогичен на означението с "/" на SM в IPv4:

Структура на адрес от протокола IPv6 – състои се от 8 hexets за разлика от 4-те октета при четвъртата версия на протокола. Адресът е разделен с : на групи числа в интервала 0000-FFFF (0-65535) за разлика от протокола IPv4, където октетите

съдържат числата от 0 до 255 (00-FF). Типичният вид на един адрес от шестата версия на протокола има следния вид:

2001:05c0:9168:0000:0000:0000:0001/128

При записването на тези адреси е допустимо:

1. премахването на водещата 0 от съответната група – например 05c0 може да бъде записано като 5c0;
2. веднъж и само веднъж в целия адрес може да бъде заменена група от последователни 0000 със символа „::“ – например 0000:0000:0000:0000 да бъде изписана като ::

Горният адрес 2001:05c0:9168:0000:0000:0000:0001/128 със спазване на горните правила може да бъде записан като 2001:5c0:9168::1/128.

Други примери за подобно изписване:

ПРАВИЛНО представяне на 60-bit префикс:

2001:0DB8:0000:CD30:0000:0000:0000/60

2001:0DB8::CD30:0:0:0/60

2001:0DB8:0:CD30::/60

От шестата версия на протокола са премахнати някои функции, усложняващи работата на маршрутизаторите:

1. маршрутизаторите повече не са длъжни да фрагментират пакетите, а просто ги отхвърлят с ICMP съобщение за надвишаване на MTU. Фрагментацията е възможна по инициатива на предаващата страна и е нейна грижа. Използва се технологията [Path MTU discovery](#) за предварително определяне на маршрута, по който ще минат пакетите до получателя им;
2. от IP заглавието на протокола е изключена контролната сума, която е приета, че е излишна при наличието на контролни суми в каналните (ethernet) и транспортни (TCP и UDP) протоколи.

Подобрения спрямо IPv4:

1. При скоростни мрежи е възможно поддръжката на огромни пакети (jumbograms) с размер до 4 gb;
2. TimeToLive (TTL) е преименуван на HopLimit;
3. Поява на етикети на потоци и класове на трафик (свързано е с QoS);
4. Поява на многоадресно (multicast) изпращане на пакети.

АВТОКОНФИГУРИРАНЕ

При първоначалната инициализация на мрежовия интерфейс, на него се дава локален IPv6 адрес, състоящ се от префикс **fe80::/10** и идентификатор на интерфейса, разположен в младшата част на адреса. Като идентификатор на интерфейса се използва 64 битовия, разширен уникален идентификатор EUI-64, асоцииран често с MAC адреса на интерфейса. Локалният IPv6 адрес е действителен само в границите на ethernet сегмента и основно се използва за обмяна на пакети по протокола ICMPv6.

За получаване на друг адрес, възелът може да изпрати ICMPv6 съобщение „Router Solicitation“ до груповия (multicast) адрес на маршрутизатора, който отговаря с ICMPv6 съобщение „Router Advertisement“, съдържащо информация за мрежовия префикс, за адреса на шлюза (gateway), за адресите на рекурсивните DNS сървъри, за MTU и още други параметри. На основата на тази информация и обединявайки мрежовия префикс и идентификатора на интерфейса, възелът избира нов адрес. За защита на персонални данни, идентификатора на интерфейса може да бъде заменен с псевдослучайно число.

За по-голям административен контрол може да бъде използван и протокола DHCPv6, позволяващ даването на конкретен адрес на конкретен възел.

ЕТИКЕТ НА ПОТОК (FLOW LABELS)

Позволява значително опростяване на процедурата на маршрутизация на еднородни потоци от пакети.

Поток – последователност от пакети, изпратени до определен адресат. Предполага се, че всички пакети от този поток ще бъдат обработени по определен начин, който се задава в допълнителните заглавия на пакета.

Допустимо е съществуването на повече от един поток между изпращача и получателя. Етикета се присвоява от възела, който изпраща пакета и представлява 20-битово псевдослучайно число. Всички пакети от един поток трябва да имат еднакви етикети, обработвани от маршрутизатора.

КЛАСОВЕ ТРАФИК

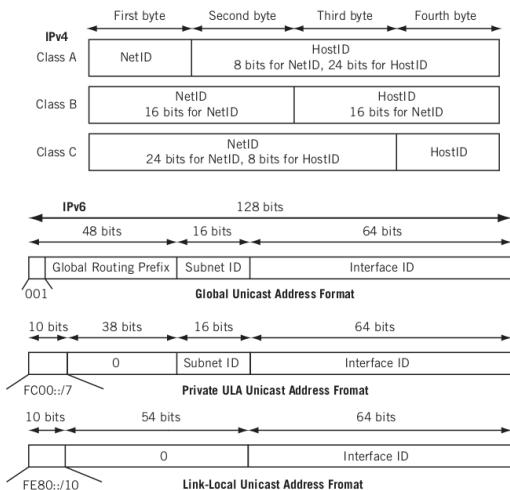
Клас на трафика	Предназначение
0	Нехарактеризиран трафик
1	Запълващ трафик (мрежови новини)
2	Несъществен информационен трафик (email)
3	резерв
4	Съществен трафик (FTP, HTTP, NFS)

5	резерв
6	Интерактивен трафик (telnet, X-terminal, SSH)
7	Управляващ трафик (маршрутна информация, SNMP)

ТИПОВЕ IPv6 АДРЕСИ

- unicast – адресират само един интерфейс, който получава само пакети, адресирани до него
- anycast – синтактично не се различават от unicast адресите, но адресират група от интерфейси. Пакет, изпратен на такъв адрес, ще се получи на най-близкия по метрика интерфейс. Този тип адреси се използват изключително от маршрутизатори;
- multicast – също адресират група от интерфейси. Пакет, изпратен до такъв адрес, ще се получи на **всички** интерфейси, присъединени към групата за много адресно разпространяване.
- **Защо в IPv6 няма Broadcast адреси?**

Основни IPv4 и IPv6 формати:



Задачи по IPv6

1. На вашия компютър изпълнете командата **ip a**. Кои са MAC, Link-local и global

scope адресите на съответните интерфейси?

2. На вашия компютър изпълнете командите:

ip address add 192.0.2.10/27 dev dummy0 и
ip address add 2001:db8:1::/48 dev dummy0

Какво постигнахте с тях?

3. На вашия компютър изпълнете команда **ip neighbor** и обясните как функциите Neighbor Discovery (ND) и Router Discovery (RD) на ICMPv6 заместват ARP. Съответно и автоконфигурирането – Stateless получаването на IPv6 адреси. Да се каже нещо и за **radvd**. (обърнете внимание: **lladdr** - link layer address, е различен от Link Local.)

4. Напишете коректните съкращения за IPv6 адресите:

2001:0d02:0000:0000:0014:0000:0000:0095

2001:0d02:0000:0000:0014:0000:0000:0095

2001:0d02:0000:0000:0014:0000:0000:0095

5. Имате MAC адрес на интерфейс wlan0 = 00:0e:2e:d1:ab:15 или 00-0C-27-A2-13-1B. Какъв ще бъде Host ID на IPv6 link local адреса на интерфейс wlan0 в двета случая?

6. Как би изглеждал IPv6 адреса 2001:4b58:acad:252::2e в разгърнат вид?

Тема № 3. NAT – NETWORK ADDRESS TRANSLATION и IPTABLES

- [RFC 1631 – The IP Network Address Translator \(NAT\)](#)
- [RFC 2663 – IP Network Address Translator \(NAT\) Terminology and Considerations](#)
- [RFC 3022 – Network Address Translation \(Traditional NAT\)](#)

Технологията NAT е предложена за решаване на проблема с изчерпването на **уникалните** IP адреси, предназначени за раздаване и връзка между възлите в Internet.

Възможни решения на този проблем са:

1. проектиране на нова версия на IP протокола (IPv6) – изисква дълго време за разработване и внедряване;
2. преминаване към безкласова адресация и маршрутизиране (CIDR), позволяващо по-рационално използване на съществуващите IP адреси – по времето, когато се взима решението за такъв преход, по-голямата част от мрежите от класове А и В вече са раздадени;
3. използване на публични и частни IP адреси и тяхното транслиране.

Използването на NAT позволява решаването на следните проблеми:

1. осигуряване на корпоративните и частни локални мрежи с голям брой частни IP адреси, като при това не възникват конфликти от използването на еднакви мрежови адреси от различни организации;
2. осигуряване на допълнителна безопасност на възлите от вътрешната мрежа чрез тяхното скриване от външната мрежа, един вид защитна стена¹;
3. организиране на достъпа до Internet през един-единствен шлюз с използване на един единствен **уникален** IP адрес.

Шлюз (aka [gateway](#)) – крайно устройство, което е едновременно свързано към повече от една мрежа. Всеки шлюз трябва да има присвоен IP адрес от всяка мрежа, към която е свързан.

Защо са необходими шлюзовете? Защото гледната точка на възел от Ethernet мрежа е ограничена – той може да обменя информация само с възлите от мрежата, в която се намира. Достъпът до всички останали възли се извършва само през машини със специално предназначение – шлюзовете.

Освен гореизброените проблеми, съвременните реализации на технологията за NAT позволяват решаването и на различни други задачи, засягащи администрацията на мрежите:

1. контрол и отчитане на трафика на крайните потребители към Internet;
2. наблюдение на поведението им в мрежата;
3. водене на статистика.

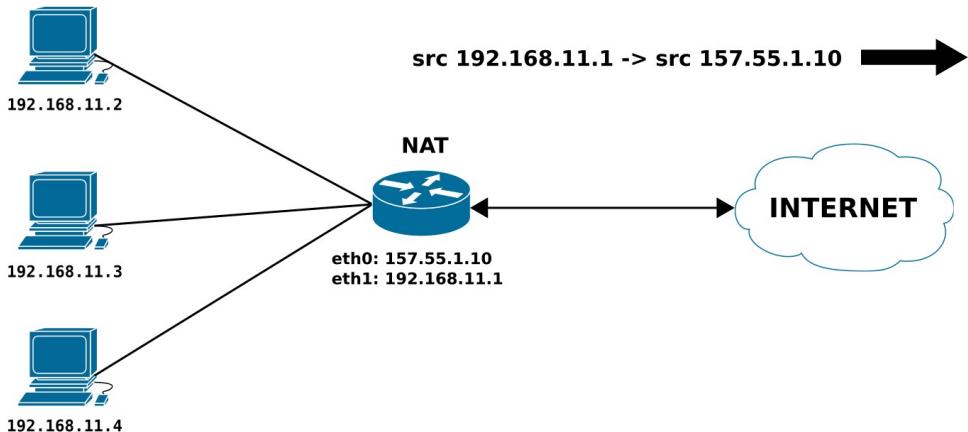
Апаратна реализация на NAT е вградена в различни ADSL и кабелни модеми, безжични и др. маршрутизатори.

Технологията NAT описва процеса на модифициране на мрежовия адрес (а понякога и на портовете), съдържащи се в заглавните части (header) на IP пакетите при тяхното предаване по мрежата.

¹ Макар, че идеята за security by obscurity не е най-доброто нещо. Но дали имаме чисто obscurity :)

Технологията NAT позволява на едно единично устройство, обикновено маршрутизатор, да играе ролята на агент между локалната (частна) мрежа и Internet, което означава, че е необходим само един, уникатен IP адрес за представяне на цялата група възли от локалната мрежа.

Нека имаме следната конфигурация:



Фигура 1. Принцип на действие на NAT

При изпращането на IP пакет от 192.168.11.3 към Internet, в неговата заглавна част (header) е записан адреса на източника (source address) – 192.68.11.3. В NAT сървъра се извършва транслацията на този адрес от 192.168.11.3 на 157.55.1.10. Обикновено възелът, който извършва това преобразуване изпълнява и функцията на защитна стена и граничен маршрутизатор.

При получаване на отговор на изпратения IP пакет неговият адрес на получател няма да бъде 192.168.11.3, а ще бъде 157.55.1.10. Решението е използване на вградена в NAT сървъра таблица, пазеща информация за всяка създадена връзка с използване на номерата на порт на източника. Всеки TCP или UDP пакет съдържа в себе си две 16 битови числа, указващи номерата на портове на източника и на получателя.

Мрежови порт – програмна абстракция, използвана за определяне на различните крайни точки на комуникационните канали в рамките на един възел от мрежата.

Мрежовият адрес, заедно с номера на порта идентифицират еднозначно крайната точка на един (комуникационен) канал в рамките на една мрежа. Комбинацията от мрежов адрес и номер на порт се нарича **транспортен адрес** (по OSI модела).

Днес, описвайки TCP съединения (сесии), говорим за сокети (sockets). Това понятие е въведено за първи път в ОС 4.2BSD Unix (1983 г.), известно като **Berkeley sockets**, програмен интерфейс (API) за между процесни комуникации (IPC). Сокет се обвързва с адресната структура **локален IP адрес и номер на порт**. В някои книги може да се срещне и определението, включващо **локален и отдалечен IP адрес и номер на порт**, които са необходими за установяване на TCP сесия. За сведение, терминът сокет за първи път се дефинира в RFC 147 (1971 г.), както е използван в ARPANET – 32-битово число.

Портовете се ползват от **транспортния слой** на OSI модела (слой 4).

Два комуникиращи си възела от мрежата могат да имат повече от един комуникационен канал помежду си, като в този случай каналите се различават поне по един от портовете си. Мрежовият порт може да се разглежда като аналогия на

апаратния порт → място на контакт между комуникиращи си процеси от различни възли в мрежата.

Таблицата, поддържана от машината, която извършва NAT може да има 65535 реда (2^{16}), в която се записва двойката **source_id** ↔ **source_port** за всеки изходящ пакет. След това се извършва както замяна на IP адреса, така и на оригиналния номер на порт на източника на пакета и той се изпраща по предназначение. Когато се получи отговор, номерът на порт на получателя се използва като индекс в таблицата за NAT, за да се извлече IP адресът и номерът на порт на възела от вътрешната мрежа, който трябва да получи този отговор.

Апаратна реализация на NAT е вградена в различни ADSL и кабелни модеми, безжични и др. маршрутизатори. Основният принцип на работа на NAT е следния: в модула, извършващ транслацията на мрежовите адреси е вградена таблица, в която се създава запис за всяка осъществена връзка. В него се съдържа IP адресите и номера на портове на източника и на получателя на изпратения пакет. С помощта на този запис се извърша транслирането на мрежовите адреси. Нека разгледаме следния пример: имаме локална мрежа от компютри с един общ изход към Internet. Един от компютрите от тази мрежа (192.168.11.3 например) осъществява връзка към друг компютър (например www.uni-sofia.bg), намиращ се някъде в глобалната мрежа Internet. Връзката към Internet преминава през маршрутизатор. Адресът на компютъра, изпращащ пакета, е 192.168.11.3, а адресът на получателя е 62.44.96.22. За всяка осъществена връзка, NAT отваря нов порт. В таблицата за NAT се добавя запис за изпратения пакет – IP address & port number. След това NAT променя полето в заглавната част на пакета (полето [Source Address](#)), като премахва адреса на компютъра от локалната мрежа (192.168.11.3) и го заменя с неговия публичен адрес (157.55.1.10), през който се осъществява връзката към Internet. Обратният пакет съдържа адрес на получателя 157.55.1.10. В таблицата на NAT се намира коя двойка IP_address и port_number отговаря на получени пакет и полето за destination_address се променя с IP адреса от вътрешната мрежа на възела, изпратил първоначално пакета.

Информация за iptables можете да намерите в [тап](#) страниците на CentOS, например:

<https://linux.die.net/man/8/iptables>

<http://ipset.netfilter.org/iptables.man.html#lbAO>

<https://upcloud.com/community/tutorials/configure-iptables-centos/>

https://fedoraproject.org/wiki/How_to_edit_iptables_rules

<https://www.digitalocean.com/community/tutorials/how-to-list-and-delete-iptables-firewall-rules>

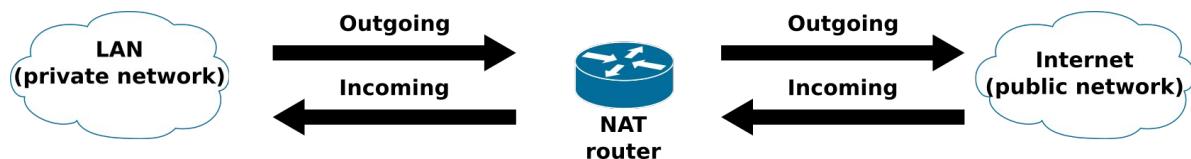
Недостатъци на NAT

1. Транслирането на мрежови адреси наруши архитектурния модел на протокола IP, според който всеки IP адрес е уникален, т.е идентифицира един единствен възел в Internet. Цялата софтуерна инфраструктура на Internet се крепи на този факт. С помощта на NAT, хиляди машини може да използват примерно адрес 192.168.11.3;
2. NAT променя характера на Internet – от connectionless ориентирана към

connection ориентирана, тъй като NAT поддържа информация за съответствието на всяка връзка, преминала през нея. Един срив на машината с NAT и всички TCP връзки ще бъдат разрушени;

3. NAT нарушава фундаменталното правило за разделяне на отделните слоеве. Излизането на една нова версия на протокола TCP, използваща 32 битови номера на портове или преминаване към друг транспортен протокол ще означава край на използването на тази технология;
4. Някои приложения включват в тялото на текста самите IP адреси. NAT не знае какво има в пакета и следователно не може да смени тези адреси, което ще доведе до пропадане на връзката с отдалечения възел. Пример за такъв протокол е FTP;
5. Тъй като номерът на порта е 16-битово число, зад един IP адрес могат да бъдат „скрити“ не повече от 65535 машини;
6. Номерата на портовете са „адреси“ на процеси, а не на възли в мрежата;
7. Маршрутизаторите са длъжни да обработват пакети само от слой 3 на модела OSI;
8. Възлите са длъжни да си взаимодействват директно, без намесата на други възли, променящи IP адреси и номера на портове.

Решения на всички горни недостатъци → преминаване към използване на протокол IPv6.



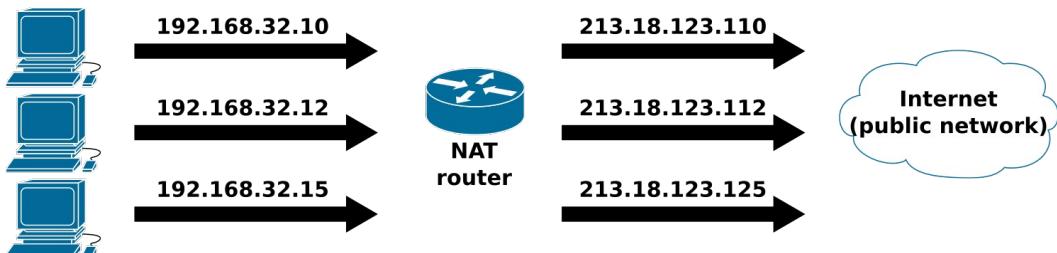
Фиг. 2. Схема на действие на NAT

ВИДОВЕ NAT

Статичен NAT

При статичния NAT имаме конфигурирани определен брой публични IP адреси, отговарящи на определен брой IP адреси от вътрешната мрежа.

Присъединяването (mapping) на локалните адреси към публичните е едно към едно – един локален адрес се заменя винаги с един и същ публичен адрес. Този подход е полезен, когато има нужда от достъп отвън до някой възел вътре в мрежата..

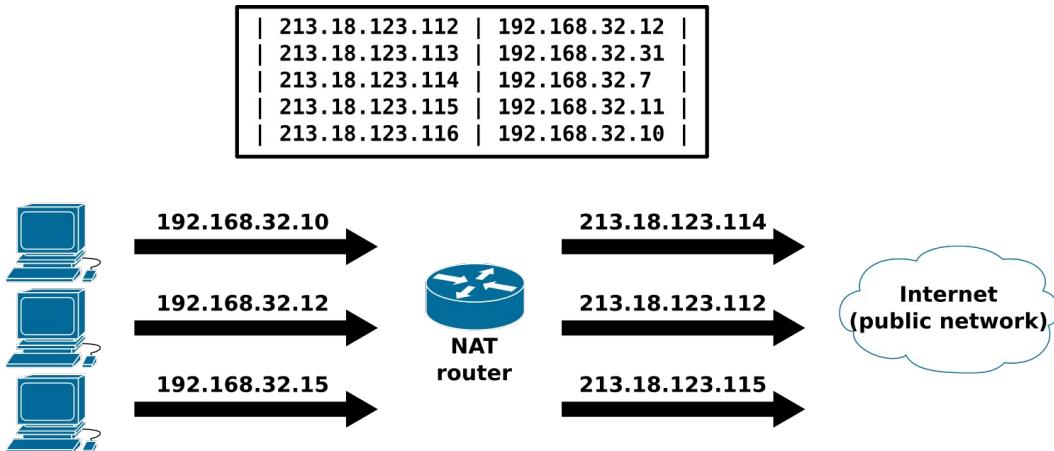


Фиг. 3 Схема на действие на статичния NAT

При статичния NAT, компютърът с адрес 192.168.32.10 винаги ще бъде транслиран до 213.18.123.110. По този начин имаме ясно изразена връзка между локалната и

публичната мрежа (Internet).

Динамичен NAT

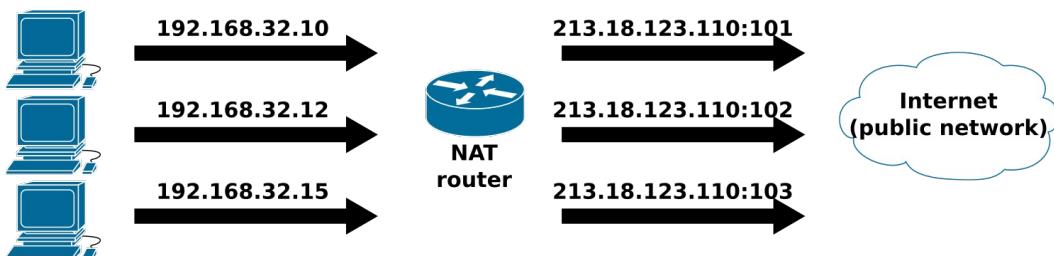


Фиг. 4 Схема на действие на динамичния NAT

При динамичния NAT, адресът на възела от вътрешната мрежа ще бъде транслиран към първия свободен адрес от отредения за транслиране обхват от публични адреси.

ПРЕТОВАРВАНЕ (OVERLOADING)

Това е разновидност на динамичния NAT.



Фиг. 5. Схема на действие на overloading

При него, множеството адреси от локалната мрежа се транслират към един-единствен публичен адрес, но с различни номера на портове.

Претоварването се използва от свойството на TCP/IP стека, наречено мултиплексиране (multiplexing), което позволява на компютъра да поддържа няколко конкурентни връзки с отдалечения компютър (или компютри), използвайки различни TCP или UDP портове.

Всеки IP пакет има заглавна част, (header), която съдържа следната информация:

- **Адрес на източник (Source Address)** - IP адресът на изпращащия пакета компютър, примерно 201.3.83.132;
- **Номер на порт на източника (Source Port)** – номерът на TCP или UDP порт, присъединен от изпращащия компютър на този пакет, примерно порт 1080;
- **Адрес на получател (Destination Address)** - IP адресът на получаващия пакета компютър, примерно 145.51.18.223;
- **Номер на порт на получателя (Destination Port)** – Номерът на TCP или UDP

порт, който изпращащият компютър е поискал да бъде отворен от получаващия компютър, примерно порт 3021.

iptables

Netfilter – пакетния филтър в CentOS, с помощта на койсто се извършва трансляцията на мрежови адреси (NAT). Той представлява рамка (framework), даваща ни достъп до пакетите извън стандартния сокет интерфейс на unix/linux.

Iptables – потребителски инструмент за дефиниране на правила за филтриране на пакети и транслиране на мрежови адреси.

На практика, често под името **iptables** се разбира цялата инфраструктура, включваща netfilter, следенето на връзките, транслирането на мрежовите адреси и самия инструмент iptables.

Дефинираните правила се групират във вериги, които от своя страна се групират в таблици.

ПРАВИЛА → ВЕРИГИ → ТАБЛИЦИ

Всяко правило дефинира условие и цел. Целта се прилага върху всички пакети, които удовлетворяват условието.

Всеки пакет преминава поне през една верига и се сравнява последователно с правилата от веригата. Ако се получи съвпадение, обхождането на веригата се прекратява и се прилага съответното правило.

Ако пакетът не удовлетвори нито едно условие, тогава върху него се прилага политиката по подразбиране на веригата.

Цел на някое право може да бъде нова верига. Ако пакетът премине през втората верига, без да удовлетвори нито едно условие от нейните правила, се продължава с първата верига. **Всяка верига представлява подреден списък с правила.**

Веригите се групират в таблици. Всяка таблица е свързана с различен вид обработка на пакетите. Няма ограничения за влагането на веригите една в друга.

В netfilter има три основни вериги – input, output и forward.

Могат да бъдат създавани нови вериги.

Три основни таблици – filter, nat и mangle.

Таблица filter – използва се за филтриране на пакетите (блокиране (drop) или разрешаване (accept)).

Тази таблица има три вериги:

INPUT – всички пакети, отиващи към защитната стена преминават през тази верига;

OUTPUT – всички пакети, излизящи от защитната стена преминават през тази верига;

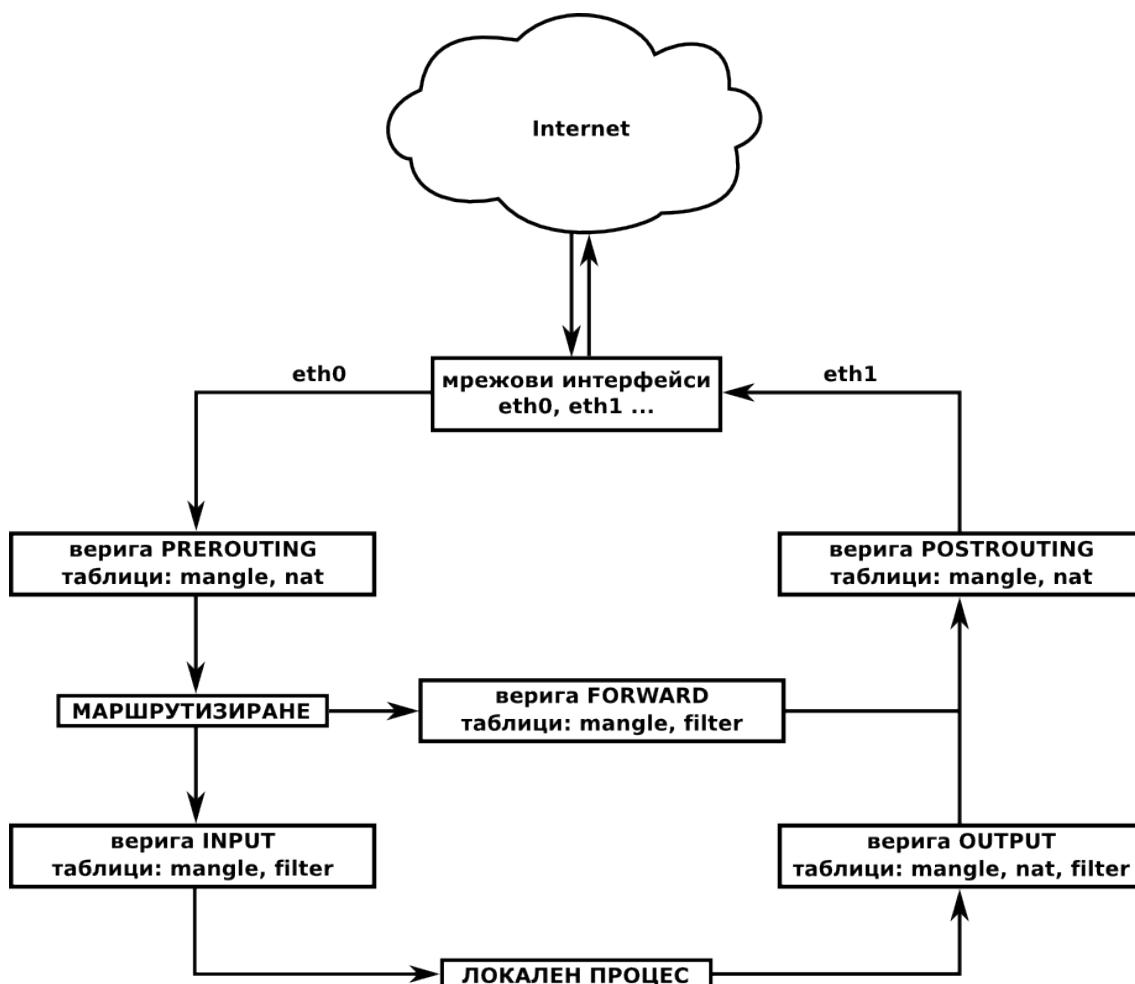
FORWARD – през тази верига преминват всички пакети, които преминава през защитната стена (такива пакети, които се маршрутизират).

Таблица nat – съхранява правилата, използвани за промяна на мрежовите адреси и номерата на портове (NAT). През тази таблица винаги преминава първият пакет на всяка нова връзка. Съдържа също три вериги:

PREROUTING – входящите пакети преминават през нея преди да се вземе решение за тяхното маршрутизиране. В тази верига се осъществява така наречения DNAT (Destination Network Address Translation) – промяна на адреса на получателя на пакета;

POSTROUTING – през нея преминават изходящите пакети, след като е взето решение за тяхното маршрутизиране. Тук се осъществява така наречения SNAT (Source Network Address Translation) – промяната на source адреса на изпращача на пакета;

OUTPUT – в тази верига се извършва ограничен DNAT над локално генерираните пакети.



Фиг. 6. Схема на действието на пакетния филтър netfilter

Таблица mangle – използва се за промяна на допълнителните полета в заглавната част (ip header) на пакетите. През нея преминават всички пакети. Поради специфичните си задачи съдържа в себе си всички предефинирани вериги:

PREROUTING – през нея преминават всички пакети, влизщи в системата;

INPUT – през нея преминават всички пакети, предназначени за системата;

FORWARD – през нея преминават всички пакети, минаващи транзитно през системата;

OUTPUT – през нея преминават всички пакети, напускащи (и произлизящи от) системата;

POSTROUTING – през нея преминават всички пакети, напускащи системата.

Както вече споменахме, всяко правило има цел. Тя може да бъде друга верига или някоя от предефинираните цели:

ACCEPT – указва на пакетния филтър да приеме пакета. В зависимост от веригата, това означава изпълнение на различни действия над пакета;

DROP – указва на пакетния филтър да отхвърли пакета и да не го обработва повече. На източника на пакета не се изпраща никакъв отговор и за него блокирането се изразява в изтичане на комуникационния таймаут (и разпадане на връзката).

Допълнителни цели – в ръководството на iptables.

MASQUERADING – ограничена форма на промяна на адреса на източника на пакета (SNAT) за мрежи, чийто IP адрес на външния интерфейс е динамичен (получава се от dhcp сървър). В този случай, вместо да се сменя SNAT правилото при смяна на адреса се използва автоматично адресът на изходящия интерфейс при транслирането.

Синтаксис:

```
# iptables [-t table] -[ADC] chain rule-specification [options]
```

Трябва да се добавят различни примери за правила на iptables

```
# iptables -t nat -A POSTROUTING -s 172.18.0.0/20 -j SNAT --to-source 62.44.102.7
```

Примери за използване на iptables

1. Показване състоянието на iptables

Става с използването на следната команда като root:

```
# iptables -L -n -v
```

изходът от тази команда може да изглежда така:

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in      out      source destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in      out      source destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in      out      source destination
```

Той ни показва, че защитната стена (iptables) не е активна. Следващият примерен изход от горната команда е от активирана защитна стена:

```
# iptables -L -n -v
```

```
Chain INPUT (policy ACCEPT 8771K packets, 902M bytes)
 pkts bytes target     prot opt in      out      source           destination
 70568 5735K DROP       all   --  eth1    *       0.0.0.0/0          0.0.0.0/0
MAC 00:0A:E6:AF:1C:50
 115K   10M ACCEPT      all   --  lo     *       0.0.0.0/0          0.0.0.0/0
```

```
2598 209K DROP      udp  --  *      *      0.0.0.0/0      0.0.0.0/0
! ctstate RELATED,ESTABLISHED udp dpt:123
```

Chain FORWARD (policy ACCEPT 778M packets, 587G bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
69184	5928K	ACCEPT	tcp	--	*	*	0.0.0.0/0	62.44.102.7
			tcp	dpt:22				
2824K	679M	ACCEPT		all	--	*	*	0.0.0.0/0
					62.44.102.206			
0	0	REJECT	tcp	--	*	*	62.44.102.23	0.0.0.0/0
			tcp	dpt:445	reject-with	tcp-reset		
3	144	REJECT	tcp	--	*	*	62.44.102.41	0.0.0.0/0
			tcp	dpt:445	reject-with	tcp-reset		
490	34938	DROP	udp	--	*	*	0.0.0.0/0	62.44.108.39
			udp	dpt:123				
750	43829	DROP	udp	--	*	*	0.0.0.0/0	62.44.108.38
			udp	dpt:123				
488	35086	DROP	udp	--	*	*	0.0.0.0/0	62.44.108.37
			udp	dpt:123				
489	33663	DROP	udp	--	*	*	0.0.0.0/0	62.44.108.36
			udp	dpt:123				
4528	178K	DROP	udp	--	*	*	0.0.0.0/0	62.44.108.35
			udp	dpt:123				
0	0	DROP	udp	--	*	*	62.44.108.35	0.0.0.0/0
			udp	spt:123	dpt:123			
97403	7803K	DROP	udp	--	*	eth1	0.0.0.0/0	0.0.0.0/0
			udp	dpt:123	! ctstate	RELATED,ESTABLISHED		
73M	54G	ACCEPT	all	--	*	*	0.0.0.0/0	62.44.108.46
4579K	1124M	ACCEPT	all	--	*	*	0.0.0.0/0	62.44.108.44
4314K	3446M	ACCEPT	all	--	*	*	62.44.108.44	0.0.0.0/0
67M	36G	ACCEPT	all	--	*	*	62.44.108.46	0.0.0.0/0
71M	29G	ACCEPT	all	--	*	*	0.0.0.0/0	62.44.108.40
74M	146G	ACCEPT	all	--	*	*	62.44.108.40	0.0.0.0/0
13M	2063M	ACCEPT	all	--	*	*	62.44.108.32/28	0.0.0.0/0
15M	11G	ACCEPT		all	--	*	*	0.0.0.0/0
				62.44.108.32/28				
0	0	ACCEPT	all	--	*	*	62.44.102.1	0.0.0.0/0
57098	3617K	ACCEPT	all	--	*	*	0.0.0.0/0	62.44.102.1
500M	55G	ACCEPT	all	--	*	*	62.44.102.2	0.0.0.0/0
737M	774G	ACCEPT	all	--	*	*	0.0.0.0/0	62.44.102.2
266K	56M	ACCEPT	all	--	*	*	62.44.102.4	0.0.0.0/0
289K	104M	ACCEPT	all	--	*	*	0.0.0.0/0	62.44.102.4
93	8511	ACCEPT	all	--	*	*	62.44.102.5	0.0.0.0/0
47582	3093K	ACCEPT	all	--	*	*	0.0.0.0/0	62.44.102.5
34M	26G	ACCEPT	all	--	*	*	62.44.102.6	0.0.0.0/0

```

35M 15G ACCEPT      all  --  *      *      0.0.0.0/0      62.44.102.6
27M 35G ACCEPT      all  --  *      *      0.0.0.0/0      62.44.102.7
    0    0 ACCEPT      all  --  *      *      62.44.102.8      0.0.0.0/0
101K 5853K ACCEPT    all  --  *      *      0.0.0.0/0      62.44.102.8
3836K 556M ACCEPT    all  --  *      *      62.44.102.9      0.0.0.0/0
3775K 1329M ACCEPT   all  --  *      *      0.0.0.0/0      62.44.102.9
    0    0 ACCEPT      all  --  *      *      62.44.102.10     0.0.0.0/0
45466 3045K ACCEPT   all  --  *      *      0.0.0.0/0      62.44.102.10
1973K 503M ACCEPT    all  --  *      *      62.44.102.11     0.0.0.0/0
1226K 2034M ACCEPT   all  --  *      *      0.0.0.0/0      62.44.102.11
    0    0 ACCEPT      all  --  *      *      62.44.102.12     0.0.0.0/0
51647 3361K ACCEPT   all  --  *      *      0.0.0.0/0      62.44.102.12
    0    0 ACCEPT      all  --  *      *      62.44.102.13     0.0.0.0/0
39292 2749K ACCEPT   all  --  *      *      0.0.0.0/0      62.44.102.13
    0    0 ACCEPT      all  --  *      *      62.44.102.14     0.0.0.0/0
50230 3272K ACCEPT   all  --  *      *      0.0.0.0/0      62.44.102.14
4453K 768M ACCEPT    all  --  *      *      62.44.102.15     0.0.0.0/0
4422K 6100M ACCEPT   all  --  *      *      0.0.0.0/0      62.44.102.15
    0    0 ACCEPT      all  --  *      *      62.44.102.16     0.0.0.0/0
46230 3102K ACCEPT   all  --  *      *      0.0.0.0/0      62.44.102.16
    0    0 ACCEPT      all  --  *      *      62.44.102.17     0.0.0.0/0
63609 3994K ACCEPT   all  --  *      *      0.0.0.0/0      62.44.102.17
1171K 68M ACCEPT      tcp  --  *      *      0.0.0.0/0      62.44.102.18
tcp dpt:80
    0    0 ACCEPT      all  --  *      *      62.44.102.19     0.0.0.0/0
42867 2914K ACCEPT   all  --  *      *      0.0.0.0/0      62.44.102.19
    0    0 ACCEPT      all  --  *      *      62.44.102.20     0.0.0.0/0
47721 3156K ACCEPT   all  --  *      *      0.0.0.0/0      62.44.102.20
6095K 8167M ACCEPT   all  --  *      *      62.44.102.28     0.0.0.0/0
5730K 5535M ACCEPT   all  --  *      *      0.0.0.0/0      62.44.102.28
7927K 2174M ACCEPT   all  --  *      *      62.44.102.67     0.0.0.0/0
8347K 1343M ACCEPT   all  --  *      *      0.0.0.0/0      62.44.102.67
    15M 27G ACCEPT     all  --  *      *      0.0.0.0/0      62.44.102.79
    19M 5942M ACCEPT   all  --  *      *      62.44.102.79     0.0.0.0/0
    18M 1400M ACCEPT   all  --  *      *      62.44.102.89     0.0.0.0/0
    18M 44G ACCEPT     all  --  *      *      0.0.0.0/0      62.44.102.89
    90M 4252M REJECT    tcp  --  eth1  *      0.0.0.0/0      0.0.0.0/0
tcp multiport dports 25,137,138,139,445 reject-with icmp-host-unreachable
    164K 14M DROP       udp  --  eth1  *      0.0.0.0/0      0.0.0.0/0
udp multiport dports 137,138,139
    44M 2241M REJECT    tcp  --  *      eth1  0.0.0.0/0      0.0.0.0/0
! ctstate RELATED,ESTABLISHED reject-with icmp-host-unreachable

```

```

    79M 8159M DROP      udp  --  *      eth1      0.0.0.0/0          0.0.0.0/0
! ctstate RELATED,ESTABLISHED

  184M  286G ACCEPT    all  --  *      eth1      62.44.96.0/19        0.0.0.0/0
  146M   29G ACCEPT    all  --  eth1      *          0.0.0.0/0
62.44.96.0/19

  614K   31M           icmp --  *      *          0.0.0.0/0          0.0.0.0/0
icmp type 8 recent: SET name: DEFAULT side: source

```

Chain OUTPUT (policy ACCEPT 26M packets, 2116M bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
------	-------	--------	------	-----	----	-----	--------	-------------

където:

- **-L** : показва правилата в iptables;
- **-v** : показва детайлна информация. Тази настройка създава списък с името на мрежовия интерфейс, настройките на конкретните правила и маската за TOS. Показват се и броя на преминалите пакети, както и тяхната големина в байтове. Големината е показана със съответните представки 'K', 'M' или 'G' за 1000, 1,000,000 и 1,000,000,000 множителя съответно.
- **-n** : показва IP адреса и номера на порт в числов формат. Не използва услугата DNS за намиране на съответните на IP адреса имена, което ускорява извеждането на списъка

Ако искаме номерата на правилата в съответната верига да бъдат показани номерирани, тогава използваме следната команда:

```
# iptables -L -n -v --line-numbers
```

Тя ще ни даде изход, подобен на този:

Chain INPUT (policy DROP)

num	target	prot	opt	source	destination
1	DROP	all	--	0.0.0.0/0	0.0.0.0/0 state INVALID
2	ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0 state
RELATED,ESTABLISHED					
3	ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0
4	ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0

Chain FORWARD (policy DROP)

num	target	prot	opt	source	destination
1	ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0
2	DROP	all	--	0.0.0.0/0	0.0.0.0/0 state INVALID
3	TCPMSS	tcp	--	0.0.0.0/0	0.0.0.0/0 tcp flags:0x06/0x02
TCPMSS clamp to PMTU					
4	ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0 state
RELATED,ESTABLISHED					
5	wanin	all	--	0.0.0.0/0	0.0.0.0/0
6	wanout	all	--	0.0.0.0/0	0.0.0.0/0
7	ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0

```

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source          destination
Chain wanin (1 references)
num  target     prot opt source          destination
Chain wanout (1 references)
num  target     prot opt source          destination

```

Тази настройка е полезна при изтриване или вмъкване на правила в защитната стена.

За да покажем правилата от конкретна верига на iptables използваме следната команда:

```
# iptables -L INPUT -n -v
# iptables -L OUTPUT -n -v --line-numbers
```

2. Спиране и пускане на iptables:

```
# service iptables stop
# service iptables start
# service iptables restart
```

Може да използваме командата iptables и за изтриване на всички правила:

```
# iptables -F
# iptables -X
# iptables -t nat -F
# iptables -t nat -X
# iptables -t mangle -F
# iptables -t mangle -X
# iptables -P INPUT ACCEPT
# iptables -P OUTPUT ACCEPT
# iptables -P FORWARD ACCEPT
```

Където:

- **-F** : изтрива (flushing) всички правила;
- **-X** : изтрива верига.
- **-t table_name** : избира таблица (в случая nat или mangle) и изтрива правилата от нея;
- **-P** : установява политиката по подразбиране на веригата (може да бъде DROP, REJECT или ACCEPT).

3. Изтриване на специфично правило в iptables

Ако искате да изтриете правило, което отхвърля невалидни входящи пакети (-A INPUT -m conntrack --ctstate INVALID -j DROP), въвеждате следната команда:

```
# iptables -D INPUT -m conntrack --ctstate INVALID -j DROP
```

Заб. Опцията -A, която показва мястото на правилото по време на създаването му, тук се пропуска.

4. Изтриване на правило по верига и номер

Друг начин да изтриете правила в iptables е по верига и номер на ред. За да видите на кой ред е съответното правило, въведете команда, която извежда списъка с правилата, като добавите опцията --line-numbers:

```
# iptables -L --line-numbers
[secondary_output Example Output: Rules with Line Numbers]
Chain INPUT (policy DROP)
num target prot opt source destination
1 ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED
2 ACCEPT all -- anywhere anywhere
3 DROP all -- anywhere anywhere ctstate INVALID
4 UDP udp -- anywhere anywhere ctstate NEW
5 TCP tcp -- anywhere anywhere tcp flags:FIN,SYN,RST,ACK/SYN ctstate NEW
6 ICMP icmp -- anywhere anywhere ctstate NEW
7 REJECT udp -- anywhere anywhere reject-with icmp-port-unreachable
8 REJECT tcp -- anywhere anywhere reject-with tcp-reset
9 REJECT all -- anywhere anywhere reject-with icmp-proto-unreachable
10 ACCEPT tcp -- anywhere anywhere tcp dpt:ssh ctstate NEW,ESTABLISHED
```

Да приемем, че искате да изтриете входното правило, което отхвърля невалидни пакети (правило 3 от веригата INPUT) въвеждате командата:

```
# iptables -D INPUT 3
```

5. Вмъкване на правила на iptables

Как се добавя правило „отгоре“, на първа позиция:

```
[root@server ~]# iptables -I INPUT 1 -p tcp --dport 80 -j ACCEPT
```

```
[root@server ~]# iptables -L
```

Chain INPUT (policy DROP)

target	prot	opt	source	destination
ACCEPT	tcp	--	anywhere	anywhere tcp dpt:http
ACCEPT	all	--	anywhere	anywhere state RELATED,ESTABLISHED
ACCEPT	icmp	--	anywhere	anywhere
ACCEPT	all	--	anywhere	anywhere
ACCEPT	tcp	--	anywhere	anywhere state NEW tcp dpt:ssh

Chain FORWARD (policy ACCEPT)

target	prot	opt	source	destination
--------	------	-----	--------	-------------

Chain OUTPUT (policy ACCEPT)

target	prot	opt	source	destination
--------	------	-----	--------	-------------

В горният пример добавеното „отгоре“ правило позволява да има свързания по http (на порт 80) от всякъде. В следващия пример пък заменяте това правило, като ограничавате връзките по http (на порт 80) само от IP мрежата 192.168.0.0/24:

```
[root@server ~]# iptables -R INPUT 1 -p tcp -s 192.168.0.0/24 --dport 80 -j ACCEPT
```

```
[root@server ~]# iptables -L
```

Chain INPUT (policy DROP)

target	prot	opt	source	destination	
ACCEPT	tcp	--	192.168.0.0/24	anywhere	tcp dpt:http
ACCEPT	all	--	anywhere	anywhere	state RELATED,ESTABLISHED
ACCEPT	icmp	--	anywhere	anywhere	
ACCEPT	all	--	anywhere	anywhere	
ACCEPT	tcp	--	anywhere	anywhere	state NEW tcp dpt:ssh

Chain FORWARD (policy ACCEPT)

target	prot	opt	source	destination
--------	------	-----	--------	-------------

Chain OUTPUT (policy ACCEPT)

target	prot	opt	source	destination
--------	------	-----	--------	-------------

Ако искаме да вмъкнем правило на точно определена позиция (prepend), така че да е преди правилото DROP, което обикновено е в края на веригата, първо трябва да видите номериран списъка с правилата:

```
[root@server ~]# iptables -L -n --line-numbers
```

Виждате изхода:

Chain	INPUT (policy DROP)					
num	target	prot	opt	source	destination	
...						
22	ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp dpt:993
23	DROP	all	--	0.0.0.0/0	0.0.0.0/0	

Вмъквате новото правило на позиция 23:

```
[root@server ~]# iptables -I INPUT 23 -p tcp --dport 5222 -j ACCEPT
```

правилото DROP отива на позиция 24:

23	ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp dpt:5222
24	DROP	all	--	0.0.0.0/0	0.0.0.0/0	

6. Запазване на въведените правила на iptables

```
[root@server ~]# iptables-save > /etc/sysconfig/iptables
```

7. Настройване на политиката по подразбиране на iptables

(a) Първо всичко е DROP:

```
[root@server ~]# iptables -P INPUT DROP
```

```
[root@server ~]# iptables -P OUTPUT DROP
```

```
[root@server ~]# iptables -P FORWARD DROP
```

(b) След това позволяваме сървърът да изпозва виртуалния си интерфейс loopback:

```
[root@server ~]# iptables -A INPUT -i lo -j ACCEPT
```

```
[root@server ~]# iptables -A OUTPUT -o lo -j ACCEPT
```

(c) После ssh по интерфейс eth0:

```
[root@server ~]# iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT
```

```
[root@server ~]# iptables -A OUTPUT -o eth0 -p tcp --sport 22 -j ACCEPT
```

(d) И накрая от подмрежа 10.1.1.0/24, но само по интерфейс eth1:

```
[root@server ~]# iptables -A INPUT -i eth1 -s 10.1.1.0/24 -p tcp -j ACCEPT
```

```
[root@server ~]# iptables -A OUTPUT -o eth1 -d 10.1.1.0/24 -p tcp -j ACCEPT
```

ЗАДАЧИ

1. Конфигурирайте nat сървър, който да позволява компютри от вътрешната мрежа с IP адреси в обхвата 172.19.18.0/24 да могат да „излизат“ към публичната мрежа с един единствен IP адрес 94.26.50.7/32. Интерфейсът към вътрешната мрежа е eth1, а към външната – eth0 (IP адрес 94.26.50.126/26). Конфигурирайте външния IP адрес на виртуален интерфейс dummy0. Защо го правите?
2. На ред 19 в iptables вмъкнете правила, които да позволяват трафик по порт 25 (SMTP) от и към сървъри в IP мрежа 62.44.96.0/19. Правилата да се присъединят към верига mailsenders.

Тема № 4. СТАТИЧНА МАРШРУТИЗАЦИЯ

1. Какво представлява маршрутизирането в Internet, в кой слой на OSI модела се извършва и защо е необходимо?
2. Видове маршрутизиране – статично и динамично, протоколи за динамично маршрутизиране, автономни системи, маршрутизираща таблица. Как се определя маршрута с мрежовите маски;
3. Статично маршрутизиране – на основата на работна станция с Centos: ifconfig; ip add & route add; traceroute, netstat, ss, mtr

МАРШРУТИЗИРАНЕ – процесът на придвижване на един пакет с информация от един физически сегмент на мрежата до друг физически сегмент се нарича маршрутизиране (*routing*). Маршрутизирането управлява процеса на изпращане на логически адресирани пакети с информация от техния източник до получателя им с помощта на междуинни устройства, наричани маршрутизатори (*routers*).

Маршрутизирането се извършва в третия слой на модела OSI, от протокола IP, който се занимава с логическото адресиране в мрежата. Може да се каже, че маршрутизатора е интелигентно устройство за разлика от комутатора. Маршрутите може да бъдат задавани административно (статична маршрутизация) или да бъдат изчислени с помощта на алгоритми (динамична маршрутизация), работещи с информация за топологията и състоянието на мрежата, получена от протоколите за маршрутизация.

Маршрутизацията в компютърните мрежи се изпълнява от специални устройства, наричани маршрутизатори. При мрежи със сравнително пристапа топология, маршрутизацията може да бъде изпълнявана и от компютри с общо предназначение, под управлението на стандартни операционни системи (UNIX, GNU/Linux, даже и Windows),

Маршрутизиращата таблица (routing table or RIB – Routing Information base) представлява структура от данни в табличен вид, в която се съхранява информацията, необходима за маршрутизирането на пакетите в мрежата (Internet). Всеки пакет съдържа информация за неговия източник (source address) и за неговата цел (destination address), а самата маршрутна таблица съдържа следната информация:

1. **Назначение** – IP адресът на следващото местоназначение (следващия hop). Това е (next hop) IP адресът, до който ще се изпрати пакетът;
2. **Метрика** – определя разстоянието до всеки маршрут, така че да може да се избере най-ефективния такъв;
3. **Маршрути** – съдържа както директно свързани подмрежи, така и индиректно свързани подмрежи (такива, които не са директно свързани към възела, но до които може да се достигне през няколко hop-а);
4. **Интерфейс** – изходният мрежови интерфейс, който трябва да се използва за препращане на пакета към крайното му местоназначение.

Три основни етапа на маршрутизирането:

1. **Намиране на MAC адреса** – използва се когато възелът изпраща дейтаграма. Намирането на този адрес е необходимо за капсулирането на IP пакета (дейтаграмата) в кадър (фрейм).

Ако някой възел иска да изпрати пакет, той трябва да вмъкне в хедъра на фрейма MAC адреса на получаващото мрежово устройство (както и на интерфейса, от който се изпраща). Този адрес може да бъде получен с помощта на таблица, поддържаща съответствието на MAC адресите и съответстващите им IP адреси в мрежата. Обикновено се използва протокола arp (Address Resolution Protocol) за изграждане на такава таблица. Тя може да се види със следната команда:

```
# arp -a
```

При IPv6 това се изпълнява от ICMPv6 - функцията *Neighbor Discovery*.

2. **Определяне на междумрежовите шлюзове (gateway)** – необходимо е, защото Internet е съставен от голям брой отделни мрежи, които се свързват помежду си с помощта на шлюзове, които имат физическа и логическа връзка с повече от една мрежа.
3. **Определяне на цифровия адрес** на получателя от неговия символен адрес. IP адресите в техния цифров вид, даже и в десетично точковата нотация са трудни за запомняне, затова се използват символни адреси (url). Услугата DNS извършва това превеждане – на цифровите адреси в символни и обратно.

Всеки маршрутизатор или възел от мрежата поддържа маршрутна таблица за възможните маршрути според адреса на получателя на пакета. В тази таблица може да бъде включена и информация за съответния резултат за всеки от маршрутите, така че ако има няколко маршрута до една и съща мрежа, да може да бъде избран най-добрят маршрут (най-добър не означава винаги най-къс или най-бърз). Този резултат се определя от метриките, определени от маршрутизатора или от маршрутизиращия протокол.

В маршрутизиращата таблица се поддържа списък на най-добрите маршрути до различни мрежи. За определяне на най-добрая маршрут се използват мерни единици, наречени **метрики**. Те представляват оценка или стойност на някакъв даден параметър на мрежовата връзка. Най-често използвани в маршрутизиращите протоколи мерни единици са:

1. **брой преходи (hop count)** – най-разпространена мерна единица. Измерва броя на маршрутизаторите, през които преминават пакетите от мрежата източник до мрежата получател;
2. **закъснение (delay)** – измерва времето, необходимо да придвижване на пакет от мрежата източник до мрежата получател. Върху закъснението влияние оказват следните фактори: пропусквателната способност на мрежата, броя заявки, обслужвани от всеки маршрутизатор, мрежовите задръствания, разстоянието между двете мрежи;
3. **пропусквателната способност (bandwidth) на мрежата** – измерва наличния капацитет на мрежовата връзка. Връзка 100 mbps е за предпочтение пред връзка 64 kbps;
4. **надеждност (reliability)** – оценява надеждността на мрежовите връзки. Някои връзки излизат от строя по-често от колкото други. Предпочитат се по-надеждните връзки. Друг параметър на надеждността е времето за възстановяване на пропаднала връзка;

5. **цена на връзката (communication cost)** – понякога доставянето на пакета за най-малко време може да не е основна цел. Цел може да бъде минимизирането на цената на мрежовия транспорт.

Тези мерни единици се ползват от различните маршрутизиращи протоколи. Някои протоколи използват комбинация от мерни единици, като задават различни нива на значимост за всяка използвана мерна единица за определяне на най-оптималния маршрут.

АДМИНИСТРАТИВНА ДИСТАНЦИЯ – използва се от маршрутизаторите, когато са налични повече от един маршрут до дадена мрежа, научени от различни маршрутизиращи протоколи, използващи различни метрики. Следователно, административната дистанция дефинира надеждността на самия протокол. Всеки маршрутизиращ протокол притежава административна дистанция. Колкото е по-малка нейната стойност, толкова по-предпочитан е даден маршрут. Статичните маршрути по подразбиране имат административна дистанция 1. Обикновено административната дистанция е първият критерий, който използват маршрутизаторите в опита си да намерят най-добрания от два или повече маршрута до дадена мрежа.

АВТОНОМНИ СИСТЕМИ – група от IP мрежи и маршрутизатори под административния контрол на една или няколко организации и придържащи се към единни и ясно дефинирани правила за маршрутизация в Internet – [RFC 1930 Guidelines for creation, selection and registration of an autonomous system \(AS\)](#).

Обикновено, но не винаги, организацията, която контролират автономните системи са доставчиците на Internet (ISP).

Всяка автономна система притежава **уникален номер**, който се дава от организацията [IANA](#).

Три категории AS:

1. **multihomed AS** – автономни системи, имащи връзка към повече от една автономна система (респективно доставчик на Internet свързаност). По този начин при отпадане на един от доставчиците, автономната система остава свързана към internet;
2. **stub AS** – автономната система е свързана само към една друга автономна система, респективно доставчик на internet;
3. **transit AS** – осигуряват връзка между автономните системи, свързани към тях. Обикновено доставчиците на Internet са автономни системи от този вид.

За да получите номер на автономна система (за Европа – от организацията [RIPE](#)), тя трябва да бъде multihomed автономна система. Например, автономната система на Софийския университет има два излаза към други автономни системи и на теория може да бъде класифицирана и като транзитна, но тя няма право да транзитира трафик, а и прилаганата в нея политика е политика на stub автономна система. В този смисъл, разликата между multihomed и transit автономните системи е по-скоро политическа, отколкото техническа.

В рамките на една автономна система се използват така наречените вътрешни маршрутизиращи протоколи ([Interior Gateway Protocol – IGP](#)). Те се разделят на два вида – с дистантен вектор ([distance vector](#)) и протоколи със следене на връзката ([link-state](#)).

За маршрутизиране между автономните системи се използват външни (екстериорни) протоколи. Такъв протокол е [BGP – Border Gateway Protocol](#).

Съществуват два основни начина за конфигуриране на един маршрутизатор и въвеждане на необходимата информация в маршрутизиращата таблица – статичен и динамичен. С динамичната маршрутизация ще се занимаем в следващото занятие, а днес ще видим как се конфигурира статично маршрутизатор на основата на работна станция под управлението на linux.

СТАТИЧНО МАРШРУТИЗИРАНЕ

1. ръчно конфигуриране на всички пътища в мрежата. Подходящо е за малки мрежи със сравнително постоянна топология;
2. при промяна в мрежата трябва да се направи ръчно преконфигуриране. Ако не се направи, ще имаме некоректно маршрутизиране. При отпадане на маршрутизатор в мрежата, маршрутизиращата таблица трябва да се преконфигурира така, че отпадналия сегмент да бъде заобиколен. В големи мрежи, статично маршрутизиране се прилага за повишаване на надеждността – ако отпадне динамично научения маршрут, тогава зададения статично се използва като резервен.

Статичните маршрути могат да бъдат постоянни във времето или да се променят на определено време (по разписание).

ДИНАМИЧНО МАРШРУТИЗИРАНЕ

Използва маршрутизиращи протоколи за автоматично построяване на маршрутизиращата таблица. При възникване на промяна в топологията на свързване поради отпадане на един или няколко маршрута, маршрутизаторите обновяват своята маршрутна таблица и намират алтернативен път за доставяне на пакетите до тяхното местоназначение. Едни от най-често използваните алгоритми за динамично маршрутизиране са [алгоритъма на Белман-Форд](#) и [алгоритъма на Дийкстра](#).

Маршрутизиращата таблица се попълва от следните три източника:

1. програмното осигуряване на TCP/IP стека. При инициализацията на маршрутизатора, то автоматично попълва няколко записи в маршрутизиращата таблица, като по този начин се създава така наречената [минимална маршрутизираща таблица](#).

В нея се намират следните записи:

- записите на непосредствено свързаните мрежи и маршрутизатори;
- записите за специалните адреси loopback, multicast и broadcast;
- маршрутите за възел на:
 - локалния интерфейс localhost;
 - на локалната подмрежа;
 - broadcast адреса на локалната мрежа;
 - вътрешния маршрут;
 - multicast адрес;
 - глобалния broadcast адрес;

- маршрута по подразбиране (default).

В някои маршрутизиращи таблици, тези записи на особени адреси може да липсват.

Съдържанието на маршрутизиращата таблица може да бъде показано с някоя от командите:

```
# ip route show
# route
```

Статичната маршрутизация се извършва с командите:

```
# ip route add
# route add
```

Записите имат дърводидна структура, тоест едни записи могат да бъдат включени в други записи. Не е възможно да има частично пресичане. Границите на адресното пространство, в което действат тези записи се изравняват с неговите размери. Маршрутната таблица се ползва само в случаите, когато трябва да се определи как да бъдат доставени пакетите.

За целите на маршрутизацията се използва само част от информацията от заглавната част (IP header) на IP пакета – destination address на пакета.

Специални адреси:

0.0.0.0 – адреса на възела, генериран този пакет; обръщение към себе си;
255.255.255.255 – пакет с такъв адрес се изпраща до всички възли в мрежата;
Забранено е да се изпраща пакет там, от където е пристигнал.

СТАТИЧНА МАРШРУТИЗАЦИЯ ПОД LINUX

За да може една работна станция под linux да се използва за маршрутизатор, тя трябва да има поне два физически мрежови интерфейса (напр., eth0 и eth1). Двата интерфейса трябва да бъдат: 1) правилно конфигурирани; 2) съответните маршрути да са добавени в маршрутизиращата таблица и 3) да бъде разрешено маршрутизирането.

1) конфигуриране на мрежовите интерфейси

```
# ip addr add 10.10.23.12/24 dev eth0
# ip addr add 10.10.24.12/24 dev eth0
```

2.1) добавяне на двете мрежи в маршрутизиращата таблица

```
# ip route add 192.168.11.0/24 dev eth0
# ip route add 172.18.0.0/24 dev eth1
```

2.2) добавяне на маршрут по подразбиране

```
# ip route add default via 92.168.1.1
```

3) проверка дали е разрешено маршрутизирането между двета мрежови интерфейса

```
# cat /proc/sys/net/ipv4/ip_forward
```

Ако горната команда върне резултат **1**, значи маршрутизирането е разрешено. А ако върне **0**, значи то не е разрешено и трябва да се изпълни следната команда:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

ИЛИ

```
vi /usr/lib/sysctl.d/00-system.conf (?)
```

Относно **iproute2** командите, изпълнете **man ip** от команден ред в CentOS системата.

2) команда **traceroute** – използва се за проследяване на маршрута, през който се преминава за достигане до даден IP адрес.

USAGE:

```
traceroute [-dFInrvx] [-g gateway] [-i iface] [-f first_ttl]
[-m max_ttl] [-p port] [-q nqueries] [-s src_addr] [-t tos]
[-w waittime] [-z pausemsecs] host [packetlen]
```

netstat (route) – netstat е полезен инструмент за проверка на конфигурацията и работата на мрежата. Всъщност това са няколко инструмента събрани заедно. Когато стартираме netstat с флага **-r**, ще бъде отпечатана таблицата с маршрути в ядрото по начин, аналогичен на командата route

```
[root@sakurajima sysctl.d]# netstat -r
```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
default	192.168.11.1	0.0.0.0	UG	0	0	0	wlp3s0
192.168.11.0	0.0.0.0	255.255.255.0	U	0	0	0	wlp3s0

```
[root@sakurajima sysctl.d]# netstat -r -n
```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
0.0.0.0	192.168.11.1	0.0.0.0	UG	0	0	0	wlp3s0
192.168.11.0	0.0.0.0	255.255.255.0	U	0	0	0	wlp3s0

```
[root@sakurajima sysctl.d]# ip r
```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	192.168.11.1	0.0.0.0	UG	1024	0	0	wlp3s0
192.168.11.0	0.0.0.0	255.255.255.0	U	0	0	0	wlp3s0

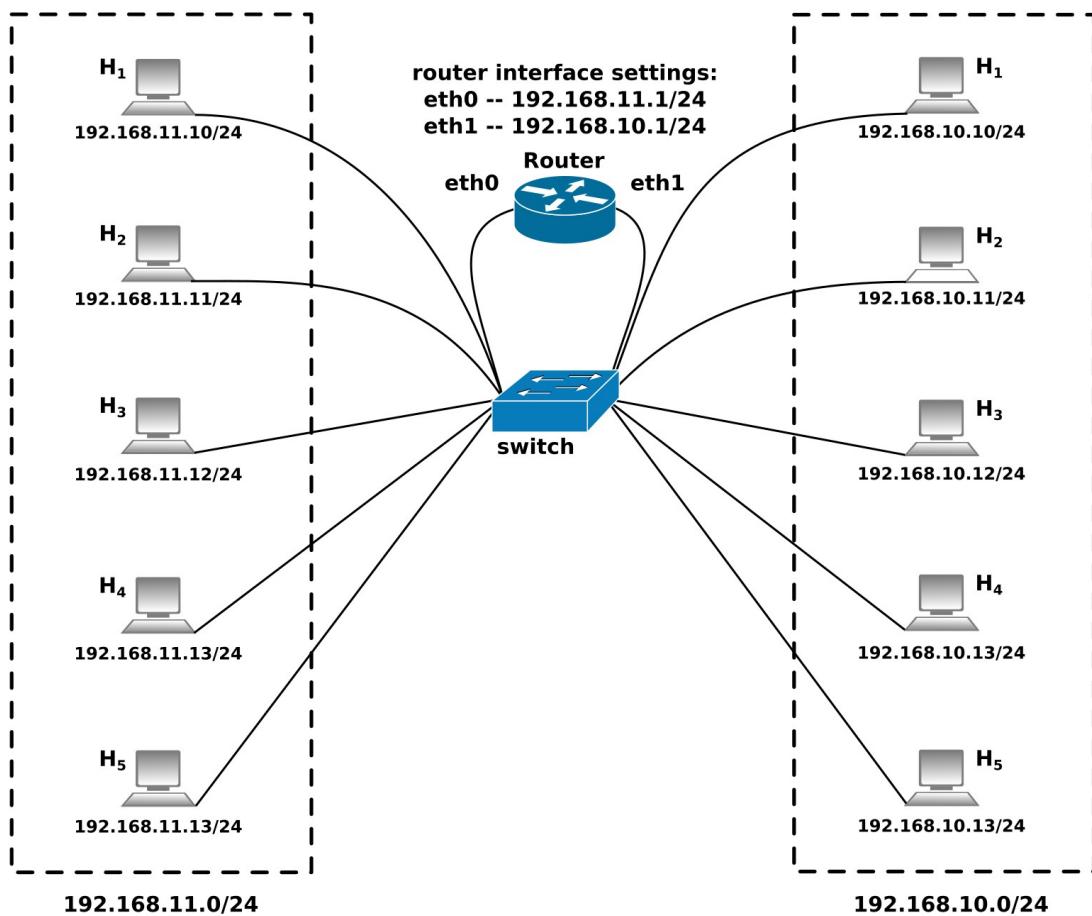
Опцията “**-n**” указва на netstat да отпечатва адресите като IP номера в десетично-точков формат, вместо да използва символните имена на хостове и мрежи. Втората колона от резултата от netstat показва шлюза, към който сочи маршрута. Ако не се използва шлюз, се извежда звезда. Третата колона показва мрежовата маска за този маршрут. Когато е даден IP адрес, за който се търси подходящ маршрут, ядрото преминава през всеки от записите в таблицата с маршрути, като извършва побитово AND на адреса и маската, преди да сравни с целта на маршрута. Четвъртата колона отпечатва следните флагове, които описват маршрута:

- G – Маршрутът използва шлюз;
- U – Интерфейсът, който ще се използва, е активен (up);
- H – През този маршрут може да се достигне само един хост;
- D – Този маршрут е създаден динамично;
- M – Записът е модифициран от ICMP съобщение за пренасочване;

- ! – Маршрутът е отхвърлящ и дейтаграмите ще бъдат игнорирани.

Задачи:

- Запознаване с командите: traceroute, iproute2, netstat (route) и тяхното действие.
- Да се проследи маршрутът до отдалечена станция чрез traceroute. Пример: www.google.com, www.microsoft.com, и т.н.
- Да се наблюдават маршрутните таблици на маршрутизираща и локална станция с команда netstat и ключове: "-nr", "-sp IP".
- Да се конфигурира Linux станция като **NAT маршрутизатор**, като се използва схемата, дадена на фигура 1. Интерфейсът на маршрутизатора, включен към мрежата на университета, да се конфигурира статично към шлюз (gateway) с адрес 10.10.23.254.



РЕШЕНИЕ

1. конфигуриране на интерфейсите на възлите (H) в мрежата:

```
ip addr add 192.168.11.xxx/24 dev eth0
ip addr add 192.168.10.xxx/24 dev eth0
```

2. конфигуриране на маршрутите:

```
ip route add 192.168.11.0/24 dev eth0
```

```
ip route add 192.168.10.0/24 dev eth0
```

3. конфигуриране на маршрут по подразбиране:

```
ip route add default via 192.168.11.1
```

```
ip route add default via 192.168.10.1
```

4. конфигуриране на възела, избран за маршрутизатор (R):

```
ip addr add 192.168.11.1/24 dev eth0
```

```
ip addr add 192.168.10.1/24 dev eth1
```

```
ip addr add 10.10.23.xxx/24 dev eth2
```

```
ip route add 192.168.11.0/24 dev eth0
```

```
ip route add 192.168.10.0/24 dev eth1
```

```
ip route add 10.10.23.0/24 dev eth2 src 10.10.23.xxx
```

```
ip route add default via 10.10.23.254 dev eth2
```

Проверяваме дали параметъра в ядрото за препращане на пакети (ip_forward) между двата интерфейса е включен:

```
cat /proc/sys/net/ipv4/ip_forward
```

Ако отговорът на тази команда е 1, значи ip_forward е активен и ядрото ще препраща пакети от един мрежови интерфейс към друг. Ако отговорът е 0, значи параметъра не е активен. За да го направим активен, ще използваме следната команда:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

след което правим повторна проверка на съдържанието на този параметър с командата cat, посочена малко по-нагоре.

Преди да се активира ip_forward (или ако е активиран, след неговото деактивиране) се проследява с командата ping достъпността до възли от собствената мрежа и до възли от другата мрежа:

```
ping -c10 192.168.11.xxx
```

```
ping -c10 192.168.10.xxx
```

При непозволен ip_forward на маршрутизатора, би трявало да има отговор на ping само от възли от собствената мрежа. При позволен ip_forward възлите от двете логически мрежи вече би трявало да се виждат един друг.

Тема № 5. ДИНАМИЧНА МАРШРУТИЗАЦИЯ

Протоколи за динамична маршрутизация се делят на вътрешни (IGP) в рамките на една автономна система и външни (EGP) между автономни системи от една страна; по отношение на алгоритъма за маршрутизация – с дистантен вектор (distance-vector) и следящи състоянието на връзката (link-state).

МАРШРУТИЗИРАНЕ – процесът на придвижване на един пакет с информация от един физически сегмент на мрежата до друг физически сегмент се нарича маршрутизация (*routing*). Маршрутизирането управлява процеса на изпращане на логически адресираните (от IP протокола) пакети с информация от техния източник до получателя им с помощта на междинни устройства, наричани маршрутизатори (*routers*).

Спецификата на даден протокол за маршрутизация зависи от това как се попълва **Маршрутизиращата таблица (routing table or RIB – Routing Information base)**. Представлява структура от данни в табличен вид, в която се съхранява информацията, необходима за маршрутизирането на пакетите в мрежата (Internet). Всеки пакет съдържа информация за неговия източник (source address) и за неговата дестинация (destination address).

В маршрутизиращата таблица се поддържа списък на най-добрите маршрути до различни мрежи. За определяне на най-добрая маршрут се използват мерни единици, наречени **метрики**. Те представляват оценка или стойност на даден параметър на мрежовата връзка.

Най-често използвани метрики за оценка на възможните маршрути на изпращане на пакетите са hop count, delay, bandwidth, reliability и communication cost.

Най-често, маршрутизиращите таблици имат следния вид:

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,

I - ISIS, B - BGP

Protocol	Destination	Metric/AD	Next Hop	Iface
0	62.44.96.140/32	[110/20]	62.44.96.219	eth1.216
0	62.44.96.141/32	[110/20]	62.44.96.220	eth1.216
0	6192.175.48.0/24	[110/20]	62.44.96.218	eth1.216
R	62.44.96.142/32	[120/2]	62.44.96.221	eth1.216
S	62.44.121.0/24	[1/0]	62.44.120.5	eth1.120
S	0.0.0.0/0	[1/0]	is directly connected	Null0
C	62.44.120.0/24		is directly connected	eth1.120
C	62.44.96.224/32		is directly connected	dummy0

Маршрутизиращата таблица се попълва от програмното осигуряване на TCP/IP стека. При инициализацията на маршрутизатора то автоматично попълва няколко записи в маршрутизиращата таблица, като по този начин се създава така наречената **минимална маршрутизираща таблица**.

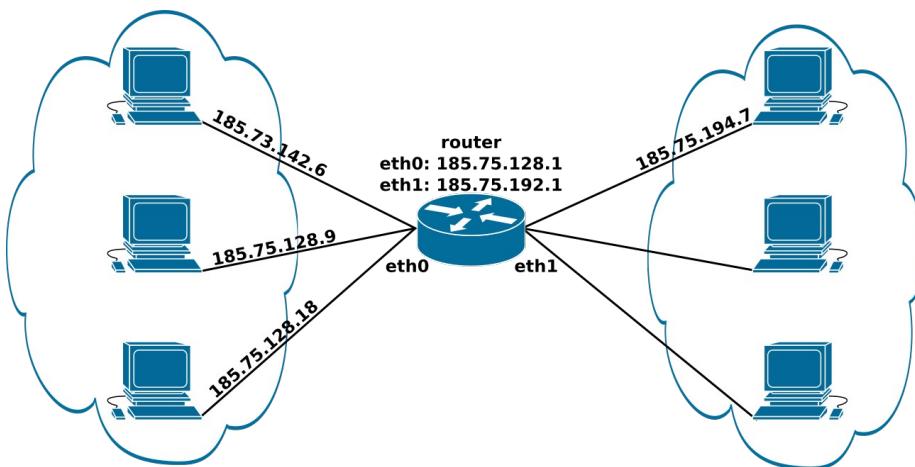
В нея се намират следните записи:

- записите на непосредствено свързаните мрежи и маршрутизатори;
- записите за специалните адреси loopback, multicast и broadcast;
- маршрути към:
 - локалния интерфейс localhost;
 - локална подмрежа;
 - отдалечена подмрежа;
 - multicast адрес;
 - маршрута по подразбиране (default).

Съдържанието на маршрутизиращата таблица може да бъде показано със следната команда:

```
# ip route
```

Записите имат дървовидна структура, тоест едни записи могат да бъдат включени в други записи. Не е възможно да има частично пресичане. Границите на адресното пространство, в което действат тези записи, се изравняват с неговите размери. Маршрутната таблица се ползва само в случаите, когато трябва да се определи как да бъдат доставени пакетите.



фиг. 1 Примерна топология

Например, маршрутизиращата таблица за H_1 , първият възел, най-горе от лявата мрежа от топологията, показана на фигура 1, ще има следния вид:

Address	Mask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	185.75.128.1	185.75.142.6	20
127.0.0.1	255.0.0.0	127.0.0.1	127.0.0.1	1

185.75.128.0	255.255.224.0	185.75.142.6	185.75.142.6	20
185.73.142.6	255.255.255.255	127.0.0.1	127.0.0.1	20
185.75.255.255	255.255.255.255	185.75.142.6	185.75.142.6	20
224.0.0.0	240.0.0.0	185.75.142.6	185.75.142.6	20
255.255.255.255	255.255.255.255	185.75.142.6	185.75.142.6	1

ДИНАМИЧНО МАРШРУТИЗИРАНЕ

Динамичното маршрутизиране използва маршрутизиращи протоколи за автоматично построяване на маршрутизиращата таблица. При възникване на промяна в топологията на свързване поради отпадане на един или няколко маршрута, маршрутизаторите обновяват своята маршрутна таблица и намират алтернативен път за доставяне на пакетите до тяхното местоназначение. Повечето протоколи за динамично маршрутизиране попадат в един от двата класа – на дистантно-векторните протоколи ([distance-vector protocols](#)), прилагащи [алгоритъма на Белман-Форд](#), или на протоколите със следене на състоянието на връзката (link-state), прилагащи [алгоритъма на Дийкстра](#).

DISTANCE-VECTOR (С ДИСТАНТЕН ВЕКТОР) ПРОТОКОЛИ

Протоколите с дистантен вектор (distance-vector protocols) най-често използват като мерна единица за оценяване на маршрутите броя преходи (hop count) до крайната цел и са разновидност на алгоритъма на Belman-Ford за изчисляване на маршрутите. При тях:

- маршрутите се анонсират като вектори;
- посока (на маршрута) – адреса на следващия възел (next hop) и интерфейса, през който се излиза;
- метрика (metrics) – броя възли, през които трябва да се премине за да се достигне до местоназначението на пакета (hop count).

Дистантно-векторните протоколи за лесни за конфигуриране, затова често се използват.

През различни периоди на развитие на Internet са прилагани различни протоколи от този клас, Routing Information Protocol – RIP v1 и RIP v2; Xerox Networking System's RIP – XNS RIP; Novel IPX RIP; Cisco Internet Gateway Routing Protocol – IGRP, DEC DNA Phase IV; Apple Talk Routing Table Maintenance Protocol – RTMP

При поставяне на нов маршрутизатор, използващ такъв протокол за маршрутизиране, той построява и обявява своя маршрутизираща таблица. Всеки маршрутизатор изгражда и поддържа маршрутна таблица, в която всеки ред съдържа адрес на местоназначение, следващата стъпка към това местоназначение по най-добрия засега маршрут и дължината на този маршрут (метриката);

Обща черта на тези протоколи е използването на маршрутизиращ алгоритъм в тях, който периодично изпраща до всички съседни маршрутизатори обновявания на тяхната маршрутизираща таблица чрез използване на broadcast адрес.

Тези периодични обновявания се изпращат след изтичането на определен период от време, обикновено между 10 (за AppleTalk) и 90 секунди (за Cisco IGRP). Поради твърде малкия интервал на обновяване е възможно при линии с тясна честотна лента (bandwidth) да се получи задръстване на линията. От друга страна, твърде голям интервал на разпращане на обновяванията ще доведе до неприемливо голям период от време, необходим за конвергенция на информацията.

Предимства на тези протоколи

1. лесни за конфигуриране;
2. не товарят паметта и процесора.

Недостатъци:

1. информацията се изпраща само до съседните маршрутизатори (намиращи се в същия физически сегмент), което води до много бавна конвергенция (времето, за което мрежата се приспособява към промените в нейната топология и преизчислява маршрутните таблици);
2. тези периодични изпращания на маршрутните таблици отнемат от честотната лента, предоставяна на потребителите;
3. имат изключително ниска скорост на сходимост на алгоритмите – добрите новини се разпространяват бързо, но лошите достигат прекалено бавно до всички маршрутизатори.

ПРОТОКОЛИ СЪС СЛЕДЕНЕ НА СЪСТОЯНИЕТО (LINK-STATE) НА ВРЪЗКАТА

Тези протоколи носят в себе си маршрутната информация до всички възли в мрежата. Тя съдържа само маршрутите до директно свързаните с маршрутизатора мрежи и тяхното състояние. Предимства на тези протоколи са:

1. намален размер на изпращаната информация, което води до по-ефикасен обмен на данни;
2. могат да използват multicast или unicast адресиране, което също намалява общия мрежов трафик;
3. информацията се предава от маршрутизатор към маршрутизатор, които само я копират, без да я променят.

Динамичните протоколи със следене на състоянието на връзката са базирани на алгоритъма на Дийкстра за намиране на най-късия път (shortest path). Такива протоколи са:

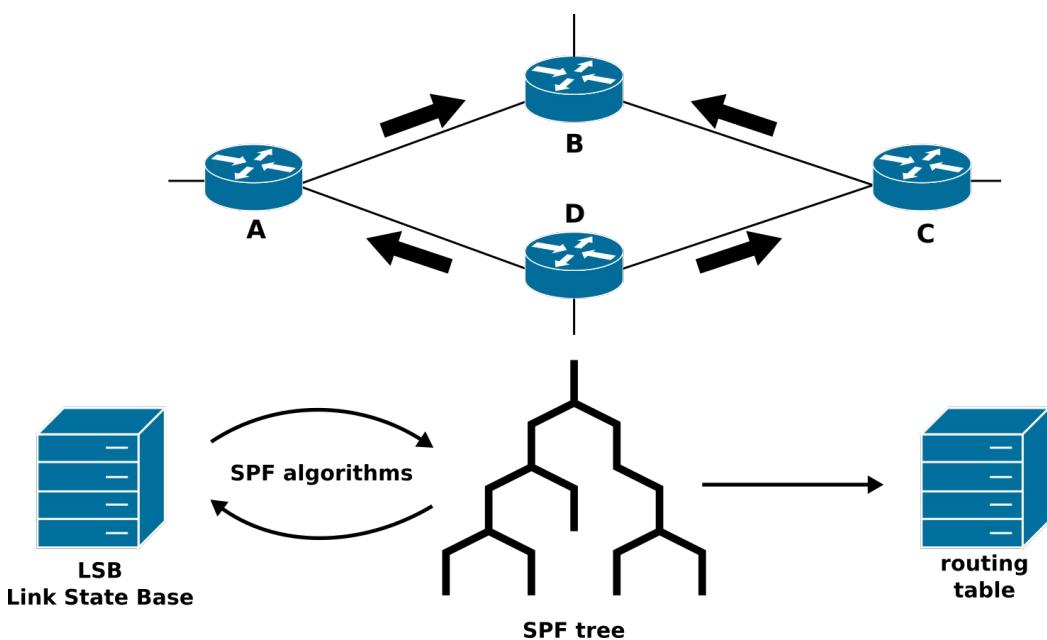
- Open Shortest Path First (OSPF);
- Intermediate System to Intermediate System (IS-IS) на ISO;
- Optimized Link State Routing Protocol (OLSR) – RFC 3626.

Всеки маршрутизатор разполага с пълната топология на мрежата и посредством

разновидност на алгоритъма на Дийкстра изчислява най-кратките пътища до всеки възел от мрежата. Поради тази причина тези алгоритми изискват много повече планиране, конфигуриране, памет и процесорна мощ, отколкото дистанционно-векторните протоколи, но за сметка на това са значително по-мощни и подходящи за използване в големи мрежи.

Протоколите със следене на състоянието на връзката извършват пет основни действия при изчисляването на маршрутната таблица:

1. откриване на съседните маршрутизатори и техните мрежови адреси;
2. измерване на стойностите на връзките до тях;
3. създаване на пакети с информация за състоянието на връзките;
4. изпращане на тези пакети до всички останали маршрутизатори;
5. изчисляване на най-късия път до всеки маршрутизатор в мрежата.



Фиг. 2 Схема на действие на маршрутизиращ протокол със следене на състоянието на връзките

Като краен резултат от горните действия имаме събрана и разпространена до всички маршрутизатори информация за цялата топология на мрежата.

SPF алгоритъм – има за цел да конструира дърво с минимална обща дължина между всичките пътища.

Както вече беше казано, динамичните протоколи за маршрутизация се разделят на два класа – вътрешни (интериорни) и външни (екстериорни) протоколи.

1. Вътрешни протоколи – Routing Information Protocol – RIP v1 и RIP v2; Xerox Networking System's RIP – XNS RIP; Novel IPX RIP; Cisco Internet Gateway Routing Protocol – IGRP, DEC DNA Phase IV; Apple Talk Routing Table

Maintenance Protocol – RTMP;

2. Външни протоколи – Border Gateway Protocol (BGP).

RIP v1 & RIP v2

RIP v1 – RFC 1058. Routing Information Protocol

RIP v2 – RFC 2453. RIP version 2

Използваната метрика в този протокол е hop count – разстоянието в брой стъпки до местоназначанието на изпращания пакет, максималния брой хопове, който може да бъде преминат в една мрежа е 15. За обмен на маршрутна информация при този протокол се използва порт 520 с транспортен протокол UDP (port 520/UDP).

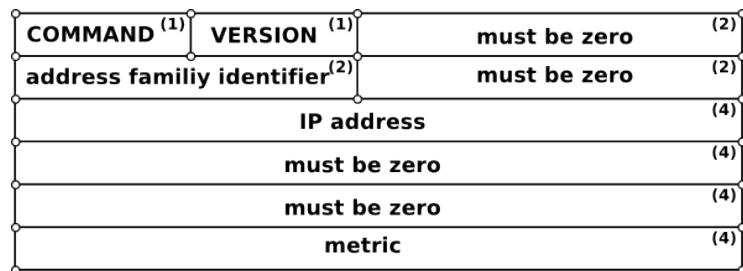
Този протокол е подходящ за използване при малки мрежи, в които относително рядко се правят промени в топологията. Всеки ред от маршрутната таблица съдържа:

- информация за направлението;
- (адресът на) следващата стъпка към това направление;
- метриката.

RIP timers:

1. На всеки 30 sec изпраща копие от маршрутизиращата таблица към съседните маршрутизатори;
2. hold down timer – 180 sec. Това е таймерът за невалиден маршрут;
3. flush timer – съобщение за изтриване на маршрут – пътя се изтрива окончателно от маршрутната таблица.

RIP v1 header



фиг. 3 Формат на заглавната част на RIP пакет

Всеки ред от заглавната част е с дължина 32 бита (4 октета). Размерът на всяко поле е посочен в октети в кръгли скоби след името на полето. Последните 6 полета (от address family identifier до metric) могат да се появят общо 25 пъти в дейтаграмата. IP address е обикновеният 4 октетен internet адрес. Специалният адрес 0.0.0.0 се използва за описание на маршрута по подразбиране (default route). Идентификатора

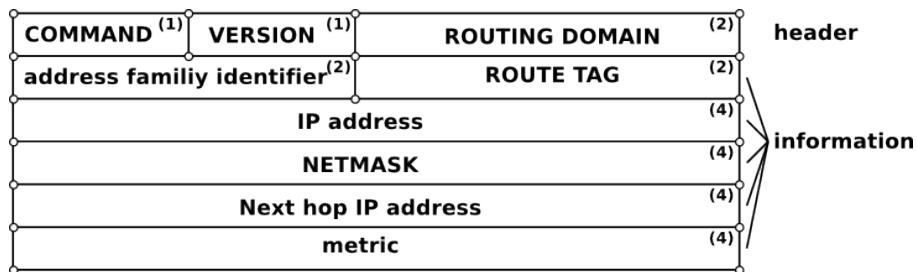
на адресното семейство за IP протокола е 2. Полето за метрика трябва да съдържа стойност между 1 и 15, определяйки текущата метрика за маршрута или да съдържа 16, ако местоназначението е недостъпно. Максималният размер на дейтаграмата на един RIP пакет е 512 октета (IP и UDP заглавните части не се броят). Всяка дейтаграма съдържа команда, номер на версия и възможни аргументи. Когато трябва да се маршрутизира дейтаграма, първо нейният адрес на местоназначение се проверява в списъка с възли на мрежи за да се провери дали съвпада с някоя позната подмрежка или номер на мрежа. Ако няма съвпадение при тези проверки, дейтаграмата се изпраща по маршрута по подразбиране.

RIP v1 не поддържа мрежови маски, респективно безкласова адресация (CIDR). В полетата, означени с етикет „address“ могат да се съдържат следните стойности:

1. адрес на възел от мрежа;
2. номер на подмрежка;
3. номер на мрежа;
4. 0, ако пакета ще се изпраща по подразбиранция се маршрут.

RIP v2

Заглавната част на протокола RIP v2 има следния вид:



фиг. 4 Заглавна част от дейтаграма на протокола RIP v2

И тук информацията от последните 6 полета може да се повтори 25 пъти в една дейтаграма. Ако таблицата е по-голяма, тогава се попълват няколко RIP v2 пакета.

Полето **command** указва дали пакетът съдържа заявка или отговор.

Полето **version** указва версията на протокола.

Полетата **routing domain** и **routing tag** не се изпълват в първата версия на протокола RIP и се запълват с 0.

Полето **address family** се попълва с 2, ако следва IP адрес или се попълва с 0, ако следва заявка за цяла маршрутна таблица.

Протоколът RIP v1 изпраща цялата информация на съответния broadcast адрес на мрежата, докато при втората версия на протокола, RIP v2, информацията се изпраща на multicast адрес 224.0.0.9.

RIPng (RFC 2080) е разширение на RIP v2, което поддържа протокола IPv6.

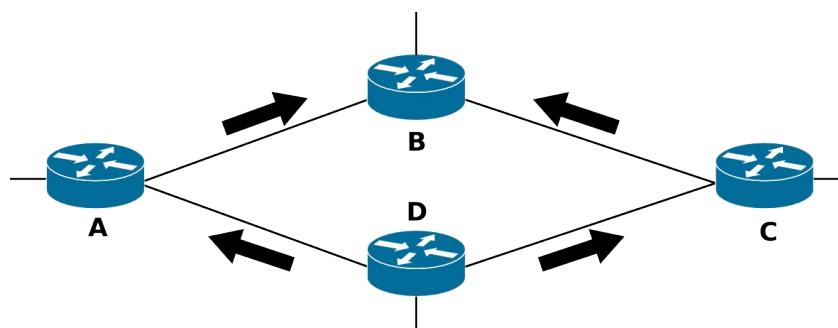
ПРОТОКОЛ OSPF

RFC 2328 – OSPF v2 за IPv4

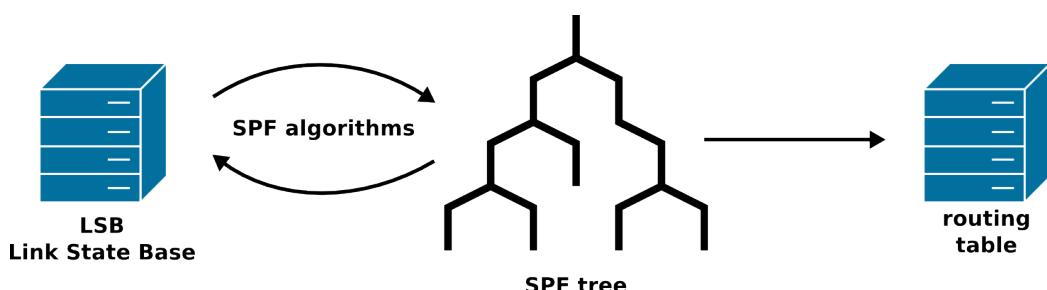
- динамичен протокол за маршрутизация;
- със следене състоянието на връзката;
- за вътрешна маршрутизация в автономни системи;
- OSPF – използва се в големи корпоративни мрежи; IS-IS се използва обикновено от доставчици на Internet; OLSR – използва се за мобилни и безжични мрежи

ХАРАКТЕРИСТИКИ

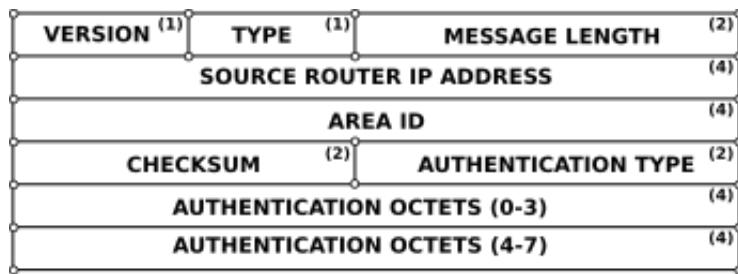
- топология – граф, възлите на който са маршрутизаторите, а клоните – комуникационните връзки между тях.



- на клоните се присвояват стойности, обратно-пропорционални на скоростта на линиите => по-бързата връзка има по-малка стойност;
- с помощта на алгоритъма на Дийкстра се изчислява „дървото на най-късия път“ (shortest path tree) по най-ниската стойност за всеки маршрут;
- информацията за състоянието на връзката се поддържа на всеки маршрутизатор под формата на база от данни LSDB – LinkState DataBase – мрежова топология и пълния граф на мрежата.



OSPF header



фиг. 5

Протоколът OSPF ...

ПРОТОКОЛ BGP

RFC 1771 – дефинира актуалната, 4-та версия на протокола.

Border Gateway Protocol (BGP) е основният протокол за маршрутизация в Internet. Поддържа таблица от IP мрежи (префикси), които определят достижимостта на мрежите между автономните системи. BGP е протокол с вектор на пътищата ([path vector protocol](#)). Той е динамичен протокол за маршрутизация и не поддържа метриката, използвана от вътрешните протоколи за маршрутизиране, а взема решението за определяне на маршрута на основата на пътя между отделните автономни системи и възприетите мрежови политики и правила за маршрутизиране. Актуалната версия на протокола е версия 4, която поддържа безкласова адресация (CIDR) и обединяването (агрегация) на маршрути, с което се намалява размера на самите маршрутни таблици. Последната версия на протокола (BGP 4/4+) е стандартизирана в RFC 4271.

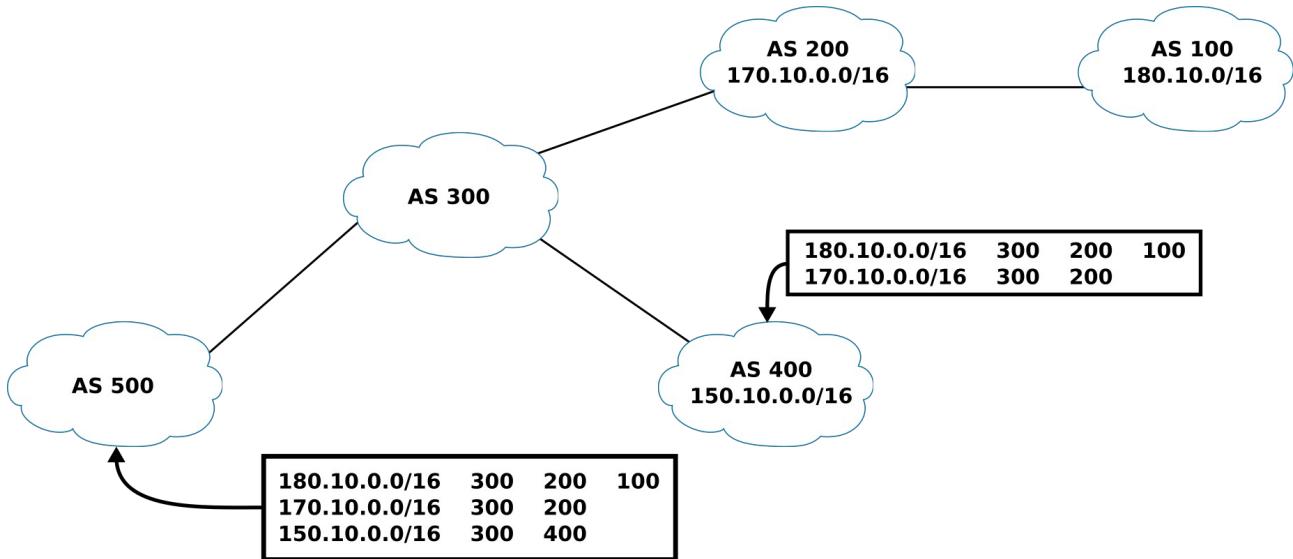
Основен протокол. Използва се при:

1. наличие на множество изходни точки, свързани към един доставчик на Internet;
2. наличие на множество маршрути през различни доставчици и нужда от управление на трафика, изпращан по тези връзки;
3. нужда от интелигентно управление на маршрутизацията в нашата мрежа, надхвърляща използването на маршрут по подразбиране;
4. ако мрежата ни се използва за транзит на трафик от други мрежи;

Съществуват 4 типа BGP маршрутизатори:

1. BGP маршрутизатори говорители – обикновените маршрутизатори, работещи с протокол BGP, без конфигурирани по тях специализирани функции;
2. Равноправни (съседни) BGP маршрутизатори – такива са свързаните към общ сегмент от мрежата маршрутизатори;
3. Вътрешни равноправни BGP маршрутизатори – равноправни възли в една автономна система;
4. Външни равноправни BGP маршрутизатори – съседни BGP маршрутизатори от

различни автономни системи.



Съседните BGP маршрутизатори (neighbors или peers) се задават ръчно в конфигурационните файлове. Между тях се установява сесия по протокола TCP на порт 179. Всеки BGP възел периодично изпраща до своите съседи 19-байтови съобщения (keep-alive packets) за поддържане на връзката между тях. Протоколът BGP е единствен между маршрутизиращите протоколи, който използва като транспортен протокол TCP, което до някаква степен го прави и приложен протокол. След като се установи TCP сесия между съседните BGP маршрутизатори, те обменят маршрутната информация помежду си. Може да бъде обменена пълната маршрутна таблица или част от нея – това зависи от склучените споразумения между отделните автономни системи, от прилаганите политики или филтри в тях и тен. При промяна в маршрутната таблица, BGP маршрутизаторите изпращат на съседите си само променените маршрути. При протокола BGP не се изпращат периодични обновления (routing updates) и се обявява (advertise) само оптималния маршрут до дадено местоназначение.

BGP атрибути

BGP атрибутите са характеристики, използвани от BGP маршрутизаторите за определяне на най-добраия път до дадено местоназначение.

1. Тежест (weights);
2. локален приоритет (local preferences);
3. метричен атрибут (metric attribut или MED – Multi-Exit Descriminator);
4. Извор (origin);
5. Път към AS (AS_Path);
6. Следващ скок (next hop);
7. Общност (community).

Критерии за избор на маршрут

Критериите се сравняват по реда, в който са написани:

1. ако пътят води към следващ скок (next hop), който е недостъпен, той се отхвърля;
2. предпочитат се маршрути с най-голяма тежест;
3. при еднакви тежести на маршрутите се предпочитат тези с най-голям локален приоритет;
4. при еднакви локални приоритети се предпочитат маршрути, които са с BGP източник, изпълняван на дадения маршрутизатор;
5. ако няма маршрути, които да са с BGP източник на дадения маршрутизатор, тогава се предпочитат маршрути с най-къс списък на атрибута AS_path;
6. при еднакви атрибути AS_path се избира маршрут, имащ по-нисък ранг на тип източник (IGP имат по-нисък ранг от EGP, а EGP имат по-нисък ранг от incomplete);
7. при еднакви рангове на източниците се предпочитат пътища с най-малък MED атрибут;
8. ако атрибутът MED е еднакъв – предпочитат се външните маршрути пред вътрешните;
9. Ако все още маршрутите са равнопоставени, тогава се избира маршрут през най-близкия IGP съсед.

Пример на маршрутна таблица, получена по BGP:

```
# sh ip route bgp

B>* 1.0.0.0/24 [20/0] via 194.141.252.21, eth1.2453, 4d03h48m
B>* 1.0.4.0/22 [20/0] via 194.141.252.21, eth1.2453, 4d03h48m
B>* 1.0.4.0/24 [20/0] via 194.141.252.21, eth1.2453, 4d03h48m
B>* 1.0.5.0/24 [20/0] via 194.141.252.21, eth1.2453, 4d03h48m
B>* 1.0.6.0/24 [20/0] via 194.141.252.21, eth1.2453, 4d03h48m
B>* 1.0.7.0/24 [20/0] via 194.141.252.21, eth1.2453, 4d03h48m
...
# sh ip route 1.0.0.0/24
```

Routing entry for 1.0.0.0/24

Known via "bgp", distance 20, metric 0, best

Last update 4d03h51m ago

* 194.141.252.21, via eth1.2453

QUAGGA ROUTING SUITE

Quagga предоставя поддръжка на OSPFv2, OSPFv3, RIPv1 и v2, RIPng и BGP4 за Unix, Linux etc.

Архитектурата quagga съдържа основен демон – zebra, който служи като абстрактно ниво на лежащите под него ядро на linux и предоставя API на zserv върху Unix или TCP поток на клиентите на quagga.

Демоните на quagga се конфигурират през командна интерфейс (CLI), наречен vty. Има и допълнителен инструмент – vtysh, действащ като frontend към тези демони.

```
yum install quagga  
setsebool -P zebra_write_config 1
```

тази команда е само за centos 7. указва на selinux да позволява на демона zebtrad да записва конфигурацията си

```
cp /usr/share/doc/quagga-xxxxxx/zebra.conf.sample /etc/quagga/zebra.conf  
service zebra start  
chkconfig zebra on  
vtysh
```

промпта се променя на:

```
site_A-RTR#  
site_A-RTR# configure terminal  
тук конфигурираме дневника на маршрутизатора  
site_A-RTR# log file /var/log/quagga/quagga-log
```

ТЕМА № 6. ТРАНСПОРТЕН СЛОЙ

1. Функции на транспортния слой
2. Протоколи от транспортния слой:
 - TCP
 - UDP
3. Програми за следене и диагностика на мрежата:

- ping – Packet Internet Gropper;
- arp – Address Resolution Protocol and Reverse ARP (rarp);
- netstat и tpscan;
- nbstat.
- програми за конфигуриране на IP: ifconfig и ip;
- програми за проследяване на маршрути – traceroute и mtr.

ТАНСПОРТЕН СЛОЙ – отговаря за осигуряването на надеждна директна връзка от тип **точка-до-точка (end-to-end)**. За постигането на тази цел се използват механизми за удостоверяване, че данните са пристигнали до своето местоназначение без загуби или повреди.

ВСИЧКИ ПРОТОКОЛИ ОТ ТОЗИ СЛОЙ СА ПРЕДНАЗНАЧЕНИ ЗА ОСИГУРЯВАНЕ НА ВРЪЗКА ОТ ТИП END-TO-END (от край до край).

За транспортния слой не е важно какви данни предава, откъде до къде ги предава – той само предоставя механизъм за предаване на тези данни. Блоковете от данни се разбиват на поредици от байтове (в протоколния стек TCP/IP – **TCP сегменти или UDP дейтаграми**), размерът на които зависи от конкретния протокол.

В този слой има няколко протокола – едни от тях осигуряват само основни транспортни функции като предаване на данните без потвърждение за тяхното получаване (UDP), други осигуряват доставянето на множество пакети от данни в съответната им последователност, мултиплексират предаването на няколко потока от данни, като осигуряват механизми за тяхното управление и гарантират достоверността на получените данни (TCP).

Протоколът UDP е протокол без установяване на връзка (connectionless), докато TCP е протокол с установяване на връзка (connection-oriented) между крайните възли в мрежата.

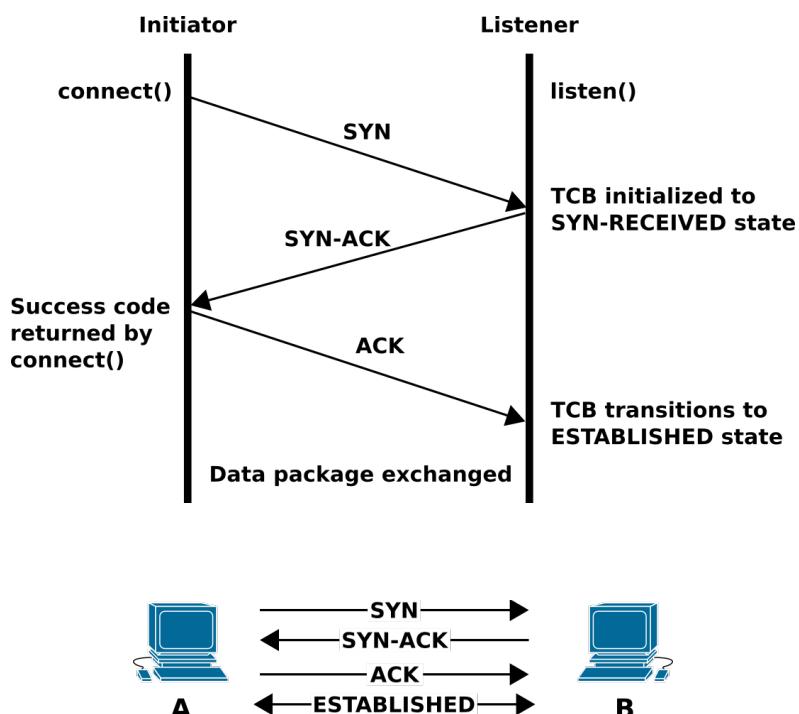
Мултиплексиране на данните – транспортния слой може да управлява едновременно няколко потока от данни, които може да постъпват от различни приложения.

Механизъм за управление на потоците от данни (Flow Control) – позволява регулирането на количеството данни, предавани от един възел към друг.

Протоколите от транспортния слой често изпълняват и функция за контрол на доставянето на данните, изисквайки от приемащия данните възел да изпраща към предаващия възел потвърждения за получаването на данните.

TCP - TRANSMISSION CONTROL PROTOCOL

TCP е протокол, ориентиран към създаването и използването на връзки (тип end-to-end). Той установява сесия между двата общуващи си възела от мрежата, преди да започне да изпраща данни. За установяване на сесията се използват съобщения за потвърждаване и отговор – three way handshaking – syn, syn-ack and ack сегменти.



фиг. 1 Схема на трикратното ръкостискане при установяване на TCP сесия

Последователността при установяване на една TCP сесия между два възела от мрежата е следната:

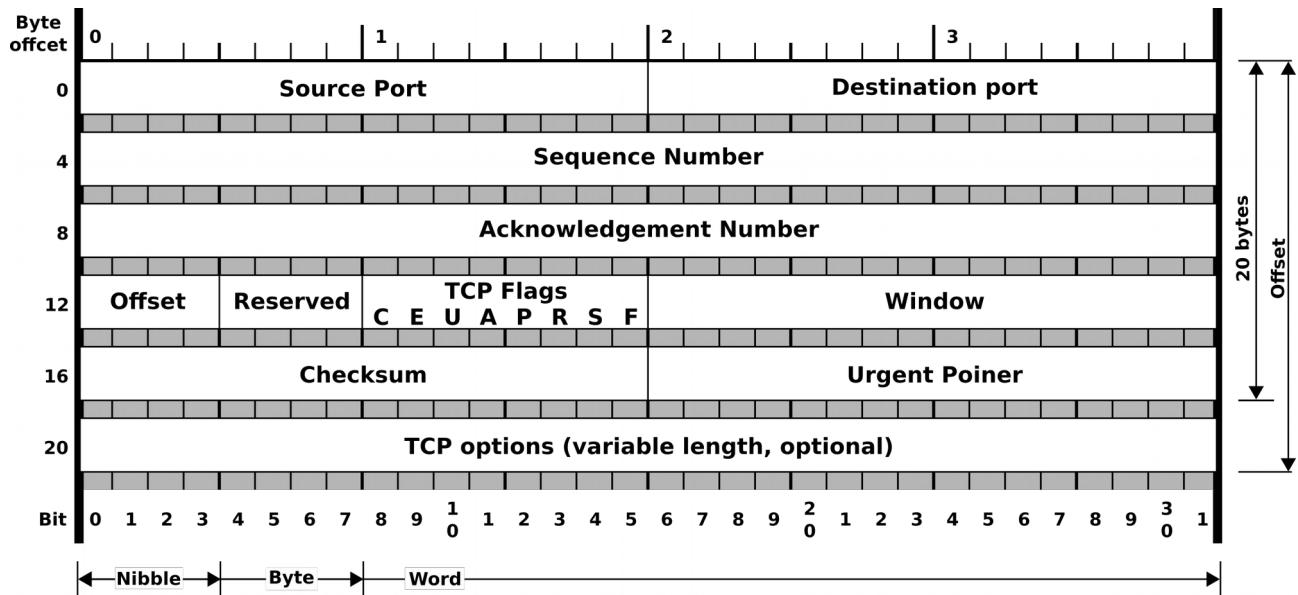
1. Възелът А изпраща към възел В TCP синхронизиращ пакет SYN;
2. Възелът В го получава;
3. Възелът В връща към възела А потвърждаващ TCP пакет SYN-ACK;
4. Възелът А получава този потвърждаващ пакет от възела В;
5. Възелът А **изпраща** TCP пакет **ACK** към възел В;

6. Възелът В получава този пакет ACK;

7. TCP socket connection is ESTABLISHED.

След установяването на връзката се извършва проверка за грешки и тяхното коригиране като данните се разделят на пакети.

Пакетите SYN и ACK се отбелязват с допълнителен SYN или ACK бит в заглавната част на пакета.



Фиг. 2 Заглавна част на TCP пакет

Към всеки пакет се добавя информация за неговата последователност, така че отделните части от съобщението да могат да се сглобят в обратен ред при тяхното получаване. Тази информация позволява на приемащия възел да открие дали няма липсващи пакети. Всичко това прави TCP протокола по-надежден от UDP, но на цената на по-ниската му производителност.

Datagram (RFC 1594 – FYI on Questions and Answers или RFC 2664 – FYI on Questions and Answers) – независима единица данни, носеща достатъчно информация за маршрутизирането ѝ от нейния източник до нейното местоназначение без да се разчита на предишен обмен между тези възли и транспортиращата мрежа (между тях).

Packet (пакет) – единица от данни, която е част от група последователни единици или „парчета“, на които е разбито дадено съобщение.

Пакетите може да бъдат доставени по различни маршрути в мрежата до крайното си местоназначение, където се сглобяват в обратен ред.

Термините **дейтаграма** и **пакет** понякога се използват взаимозаменяемо.

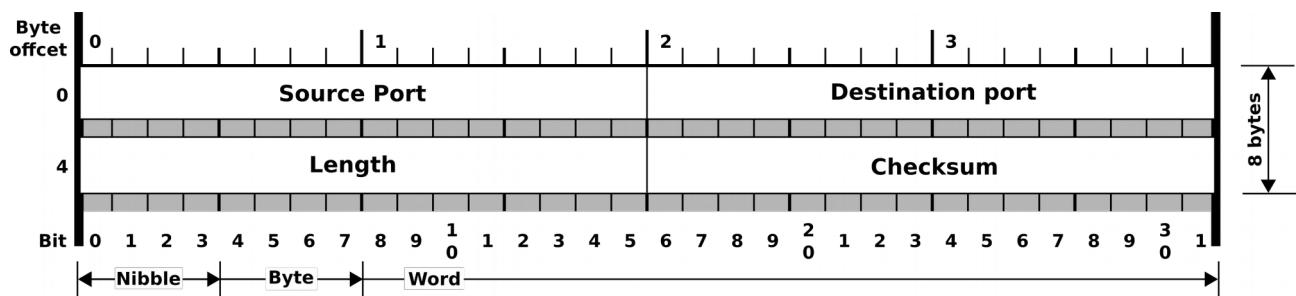
Терминът дейтаграма се използва за описание на по-простите и неподредени единици от данни, предавани по UDP протокол.

UDP – USER DATAGRAM PROTOCOL

За разлика от TCP, той е протокол, който не изисква установяването на връзка между крайните възли в мрежата (connectionless protocol) – между изпращащият възел и възела, за който са предназначени изпращаните данни.

Той не поставя последователни номера ([sequences numbers](#)) на пакетите, които изпраща, което го прави подходящ за изпращане на малки съобщения, които могат да се съберат в един пакет. UDP не следи какво изпраща и не изисква потвърждение дали е получено. Но все пак генерира контролна сума на изпратените данни за да гарантира, че те са пристигнали неповредени.

По тези причини (не генерира последователност на пакетите и не проверява за грешки), UDP протоколът е бърз. Неговите заглавни части са по-прости от тези на TCP протокола.



Фиг. 3 Заглавна част на UDP пакет

Протоколи, които използват UDP протокол:

- RIP – Routing Information Protocol;
- TFTP – Trivial File Transfer Protocol;
- DNS – Data Name Service.

Кой от двата протокола (TCP или UDP) ще се използва за предаване на данните се определя от харектера и нуждите на това предаване на данни.

TCP се използва, когато най-важна е надеждността на връзката, а UDP – когато с най-висок приоритет за нас е производителността (скоростта) на връзката.

Всеки TCP сегмент се разделя на две части:

1. заглавна част (header) – с фиксиран размер от 20 байта;

2. данни – с максимална дължина 65535 байта.

Всеки краен възел на връзката се идентифицира с комбинацията от IP адрес и номер на използван порт (така наречения **транспортен адрес** от упражнението за NAT). Номера на порта се определя от съответната програма от приложния слой, която използва тази връзка.

Socket – комбинацията от IP адреса и номер на порта (транспортен адрес) на двата възела от мрежата, участващи във връзката.

Всеки TCP сегмент съдържа номерата на портове на източника и на приемника → те определят за коя приложна програма е предназначен съответния сегмент.

Транспортния адрес на приемника и този на източника образуват уникална комбинация, идентифицираща TCP връзката. Един socket (гнездо) може да се използва едновременно от няколко TCP връзки.

Портове с номера от 1 до 1023 се наричат **добре известни портове**. Портовете от 1024 до 65535 са свободни за използване.

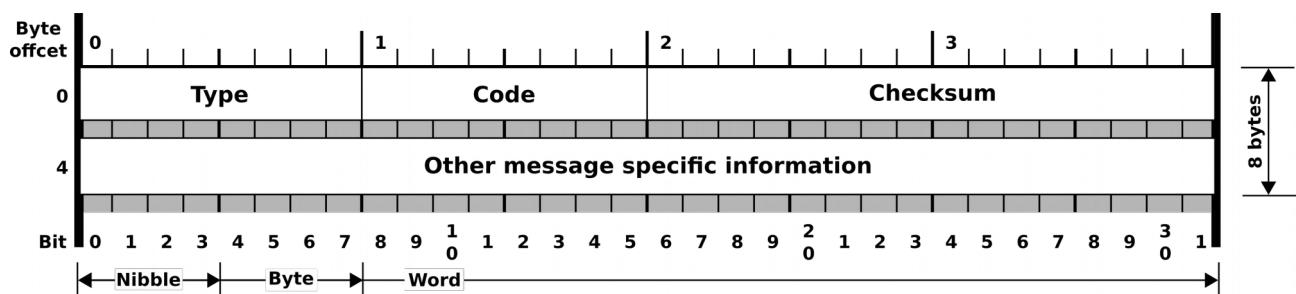
Помощни програми за следене и диагностика

ping – проста, но полезна програма за работа от команден ред. Включена е в повечето реализации на TCP/IP стека. Може да се използва както с името на възела, така и с неговия IP адрес.

Командата ping изпраща ICMP echo request пакет към възела, чийто адрес сме посочили в нея:

```
# ping 62.44.96.142
# ping google.bg
```

Възелът, който получи такъв ICMP echo request пакет трябва да отговори с echo reply пакет.



Фиг. 4 Заглавна част на ICMP пакет

Командата **nslookup** връща IP адреса на дадено име на възел или името на възела на въведен IP адрес:

```
[nick@sakurajima ~]$ nslookup google.bg
```

Server: 95.87.194.5

Address: 95.87.194.5#53

Non-authoritative answer:

Name: google.bg

Address: 216.58.211.35

или

[nick@sakurajima ~]\$ nslookup 62.44.96.142

Server: 95.87.194.5

Address: 95.87.194.5#53

Non-authoritative answer:

142.96.44.62.in-addr.arpa name = ns.uni-sofia.bg.

ARP и RARP

ARP – отнася се до самия протокол (ARP – Address Resolution Protocol) и до самата команда, използвана за разглеждане и манипулиране на ARP кеша.

Протоколът ARP е средството, с което възлите в мрежата съпоставят логическите (IP) адреси с физическите (MAC) адреси. Протоколът ARP изгражда и поддържа таблица, наричана ARP кеш, в която се съдържат тези съпоставления. Протоколът RARP се използва от машина, която не знае собствения си IP адрес, за да получи информация за него на базата на своя MAC адрес.

Програмата arp може да се използва за разглеждане и промяна на съпоставленията между IP и MAC адресите.

```
# arp -s address hw_address - въвежда ново съответствие MAC/IP адрес  
# arp -d address - изтрива съответствието IP/MAC адрес.
```

Повече настройки за използване с командата arp могат да се видят на man страницата на командата:

```
# man arp
```

netstat – команда, показва информация за TCP/IP връзките и протокола, използван за тези връзките:

```
# netstat
```

```
# netstat | grep TCP
```

tcp	0	0	sakurajima:17595	88.87.13.191:51714	ESTABLISHED
tcp	0	0	sakurajima:17595	212.5.152.1:53766	ESTABLISHED
tcp	0	0	sakurajima:17595	212.5.152.48:51879	ESTABLISHED
tcp	0	0	sakurajima:45774	db3msgr5012709.ga:https	ESTABLISHED
tcp	0	0	sakurajima:53157	xmpp.org:xmpp-client	ESTABLISHED
tcp	0	0	sakurajima:17595	212-5-158-212.btc:35809	TIME_WAIT
tcp	32	0	sakurajima:51365	6-55-236-85.rev.c:https	CLOSE_WAIT
tcp	0	0	sakurajima:48331	server-54-192-96-:https	ESTABLISHED
tcp	0	0	sakurajima:55749	kyufte.mnet:xmpp-client	ESTABLISHED
tcp	0	0	sakurajima:43488	157.56.116.204:12350	ESTABLISHED
tcp	0	587	sakurajima:17595	212-5-158-212.btc:33324	ESTABLISHED
tcp	0	0	sakurajima:17595	212.5.152.48:51759	ESTABLISHED
tcp	0	0	sakurajima:17595	87-104-159-150-dy:35073	ESTABLISHED
tcp	0	0	sakurajima:50637	213.199.179.166:40016	ESTABLISHED
tcp	0	0	sakurajima:17595	188-254-235-254.s:51868	ESTABLISHED
tcp	0	0	sakurajima:17595	92.247.150.1:raw-serial	ESTABLISHED

netstat ни показва списък на връзките, които са активни в момента.

```
# netstat -s – показва мрежова статистика
```

```
[root@sakurajima ~]# netstat -s
```

Ip:

```
313526 total packets received  
157 with invalid addresses  
0 forwarded  
0 incoming packets discarded  
301849 incoming packets delivered  
241589 requests sent out  
24 outgoing packets dropped
```

Icmp:

```
217 ICMP messages received  
0 input ICMP message failed.  
ICMP input histogram:  
destination unreachable: 217
```

```
125 ICMP messages sent  
0 ICMP messages failed  
ICMP output histogram:  
destination unreachable: 125
```

IcmpMsg:

```
InType3: 217  
OutType3: 125
```

Tcp:

```
2663 active connections openings  
3025 passive connection openings  
35 failed connection attempts
```

595 connection resets received
7 connections established
201424 segments received
201507 segments send out
2200 segments retransmited
145 bad segments received.
720 resets sent

Udp:

129245 packets received
52 packets to unknown port received.
0 packet receive errors
38005 packets sent
0 receive buffer errors
0 send buffer errors

UdpLite:

TcpExt:

10 invalid SYN cookies received
28 resets received for embryonic SYN_RECV sockets
866 TCP sockets finished time wait in fast timer
8260 delayed acks sent
4 delayed acks further delayed because of locked socket
Quick ack mode was activated 498 times
1 SYNs to LISTEN sockets dropped
88 packets directly queued to recvmsg prequeue.
1448 bytes directly in process context from backlog
28761 bytes directly received in process context from prequeue
104730 packet headers predicted
15 packets header predicted and directly queued to user
27655 acknowledgments not containing data payload received
30870 predicted acknowledgments
247 times recovered from packet loss by selective acknowledgements
7 congestion windows recovered without slow start by DSACK
22 congestion windows recovered without slow start after partial ack
1 timeouts after SACK recovery
6 timeouts in loss state
247 fast retransmits
19 forward retransmits
23 retransmits in slow start
537 other TCP timeouts
TCPLossProbes: 1075
TCPLossProbeRecovery: 493
33 SACK retransmits failed
647 DSACKs sent for old packets
185 DSACKs received
184 connections reset due to unexpected data
204 connections reset due to early user close
14 connections aborted due to timeout
TCPDSACKIgnoredOld: 5
TCPDSACKIgnoredNoUndo: 68

TCPSpuriousRTOS: 7
TCPSSackShiftFallback: 277
TCPRecvCoalesce: 23955
TCPFOQueue: 999
TCPChallengeACK: 147
TCP SYN Challenge: 145
TCPSpuriousRtxHostQueues: 69
TCPAutoCorking: 14017
TCPWantZeroWindowAdv: 30
TCPSynRetrans: 543
TCPOrigDataSent: 90208
IpExt:
InMcastPkts: 36275
OutMcastPkts: 293
InBcastPkts: 5347
OutBcastPkts: 4
InOctets: 467732627
OutOctets: 40231400
InMcastOctets: 11493421
OutMcastOctets: 42982
InBcastOctets: 477160
OutBcastOctets: 196
InNoECTPkts: 511090
InECT1Pkts: 11
InECT0Pkts: 107
InCEPkts: 1

ss – извежда статистика от съответния сокет, подобна на **netstat**

ip a - извежда информация за TCP/IP конфигурацията на конкретен възел от мрежата;

traceroute – за проследяване на маршрута, по който даден пакет минава от източника до приемника.

Следене на трафика

Два типа начина за събиране на информация:

- 1. monitoring** – не събира самите пакети, а само статистика за трафика през даден мрежов интерфейс;
- 2. capturing** – залавянето на самите пакети позволява следенето на същите тези статистики, но със запазване на пакетите за последващ анализ – декодиране на заглавните части, добавени от различните протоколи.

Предназначение на програмите за следене на трафик:

1. Откриване и диагностициране на проблеми в мрежата;

2. Оценка на натовареността на мрежата и разпределение на трафика по протоколите

Програми – wireshark и tshark; tcpdump

Тема № 7. Netfilter & IPtables

Пакетният филтър в netfilter представлява рамка (framework), позволяваща достъп до мрежовите пакети извън стандартния socket интерфейс на unix/linux операционните системи.

iptables представлява потребителски инструмент за дефиниране на правила за филтриране на мрежови пакети и транслиране на мрежови адреси.

На практика, често под името iptables се разбира цялата инфраструктура на netfilter & iptables заедно със следенето на връзките и транслирането на мрежовите адреси.

iptables групира правилата за обработка на мрежовите пакети в таблици по функции (фильтриране на пакети, транслиране на мрежови адреси, други модификации на пакетите), всяка от които има вериги (chains, поредици) от правила за обработване на пакетите. Правилата се състоят от условия за съвпадение (matches), които се използват за определяне на това към кое правило да бъдат насочени пакетите и цели (targets), които определят какво ще се прави с удовлетворилите условието пакети. Целта се прилага върху всеки пакет, който удовлетворява условието на правилото.

iptables работи в мрежовия слой (layer 3) на OSI модела. За каналния слой (layer 2) се използват други технологии за филтриране – например ebtables.

Всеки мрежов пакет преминава поне през една верига и се сравнява последователно с правилата от нея. Ако се получи съвпадение, обхождането се спира и се прилага съответното правило. Ако пакетът не удовлетвори нито едно условие, тогава върху него се прилага подразбиращата се политика на веригата.

Всяко правило дефинира условие и цел. Целта се прилага върху всеки пакет, който удовлетворява условието на правилото.

Целта на някое правило може да бъде нова верига. Ако пакетът премине през новата верига, без да удовлетвори някое условие от нея, се продължава с обхождането на първата верига.

Всяка верига представлява подреден списък с правила.

Веригите се групират в таблици, като всяка таблица е свързана с различен вид обработка на мрежовите пакети. Няма ограничение за влагането на веригите една в друга.

КОНЦЕПЦИЯ НА IPTABLES

точки на скачване (въздействие) – hook points

iptables дефинира пет точки на скачване (въздействие) по пътя на обработването на мрежовите пакети от ядрото на linux:

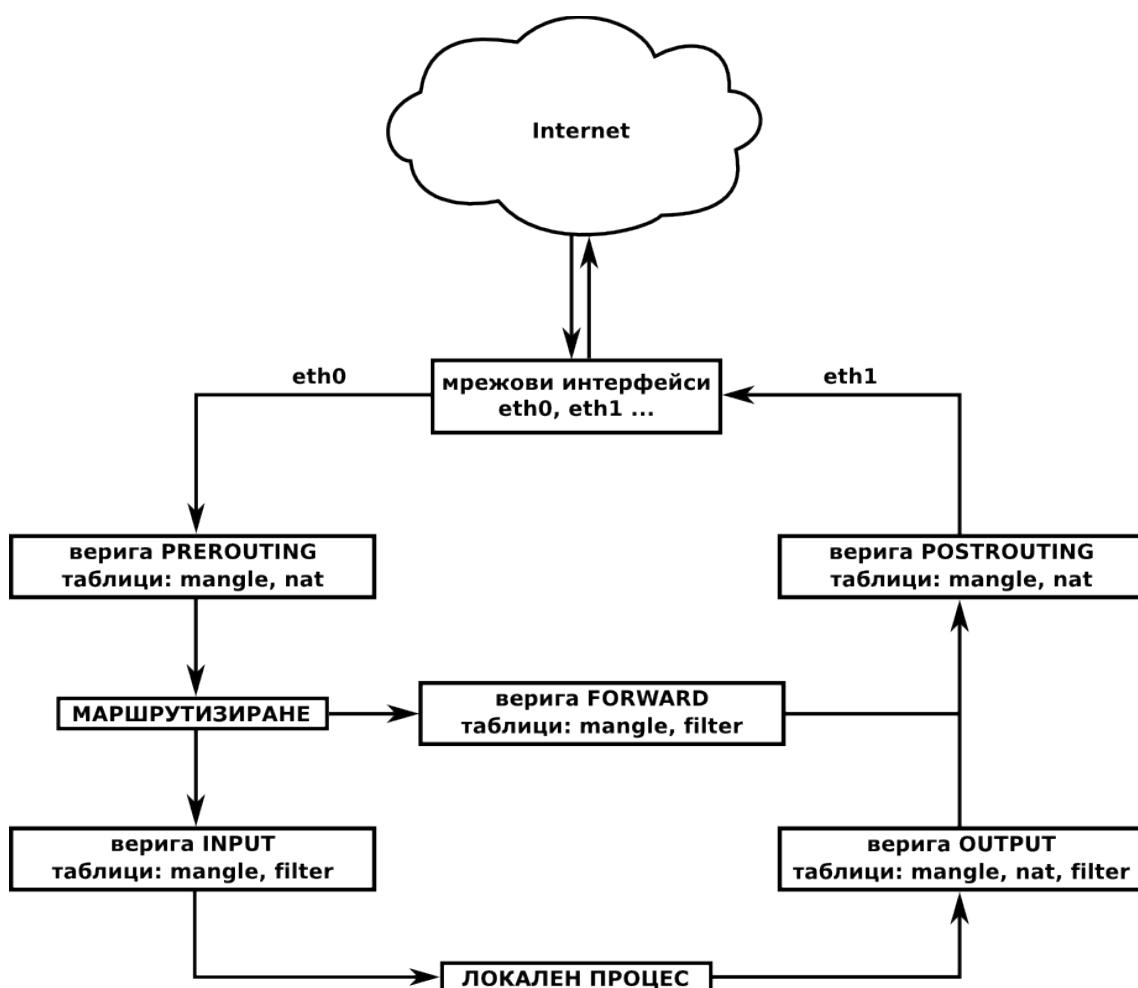
1. PREROUTING

2. INPUT**3. FORWARD****4. OUTPUT****5. POSTROUTING**

Всяка от тези точки дава възможност за следене или оказване на въздействие върху потока от пакети. Към тези точки се прикачват вградените вериги (от правила), но към тях може да се добавят поредици и от допълнителни правила.

Обикновено се казва, че „веригата PREROUTING от таблицата nat“, което въсъщност не е точно така. Веригите и таблиците са свързани само частично помежду си и не принадлежат една на друга. Веригите представляват точки на скачване (въздействие) в потока от данни, а таблиците представляват типа обработка, която може да се извърши в съответната точка на скачване.

Фигура 1 ни показва всички позволени комбинации и реда, по който те се преминават от мрежовите пакети, минаващи през системата.



Фигура 1.

В iptables са дефинирани следните точки на скачване (hook points):

- 1. FORWARD** – обработва пакетите, преминаващи през възел, използван за шлюз (gateway), пристигащи на един мрежов интерфейс и излизати веднага през друг;
- 2. INPUT** – обработва мрежовите пакети точно преди да бъдат доставени на локалния процес, за който са предназначени;
- 3. OUTPUT** – обработва мрежовите пакети веднага след генерирането им от някой локален процес;
- 4. POSTROUTING** – обработва мрежовите пакети точно преди да излязат през някой мрежов интерфейс;
- 5. PREROUTING** – обработва всички мрежови пакети веднага след пристигането им на някой от мрежовите интерфейси (след изхвърлянето на всякакви пакети в резултат на това, че интерфейса работи в нефильтриращ режим и след проверка на контролните суми).

Изборът на верига се основава на това, в коя част от жизнения цикъл на пакетите искаме да приложим своите правила. Филтрирането на изходящите пакети се прави във веригата OUTPUT, тъй като веригата POSTROUTING не е асоциирана с таблицата за филтриране filter.

Политиките по подразбиране на веригите са:

- iptables -P INPUT DROP
- iptables -P FORWARD DROP
- iptables -P OUTPUT ACCEPT

Повечето системи контролират входящия си трафик, а не изходящия.

НАЧИН НА ДЕЙСТВИЕ

1. получаване на мрежовия пакет – пакетът се изследва да се определи дали е предназначен за този възел;
2. ако пакетът е за този възел, той се обработва локално;
3. ако пакетът не е предназначен за този възел и е активирано ip прехвърлянето (в /etc/sysctl.conf), се извършва търсене за подходящ маршрут в маршрутизиращата таблица и пакета се прехвърля на съответния мрежов интерфейс. Ако не бъде намерен такъв маршрут, пакетът се отхвърля;
4. пакетите, генериирани от локалните процеси се изпращат за

маршрутизиране за да бъдат предадени на съответния мрежови интерфейс.

Изходящият пакет се изследва, за да се определи дали съществува валиден маршрут, по който да поеме. Ако няма, той се изхвърля (игнорира се напълно) или се отхвърля (игнорира се след изпращане на ICMP съобщение, обясняващо, че няма маршрут до търсения възел;

5. пакетът се предава.

По този начин, iptables може да осъществява филтриране на пакетите, пристигащи във възела, да филтрира тези, които ще бъдат препредадени от възела, и да филтрира пакетите, които са готови за предаване.

ТАБЛИЦИ В IPTABLES

iptables има три вградени таблици: filter, nat и mangle. Всяка от тях е предварително конфигурирана с вериги, отговарящи на една или повече точки на скачване.

Таблица **filter** – използва се за задаване на политиките за типа на трафика, на който е позволено да влиза, да минава транзитно през и да излиза от възела. Ако не сте изразили изрично предпочтение към някоя от другите таблици, iptables по подразбиране ще работи върху веригите на тази таблица. Нейните вградени вериги са **FORWARD, INPUT и OUTPUT**.

Таблица **mangle** – използва се за специални промени по пакетите, като например сваляне на IP опции. Нейните вградени вериги са **FORWARD, INPUT, OUTPUT, POSTROUTING и PREROUTING**.

Таблица **nat** – използва се заедно със следенето на връзките, за да пренасочва връзките за NAT, базирайки се обикновено на адресите на източника и получателя. Нейните вградени вериги са **OUTPUT, POSTROUTING и PREROUTING**.

ВЕРИГИ

По подразбиране, всяка таблица притежава вериги (първоначално празни) за някои или за всички точки на скачване. Освен това, има възможност за добавяне на собствени вериги с цел организиране на собствени правила.

Политиката на веригите се използва за определяне на съдбата на пакетите, които стигат до нейния край без да удовлетворят някое условие и по този начин изпратени към определена цел. Само вградените цели ACCEPT и DROP могат да се използват като политики за вградените вериги, като по подразбиране е използва ACCEPT. Всички дефинирани от потребителя вериги имат заложена политика RETURN, която не може да бъде променяна.

Ако искате да имате по-сложна цел на политиката за някоя вградена верига или политика, която да е различна от RETURN за потребителска верига, на края на веригата може да добавите правило, което да съвпада с всички пакети. Това правило вече може да има произволна цел.

ПРАВИЛА

Правилата в iptables се състоят от един или повече критерии за съвпадение, определящи кои мрежови пакети ще бъдат засегнати от правилото и цел, определяща как точно ще бъдат засегнати тези пакети. За да съвпадне някое правило с даден пакет, трябва да бъдат удовлетворени всички опции за съвпадение.

iptables поддържа броячи на пакетите и байтовете за всяко правило. Всеки път, когато даден пакет достигне до някое правило и удовлетвори неговите критерии, броячът на пакетите се увеличава с едно, а брояча на байтовете се увеличава с размера на пакета.

Критериите за съвпадение и за целта на правилата не са задължителни. Ако няма критерий за съвпадение, приема се, че всички пакети съвпадат. Ако няма цел, с пакетите не се извършват никакви действия, но пакетите се обработват все едно, че правилото не съществува, но броячите на пакетите и байтовете ще бъдат обновени. Подобно празно правило е:

```
# iptables -t filter -A FORWARD
```

СЪВПАДЕНИЯ (matches)

Има голямо разнобразие от съвпадения, които могат да бъдат използвани с iptables. Някои от тях са достъпни само при ядра с активирани определени модули, други са приложими за всички IP пакети (например тип протокол или адрес на източник или получател). В допълнение към общодостъпните съвпадения, iptables предлага и множество специализирани съвпадения, които са достъпни чрез динамично зареждани разширения (с опцията -m или -match). Има едно разширение, което е предназначено да работи с каналния слой (data-link layer) – mac. То търси съвпадение на базата на ethernet media access controller (MAC) адресите.

ЦЕЛИ (TARGETS)

Целите се използват за задаване на действията, които трябва да се предприемат, когато някой пакет удовлетвори критериите от някое правило. С тях се задават и политиките на веригите. В iptables има четири вградени цели, а чрез разширителните модули може да се въведат и други цели. Вградените цели са:

ACCEPT – позволява на пакета да премине към следващия етап от обработката, спира обхождането на текущата верига и преминава към следващия етап от фигура 1;

DROP – прекъсва напълно обработката на пакета и не го проверява повече с никакви други правила, таблици и вериги. Ако искате да предоставите някаква обратна връзка на подателя, тогава използвайте разширението за цели REJECT;

QUEUE – изпраща пакета в потребителското пространство (user space);

RETURN – от правило в някоя потребителска верига: прекъсва обработката на тази верига и възобновява обхождането от следващото правило от извикващата верига, което е след правилото, при което е станало прекъсването.

За да може ядрото на linux да поддържа използването на защитни стени, то трябва да бъде конфигурирано по подходящия начин:

```
# make menuconfig
```

в секцията Network options → [*] Network packet filtering (replaces ipchains) се конфигурира IP: Netfilter Configuration.

За да може да се използва команда iptables, трябва модула netfilter да бъде зареден в ядрото на системата, което се извършва по следния начин:

```
# modprobe ip_tables
```

ИЗПОЛЗВАНЕ НА iptables

За да се улесни конфигурирането на iptables, има две таблици с правила, наречени filter и nat. Таблицата filter се приема за дадена по подразбиране, ако не бъде предефинирана с опцията -t. Има и вградени 5 вериги – **OUTPUT, INPUT, FORWARD, PREROUTING и POSTROUTING**.

Общийят синтаксис на командата iptables е следния:

```
# iptables опция правило разширение
```

Повечето от опциите на командата iptables могат да бъдат групирани в подкоманди и критерии за съвпадение с правила. Някои от опциите на iptables са описани малко по-надолу:

1. **-c пакети байтове или --set counters** – когато бъде комбинирана с подкомандите -A, -I или -R, задава стойността пакети на брояча на пакетите и стойността байтове на брояча на байтове за новото или променено правило;
2. **--exact или -x** – показва точният брой на пакетите и байтовете, а не подразбиращия се съкратен формат с метрични представки (K, M или G);
3. **-h или -help** – показва помощна информация за използването на iptables;

4. **-j target [options] или --jump target [options]** – определя какво да се прави с пакетите, удовлетворяващи критериите на това правило. Target може да бъде името на някоя потребителска верига, някоя от вградените цели или разширение на iptables (в който случай може да има още допълнителни настройки);
5. **--line numbers** – когато е в комбинация с -L, показва номерата на правилата във всяка верига, така че да може да се обръщаме към тях с индекси, когато вмъкваме (-I) или изтриваме (-D) правило от някоя верига. Тези номера се променят след изтриване или добавяне на правила от веригата.
6. **-m съвпадение или --match** – извикване на разширено съвпадение (евентуално с допълнителни опции към него);
7. **-M cmd или --modprobe=command** – използва се за зареждане на нов модул на iptables при промяна на правила;
8. **-p или --numeric** – показва адресите и портовете в числов вид, вместо да търси имената на домейните за IP адресите и имената на услугите за номерата на портовете. Тази възможност е полезна, когато DNS услугата в мрежата работи бавно или въобще я няма.
9. **-t table или --table table** – изпълнява дадената команда върху съответната таблица. Ако тази опция не е указана, се използва таблицата filter.
10. **-v или --verbose** – показва по-подробно резултатите.

Зашитната стена (firewall) е решение, което първо забранява всичко, а после вече разрешават само „бели“ списъци (“добрая” трафик). Т.е. първо при нейната инсталация се забраняват всички съединения между защищаваната и отворената мрежи, а след това се добавят специфични правила, които позволяват на определен трафик да преминава през зашитната стена.

Съществува и противоположен подход: разрешава се целия трафик, като с „черен“ списък се задава забранения трафик. Защитните стени са просто системи, основани на правила, които разрешават или забраняват преминаването на пакетите през тях.

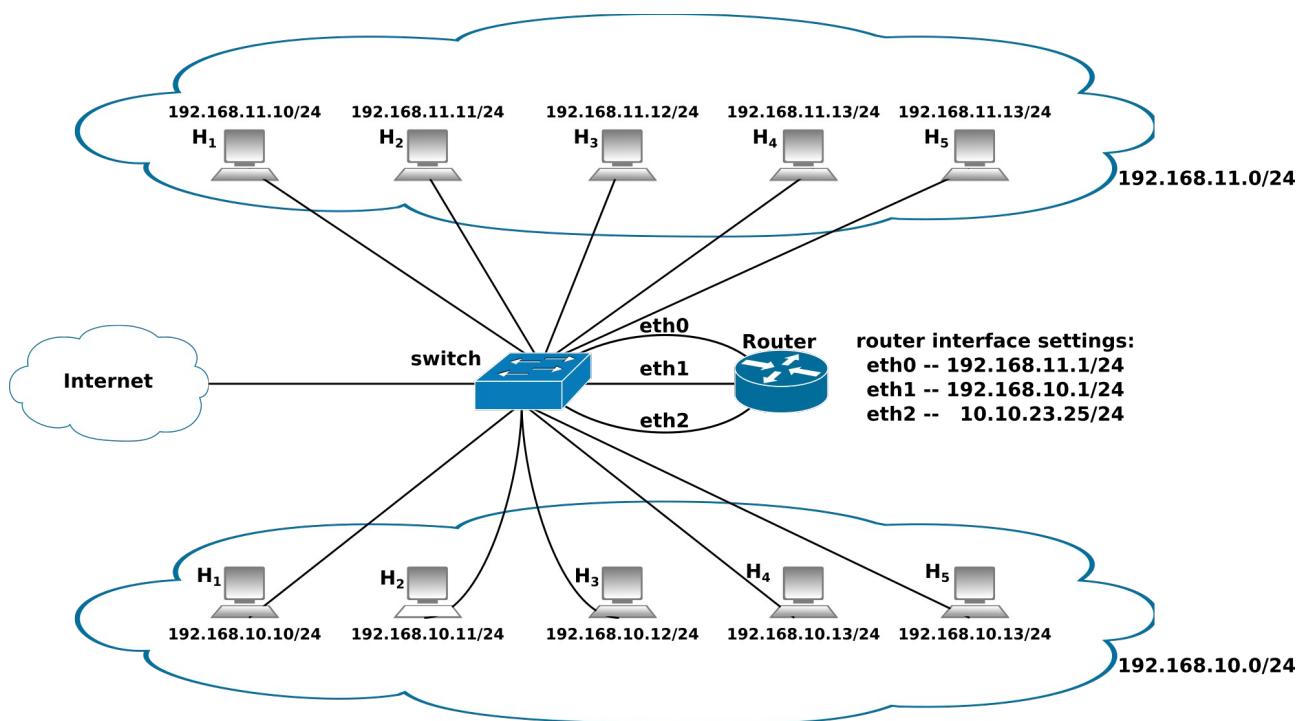
Понеже във всеки пакет се намират няколко заглавия на различни протоколи, проверяват се само тези от тях, които са важни за филтрацията на пакетите. Като правило следва да се отхвърлят пакети на всички протоколи, които не се използват в мрежата или позволяват промяна в настройките.

Например с ICMP пакети може да се промени маршрутната таблица или да се съобщи за недостъпност на определен възел. ICMP пакетите намират множество приложения. Те се използват за разузнаване на мрежата. Една от функциите на мрежовия филтър е в предотвратяване

на получаването от външни хора на всякакви сведения за възлите в мрежата. Затова следва да се блокират съобщенията от следните типове:

- Входящи съобщения echo request и изходящи echo reply. Така ping може от вътре навън да се ползва, но отвън няма да позволи сканиране.
- Входящи съобщения redirect. Те позволяват промяна на маршрутната таблица.
- Изходящи съобщения destination unreachable и входящи service unavailable. Злосторник няма да може да определи използваните услуги и възлите ще са му недостъпни.

ПОСТАНОВКА НА ЗАДАЧАТА



Фиг. 1 Топология на примерната мрежа

Да се реализира топологията, показана на фигура 1. Компютрите в залата се разделят на две групи, които се конфигурират в две различни локални мрежи – 192.168.10.0/24 и 192.168.11.0/24. Един възел се конфигурира като маршрутизатор със следните настройки: eth0 – 192.168.10.1/24, eth1 – 192.168.11.1/24 и eth2 – 10.10.23.10/24.

конфигуриране на отделните възли:

```
ip addr add 192.168.11.xxx/24 dev eth0
ip addr add 192.168.10.xxx/24 dev eth0
```

конфигуриране на маршрутите на отделните възли:

```
ip route add 192.168.11.0/24 dev eth0  
ip route add 192.168.10.0/24 dev eth0
```

конфигуриране на маршрут по подразбиране:

```
ip route add default via 192.168.11.1  
ip route add default via 192.168.10.1
```

конфигуриране на маршрутизатора:

```
ip addr add 192.168.11.1/24 dev eth0  
ip addr add 192.168.10.1/24 dev eth1  
ip addr add 10.10.23.xxx/24 dev eth0  
ip route add 192.168.11.0/24 dev eth0  
ip route add 192.168.10.0/24 dev eth1  
ip route add 10.10.23.0/24 dev eth0 src 10.10.23.xxx  
ip route add default via 10.10.23.254 dev eth2
```

Проверяваме дали параметъра (`ip_forward`) в ядрото за препращане на пакети между двата интерфейса е включен:

```
cat /proc/sys/net/ipv4/ip_forward
```

Ако отговорът на тази команда е 1, значи `ip_forward` е активен и ядрото ще препраща пакети от един мрежови интерфейс към друг. Ако отговорът е 0, значи параметъра не е активен. За да го направим активен, ще използваме следната команда:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

след което правим повторна проверка на съдържанието на този параметър с командата `cat`, посочена малко по-нагоре.

Преди да се активира `ip_forward` (или ако е активиран, след неговото деактивиране) се проследява с командата `ping` достъпността до възли от собствената мрежа и до възли от другата мрежа:

```
ping -c10 192.168.11.xxx  
ping -c10 192.168.10.xxx
```

При непозволен `ip_forward` на маршрутизатора, би трявало да има отговор на `ping` само от възли от собствената мрежа. При позволен `ip_forward` възлите от двете логически мрежи вече би трявало да се виждат един друг.

Трябва да се конфигурират и правила в iptables, които да маскират пакетите, изпращани от локалните мрежи към internet:

```
# iptables -t nat -A POSTROUTING -o $EXT_IFACE -j MASQUERADE (?!)
```

ПРИМЕРИ:

Правило за филтриране на пакети

Тази команда може да се използва за отделяне на целия не-HTTP трафик

нека eth0 е ethernet интерфейсът към локалната мрежа, а eth1 - е ethernet интерфейса към Internet.

```
# iptables -t filter -P FORWARD DROP  
# iptables -t filter -A FORWARD -i eth0 -p tcp --dport 80 -j ACCEPT  
# iptables -t filter -A FORWARD -i eth1 -p tcp --sport 80 -j ACCEPT
```

Първата команда определя политиката по подразбиране на веригата FORWARD от таблицата filter да изхвърля (DROP) всички пакети. Втората команда разрешава всички изходящи HTTP заявки, а третата - всички входящи заявки.

Правило за превод на мрежов адрес:

```
# iptables -t nat -A PREROUTING -i eth1 -p tcp -dport 80 -j DNAT  
-to-destination 12.34.56.78:8080
```

Правило, разрешаващо преминаване на трафик по 80-ти порт по TCP протокол:

```
# iptables -A FORWARD -m state --state NEW -p tcp --dst $HTTP_IP --dport 80  
-j ACCEPT
```

state - проверка на признак за състоянието от netfilter. Това са new (пакетът отваря ново съединение или принадлежи на еднопосочен поток), established (пакетът принадлежи на вече установено съединение, през което пакетите вървят в двете посоки), related (пакетът принадлежи на вече съществуващо съединение, но при това отваря ново съединение) и invalid (пакетът е свързан с неизвестен протокол или съединение и вероятно съдържа грешка в данните или заглавието).

Разрешаваме пакетите, принадлежащи към вече установено съединение/ разрешаване на всеки изходящ трафик:

```
iptables -A FORWARD -m state --state ESTABLISHED, RELATED -j ACCEPT
```

Използването на състояния позволява построяване на мощна и ефективна защита.

Признакът NEW не е еквивалентен на вдигнат бит SYN при TCP протокол.

Да се разрешат входящи уеб съединения (без използване на състояния, без функция на рутер, на самия сървър):

```
# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Редът на правилата е критически важен.

net.ipv4.conf.rp_filter=1 Верификация на IPsrc (защита от IP спуфинг)

Да се спре ping единствено между двойка съседи.

```
# iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

Да се фиксира двойка съседи: ляв ssh сървър единствено за десен ssh клиент и десен е единствено ssh клиент за левия ssh сървър. (Политиката е ACCEPT, не се променя).

Правило, отхвърлящо всички изходящи мрежови връзки

Вторият ред от правилата позволява само текущите изходящи и вече създадени връзки. Това е полезно, когато ще се свързвате отдалечно със сървъра през ssh или telnet.

```
# iptables -F OUTPUT  
# iptables -A OUTPUT -m state --state ESTABLISHED -j ACCEPT  
# iptables -A OUTPUT -j REJECT
```

Правило, отхвърлящо всички входящи мрежови връзки

Вторият ред на правилото позволява само текущите изходящи и установени съединения. Това е много полезно, когато сте се логнали към сървър по ssh или telnet

```
# iptables -F INPUT  
# iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT  
# iptables -A INPUT -j REJECT
```

Правило, отхвърлящо всички мрежови връзки

Това правило ще отхвърля и блокира всички мрежови връзки, както входящи, така и изходящи. От значение е, че ще се приложи и към вече създадени изходящи връзки.

```
# iptables -F  
# iptables -A INPUT -j REJECT  
# iptables -A OUTPUT -j REJECT  
# iptables -A FORWARD -j REJECT
```

Правило за отхвърляне на входящи ping заявки

Това правило на iptables ще отхвърля (DROP) всички входящи ping заявки.

Възможно е вместо DROP да се използва (целта) REJECT. Разликата между тях е, че DROP тихомълком ще отхвърли всички входящи пакети, докато REJECT ще върне съобщение за ICMP грешка.

```
# iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

Правило за отхвърляне на изходящи telnet връзки

Това правило ще блокира всеки изходящ трафик към всеки възел, където номера на порта е 23 (telnet).

```
# iptables -A OUTPUT -p tcp --dport telnet -j REJECT
```

Правило за отхвърляне на всички входящи telnet връзки

Това правило ще отхвърля всички входящи връзки към локален порт 23.

```
# iptables -A INPUT -p tcp --dport telnet -j REJECT
```

Правило за отхвърляне на изходящи ssh връзки

```
# iptables -A OUTPUT -p tcp --dport ssh -j REJECT
```

Правило за отхвърляне на входящи ssh връзки

отхвърля всички входящи връзки към локален порт 22 (ssh).

```
# iptables -A INPUT -p tcp --dport ssh -j REJECT
```

Правило, отхвърлящо входящия трафик с изключение на ssh и локални връзки

```
# iptables -A INPUT -i lo -j ACCEPT
```

```
# iptables -A INPUT -p tcp --dport ssh -j ACCEPT
```

```
# iptables -A INPUT -j REJECT
```

Правило, позволяващо входящи ssh връзки от точно определен IP адрес

Използвайки това правило, ние ще блокираме всички входящи връзки към порт 22 (ssh), с изключение на тези, идващи от IP адрес 77.66.55.44, което означава, че само възелът с този адрес ще може да се свърже по ssh.

```
# iptables -A INPUT -p tcp -s 77.66.55.44 --dport ssh -j ACCEPT
```

```
# iptables -A INPUT -p tcp --dport ssh -j REJECT
```

Правило, приемащо входящи ssh връзки от точно определен MAC адрес.

Това правило блокира всички входящи връзки на порт 22 (ssh), с изключение на тези, идващи възел с MAC адрес 00:e0:4c:f1:41:6b. По този начин, всички ssh връзки ще бъдат ограничени до единичен възел с този MAC адрес.

```
# iptables -A INPUT -m mac --mac-source 00:e0:4c:f1:41:6b -p tcp --dport ssh -j ACCEPT  
# iptables -A INPUT -p tcp --dport ssh -j REJECT
```

Правило, отхвърлящо входящите връзки към точно определен TCP порт

Това правило ще отхвърля всички входящи връзки към TCP порт 3333:

```
# iptables -A INPUT -p tcp --dport 3333 -j REJECT
```

Правило, отхвърлящо всички входящи връзки към точно определен мрежов интерфейс

Това правило ще отхвърля входящия трафик върху точно определен мрежов интерфейс, идващ от подмрежа 192.168.0.0/16. То е полезно за предпазване от подменени IP адреси. Ако eth0 е външен мрежов интерфейс, на него не трябва да попада входящ трафик, произхождащ от вътрешната мрежа.

```
# iptables -A INPUT -i eth0 -s 192.168.0.0/16 -j DROP
```

Правило, извършващо просто маскиране на пакетите

То създава прост шлюз за маскиране на IP адреси, позволяващ на всички възли от една и съща подмрежа да имат достъп до Internet. Използваният в него мрежов интерфейс eth0 е външният мрежов интерфейс, свързан към Internet.

```
# echo "1" > /proc/sys/net/ipv4/ip_forward  
# iptables -t nat -A POSTROUTING -o $EXT_IFACE -j MASQUERADE
```

Правило, отхвърлящо входящия telnet трафик, освен от точно определен IP адрес

Това правило ще отхвърля всичкия входящ telnet трафик, с изключение на заявките за връзка от IP адрес 222.111.111.222

```
# iptables -A INPUT -t filter ! -s 222.111.111.222 -p tcp --dport 23 -j REJECT
```

Правило, отхвърлящо всичкия входящ трафик, освен този от точно

определен адресен обхват

Това правило ще отхвърля целият ssh трафик с изключение на заявките за връзка от адресния обхват 10.1.1.90 – 10.1.1.100. Премахването на символа „!” от долното правило ще доведе до отхвърлянето на целият ssh traffic, произхождащ от адресния обхват 10.1.1.90 – 10.1.1.100.

```
# iptables -A INPUT -t filter -m iprange ! --src-range  
10.1.1.90-10.1.1.100 -p tcp --dport 22 -j REJECT
```

Правило, отхвърлящо изходящия трафик към точно определен отдалечен възел от мрежата

Това правило ще отхвърли всичкия изходящ трафик, адресиран към отдалечен възел от мрежата с IP адрес 222.111.111.222

```
# iptables -A OUTPUT -d 222.111.111.222 -j REJECT
```

Правило, блокиращо достъпа до определен web сайт

Това правило ще блокира всичкият входящ трафик от facebook.com, в който порта на източника е 80/www.

```
# iptables -A INPUT -s facebook.com -p tcp --sport www -j  
DROP
```