1) Протоколен стек за RIP, OSPF, BGP

Отг: RIP, OSPF, BGP са протоколи за динамична маршрутизация.
RIP - ползва се в сравнително малки и рядко менящи си топологията мрежи. Има бавна скорост на сходимост, метриката която ползва е хопове. (би предпочел пътят по-близък по брой междинни рутери, не по скорост на връзката)
OSPF - Динамичен протокол за маршрутизация, ползван в рамките на АС (автономна система). Има бърза скорост на сходимост и знае цялостната топология на мрежата. Метриката му е комплексна, един от критериите е bandwidth (скоростта на връзката)
*АС(автономни системи) - област на единно администриране. Например СУ или по-големите Интернет доставчици.
BGP - Динамичен протокол за маршрутизация между автономни системи.
*Скорост на сходимост/конвергенция -> времето за което промяна в топологията бива разпространено до всички участници в схемата.

2) Йерархична маршрутизация при OSPF

Отг: Обявяването на маршрути чрез OSPF е реализирано в йерархия. Има една главна област и множество подобласти. Главната област се обозначава с номер 0, подобластите с номер по-голям от 0.

3) Изисквания към маршрутните алгоритми

Отг: Да реагират своевременно на отпадане на маршрутизатор или връзка между тях. (т.е. устройство или интерфейс(изгоряла мрежова карта/порт) или скъсан кабел поради копаене)
Да могат да откриват резервни (втори/трети..) път до крайната цел.
Да не са сложни за работа.

4) Каква информация съдържа маршрутната таблица на BGP
Отг: Съдържа информация коя мрежа зад кой next-hop се намира и списък с автономни системи през които трябва да премине, също така има поле за метрика, localpreference и weight.

5) Външна и вътрешна маршрутизация
Отг: За външна маршрутизация най-популярен е протоколът BGP. Ползва се за комуникация между АС (автономни системи)
За вътрешна маршрутизация най-популярен е протоколът OSPF. Ползва се в рамките на АС. Протоколът знае за цялостната топология на мрежата, благодарение на което може да намери оптимален маршрут, спрямо различни критерии, например широчина на лентата a.k.a bandwidth a.k.a скорост на връзката a.k.a пропускливост на комуникационния канал.

6) Какви полета съдържа MT(маршрутната таблица) на OSPF
Отг:
Мрежа, административна дистанция(110)+метрика(20), next-hop, интерфейс, таймер от кога знаем за мрежата от съответния интерфейс
Ред от ospf MT:
O>* 172.16.1.0/30 [110/20] via 10.10.10.2, eth0, 00:14:14
*Административна дистанция - всеки маршрутизиращ протокол има по подразбиране стойност на административна дистанция. Така ако сме научили за съществуването на дадена мрежа от протокола RIP и в същото време по протокола OSPF, ще се вземе пътя от протокола с по-добра административна дистанция (OSPF = 110, RIP = 120). Колкото по-малка е административната дистанция, толкова по-значима е. Директно вързаните мрежи към нас са с административна дистанция 0, статично конфигурираните са с АД 1.

7) Свойства на маршрутните алгоритми
Отг: Маршрутните алгоритми биват два вида неадаптивни и адаптивни. (неадаптивни === статични, администраторът ръчно попълва MT. Адаптивни === MT се попълва от динамичен протокол за маршрутизация)
Примерно свойство за адаптивните алгоритми е да определят оптимален маршрут до дадена мрежа.

8) Как се оценява маршрут при RIP, OSPF, BGP
Отг: RIP - спрямо брой междинни възли (hops)
OSPF - спрямо bandwidth-а от точка до точка.
BGP - избира пътя с най-висок weight и localpref и най-малко на брой автономни системи през които трябва да премине.

OSPF – динамичен протокол за маршрутизация.Той е протокол със следене на състоянието на връзката.Попада в протоколите за вътрешна маршрутизация.Приложим в големи корпоративно мрежи.Разпознава промени в мрежата.При отпадане примерно на възел за секунди се конвергира в нова топология без зацикляне.
TCP – Основен протокол на транспортния слой в TCP/IP модела.Той предоставя надеждно обслужване с установена връзка (connection oriented).Той внася допълнително закъснение заради спазване на реда за подаване на единиците с данни(сегментите) и функциите по надеждност.TCP се ползва от най-популярните интернет приложения: FTP, E-mail,WWW. Не е подходящ за доставяне на съобщения в реално време.Всеки TCP сегмент има 20 байта служебна информация.
UDP – Оснвен протокол на транспортния слой в TCP/IP модела.Той е по-опростен протокол с неустановена връзка(connectionless) и сесии не се установяват. Той е по-скоро транзакционен протокол тоест ако приложението има данни за предаване той ги предава.При изпращане на много дейтаграми те могат да поемат по различни пътища в мрежата и да пристигнат в различен ред.UDP не следи последователността на дейтаграмите при приемане като TCP. Подходящ за доставяне на съобщения в

реално време. UDP дейтаграмите са само 8 байта.
BGP –Основният протокол за маршрутизация в INTERNET. Поддържа таблица от IP мрежи(prefix), които определеят достижимостта на мрежите между автономните системи.Той е протокол с вектор на пътищата(path vector protocol) BGP не използва метрика на вътрешните протоколи,а взема решения за определяне на маршрути на база на пътя м/у ASs(автономни системи), мрежова политика и/или множество правила.
IP(Internet Protocol) – протокол за комуникация,стоящ в основата на Интернет.Задачата му е да извърши успешно предаване на пакети от източника до получателя,без значение дали те са в една и съща мрежа или не.IP се използва от транспортни протоколи като TCP и UDP
MTU (Maximum Transmission Unit) – В компютърните мрежи MTU в протокол на даден слой е размера(в байтове) на най-големия протоколен блок за данни(PDU),който може да понесе дадения слой.По-голям MTU означава по-голяма ефективност.
MSS –(Maximum Segment Size) е опция на TCP протокола,която определя най-голямото количество данни(в байтове) което компютър или комуникационно у-во може да получи в единичен,нефрагментиран сегмент.Всеки хост трябва да може да приема минимум 536 байта сегмент.
DHCP Dynamic Host Configuration Protocol е протокол който раздава динамично мрежови настройки като например раздаването на IP адресите.

<u>Команди:</u>
Ping- служи за проверка на мрежовата свързаност, тестване на връзката с другите компютри.Използва протокола ICMP. Визуализира се времето за изпращане и получаване на пакет.
ARP - използва се за визуализация и модификация на таблицата IP-към MAC адрес. ARP протоколът извършва съпоставяне м/у IP и MAC адреси.
IPCONFIG- предоставя информация за TCP/IP конфигурацията на всички мрежови карти, включени към
компютъра.(В LINUX е ifpconfig)
Netstat – показва информация за мрежовите сесии(активни връзки) на съответния компютър.Сесията е от
порта на един хост до порта на друг хост.За диагностика на IP,ICMP,TCP,UDP
Nbtstat - предоставя информация за имената на компютрите и групите известни на даден компютър
Tracert - проследява маршрута през мрежата до компютъра-местоназначение по даден IP адрес или име(Linux traceroute)
RARP (Reverse) превръща от MAC към IP
RTT(Round Trip Time) –времето на пакет да стигне от клиента до сървъра и обратно.Колкото е по-малка е стойността на RTT толкова мрежата е по-добра и по-бърза. На приложно ниво всеки процес се определя еднозначно от сокета (IP

адрес+номер на порт) ,а всяко съединение с двойка сокети.Анализатор на протоколи(функция)-Програма или устройство чиято цел е да разбере съдържанието на капсулираната от протокола информация.
Какво връща ARP заявката: Връща MAC адреса. Кои протоколи на TCP/IP реализират адресно преобразуване.: ROUTE С командата Route са възможни следните операции:да се добавят нови маршрути,да се трие запис на шлюз,да се изведе списък на съществуващи маршрути. Дейтаграмните протоколи са UDP и IP.За тях е характерно че не установяват съединение(connectionless)

Анализатор на протоколи(функция)-Програма или устройство чиято цел е да разбере съдържанието на капсулираната от протокола информация.

1.Характеризирайте IP адрес 10.0.0.0
Това е IP адрес от клас А за частни мрежи с маска 255.0.0.0 по подразбиране.

2.**Каква е основната разлика м/у RIP1 и RIP2?**
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.

3.**ICMP-подлежи ли на маршрутизация? Защо?**
Да. ICMP тества свързаността на хоста и има пълен IP хедър с адрес на дестинация, който не е задължително да бъде локален.

4.**Защо TCP 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 ACK-нати, 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.

6.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.

7.**Коя е командата,за да ти изведе списък за отворени съединения**?(нещо такова...)
netstat

8.Даден е някакъв IP address **да се определи маска,мрежа,подмрежа.**
Знаем как става от предните отговори на теста10.Коя е подразбиращата се маска и какъв е броя на хостовете за клас C?
Поддържа 254 хоста за всяка от 2 милиона мрежи. 255.255.255.0 маска

12.**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.

13.**Кой е метода за приемане и изпращане на данни едновременно?**
Full duplex

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

1.За какво се използва **функцията forwarding**?
Forwarding е предаването на пакети от един мрежов сегмент към друг посредством възли
в компютърна мрежа. Има няколко forwarding модела: uncasting, broadcasting и multicasting.

2.Какво е значението на **протокола с хлъзгащия се прозорец**?
Те са по-ефективни от протокола спри и чакай, тъй като позволяват изпращане на повече от един кадър, преди да се чака за потвърждение. При тези протоколи всеки кадър се номерира с число от 0 до някакъв максимум, обикновено от вида 2^n - 1, така че номерът да се вмества точно в n бита.

3.**Каква е целата на AS**?
още едно ниво на маршрутизация, необходими са при връзката м/у различни ас

4. Смятане на **broadcast адреси, адреси на мрежи и как да сметнем адреса на 5-я хост**
на нашата мрежа?

Да предположим, че имаме IP address 101.35.15.10 със subnet mask 255.248.0.0.
За адреса на мрежата.
Следователно, представяме ги в двоична бройна система:
101.35.15.10 = 1100101 00100011 00001111 00001010 (binary)
255.248.0.0 = 11111111 11111000 00000000 00000000 (binary)

101.32.0.0 = 1100101 00100000 00000000 00000000 (binary)
Прилагаме побитово “и” на тези репрезентации и получаваме 101.32.0.0.
Смятане на broadcast address.
При смятането на broadcast address е същото, но слагаме празните битове на маската като 1
в резултата.
101.35.15.10
= 1100101 00100011 00001111 00001010 (binary)
255.248.0.0
= 11111111 11111000 00000000 00000000 (binary)

101.39.255.255 = 1100101 00100111 11111111 11111111 (binary)
Да сметнем стойността на 5-тия хост от мрежата.
Мрежовият адрес е първото не използващо се ip получаваме:
1100101 00100000 00000000 00000000 (Net addr)
1100101 00100000 00000000 00000001 (1st Host)1100101 00100000 00000000 00000010 (2nd host)
1100101 00100000 00000000 00000011 (3rd host)
1100101 00100000 00000000 00000100 (4th host)
1100101 00100000 00000000 00000101 (5th host)
...
1100101 00100111 11111111 11111111 (bcast)
Така когато превърнем 5-тия хост в десетична бройна система получаваме: 101.32.0.5

5.Каква е **ролята на ICMP** протокола?
ICMP Internet Control Message Protocol е протокол от ниво три (Network layer) и се използва в мрежите главно за откриване на грешки по мрежата и изпращане на съобщения за това. В него влиза командата ping.

Протоколът 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.

6.**Ip адреса за broadcast предаване за подмрежа** 1.2.0.0/29 е?
00000001 00000010 00000000 00000000 = 1.2.0.0/29
тоест първите 29 бита от това представяне са сетнати и правим останалите нули в 1-ци
00000001 00000010 00000000 00000111 = 1.2.0.7

7.Kakwa trqbwa da e **maskata** за мрежа 172.16.0.0 така,че да имаме 400 хоста?
172.16.0.0 = 10101100 00010000 00000000 00000000 (binary)
mask = 11111111 11111111 11111110 00000000
172.16.1.255 = 10101100 00010000 00000001 11111111
400th host
Следователно:
mask = 255.255.254.0

8.Имаш два и**нтерфейса на рутер,**двата са свързани към **различни подмрежи** и **използват различни протоколи** едната мрежа е Token Ring ,другата е Ethernet.**Ще може ли да си пращат пакети двете едни на други**?
Да, рутерът ще осигури комуникацията.

9.**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).

10. **Ако имаме един рутер свързващ 2-ве мрежи с ралична маршрутизация ще може ли да си комуникира**?
Да.11.Защо mss=1460 при Ethernet протокола? Големината на предаваните пакети е 4500 байта за FDDI и 1500 (максимум MTU) за Етернет. При изпращането на SYN сегмент от TCP максималната стойност на MSS е ограничен от стойността на MTU минус фиксирания размер на заглавните части на TCP и IP. За стандарта Етернет това означава, че максимална стойност на MSS е до 1460 байта

12.**Ако даден отдалечен сървър е достъпен ,но ping-a не работи къде може да се крие проблема**?
ICMP дава ping, ако е disabled ще има достъп, но не и ping.

14.Какви операции може да се извършат с **route върху маршрутната таблица**?
Показване на маршрутизиращата таблица route
Премахване на маршрут
route [-v] [-A family] del [-net|-host] target [gw Gw] [netmask Nm] [metric N] [[dev] If]
Прибавяне на статичен маршрут
route [-v] [-A family] add [-net|-host] target [netmask Nm] [gw Gw] [metric N] [mss M] [window

W] [irtt I] [reject] [mod] [dyn] [reinstate] [[dev] If]
Примерно:
Прибавяне на default gateway
route add default gw 10.0.0.1
ще изчезне след рестарт.
route add -net 192.168.100.0 netmask 255.255.255.0 eth0
Това ще насочи всичкия трафик към подмрежата към eth0 интерфайса
И да прибавим статичен път който не преминава през default gw
route add -net 10.8.100.0 netmask 255.255.255.0 gw 10.0.16.140

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 записа 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).