**2. Маршрутизиращи алгоритми**Маршрутизиращите алгоритми са два вида -неадаптивни и адаптивни.  
При неадаптивните маршрутизацията не се извършва на базата на текущата топология на мрежата.  
Маршрутите между всеки два възела в мрежата се изчисляват предварително и се записват ръчно от мрежовите администратори, след което влизат в маршрутните таблици.  
При промяна на топологията на мрежата (например при отпадане на възел или на връзка), администраторите ръчно трябва да променят маршрутите.  
Това прави неадаптивните алгоритми приложими само в малки мрежи, при които рядко настъпват промени.  
Неадаптивните алгоритми се наричат още статични.  
 **3. С какви цели може да се използва arp команда?**C командата аrр могат да се използват следните ключове:

* аrр -а - Показва кеша
* аrр -S - Добавя перманентно съпоставяне между IP и МАС адрес
* аrр -d - Изтрива запис

**4.Сравнете репитер и хъб. На кой слой работят?**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 единия 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.  
  
**5. Сравнете 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.

**6. С кои команди бихте могли да определите MAC адрес на хост, който се намира в локалната мрежа?**

arp –a

**7. Защо за маршрут по подразбиране стойностите за мрежа и мрежова маска са нули?**

Маршрутът по подразбиране в IPv4 (в CIDR нотация) е 0.0.0.0/0. Тъй като дадената маска на подмрежата е / 0, тя на практика не задава мрежа, и е "най-краткия" възможeн път?. Маршрутна справка, която не съвпада с нищо, ще върне обратно върху този маршрут.

**8. Определете слоевете от OSI модела, на които функционират следните устройства: рутер (маршрутизатор), суитч (комутатор), хъб (концентратор).**

**Hub** - устройство за свързване на няколко Ethernet устройства заедно и ги прави да действат като единен сегмент на мрежата. Той има множество I/O портове, в които сигнал, въведен на входа на порт, се появява на изхода на всеки порт, освен оригиналните.Хъб работи на Physical layer (слой 1) на модела OSI.

Мрежовите хъбове са опростени предавателни устройства. Те не управляват трафика, който минава през тях, а само го предават на всички портове. Поради това се получава натоварване на мрежата. Хъбовете не са наясно с това какъв е източникът и кой е получателят на пакетите, които минават през тях.

**Switch** - компютърно мрежово устройство, което свързва мрежови сегменти или мрежови устройства. Както и при хъбовете, мрежовите комутатори се използват главно в [Етернет мрежи](https://bg.wikipedia.org/wiki/%D0%95%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82). Комутаторите са няколко типа. Те се категоризират на базата на слоя в OSI модела, на който работят. Стандартните комутатори работят в data link( слой 2) от OSI модела. Съществуват обаче и подобрени комутатори, които работят в network layer  
(слой 3). Това са маршрутизатори, но от специален тип, които изпълняват ролята и на комутатори.

**Router** - самостоятелно устройство, което служи за управление на разпределянето на трафика (пакетите) информация между различни мрежи или различни сегменти от дадена мрежа. Маршрутизаторът работи на слой 3 от седемслойния OSI модел. Тоест, маршрутизаторът работи с IP, а не с MAC адреси, по което се различава от switch и хъба. Ако до някое IP връзката е през маршрутизатор, а не през суич или хъб, то ние не научаваме неговия MAC адрес.

**9. Кои са източниците на записи в маршрутната таблица?**

Обикновено, рутерите са свързани към няколко мрежи и са отговорни за насочване на трафика в тези мрежи. Всеки рутер поддържа таблица за маршрутизация, който е даден списък на известни мрежи и упътване за това как да се достигне до тях. При обработката на входящите пакети на устройство за сигурност, рутера извършва справка в маршрутната таблица, за да намери подходящия интерфейс, който води до адреса на получателя.

Всеки запис в таблицата за маршрутизация-нарича се *route entry* or *route*-е идентифициран от целевата мрежа, по която трафикът може да бъде предаден. Целевата мрежа, под формата на IP адрес и мрежова маска, може да бъде IP мрежа, подмрежа, supernet или хост

**Записи на маршрутната таблица могат да произхождат от следните източници:**

• пряко свързани мрежи (целевата мрежа е IP адресът, който ще зададете на интерфейс в режим Route)

• Динамични протоколи за маршрутизация, като OSPF, BGP, или RIP

• маршрути, които са внесени от други маршрутизатори или виртуални рутери

• Статично конфигурирани маршрути

**10. Какво ще се случи, ако при предаване на фрагментиран IP пакет, един от фрагментите не достигне до получателя след изтичане на съответния таймаут?**

Ако това изчакване отпадне, частично-сглобената дейтаграмата трябва да се изхвърли и ICMP Time Exceeded съобщение трябва да бъде изпратено до хоста-източник (ако е получен фрагмент нула).

**11. Вярно ли е, че алгоритъмът за избор на маршрут е универсален и не зависи от протокола за маршрутизация?**

Не е вярно.

Рутерът използва маршрутния алгоритъм за изчисляване на пътя, който най-добре ще послужи за транспортиране на данните от източника до местоназначението. Въпреки това, не можете директно да изберем алгоритъма,който да използва маршрутизаторът. Протоколът за маршрутизация, който сме избрали за мрежата, определя кой алгоритъм  
ще използваме. Например, докато маршрутният протокол RIP може да използва един вид алгоритъм, OSPF използва друг.

**12. Коя е командата, чрез която манипулирате с маршрутната таблица на устройството?**

Route:  
манипулира IP таблици за маршрутизация на ядрото. Основната му употреба e за създаване на статични маршрути до определени хостове или мрежи чрез интерфейс, след като е била конфигурирана с ifconfig.

**13. Каква е ролята на ARP протокола?**

Протокол за преобразуване на адреси. Превръща 32-битови IP-адреси в адреси от физическата мрежа, които са 42-битови адреси на Ethernet.

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 изпращача.

Дейтаграмите, чийто получател е хост от друга IP мрежа (подмрежа), се изпращат към маршрутизатора, включен в локалната мрежа. Неговият Ethernet адрес се получава чрез ARP заявка, ако не е кеширан. Този маршрутизатор избира маршрут и препраща дейтаграмата към нейния получател.

**14. Каква е ролята на ICMP протокола? На кой слой от OSI модела функционира ICMP?**

Протокола се използва за да докладва за проблеми с доставката на IP дейтаграми в IP мрежа. Може да бъде използван да показва кога определена крайна система End System (ES) не отговаря, кога IP мрежа не е достижима, кога даден възел е пренатоварен, когато настъпи грешка е IP header информацията и тн. Протоколът също често се използва от системни оператори да проверят коректността на операциите в End Systems (ES) и да проверяват дали рутерите коректно предават пакети към определените получатели.

Функционира на Network Layer в OSI модела

Много мрежови средства за диагностика се базират на ICMP. Средството ping се реализира с ICMP "Echo request" и "Echo reply" съобщения.

**15. Сравнете протоколите RIPv1 и RIPv2.**1ви начин:

**RIP** (routing information protocol) e широкоизползван маршрутизиращ протокол с вектор на разстоянието (distance vector).  
1.Първата версия на RIPv1 не поддържа subnet маски, т.е. VLSM, респ. CIDR.  
Втора версия на протокола - RIPv2, поддържа VLSM, респ. CIDR.  
  
2.RIPv1 (RFC 1058) прилага само classful маршрутизация.

Т.е периодичните updates не носят subnet информация  
  
RIPv2 прилага classless маршрутизация и има възможност да носи subnet информация.  
  
3. RIPv1 не поддържа VLSM (променлива дължина подмрежата Masking),   
RIPv2 поддържа.  
4. Максималният брой хопове в RIP е 15.  
5. За да не се товарят хостове, които не са участници в RIP, RIPv2 “мултикаства ” обновленията на адрес 224.0.0.9, за разлика от RIPv1, който   
е broadcast.

2ри начин:

RIPv1 работи с броадкаст съобщения, прилага само classful маршрутизация. Т.е периодичните updates не носят subnet информация. Не е възможно да имаме подмрежи от един и същи клас с различни маски. С други думи, всички подмрежи от даден клас трябва да бъдат с еднакви маски.  
RIPv2 има възможност да носи subnet информация, да поддържа CIDR. За поддържане на обратна съвместимост с версия 1 запазено е ограничението от 15 хопа. За сигурност е въведена аутентикация с явен текст, подобрена с MD5 (RFC 2082). За да не се товарят хостове, които не са участници в RIP, RIPv2 “мултикаства” обновленията на адрес 224.0.0.9, за разлика от RIPv1, който е broadcast.

**16. Подлежат ли ICMP пакетите на маршрутизация?**

Да, защото те се опаковат в IP пакети и оттам нататък всички свойства на IP пакетите важат за тях.

**17. Какво представлява RTT?**

Round-trip time (RTT), също round-trip delay, е времето нужно за сигнал или пакет да стигне от изоточника до избраната дестинация, и обратно. Източникът е компютър, а дестинацията е отдалечен компютър или система, която получава сигнал и го препредава.

**18. Какви транспортни протоколи познавате?**

Двата основни протокола на транспортния слой в TCP/IP модела са Transmission Control Protocol (TCP) и User Datagram Protocol (UDP).

И двата управляват комуникациите между приложения, работещи на компютри в Мрежата и са от типа “край до край” (end to end).

Типични приложения на TCP са:

- Web браузъри и сървъри   
- E-mail

- сигурен обмен на файлове (FTP)

Типични приложения на UDP са:   
- Domain Name System (DNS)  
 - Video Streaming   
- Voice (Video) over IP (VoIP); Video over IP   
- мониторинг и управление на мрежите (SNMP)  
 - опростен пренос на двоични файлове (Trivial FTP).

UDP е по-опростен, осигурява ненадеждно обслужване с неустановена връзка (connectionless), дефиниран в RFC 768. Предимство е ниското закъснение.   
Протоколните единици в UDP се наричат дейтаграми, за които подобно на IP пакетите се полагат максимални усилия за доставяне - "best effort".

**19. Какво представлява една автономна система, i.e. AS?**

Автономна система в Интернет се нарича съвкупността от IP мрежи и маршрутизатори, които са под управлението на една или повече компании с еднакви правила за маршрутизация от и към Интернет.

Целта на AS е още едно ниво на маршрутизация, необходими са при връзката м/у различни АS.

**20. Кой протокол използва командата ping? Какъв тип заявка генерира тази команда?**

Ping е инструмент за тестване на достижимостта 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.

Често се използва за дебъгване на мрежови конекции.(Ping фиксира момента на изпращането на ехо-заявката и тази информация се връща в отклика, което позволява ping правилно да изчислява стойността RTT - времето необходимо на пакет с малка дължина да стигне от клиента до сървъра и обратно)

**21. Благодарение на кое поле от IP хедъра функционира програмата traceroute?**

Destination IP address

**22. Какви записи съдържа маршрутната таблица?**

Маршрутната таблица съдържа най-малко следните три информационни полета:

1. id на мрежата: това е подмрежата местоназначение
2. цена/метрика: това е цената или метриката на пътя, през който пакетът ще бъде изпратен
3. следващ скок (*hop*): следващият скок, или [гейтуей](https://bg.wikipedia.org/wiki/%D0%93%D0%B5%D0%B9%D1%82%D1%83%D0%B5%D0%B9_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D1%8A%D1%80%D0%BD%D0%B8_%D0%BC%D1%80%D0%B5%D0%B6%D0%B8)), е адреса на следващата станция (компютър или друго устройство в мрежата), към който пакетът ще бъде изпратен по пътя до неговата крайна дестинация

**23. Къде се извършва реасемблирането на фрагменти, в случай че пакет е претърпял фрагментация?**

Фрагментиран IP пакет е обикновено дефрагментиран от хоста на местоназначението, но междинните устройства, които трябва да разгледаме в целия IP пакет може да трябва също да се дефрагментират. Два примера за такива устройства са firewalls и Network Address Translation (NAT) рутери.

**24. Съществува ли зависимост между MSS и MTU? Каква е тя?**

Headers + MSS ≤ MTU

МSS(maximum segment size) – максималният размер на сегмента  
MTU(maximum transmission unit ) – маскимална единица за предаване

**25. Какъв транспортен протокол използва HTTP?**

TCP

**26. Защо в локалната мрежа Ethernet е необходимо да работи broadcast предаване?**

За да изпратим пакета към някой в LAN, трябва да му знаем MAC адреса, а това го научаваме посредством ARP протокол, който трябва да може да изпрати broadcast съобщения в рамките на мрежата.

**27. Защо в случаите на използване на маска в IP пакетите, стойността на маската не с предава?**Информацията, изпратена по мрежата е във вид на данни или пакети от данни. Ако един компютър ( хост А) желае да изпрати данни до друг компютър ( хост В), данните трябва първо да бъдат опаковани чрез процес, наречен енкапсулация. Този процес обгръща данните в необходимата протоколова информация, преди изпращането им през мрежата. Затова , когато данните преминават през отделните пластове на OSI Модела, те получават хедър, опашка и друга информация.

**28. Какво означава енкапсулация?**

Всички комуникации през мрежата започват от източника и се изпращат до дестинацията. Информацията, изпратена по мрежата е във вид на данни или пакети от данни. Ако един компютер ( хост А) желае да изпрати данни до друг компютер ( хост В), данните трябва първо да бъдат опаковани чрез процес, наречен енкапсулация. Този процес обгръща данните необходимата протоколова информация преди изпращането им през мрежата. Затова , когато данните преминават през отделните пластове на OSI Модела, те получават хедър, опашка и друга информация

**29. На приложно ниво всеки процес се опрделя еднозначно от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ?**

socket

**30. Кой ТСР порт обикновено се използва за HTTP трафик?**

Port 80

**31. Адресът на кой възел влиза в аrp таблицата на хост, изпращащ дейтаграма в друга IP мрежа?**  
Ако е IP адрес от различна подмрежа , MAC адресът ще бъде този на интерфейса на рутера, който е най близо до нас.

**32. Какво е характерно за дейтаграмните протоколи?**

UDP е протокол, използван за транспортиране на данни през IP .UDP не извършва договаряне каkто TCP прави , или да провери за грешки , или дори да се види дали са получени предадените данни , така че UDP е посочен като ненадежден протокол. Въпреки това, тъй като UDP пропуска потвърждаване на установената връзка и е фокусирана върху чисто предаване , той има по-ниски режийни и по този начин е по-бързо от TCP . UDP ще осигури по-добра пропускателна способност на мрежата , където физическите и DATALINK протоколи слой са надеждни.

**33. В какво се изразява ненадеждността в IP протокола?**

Пристигането на дейтаграмите до местоназначението им не е гарантирано тъй като е възможно те да надвишат допустимото време, да бъдат погрешно маршрутизирани или да бъдат унищожени при неуспешна фрагментация или сглобяване. Интернет протоколът не поддържа управление но потока от данни и няма вградени средства, за да провери дали дадено изпратено съобщение е пристигнало успешно. При него единствено се използуват контролни суми на заглавната част, но не и за данните, които пренася дейтаграмата. Проверката дали данните са пристигнали успешно, управлението на потока и въобще надеждността на комуникацията се осигурява от протоколите от по-горните слоеве (за пример може да послужи протоколът от транспортния слой ТСР).

**34. С коя команда може да се открие мястото на поява на грешка в приетия пакет?**

Tracert

**35. Кои протоколи на TCP/IP реализират адресно преобразуване?**

Arp, rarp, dns(?)

**36. Как обработват рутерите полето Destination IP adress?**  
  
Маршрутизаторът се счита за Layer 3 устройство , тъй като неговото основно решение се основава на информацията в Layer 3 IP пакет , специално за дестинацияна на IP адреса . Този процес е известен като маршрутизиране. Когато всеки маршрутизатор приема пакет , търси своята таблица за маршрутизация , за да намерите най-добрият път между дестинацията на IP адреса на пакета и един от мрежовите адреси в таблицата за маршрутизация . След като даден път е намерен, пакетът е капсулиран в Layer 2 Link Data frame за този изходящ интерфейс .

**37. Нека имаме хост с два мрежови интерфейса, всеки с по един IP адрес (I1 и I2). Може ли този хост да изпати и получи IP дейтаграма между I1 и I2?**

Да, може

**38. Как влияе стойността на RTT на ефективната работа на канала?**

**39. Защо се изпраща arp заявка със собствения IP адрес?**

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. Този хост изпраща ARP пакет-отговор само на подателя, тъй като вече знае неговия Ethernet адрес от получената заявка.

**40. Колко едновременни съединения могат да се поддържат с NAT протокол с единствен IP адрес на рутера?**

повече от 60 хил. съединения

**41. За какво се използва функцията forwarding?**

Препращане на пакети м/у интерфейсите на 1 компютър.

**42. Какво е значението на протокола с хлъзгащия се прозорец?**

В TCP протокола размерът на буфера за входни данни може да варира в зависимост от натовареността на приложението. Този размер се описва чрез window size. Затова ни трябва механизъм за стесняване/разширяване на размера на прозореца. Sliding window изпълнява тази задача.

**43. Какво ще стане с пакет ако има DF=1 ,но му се налага да се дефрагментира ?**

Тогава пакета няма да се дефрагментира и ще се върне съобшение за това, понеже DF=1(Don’t Fragment = 1).

**44. Защо mss=1460 при Ethernet протокола?**

MSS + header <= MTU

MTU = 1500, header = 40 => MSS = 1500-40 = 1460

**45. Ако даден отдалечен сървър е достъпен ,но ping-a не работи къде може да се крие проблема?**Може да има филтрация на IP адреси в отдалечения сървър.

**46. Коя комада се използва за проверяване на скороста на изпращане спрямо големина на пакетите?**

**47. Защо ТCP е надежден протокол?**

• Acknowledgements: При размяната на един или повече пакети, получателя връща acknowledgement (наречено "ACK") към изпращача, показвайки, че е получил пакетите. Ако пакетите не са ACKнати, изпращача може да преизпрати пакетите(или да спре връзката ако си мисли чр получателя е крашнал).

• Flow control: Ако изпращача изпраща пакети прекалено бързо, получателя изпуска пакети. Тогава се изпраща съобщение за забавяне на скоростта на изпращане.

• Packet recovery services: Получателя може да поиска преизпращане на пакетите.

**48. Каква е основната разлика между ping и traceroute?**

И ping и traceroute използват ICMP, но ping ни връща само инфорамция дали има път от нашата мрежа до някоя друга, а traceroute ни връща информация за мрежите, през които минаваме, за да стигнем определената.

**49. Защо Ethernet има 1048 фрагмента?**

wtf zomfg

**50. Сравнете switch и bridge.От кой слой са?**суич-овете могат да работят на 1, 2,3,4-ти или 7-ми слой от OSI, а мостовете на 2-ри. Мостовете разчитат на наводняването по всички адреси предоставени от хедърите на пристигналите пакети.

**51. Кой е метода за приемане и изпращане на данни едновременно?**

Full duplex

**52. Даден е адрес.Кой протокол се използва,за да стигнат данните от мрежата до Интернет?**

Bgp?

**53. Какво е анализатор на мрежи(wireshark)?**Wireshark е безплатен и с отворен код [анализатор на мрежови протоколи](https://bg.wikipedia.org/w/index.php?title=%D0%90%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80_%D0%BD%D0%B0_%D0%BC%D1%80%D0%B5%D0%B6%D0%BE%D0%B2%D0%B8_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D0%B8&action=edit&redlink=1). Той се използва за отстраняване на проблеми в [мрежата](https://bg.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D1%8A%D1%80%D0%BD%D0%B0_%D0%BC%D1%80%D0%B5%D0%B6%D0%B0), анализ, разработка на [софтуер](https://bg.wikipedia.org/wiki/%D0%A1%D0%BE%D1%84%D1%82%D1%83%D0%B5%D1%80) и [комуникационни протоколи](https://bg.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B8_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D0%B8) и образование

**54. Какви са характреристиките на маршрутните политики?**  
  
Базиран на правила за маршрутизация ( PBR ) е техника, използвана за вземане на решения за маршрутизация въз основа на полици , определени от администратора на мрежата . Когато маршрутизатор приеме пакет, тя обикновено решава къде да го предаде на базата на адресната дестинация в пакета , който след това се използва, за да търси път в таблица за маршрутизация . Въпреки това, в някои случаи , може да има нужда да се препрати пакета въз основа на други критерии . Например, един администратор може да иска да предаде пакет въз основа на адреса на източника , а не адреса на получателя .

Маршрутизацията базирана на рутирането може също да бъде въз основа на размера на пакета , протокола на payload-а , или др. Това позволява маршрутизиране на пакети с произход от различни източници на различни мрежи , дори когато дестинациите са същите и могат да бъдат полезни при свързване на няколко частни мрежи.

**55. Характеризирайте repeater и hub. От кой слой на OSI са?**

Повторителят е устройство, което поема входния сигнал, усилва го и го предава към преносната среда. Повторителите могат да се използват за увеличаване на максималните дължини на кабелите в локалната мрежа или за съединяване на различни типове кабели. Тези устройства могат да свържат две идентични мрежи, но не могат да се използват за свързване на мрежи с различна архитектура или метод за достъп.

**56. Какви са предимствата като имаме default gw?**Ако компютърът местоназначение е в различна подмрежа, съобщението се изпраща към адреса на подразбиращия се шлюз (default gateway), който е адресът на интерфейса на маршрутизатора (маршрутизаторът служи като шлюз към останалите подмрежи).

**57. Колко IPта ни трябват ако искаме да свържем 2 локални мрежи всяка с по 500 хоста?**

**58. Коя команда се използва за да видим всички активни и неактивни интерфейси?**

Ifconfig –a (-a за да покаже и inactive ifaces)

**59. Кои устройства осигуряват локализация на трафика?**

switch

**60. Какви полета се съдържат в статичната маршрутна таблица?**

**61. Какво осигурява процесът на демултиплексиране при UDP протокола?**

**62. С коя команда може да се намери MTU?**

ifconfig

**63. Получено е icmp съобщение за грешка. Как може да се определи причината за грешката?**

В ICMP пакета се съдържа поле type, на базата на което се определят типа грешка.

**64. Какъв е адресът, който ползват всички в работата си с Етернет устройствата**

**65. Кога при TCP се използва механизма за повторно предаване на данни?**

Packet recovery services: Получателя може да поиска преизпращане на пакетите.

**66. Как се задава метриката в RIP и OSPF протокол съответно?**

Mетриката използвана от RIP протокола е брой хопове.(next hop)

Метриката в OSPF е стойността на пътя - маршрута (path cost).

Тя се определя от скоростта (bandwidth), зададена на интерфейса,

водещ към съответния маршрут.

**67. При отсъствие на запис за определяне на next hop в RT къде ще се пренасочи пакета?**

Пакет, който не намери съвпадение в маршрутната таблица, поема към “gateway of last resort”. Това е рутер с по-подробна информация за маршрутите.

Ако няма default route и адреса на получателя не бъде открит в таблицата, пакетът се изхвърля и на IP адреса на източника се въща ICMP съобщение: ‘Destination or Network Unreachable’.

**68. При TCP протокол при какви условия се реализира преход от едно състояние в следващо?**

**69. В какво се изразява принципната разлика в работата на ARP и RARP протоколите?**  
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).  
  
RARP (Reverse Address Resolution Protocol) е протокол за намиране на IP адреси по Ethernet адреси.

АRP: IP =>MAC  
RARP: MAC => IP

**70. Ако съобщението е фрагментирано и по пътя си попада в участък с MTU с по-голям размер на фрагмента, тогава къде ще се осъществи събирането на фрагментите?**

Няма да е в някой от междинните рутери, а в крайната цел.   
  
**71. 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).

**72. Защо трябва да се използва TTL при мултимедийни данни?**

**73. По какво се различават задачите на мрежово ниво при локални и глобални мрежи?**

**74. Състоянието LISTEN е характерно за \_\_\_\_\_\_\_\_\_ ?**

Сървър

**75. Какви задачи решава IP протокола?**Задачата на IP протокола е да извърши успешно предаване на пакети от източника до получателя, без значение дали те са в една и съща мрежа или в различни.  
Транспортното ниво взима потоци от байтове и ги разделя на сегменти (TCP) или дейтаграми(UDP), които се „обличат“ като пакети.  
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 я вмъква в съответния поток от байтове.

**76. За какви цели може да се използва iproute2?**

Iproute2 – сбор от средства за контрол на TCP/IP мрежи и трафик в Linux.

iproute2 се използва за контролиране на [TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) и [UDP](https://en.wikipedia.org/wiki/User_Datagram_Protocol)[IP](https://en.wikipedia.org/wiki/Internet_Protocol) мрежи и [трафик контрол](https://en.wikipedia.org/wiki/Network_traffic_control) в Linux ядрото, в [IPv4](https://en.wikipedia.org/wiki/IPv4) и [IPv6](https://en.wikipedia.org/wiki/IPv6) , както и за конфигуриране на [драйвери на устройства](https://en.wikipedia.org/wiki/Device_driver) за [мрежови интерфейсни контролери](https://en.wikipedia.org/wiki/Network_interface_controller) (мрежови карти) и [безжични мрежови контролери интерфейс](https://en.wikipedia.org/wiki/Wireless_network_interface_controller) (WNICs).

**77. На транспортния слой какви варианти могат да се използват за филтрация на пакети?**

**78. Дължината на UDP datagram е 1472 байта. При предаване в Етернет мрежа този пакет ще се фрагментира ли? Защо?**

Според мен да, Тъй като в Ethernet е заложено максималният обем данни в един кадър да бъде 1500 B (MTU = 1500), обикновено не се ползват пакети с по-голяма дължина.

MSS на Етернет = 1460<1472

**79. В пакета DF = 1. По пътя си дейтаграмата попада в участък, където е необходима фрагментация. Как се решава този проблем?**

**80. За кой протокол се използва дейтаграма?**

UDP

**81. Ако направиш ping с 1472 bytes дата ще се фрагментира ли?**

Според мен да, защото MSS на Етернет = 1460<1472

# **82. Какво е мултиплексиране? Мултиплексиране (**multiplexing**)**

Технология на разделяне на средствата за предаване на данни между група използващи ги обекти.

В резултат на мултиплексирането в един [физически канал](http://tuj.asenevtsi.com/ComN/ComN014.htm) се създават група [логически канали](http://tuj.asenevtsi.com/ComN/ComN018.htm).

Устройството, в което се извършва мултиплексирането, се нарича [мултиплекс](https://bg.wikipedia.org/wiki/%D0%9C%D1%83%D0%BB%D1%82%D0%B8%D0%BF%D0%BB%D0%B5%D0%BA%D1%81) — (MUX), а обратното устройство — демултиплекс (DEMUX).

**83. Команда netstat за кой протокол вади статистика за брой грешки при фрагментация?**

ICMP?

**84. С коя команда може да разбереш къде точно се е получила грешка при получения пакет?**

**85. Защо MTU за интерфейс loopback може да бъде по-голям от 1500 (в Ethernet)**

**86. Локални мрежи отдалечени една от друга могат ли да бъдат в една автономна система ?**

**87. IP tables за какво се ползва**

iptables - administration tool for IPv4 packet filtering and NAT

**88. Какви механизми използва RIP протокола за уведомяване за несъществуващ маршрут?**RIP - Когато даден път бъде отбелязан като невалиден, се изпращат съобщения с тази информация към съседните маршрутизатори и се преустановява използването му.

**89. Какво осигурява процесът на мултиплексиране при TCP протокола?**

**90. За да използвате хост с OS Linux за маршрутизация на IP трафик между два мрежови сегмента, какво трябва да направите?**

Нещо с командата brctl...???

**91. С командата netstat за кой протокол се извежда статистика за брой създадени сегменти?**TCP

**92. Каква е задачата на маршрутния протокол?**Маршрутния протокол- има за задача да определи динамично пътя за изпращане на пакетите.

**93. Кои полета на заглавната част на IP дейтаграмата анализира маршрутизатора**

Destination address,Header checksum,TTL,DF

**94. Какво е quagga?**Quagga e open source софтуерен пакет за маршрутизация. Поддържа: RIPv1, RIPv2, RIPng, OSPFv2, OSPFv3, BGP-4 и BGP-4+ (т.е IPv4 и IPv6)

**95. Напишете най-характерното за работата на един комутатор (switch)?**

Основното предназначение на един суич (**switch**, комутатор) е да избере път, по който да изпрати данните от източника до тяхното местоназначение в дадена локална мрежа.

**96.Напишете най-характерното за работата на един маршрутизатор (router)?**

**Разлики :**  
**Switch** (комутатор): получава пакет по един порт, и го изпраща на порта, на който е свързан съответния целеви МАК адрес. Поддържа таблица с МАК адреси, като запомня от кой порт е получил пакет от кой МАК адрес. Има и протоколи за тази работа.  
Скоростта на пренос на данните може да е много по-висока от скоростта на всеки порт по отделно.  
По-модерните и по-скъпи комутатори могат да правят елементарен анализ на пакетите с цел филтриране.  
Комутатора не променя съдържанието на пакета!

**Router** (маршрутизатор): получава пакет на един интерфейс, и го препраща на друг интерфейс, където се намира съответния IP адрес. Поддържа маршрутна таблица, в която има описани адресни пространства наричани Мрежи, и метода за достигане до съответната мрежа: интерфейс, и адрес на следващия маршрутизатор. Мрежите се описват най-често като CID префикс.  
Маршрутизатора може да променя съдържанието на пакета! Най-често се променя само антетката (заглавка, хедър) на пакета. По този начин се реализира NAT/Masquerade.

**98. Опишете поведението на маршрутизатор в режим на динамичен**....  
Динамичната маршрутизация е подходяща за по-големи мрежи. Използват се протоколи за динамично маршрутизиране като [OSPF](https://bg.wikipedia.org/wiki/OSPF), [IS-IS](https://bg.wikipedia.org/w/index.php?title=IS-IS&action=edit&redlink=1), [BGP](https://bg.wikipedia.org/wiki/BGP), [RIP](https://bg.wikipedia.org/wiki/RIP) и др. Те позволяват маршрутизаторите автоматично да намират най-добрите пътища помежду си.  
  
**99.Дайте пример за IGP EGP протоколи на маршрутизация**.  
Маршрутизацията в интернет може да се раздели на два класа: вътрешна ([IGP](http://www.webopedia.com/TERM/I/IGP.html), Interior Gateway Protocol) и външна ([EGP](http://www.webopedia.com/TERM/E/EGP.html), Exterior Gateway Protocol). Вътрешните протоколи работят вътре в една автономна система, докато външните свързват различни AS.   
Пример за IGP протоколи са OSPF, IS-IS и RIP.  
  
**100.Мрежова маска.**  
Маршрутизиращият префикс на един адрес е написан във форма идентична на тази на самият адрес. Това се нарича [мрежова маска](https://bg.wikipedia.org/w/index.php?title=%D0%9C%D1%80%D0%B5%D0%B6%D0%BE%D0%B2%D0%B0_%D0%BC%D0%B0%D1%81%D0%BA%D0%B0&action=edit&redlink=1) на адреса. Например, една спецификация на най-старшите 18 бита на IPv4 адрес, 11111111.11111111.11000000.00000000, е написана като 255.255.192.0. Ако тази маска обозначава една подмрежа в една по-голяма мрежа се нарича още подмрежовата маска. Тази форма на обозначение обаче се използва само за IPv4 мрежи.

**101.Дефинирайте три вида NAT....**Статично преобразуване (static NAT): на маршрутизатора са конфигурирани определен брой IP-адреси, които отговарят на друг определен брой адреси, използвани във вътрешната мрежа, така че между вътрешната и външната мрежи съществува ясна връзка.  
Динамично преобразуване (dynamic NAT)**:** на маршрутизатора са конфигурирани определен брой IP-адреси, които се вземат в употреба за вътрешните адреси според нужда, така че във вътрешната мрежа може да има най-много определен брой активни връзки към външната, но адресите на вътрешната мрежа могат да бъдат повече от този брой активни връзки.  
  
**103. Тристранното ръкостискане (three-way handshake) при TCP.**  
Three-ways handshake при TCP:1. Клиентът-инициатор изпраща сегмент SYN, съдържащ начална стойност на последователността SEQ,и представляващ заявка за начало на сесия.  
2. В отговор сървърът изпраща сегмент,съдържащ стойност за потвърждение

3. Клиентът-инициатор отговаря със стойност ACK, равна на (получена SEQ + 1). С това съединението е установено

**104. Защо при IPv4 на всеки междинен рутер се преизчислява полето контролна сума?**

IPv4 преизчислява полето контролна сума, за да провери дали има загуба на пакети.  
  
**105. С коя команда можем да видим различни статистики за най-използваните протоколи?**С команда Netstat можем да видим различни статистики за най-използваните протоколи.

**106.С коя команда се измерва RTT?**  
RTT се измерва с команда ping.

**107.В какво се изразява контролът на потока при TCP?**Контролът на потока при TCP се използва за контролиране на размера на пакета,които получателят трябва да получи, за да може да получи обратно потвърждение.

**108.Каква е структурата на MAC адреса?**

МАС адресът е 48 битов адрес в Layer 2 в OSI модела.  
  
  
**109.Какви са начините за предаване на данни спрямо броя получатели?**при IPv4 - Broadcast, Multicast, Unicast  
при IPv6 - Anycast, Multicast, Unicast   
  
  
**110.Какви варианти за филртрация на пакети могат да се използват в транспортния слой?**Получателят може да определи размера на пакета, който получава и се изпраща.  
  
**111. DNS**  
Domain Name System (DNS) е йерархична разпределена база от данни.

Тя съхранява информация за съотвтствието между Internet хост имена и IP адреси и обратно, информация за маршрутизиране на ел. поща и др. данни, използвани от Internet приложения.  
Данните, съхранени в DNS са domain names, организирани в дървовидна структура.Всеки възел в дървото се нарича domain и му се дава етикет.Името на домейна във възела е поредица от етикетите, показващи пътя от възела до корена (root).

**112. DNS протокол**  
DNS основно използва User Datagram Protocol (UDP) на порт 53 за обслужване на заявки.

DNS заявките се състоят от една единствена UDP заявка от клиента, последвана от един единствен UDP отговор от сървъра.

Transmission Control Protocol ( TCP) се използва, когато в отговора се съдържат повече от 512 bytes или при трансфер на зони.