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

arp –a

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

The default route in IPv4 (in CIDR notation) is 0.0.0.0/0, often called the quad-zero route. Since the subnet mask given is /0, it effectively specifies no network, and is the "shortest" match possible. A route lookup that doesn't match anything will naturally fall back onto this route.

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

**Hub** – device for connecting multiple Ethernet devices together and making them act as a single network segment. It has multiple I/O ports, in which a signal introduced at the input of any port appears at the output of every port except the original incoming. A hub works at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

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** - computer networking device that connects network segments or network devices. The term commonly refers to a multi-port network bridge that processes and routes data at the data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3) and above are often referred to as layer-3 switches or multilayer switches.

A switch is a telecommunication device which receives a message from any device connected to it and then transmits the message only to that device for which the message was meant. This makes the switch a more intelligent device than a hub (which receives a message and then transmits it to all the other devices on its network.) The network switch plays an integral part in most modern Ethernet LANs.

An Ethernet switch operates at the data link layer of the OSI model to create a separate collision domain for each switch port. With 4 computers (e.g., A, B, C, and D) on 4 switch ports, A and B can transfer data back and forth, while C and D also do so simultaneously, and the two conversations will not interfere with one another. In the case of a hub, they would all share the bandwidth and run in half duplex, resulting in collisions, which would then necessitate retransmissions. Using a switch is called microsegmentation. This allows computers to have dedicated bandwidth on point-to-point connections to the network and to therefore run in full duplex without collisions.

**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 суича и хъба. Ако до някое IP връзката е през маршрутизатор, а не през суич или хъб, то ние не научаваме неговия MAC адрес.

За определяне на пътя за предаване на данните и насочване на пакетите маршрутизаторът използва таблица за маршрутизация въз основа на информацията за топологията на мрежите, към които е свързан. Тази таблица маршрутизаторът си прави сам, като си набавя информация, а при някаква промяна си актуализира сам, „разпитвайки“ другите маршрутизатори кой докъде е свързан. Това става чрез съответните протоколи за маршрутизация. Възможно е и ръчна намеса в тази таблица, ако по някакви съображения се желае дадена връзка да се прекарва само по някой от възможните пътища. Ако в таблицата му липсва даден маршрут, започва разпитване дали някой от достъпните маршрутизатори не знае, а те разпитват по-натам по веригата. Ако се намери път, таблицата се допълва, а пакетът се изпраща. Ако не се намери, пакетът се отхвърля.

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

Typically, routers are attached to multiple networks and are responsible for directing traffic across these networks. Each router maintains a routing table, which is a list of known networks and directions on how to reach them. While processing an incoming packet on a security device, the router performs a routing table lookup to find the appropriate interface that leads to the destination address.

Each entry in a routing table—called a *route entry* or *route*—is identified by the destination network to which traffic can be forwarded. The destination network, in the form of an IP address and netmask, can be an IP network, subnetwork, supernet, or a host.

Routing table entries can originate from the following sources:

* Directly connected networks (the destination network is the IP address that you assign to an interface in Route mode)
* Dynamic routing protocols, such as OSPF, BGP, or RIP
* Routes that are imported from other routers or virtual routers
* Statically configured routes

<http://www.juniper.net/techpubs/en_US/nsm2010.1/topics/concept/security-service-firewall-screenos-routing-table-entry-overview.html>

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

If this timeout expires, the partially-reassembled datagram MUST be discarded and an ICMP Time Exceeded message sent to the source host (if fragment zero has been received).

<http://tools.ietf.org/html/rfc1122>

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

Не е вярно.

The router uses the routing algorithm to compute the path that would best serve to transport the data from the source to the destination. However, you cannot directly choose the algorithm that your router uses. Rather, the routing protocol you choose for your network determines which algorithm you will use. For example, whereas the routing protocol RIP may use one type of routing algorithm to help the router move data, the routing protocol OSPF uses another.

Many of the differences between particular routing protocols are directly related to differences in their routing algorithms. The routing algorithm a protocol uses cannot be changed or altered. If the algorithm a particular protocol uses does not favor your networking environment, the only way to change it is to change routing protocols.

<http://www.informit.com/articles/article.aspx?p=27267>

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

Route:

manipulates the kernel's IP routing tables. Its primary use is to set up static routes to specific hosts or networks via an interface after it has been configured with the ifconfig program.

When the add or del options are used, route modifies the routing tables. Without these options, route displays the current contents of the routing tables.

<http://linux.about.com/od/commands/l/blcmdl8_route.htm>

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

преобразуване от IP адрес във физически(Ethernet) адрес

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.За целта, за установяване на съответствието между IP адреса и Ethernet адреса на хостовете в локалната мрежа се използва протокол за право преобразуване на адресите ARP.

Когато даден хост трябва да изпрати 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” са записани съответните адреси на хоста, който изпраща ARP заявката. 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. 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 шестнадесетичен вид) на хоста, изпращащ пакета-отговор.

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.

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

Използва се от мрежовите ОС главно за откриване на грешки по мрежата и изпращане на съобщения за това

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.

**10. Сравнете протоколите RIPv1 и RIPv2.**

The Routing Information Protocol (RIP) is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and used to deprecate inaccessible, inoperable, or otherwise undesirable routes in the selection process.

RIP uses the User Datagram Protocol (UDP) as its transport protocol, and is assigned the reserved port number 520. It works on Application Layer.

RIPv1: The original specification of RIP, it uses classful routing. The periodic routing updates do not carry subnet information, lacking support for variable length subnet masks (VLSM). This limitation makes it impossible to have different-sized subnets inside of the same network class. In other words, all subnets in a network class must have the same size. There is also no support for router authentication, making RIP vulnerable to various attacks.

RIPv2: It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained. In an effort to avoid unnecessary load on hosts that do not participate in routing, RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast. Unicast addressing is still allowed for special applications.

**11. 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.

**12. Какво представлява RTT?**

Round-trip time (RTT), also called round-trip delay, is the time required for a signal pulse or packet to travel from a specific source to a specific destination and back again. In this context, the source is the computer initiating the signal and the destination is a remote computer or system that receives the signal and retransmits it.

More: <http://searchnetworking.techtarget.com/definition/round-trip-time>

**13. Какви транспортни протоколи познавате?**

TCP, UDP

**14. 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.

On the Internet, an autonomous system (AS) is the unit of router policy, either a single network or a group of networks that is controlled by a common network administrator (or group of administrators) on behalf of a single administrative entity (such as a university, a business enterprise, or a business division). An autonomous system is also sometimes referred to as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN).

Networks within an autonomous system communicate routing information to each other using an Interior Gateway Protocol (IGP). An autonomous system shares routing information with other autonomous systems using the Border Gateway Protocol (BGP). Previously, the Exterior Gateway Protocol (EGP) was used. In the future, the BGP is expected to be replaced with the OSI Inter-Domain Routing Protocol (IDRP).

The Internet's protocol guideline for autonomous systems, after offering a definition similar to the one above, provides a more technical definition as follows:

*An AS is a connected group of one or more Internet Protocol prefixes run by one or more network operators which has a SINGLE and CLEARLY DEFINED routing policy.*

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

ping uses the ICMP protocol's mandatory ECHO\_REQUEST datagram to elicit an ICMP ECHO\_RESPONSE from a host or gateway.

инструмент за тестване на достижимостта на даден хост по IP мрежата, Изпраща ECHO\_REQUEST пакет към зададения хост. Достижимите хостове връщат пакет с отговор.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)

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

Destination IP address

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

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

A fragmented IP packet is normally defragmented by the destination host, but intermediate devices that need to look at the entire IP packet may have to defragment it, too. Two examples of such devices are firewalls and Network Address Translation (NAT) routers.

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

Headers + MSS ≤ MTU

Maximum transmission unit (MTU) of a communications protocol is the size (in bytes) of the largest protocol data unit that the layer can pass onwards. A larger MTU brings greater efficiency because each packet carries more user data while protocol overheads, such as headers, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU also means processing of fewer packets for the same amount of data. In some systems, per-packet-processing can be a critical performance limitation.

However, this gain is not without some downside. Large packets can occupy a slow link for some time, causing greater delays to following packets and increasing lag and minimum latency. For example, a 1500-byte packet, the largest allowed by Ethernet at the network layer (and hence over most of the Internet), ties up a 14.4k modem for about one second. Large packets are also problematic in the presence of communications errors. Corruption of a single bit in a packet requires that the entire packet be retransmitted.

The maximum segment size (MSS) is the largest amount of data, specified in bytes, that a computer or communications device can handle in a single, unfragmented piece.

<http://searchnetworking.techtarget.com/definition/maximum-segment-size>

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

TCP

Въпроси от предишни тестове които изкопах от най-различни източници. Някои са взети от снимки от контролни, други от разни текстови файлове с неясен произход.

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

за да изпратим пакета към някой в лан трябва да му знаем мак адреса, а това го научаваме посредством арп протокол, който трябва да може да изпрати broadcast съобщения в рамките на мрежата

**2. Защо в случаите на използване на маска в IP пакетите, стойността на маската не с предава?**

**3. Какво означава енкапсулация?**

the encapsulation means the lower layer of TCP/IP protocol suite would wrap (encapsulate) the upper layer’s data, header and add its own header/footer with protocol information, then send to lower layer again till the encapsulated data is sent out to other networking device, finally the unwrapping (decapsulation) process on the received data would be enforced at the destination.

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

socket

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

80

**6. Адресът на кой възел влиза в аrp таблицата на хост, изпращащ дейтаграма в друга IP мрежа?**

if you try to arp-resolve an IP address from a different subnet, the resulting MAC address will be that of the router interface nearest you

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

User Datagram Protocol (UDP) is a protocol used for transport of data across an Internet Protocol (IP) based network.UDP does not perform handshaking as TCP does, or check for errors, or even to see if the transmitted data was received, so UDP is referred to as an unreliable, connectionless protocol. However, because UDP skips the handshaking and is focused on pure transmission, it has lower overhead and is thus faster than TCP. UDP will provide better throughput on a network where the physical and datalink layer protocols are reliable.

**8. 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).

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

Tracert

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

Arp, rarp, dns(?)

**11. Как обработват рутерите полето Destination IP adress?**

A router is considered a Layer 3 device because its primary forwarding decision is based on the information in the Layer 3 IP packet, specifically the destination IP address. This process is known as routing. When each router receives a packet, it searches its routing table to find the best match between the destination IP address of the packet and one of the network addresses in the routing table. Once a match is found, the packet is encapsulated in the Layer 2 data link frame for that outgoing interface. A router does not look into the actual data contents that the packet carries, but only at the layer 3 addresses to make a forwarding decision.

**12. 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

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

**14. 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.

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

?повече от 60 хил. съединения?

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

препращане на пакети м/у интерфейсите на 1 комп

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

В TCP протокола размерът на буфера за входни данни може да варира взависимост 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.

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

An internet datagram can be marked "don't fragment." Any internet datagram so marked is not to be internet fragmented under any circumstances. If internet datagram marked don't fragment cannot be delivered to its destination without fragmenting it, it is to be discarded instead.

ICMP message is sent, informaing the cause of the problem.

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

MSS + header <= MTU

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

**20. Ако даден отдалечен сървър е достъпен ,но ping-a не работи къде може да се крие проблема?**

?Филтрация на някои IP адреси например?

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

**22. 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.

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

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.

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

wtf zomfg

**25. Сравнете switch и bridge.От кой слой са?**

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

Full duplex?

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

Bgp?

**30. Какво е анализатор на мрежи(wireshark)?**

**31. Какви са характреристиките на маршрутните политики?**

Policy-based routing (PBR) is a technique used to make routing decisions based on policies set by the network administrator. When a router receives a packet it normally decides where to forward it based on the destination address in the packet, which is then used to look up an entry in a routing table. However, in some cases, there may be a need to forward the packet based on other criteria. For example, a network administrator might want to forward a packet based on the source address, not the destination address.

Policy-based routing may also be based on the size of the packet, the protocol of the payload, or other information available in a packet header or payload. This permits routing of packets originating from different sources to different networks even when the destinations are the same and can be useful when interconnecting several private networks.

**32. 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.

**34. Какви са предимствата като имаме default gw?**

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

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

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

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

switch

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

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

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

ifconfig

**41. 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.

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

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

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

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

RIP – next hop

OSPF -

**45. 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’.

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

**47. В какво се изразява принципната разлика в работата на ARP и RARP протоколите?**

АRP: IP =>MAC, RARP: MAC => IP

**48. 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.

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

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

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

Сървър

**52. Какви задачи решава IP протокола?**

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

*Това всъщност е командата ip, която обединява много от другите. За нея Гешев ни каза няколко думи на консултацията.*

iproute2 is a collection of utilities for controlling TCP and UDP IP networking and traffic control in Linux, in both IPv4 and IPv6 networks.

iproute2 is intended to replace an entire suite of standard Unix networking toolsthat were previously used for the tasks of configuring network interfaces, routing tables, and managing the ARP table. Tools replaced by iproute 2 are: ifconfige, route, arp, netstat и др.

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

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

Според мен да защото MSS на Етернет = 1460<1472

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

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

UDP

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

Според мен да. Виж въпрос 55.

**59. Какво е мултиплексиране?**

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

ICMP?

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

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

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

**64. IP tables за какво се ползва**

iptables - administration tool for IPv4 packet filtering and NAT

**65. Какви механизми използва RIP протокола за уведомяване за несъществуващ маршрут?**

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

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

Нещо с командата brctl...???

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

**69. Каква е задачата на маршрутния протокол?**

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

Destination address,Header checksum,TTL,DF

**71. Какво е quagga?**