NAT - Използва се при IPv4 за замаскирване на група от IP адреси с един общ IP адрес. Например ако имаме мрежа от компютри с различни IP адреси свързани със switch до рутер, който е конфигуриран с NAT и има някакво IP, то IP-тата на всички компютри от тази мрежа ще са невидими извън нея и ще имат едно общо IP - това на рутера. По този начин се нарушава прозрачността от край до край и не може да се разбере, кой от всички компютри в мрежата седи зад IP-то на рутера в даден момент.
NATv6 - Използва се за транслирането на IPv6 в IPv4 адреси. Подобно е на NAT, но има за цел да осъществи успешна комуникация между отделни участници в мрежата, когато имаме рутер с IPv6 адрес, а е необходимо изпращане до IPv4 адрес. Тогава IPv6 адреса се замаскирва с IPv4 адрес от NAT64.

IPv4 vs IPv6 разлики:

- контролна сума (checksum)

При IPv4 има checksum поле в пакета, а при версия IPv6 това поле липсва и задачата на контролната сума се оставя на горния слой (Network layer).

- адрес на протокола

При IPv4 адресът е 32 битово число, разделено на 4 октета с разделител “.” и за простота се записва в 10-тична бройна система. При IPv6 адресът е 128 битово число. За простота се записва в 16-тична бройна система и се записва в 8 хекстета с разделител “:”. Също има опция за съкращаване на ненужните нули (:: и изпускане на водещите 0-ли)

- брой на ретранслационните възли

Ретранслационните възли са броя hop-ове който може да направи един пакет. При IPv4 за това отговаря TTL (Time to Life) полето, а в IPv6 то се нарича hop limit поле. И двете полета са 8 битови и по default са сетнати на 64, но може да се променят от 0 до 255 hop-а.

- фрагментиране на IP модула

При IPv4, ако имаме пакет от 1GB то той ще трябва да се раздели на по- малки части, за да може да се изпрати по мрежата. Първоначално се разделя на фрагменти от по 1500 байта, защото това е максимум MTU за Ethernet. Но ако по мрежата имаме switch, който може да работи с пакети от максимум 1000 байта, то при стигане до него ще се discard- не пакета и ще се върне съобщение до изпращача, че е необходимо да се фрагментира на по-малки фрагменти. Докато при IPv6 предварително се намира минималния размер за пакетите и се фрагментира с този размер. Така се избягват ненужните фрагментации

DHCP - Dynamic Host Configuration Protocol е протокол който раздава динамично мрежови настройки като например раздаването на IP адресите.

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.

Ethernet protocol - протокол на втория слой от OSI модела (Data-link layer). Това е протокола на локалната мрежа.

MAC - Физически адрес, служи за разпознаване на устройствата в рамките на локална мрежа. MAC адресът представлява 48 битово число, което се записва в 16-тичен формат. Пр. 00:1D:1F:37:33:AA. Състои се от 6 двойки от по 8 бита. Първата половина от MAC адреса е за информация за производителя (vendor), а втората половина е потребителската.

Broadcast MAC адрес - FF:FF:FF:FF:FF:FF

ARP - Address Resolution Protocol отговаря за преобразуването на MAC в IP адрес и запазва временно резултата в MAC таблицата

RARP - Reverse ARP преобразува от IP в MAC адрес

CSMA/CD - протокол за комуникация между хостове едновременно, като при колизия, тя се засича и се разбира единия пакет да се пренесе след произволно време. CD е Colision Detection когато канал се използва едновременно за 2 или повече хоста

Какво е OSPF – OSPF е динамичен протокол за маршрутизация.Той е протокол със следене на 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.

Какво е 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.

Какво е 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.

Какво е 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, мрежова политика и/или множество правила.

Какво е 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.

Разлика RIPv1(broadcast) и RIPv2(multicast) – RIPv1 не поддържа subnet маски.

Команди:

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)