Изпитна тема № 10: **Компютърни мрежи**

Структура на компютърна мрежа. Мрежов хардуер и софтуер. Използване на периферни устройс-тва. Мрежова преносна среда. Категории мрежи според физическия обхват, метод на администст-риране, използвана операционна система, топология, архитектура. Създаване и конфигуриране на мрежа. Инструменти за диагностика на мрежата. Мрежови модели и протоколи. Модели OSI и TCP/IP. Протоколи: TCP/IP, IPv6, приложни протоколи. Мрежова сигурност на компютърните мрежи и защита от атаки. Настройка на защитната стена. Криптиране на безжична мрежа. Дефи-ниране права на достъп до ресурсите на мрежата.

Дидактически материали: *Компютър с подходящ софтуер, задачи и казуси.*

Критерии за оценяване на изпитна тема № 8	**Максимален брой точки**
Дефинира понятията: компютърна мрежа, мрежов хардуер и софтуер. Изброява, обяснява и посочва компоненти на компютърна мрежа.	10
Дава пример за структура на компютърна мрежа.	4
Обяснява категориите компютърни мрежи.	4
Разработва и модифицира модел на компютърна мрежа, като определя размера, структурата и организацията на мрежата според изискванията в поставена задача. Демонстрира знания за свързване и конфигуриране на мрежа.	18
Различава оптичната от безжичната мрежа и прави заключения за предимствата и недостатъците им.	12
Диференцира и представя графично мрежовите модели.	16
Обяснява и прави заключения и изводи за мрежовите протоколи.	12
Доказва необходимостта от използването на инструменти за диагностика на мрежата.	6
При поставена задача прави изводи за хардуерните и софтуерните заплахи на компютърната мрежа и избира подходящ метод за защита с цел осъществяване на максимална мрежова сигурност.	8
Обяснява криптирането на безжичната мрежа. Демонстрира знания за видовете нива на достъп до ресурсите на мрежа.	10
	Общ брой точки: 100

1. Дефинира понятията: компютърна мрежа, мрежов хардуер и софтуер. Изброява, обяснява и посочва компоненти на компютърна мрежа. 10т.

компютърна мрежа - два или повече компютъра и други устройства свързани помежду си с цел използване на общи ресурси и комуникация помежду им. Компютърните мрежи се организират за да се създаде възможност за :

- обмен на данни между потребителите на различни компютри;
- съвместно ползване на общи ресурси/апаратни, софтуерни и информационни;
- разпределена обработка на данни, т. е. обработка чрез различни компютри на данни, части от които се съхраняват в паметта на различни компютри;

мрежов хардуер и софтуер :

- ***Мрежова преносна среда*** - осигурява предаване на сигналите между компютрите и останалите устройства включени в компютърната мрежа. Основният начин за връзка е с помощта на кабел (коаксиален или с усукани двойки-UTP, FTP, STP, SFTP, Fiber optical). Съществуват и други технологии за пренос на информация – безжични връзки.

- ***мрежовата интерфейсна карта – NIC (Network Interface Card)***- основен компонент, необходим за включването на един компютър в мрежа. Нарича се още мрежова адаптерна карта. Тя преобразуване на паралелния сигнал от компютъра в серийна (последователна) форма, която се изпраща по мрежовия кабел. Цифровият сигнал се преобразува в електрически импулси, светлинни импулси или радиовълни, в зависимост от преносната среда, която се използва. При получаване на сигнал от мрежата се извършва обратното преобразуване в цифров сигнал. Всяка мрежова карта има уникален адрес наречен MAC (Media Access Control) адрес. Този адрес се записва от производителя в чипа на мрежовата карта. MAC адресът се използва при изпращане на информация от един компютър към друг. По този адрес останалите устройства от мрежата различават данните от коя мрежова карта са изпратени и за коя са предназначени. MAC адресът представлява 48 битово число, което се представя като 6 шестнадесетични числа разделени с тирета – например 00-aa-00-62-c6-09.
- ***Пасивни мрежови устройства -*** осигуряват точката на свързване без да модифицират или усилват сигнала. Това са: свързващи букси (jack couplers), розетки (wall plates), свързващи панели (patch panels), пасивни хъбове (passive hub).
- ***Активни мрежови устройства -*** могат да усилват сигнала преди да го предадат нататък по мрежата и дори да го преобразуват от един тип преносна среда към друг. Това са : конвертори на преносната среда, повторители и активни хъбове.
- ***Устройства за разделяне на сегменти и подмрежи – това са***

Мостове (bridge) - устройство, което свързва два сегмента от една локална мрежа. Основната му задача е да филтрира трафика между двата сегмента, с цел да се намали претоварването при една по-голяма локална мрежа. Те могат да бъдат самостоятелни устройства или да се реализират като хардуер и софтуер в един компютър. След разделяне на голямата мрежа на две по-малки, трафиците на сегментите ще бъдат изолирани и няма да си влияят взаимно. Мостовете работят с физически **MAC адреси.**

Комутатори (switch) - устройство за свързване на компютри в мрежа с топология „звезда”. Той увеличава скоростта на мрежата и е сравнително евтино устройство. Суича е е многопортов мост и работи по следния начин: При получаване на един пакет на даден порт,

той прави проверка за това дали пакетът е коректно получен, след което проверява в собствената си таблица дали има направен запис за MAC-адреса на получателя. Възможните варианти са два:

Няма запис на MAC адреса. В този случай суича изпраща пакета към всичките си портове, след което получава отговор от устройството за което е предназначен пакета, записва в таблицата си на кой изходен порт отговаря този MAC-адрес. Всички следващи пакети с този адрес се препращат директно на съответния порт.
Съществува запис на MAC адреса. Суича препраща пакета директно към съответния порт.

Маршрутизатор(router, рутер) - устройство, което служи за управление на разпределянето на трафика (пакетите) информация между различни мрежи или различни сегменти от дадена мрежа. Той работи с логически **IP адреси**.

Маршрутизаторите са интелигентни устройства – те могат да избират най-добрия маршрут до даден адрес измежду множество възможни пътища. За определяне на пътя за предаване на данните и насочване на пакетите маршрутизаторът използва **таблица за маршрутизация**, в която се съхраняват IP адресите на други маршрутизатори. Тази таблица маршрутизаторът си създава сам, като си набавя информация, а при някаква промяна сам я актуализира, „разпитвайки“ другите маршрутизатори кой докъде е свързан.

Рутерите се използват в следните случаи:

- при свързване на една локална мрежа към Интернет (с реални IP адреси);
- при свързване на две или повече локални мрежи;
- за разделяне на една локална мрежа на две или повече подмрежи.

Използването на маршрутизатор като устройство за свързване ще доведе до намаляване на трафика между отделните мрежи и подобряване на сигурността в локалната мрежа.

- Физическото свързване на компютрите в мрежата не означава, те ще могат да работят заедно. Затова е необходима подходяща ***мрежова операционна система***, която да осигурява взаимодействието между различните устройства и програмни системи. Най популярните съсвърни ОС са : Windows Server (операционни системи за сървъри, базирани на Windows NT, 2003 2008 R2 2012 и по-нови – Windows Сървър 2022,Windows Сървър версия 20H2 и Windows 10, версия 20H2, Windows Сървър версия 2004 и Windows 10, версия 2004, Windows Сървър версия 1809, Windows 10 версия 1809 и Windows Server 2019, Windows Server 2016). CentOS, Debian, Red Hat Enterprise Linux, Ubuntu Server, Gentoo, Fedora.
-

2. Дава пример за структура на компютърна мрежа. 4т.

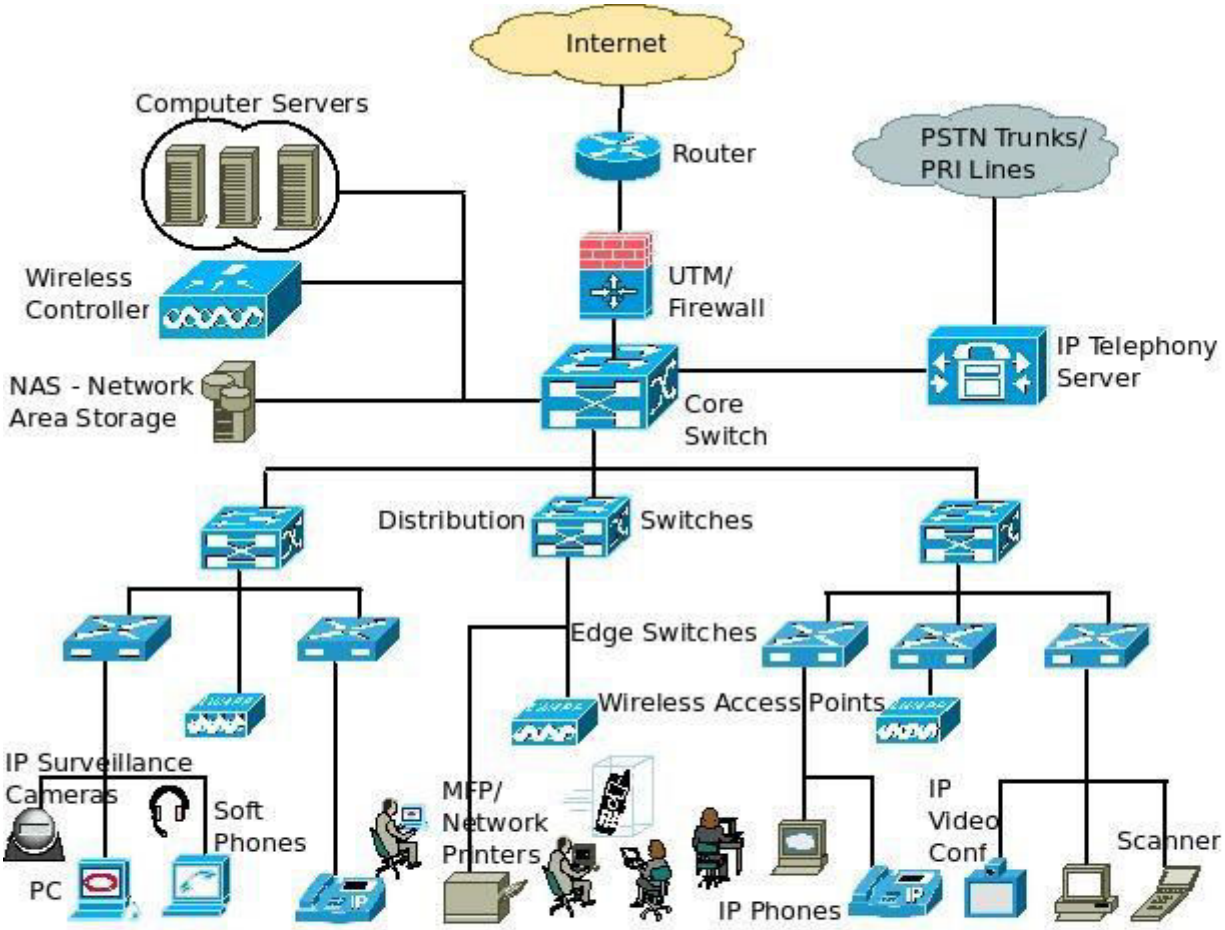
Мрежата е технология, позволяваща на независими устройства с възможност за комуникация да се свързват помежду си или да използват общи ресурси. Измислен е йерархиченя дизайн на компютърните мрежи, който разделя всички компютърни мрежи в 3 нива и всяко ниво има своите отговорности.

1. Ниво на достъп [access layer]
Това е най-ниското ниво и работи със самите компютри, като ги обединява в локална мрежа. То отговаря за достъпа на хостове в локална мрежа. Устройствата, който работят на това ниво са хъб и суич.

(опишете всички възможни крайни устройства от схемата)

2. Дистрибуционно ниво[distribution layer]
То управлява и свързва няколко нива на достъп.Устройството, което работи на това ниво е рутер. Той работи с IP адреси

3. Основно ниво [core layer]
То управлява и свързва няколко дистрибуционни нива. Отговаря за високо-скоростна връзка между устройствата от дистрибуционно ниво. Устройствата, който работят на това ниво са мощни рутери и умни суичове. Рутерите от това ниво поддържат трафик с много висока скорост.



Structure of Network

3. Обяснява категориите компютърни мрежи.

а) според физическия обхват
Физическият обхват включва географската област, която се заема от мрежата. Според физическия обхват съществуват следните категории мрежи:

- Локална мрежа (LAN) - компютрите обикновено са разположени на близки разстояния. Те могат да бъдат в една стая, съседни стаи на един етаж, на няколко етажа или дори в съседни сгради. Броят на компютрите включени в мрежата може да варира значително. Може да съществува локална мрежа от два компютъра, десетки или дори стотици компютри.

- Градска мрежа (MAN- Metropolitan Area Network) – състои се от няколко локални мрежи свързани помежду си в границите на един град. Градските мрежи се реализират много по-рядко. Повечето мрежи са в рамките на сграда

или съседни сгради – съответно те се класифицират като LAN или обхващат по-големи територии – няколко града, различни държави – тогава ги класифицираме като WAN. Максималното разстояние, което покрива една градска мрежа е до 80 км;

- Глобална мрежа (WAN-Wide Area Network) - обхваща голяма географска област. Компютрите включени в мрежата могат да бъдат в различни градове или различни държави. Най-голямата глобална мрежа е ***Интернет (Internet – Inter**national **Net**work)*. Глобалната мрежа може да бъде и частна собственост. Глобалната мрежа най-често се състои от множество свързани помежду си локални мрежи. За връзка между тях обикновено се използват обществени среди за пренос на информация, например обществената телефонна система.Частните глобални мрежи се изграждат с технологии – хардуерни и софтуерни – предназначени и използвани в глобалната мрежа Интернет. Затова те се наричат ***интранет***-мрежи. *Интранет мрежите използват за преносна среда собствени кабелни или безжични трасета на връзка или наемат такива от телекомуникационна компания*. Значително по-евтино е при изграждането на частна мрежа да се използва *Интернет като преносна среда*. Прилагат се VPN (Virtual Private Networks) технологии, които гарантират висока сигурност и изолират частната мрежа от публичната чрез криптиране на обменяните данни. Такива мрежи е прието да се наричат ***екстранет***.

б) **според метода на администриране**

Биват два вида – равноправни и клиент-сървър

- Равноправна мрежа - всички компютри са равнопоставени. Всеки компютър работи и като клиент и като сървър. Няма администратор за цялата мрежа. Потребителите сами администрират собствения си компютър. Обикновено при равноправната мрежа компютрите не са повече от 10. Равноправната мрежа е сравнително проста. Тя няма нужда от мощен централен сървър и допълнителни компоненти, затова е сравнително евтина. При равноправната мрежа не е необходимо мрежовият софтуер да има висока производителност и ниво на защита. При нея потребителите са администратори на своите компютри и планират собствената си система за сигурност. Подходяща е за случаите, когато потребителите се намират на едно и също място, не е задължителна защита на мрежата и няма да се разраства в близко бъдеще. При равноправната мрежа всеки компютър работи и като клиент и като сървър, затова потребителите трябва да бъдат квалифицирани, за да могат да работят и като администратори и като обикновени потребители.

- Мрежа клиент-сървър - в този тип мрежа има един главен компютър, наричан сървър, който обслужва мрежата. Той съхранява информация и ресурси и ги прави достъпни за останалите компютри в мрежата. Останалите компютри, включени в мрежата, са клиенти. Инсталирането на сървър позволява да се премине към централизирано управление на всички компютри в мрежата. Той позволява на останалите потребители да влизат в мрежата чрез уникално име на потребител и парола. Този вид мрежа е по-добрият вариант, когато компютрите са повече от десет. Администрирането на клиент-сървър мрежите е по-опростено особено за мрежи с голям брой компютри и споделени ресурси. Споделените файлове се съхраняват на сървъра, така че да могат лесно да бъдат архивирани и намирани. Управлението на този вид мрежи се осъществява от системен администратор – специално обучен човек, който упражнява контрол върху всички мрежови операции и ресурси. Сигурността на

системата е значително по-добра от тази при равноправните мрежи. За да влезе в мрежата всеки потребител трябва да има потребителско име и парола, създадени на сървъра. Мрежовият администратор може да даде различни права за достъп до даден ресурс на различните потребители. По-добрият вариант е отделните потребители да се обединят в групи и да се назначат права за отделните групи от потребители.

в) **според използваната ОС**

- **Операционни системи на Windows**

Започвайки с Windows NT 3.51 Server Следващите версии са 4.0, 2000, 2003 и 2008 , 2012 Server.

Сървърната ОС предлага следните роли:

Терминален сървър – Terminal Services - позволява отдалечените компютри да имат достъп до „екрана" на сървъра. Работейки отдалечено, потребителите могат да стартират програми, да използват локалните и мрежовите ресурси по същия начин, както ако работят локално на сървъра.

Файлов сървър – File Server - осигурява достъп до локалните файлове на сървъра от мрежовите потребители

Принт сървър – Print Server - възможност за включване към мрежов принтер през web интерфейса.

Сървър за приложения - Application Server (IIS, ASP.NET) - служи за поддържане на web технологията за създаване на динамични страници ASP.NET. При избор на тази роля се инсталира web сървъра IIS 6.0 и технологиите COM+ и ASP.NET. При сървъра за приложения се включват всички функции и услуги, използвани при разработване и настройване на web приложения на базата на XML. Операционната система не допуска претоварване, задава се време през което процесите на приложенията да се рестартират, което освобождава всички ресурси, заети от приложенията. Вградените мерки за безопасност на приложенията повишават надеждността и съкращават времето за администриране.

Сървър за електронна поща - Mail Server - обслужва пощенските кутии на множество клиенти. Инсталират се компонентите за работа с протоколите POP3 (Post Office Protocol) и SMTP (Simple Mail Transfer Protocol).

Сървър за отдалечен достъп (RAS) и VPN сървър - Позволява отдалечен достъп до ресурсите на локалната мрежа чрез комутируема връзка или VPN съединение.

Мултимедиен сървър – Streaming Media - може да се управляват поточните аудио и видеопредавания, тяхното архивиране и отдалечен достъп чрез интранет или Интернет.

DNS сървър - позволява на клиентските компютри да регистрират DNS имена (които се запомнят и използват по-лесно) и да ги използват вместо IP адреси.

DHCP сървър - позволява централизирано управление на IP адресите и свързаната с тях информация за конфигуриране на DNS, WINS и други услуги.

- UNIX/Linux мрежи

включват пълен набор протоколи и услуги за обезпечаване на интернет инфраструктурата:

- протоколите DHCP (BOOTP) и DNS;
- файлов достъп: FTP;
- web съдържание: HTTP;
- изпращане на електронна поща (MTA – Mail Transfer Agent): SMTP;
- получаване на електронна поща (MDA – Mail Delivery Agent): POP3, IMAP4;
- споделяне на файлове и принтери: NFS и др.

Linux е безплатна операционна система, подобна на UNIX, използвана както за сървъри, така и за персонални компютри. Всички популярни версии включват интернет протоколи и услуги, както и Apache Web сървър, PHP, Perl, MySQL, Java.

4. Разработва и модифицира модел на компютърна мрежа, като определя размера, структурата и организацията на мрежата според изискванията в поставена задача. Демонстрира знания за свързване и конфигуриране на мрежа. 18т.

Да се проектира локална компютърна мрежа с 15 компютъра, предназначена за учебна зала. Всеки компютър трябва да има достъп до Internet. Каква мрежа ще изградите (изберете топология, архитектура, преносна среда) ? Да се начертае мрежата и се направи разпределение на IP адресите на всички устройства.

5. Различава оптичната от безжичната мрежа и прави заключения за предимствата и недостатъците им. 12т.

Оптичен кабел

Оптичният кабел (fiber-optic) се различава от останалите форми на мрежово окабеляване, защото предава импулси от светлина, а не електрически импулси. Той се състои от едно или повече стъклени или пластмасови влакна, които предават светлината. Всяко влакно е оградено от защитен метален слой, обвит в слой пластмаса, наречен буфер. Най-отвън има твърда пластмасова обвивка.

Оптичният кабел може да работи в един от следните два режима:

- **Единичен режим (Single mode)** – светлината пътува по оста на кабела. По-бърз режим, използва се предимно в WAN мрежите за разстояния до 70 км.

- **Множествен режим (Multi mode)** – светлинните вълни навлизат в стъкления канал под различни ъгли като непрекъснато се отразяват и отскачат от стените на стъклената тръба. По-бавен от единичния поради дисперсията на светлината. Използва се в LAN мрежите за разстояния до 2000 м.

Безжична преносна среда

Предимства:

- отпада необходимостта от окабеляване;
- компютрите не се обвързват с конкретно работно място;
- лесно се включва нов компютър към мрежата.

При изграждане на безжична компютърна мрежа важен момент, на който трябва да се обърне особено внимание е сигурността на данните.

При безжичните комуникации има три основни метода за предаване на информация:

- чрез лазер;
- с инфрачервени лъчи;
- с помощта на радиовълни.

Лазер (Laser)

Сигналът при лазерните мрежи представлява импулси от лазерна светлина. Самата технология изисква пряка видимост между две устройства за осъществяване на комуникация. Това е и основният недостатък на лазерните безжични комуникации.

Инфрачервени лъчи (Infrared – IrDA)

Сигналът за пренос на информация представлява съвкупност от лъчи в инфрачервения спектър. За изграждане на компютърна мрежа се използват устройства по спецификациите IrDA (Infrared Data Association). Разстоянията между излъчвателя и приемника са от 5cm до 60cm. IrDA е технология с най-малък обсег.

Радиовълни

WLAN (безжична локална мрежа) – използват се широко разпространените Wi-Fi технологии. Това е мрежа от компютри на разстояния от няколкостотин метра, която използва радиочестотни сигнали с висока честота за предаване и получаване на данни Стандарта се основава на групата стандарти IEEE 802.11. Недостатък за тези устройства е необходимост от пряка видимост между устройствата, висока степен на поглъщане от сгради и предмети.

Протокол	**Година**	**Честота**	**Скорост на трансфер (средна)**	**Скорост на трансфер (максимална)**	**Обхват (в сграда)**	**Обхват (на открито)**
Базов	1997	2.4 GHz	0.9 Mbit/s	2 Mbit/s	20 m	100 m
802.11a	1999	5.15-5.35 GHz 5.47-5.725 GHz 5.725-5.875 GHz	25 Mbit/s	54 Mbit/s	35 m	120 m
802.11b	1999	2.4-2.5 GHz	6.5 Mbit/s	11 Mbit/s	38 m	140 m
802.11g	2003	2.4-2.5 GHz	25 Mbit/s	54 Mbit/s	38 m	140 m
802.11n	2007	2.4 или 5 GHz	200 Mbit/s	540 Mbit/s	70 m	250 m

Стандарти 802.11

WWAN (Безжични глобални мрежи) използват 2G и 3G технологиите, изграждащи на мрежи от клетъчни телефони (wide area cellular telephone networks). Такива са GSM (9600bps), GPRS (2G) – 56 и 114 kbps, UTMS (3G) downlink до 384 kbps и uplink до 64 kbps, CDMA2000 (3G) – до 1.8 Mbps, HSDPA (3.5G) – 1.8, 3.6, 7.2 и 14.4 Mbps. Днес се използват стандартите на 4G и 5G мрежите

6. Диференцира и представя графично мрежовите модели. 16т.

Обикновено когато искаме де опишем нещо абстрактно използваме понятието модел. Целта на мрежовите модели е да ни помогнат при изучаването и разбирането на мрежовите комуникации. Мрежовите модели са в основата на стандартизацията на мрежовото оборудване.

Моделът OSI (Open System Interconnect) е абстрактен модел, който описва начина на комуникация в компютърните мрежи. Той е стандарт, който производителите на мрежово оборудване използват при проектиране на хардуер, операционни системи и протоколи.

Той включва 7 слоя, всеки от които е една стъпка в процеса на комуникация.

Application	Приложен слой	слой 7
Presentation	Представителен слой	слой 6
Session	Сесиен слой	слой 5
Transport	Транспортен слой	слой 4
Network	Мрежови слой	слой 3
DataLink	Канален слой	слой 2
Physical	Физически слой	слой 1

Приложен слой - служи като посредник между софтуерните приложения и мрежовите услуги. В този слой работят протоколите HTTP, FTP, Telnet, SMTP, POP3, IMAP4, SNMP. Задачата на слоя е да управлява общия мрежов достъп, контрола на потоците от данни и поправката на грешки.

Представителен слой - определя използвания формат за обмен на данните. Тук получените от приложния слой данни се представят във вид на пакети („универсален" формат за пренос). Този слой отговаря за преобразуването на данните:

· компресиране – намаляване на техния размер;

· криптиране – кодиране с цел защита от неоторизиран достъп;

· транслация на протоколи – с цел пренасяне между различни хардуерни платформи и операционни системи.

Сесиен слой - отговаря за изграждане на канал за връзка – сесия – между два компютъра в мрежата.

Транспортен слой - отговаря за транспортирането на пакетите с данни без грешки, в точна последователност и без загуби. Транспортните протоколи TCP, UDP от TCP/IP и услугата за преобразуване на имена – Domain Name System (DNS) работят в този слой.

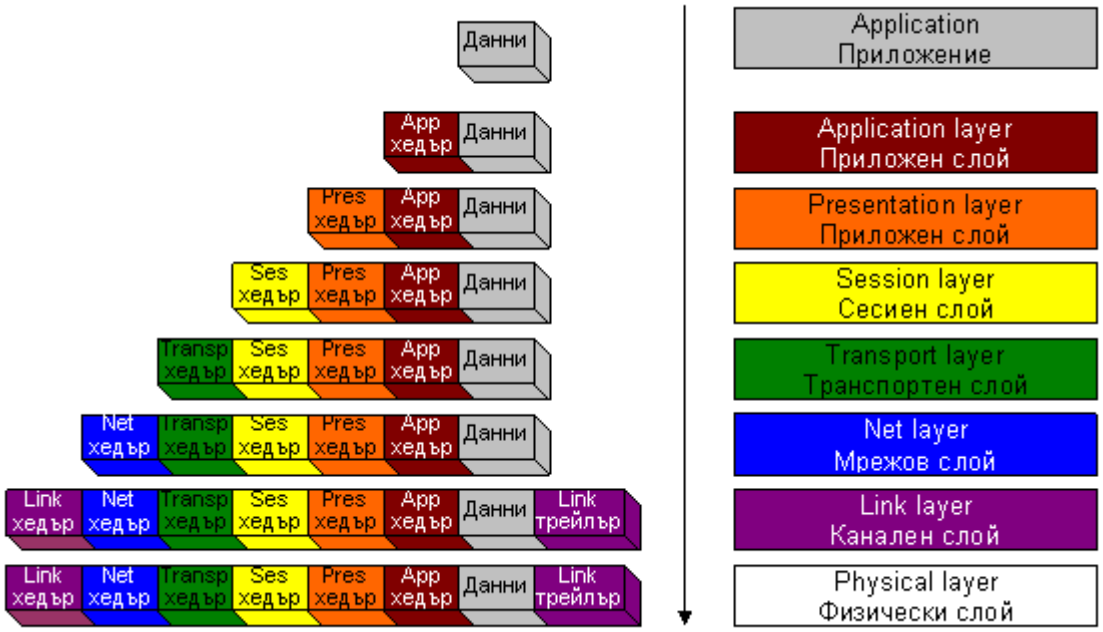
Мрежови слой - отговаря за адресирането на съобщенията и за определянето на маршрут, по който да преминат данните от компютъра – източник до компютъра – получател.
Протоколът IP от TCP/IP работи в този слой. Тук работят маршрутизаторите.

Канален слой - изпраща кадрите с данни от мрежовия слой към физическия слой. Той включва два подслоя:

Контрол за достъп до преносната среда – Media Access Control (MAC) - разпределя достъпа на компютрите до физическата преносна среда. Той дефинира MAC адресите.

Контрол на логическите връзки – Logical Link Control (LLC). Дефинира логическата топология.

В каналния слой работят устройствата мост и суич.



Път на данните в OSI модела

Физически слой - предава потока от битове (единици и нули) от мрежовата карта към преносната среда. Битовете са кодирани като електрически или светлинни импулси (при безжичните системи са електромагнитни вълни). Този слой определя типа на връзката между мрежовата карта и кабела, както и техниката на предаване на информацията по мрежата.

Устройствата, които работят на това ниво са мрежови карти, повторители, хъбове, медиа конвертори.

Моделът DoD

Този модел е разработен съвместно с TCP/IP – част от проекта ARPAnet. Протоколите на TCP/IP са проектирани в този модел. Затова и този модел е известен с наименованието TCP/IP модел.

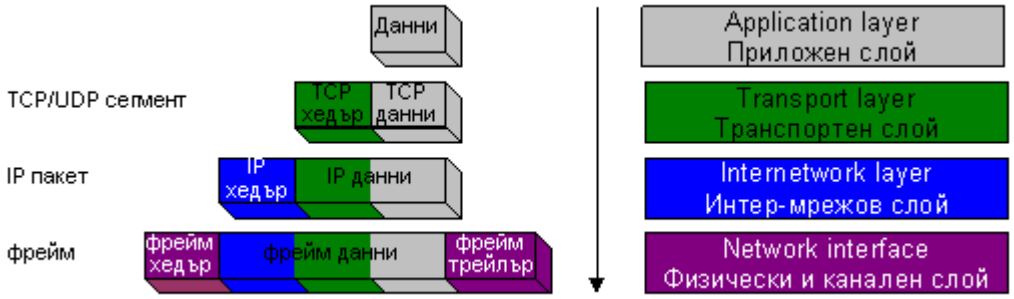
Състои се от четири слоя:

Слой 4. Приложен (application layer) – най-горният слой от модела. Обхваща функциите на трите най-горни слоя на OSI модела;

Слой 3. Транспортен (хост до хост) (host to host (transport) layer) – съответства на транспортния слой на OSI модела. Тук работят TCP, UDP, DNS;

Слой 2. Слой интер-мрежа (internetworking layer) – съответства на мрежовия слой на OSI. Занимава се с маршрутизацията основана на логическите IP адреси.
Протоколът Address Resolution Protocol (ARP) преобразува логическите IP адреси в MAC адреси;

Слой 1. Мрежов интерфейс (network interface layer) – съответства на двата слоя – канален и физически на модела OSI. Тук работят Ethernet и Token Ring протоколите. В този слой се използват само MAC адреси.



Път на данните в TCP/IP модела

7. Обяснява и прави заключения и изводи за мрежовите протоколи. – 12т.

Мрежовият протокол е съвкупност от правила, чрез които компютрите и останалите устройства в мрежата комуникират помежду си.
Съществуват:

- немаршрутизируеми протоколи – за предаване на данни в една локална мрежа;
- маршрутизируеми протоколи – използват се за предаване на данните от една локална мрежа към друга по един от няколко възможни пътя (маршрута).

Протоколите се разделят на следните три групи:

- Приложни – осигуряват обмена на данни и взаимодействието приложение- приложение (SMTP, FTP, Telnet, HTTP и др.);
- Транспортни – отговарят за надеждността при придвижване на данните в мрежата (TCP, NetBEUI);
- Мрежови – осигуряват така наречените свързващи услуги. Управляват адресиращата и маршрутизираща информация, осъществяват проверките за грешки и заявките за повторно предаване (IP).

Някои мрежови протоколи:

NetBIOS - има два режима на комуникация – сесиен и дейтаграмен режим. В сесиен режим NetBIOS позволява да се осъществи връзка (сесия) с откриване на грешки и възстановяване. В дейтаграмен режим съобщенията се изпращат без установяване на връзка. Откриването на грешки и коригирането им е задача на приложението.

NetBIOS осигурява услуга за именуване на хостовете. Адресацията става по име на компютър като компютрите са обединени в работни групи.

TCP/IP - (Transmission Control Protocol/Internet Protocol) е основен протокол в глобалната мрежа Интернет. TCP/IP е сложен протокол, който се състои от други протоколи. Първият и най-важен от тях е IP (Internet Protocol).

IP протоколът използва технология за обмен на информация, наречена ***комутация на пакети***. Използват се две версии на IP протокола – IPv4 и IPv6. IPv4 използва 32 битови интернет адреси, а IPv6 – 128 битови.
TCP е основния транспортен протокол, включен в пакета TCP/IP. Осигурява високо ниво на надеждност при предаване на данните. При него се гарантира, че всяко изпратено съобщение ще бъде получено. В TCP се следи за изгубени, повторно изпратени, не поредно получени и т.н. пакети. За това и този протокол е по-бавен.

UDP е другият транспортен протокол. Той е сравнително прост протокол – не се занимава с установяване на последователност на пакетите, с препредаването им при грешка. При него не се гарантира достигането на съобщението до получателя. Подходящ е за: кратки съобщения, които могат да се предадат в един пакет, за приложения работещи в реално време като VoIP (разговори по интернет), поточно аудио и видео.

8. Доказва необходимостта от използването на инструменти за диагностика на мрежата. – 6т.

В операционната система Windows са включени няколко помощни програми за разглеждане на конфигурационната информация и отстраняване на проблеми. Тези приложения в Windows се наричат *конзолни*. За да се стартира команден режим на работа се въвежда от Start/Run командата ‘cmd’.
основни TCP/IP помощни програми:

- ***ping –*** Packet Internet Grouper - помощна програма за проверка на мрежовата свързаност. Използва протокола ICMP (Internet Control Message Protocol). Може да работи с въведен параметър **име на хост** или **IP адрес**. В мрежата се изпраща пакет до конкретен host или група host-ове. Всеки host (ако протокола ICMP не е забранен) връща пакет до изпращача. Визуализира се времето за изпращане и получаване на пакет. Ако пакетът не се ‘завърне’ до зададения тайм-аут (или е изгубен), се изписва съобщение „Request timed out”.

- ***arp –*** Address Resolution Protocol - използва се за визуализация и модификация на таблицата IP-към-Физически адрес.ARP протоколът (Address Resolution Protocol) извършва съпоставяне между логическите IP адреси и физическите (MAC) адреси.

Синтаксис:
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
-a Показва текущата ARP таблица.
inet_addr Интернет адрес.
-d Изтрива host от таблицата
-s Добавя връзка IP-към-Физически адрес

Пример:
C:\>arp -a
Interface: 192.168.0.101 --- 0x2
Internet Address Physical Address Type

192.168.0.1 00-17-9a-db-4f-a4 dynamic

- ***netstat*** – Network Status **-** показва информация за мрежовите сесии (активни връзки) на съответния компютър. Сесията е от порта на един хост до порта на друг хост.

netstat без параметри показва активните сесии
netstat –a показва всички сесии

Чрез **netstat** получаваме информация за използвания протокол, името на локалния компютър и използвания порт, името на другия компютър, с който има изградена сесия и състоянието на сесията.

- ***nbtstat –*** NetBIOS Over TCP/IP - предоставя информация за имената на компютрите и групите, известни на конкретен компютър. За задаване на компютъра по IP адрес се използва параметър '–A', за задаване на компютъра по име – параметър '–a'.

- ***ipconfig, ifconfig*** – Internet Protocol Configuration, Interface Configuration **- п**редоставя информация за TCP/IP конфигурацията на всички мрежови карти, включени към компютъра. В UNIX/Linux системи командата се нарича ifconfig.

Тя извежда информация за: IP адрес, подмрежова маска, Gateway – подразбиращ се шлюз.
Командата **ipconfig /all** предоставя допълнителна информация за мрежовите карти като: физически MAC адрес, адреси на DNS сървъри, DHCP информация и др.

- ***tracert, traceroute*** – Trace Route - проследява маршрута през мрежата до компютъра – местоназначение по зададен IP адрес или име. Изпраща по три пакета до маршрутизатор и показва времето за връщане (* за загубени пакети). В UNIX/Linux системи командата се нарича traceroute.

Синтаксис:
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:

-d	Не се разрешават адресите до имена на host-ове.
-h maximum_hops	Максимален брой ходове до целта.
-w timeout	Времето (Timeout) в милисекунди, в който се чака отговор.

Стойност по подразбиране на параметъра h е 30 стъпки (host-а).
На екрана се визуализират:IP адрес на маршрутизатор, име на хоста – маршрутизатор, брой стъпки (маршрутизатори) през които преминава пакета, времената за отиване и връщане на пакета.

9. При поставена задача прави изводи за хардуерните и софтуерните заплахи на компютърната мрежа и избира подходящ метод за защита с цел осъществяване на максимална мрежова сигурност. 8т.

За горната компютърна мрежа запишете какви са хардуерните и софтуерните заплахи и предложете подходящ метод за защита с цел осъществяване на максимална мрежова сигурност.

(изберете от материала по-долу)

Съвременните информационни системи поради сложността си са предразположени към пробиви и грешки. Те съхраняват поверителна информация, която трябва да се предпази от злоупотреби, затова трябва да имат добре планирана и реализирана сигурност. Пробивът в сигурността може да се дефинира като нелегален достъп до информация, който може да причини разкриване, заличаване или смяна на информацията. Обикновено това означава използване или достъп до информация или системи за незаконни цели или за цели, за които информацията или системите не трябва да се използват.

Пробивът в сигурността може да бъде :

- Достъп до информация на абонати за изпращане на спам съобщения
- Неупълномощен достъп до поверителна информация с цел създаване на подправена самоличност
- Подслушване
- Придобиване на неупълномощен достъп до мрежа с цел достъп до фирмена информация
- Вирусни атаки
- DNS превземане
- DoS(denialofservice) атаки
- DDoSатаки
- Пробив във физическите граници на организация

Заплахите според произхода си могат да бъдат – външни, вътрешни, физически и електронни

Според източника на атаките – случайни, злонамерени, заплахи за пълномощията, заплахи за приложенията, заплахи за поверителността, заплахи за контрола на достъпа

Случайни заплахи - резултат от човешки грешки: лош избор на пароли, случайни или погрешни бизнес транзакции, случайно разкриване на информация, използване на неподходящ или остарял софтуер, недостатъчни познания в системите за сигурност, неправилната конфигурация на устройствата за сигурност, изтичане на информация поради незащитен трансфер на данните.

Злонамерен софтуер -злонамереният софтуер е програмен код, който е целенасочено написан, за да причини вреда на система или мрежа. Вирусите, червеите и троянските коне са типични примери за злонамерени програми;

Вирусните атаки се причиняват от компютърни вируси - злонамерена програма, която е устроена да се прикрепя към друга програма, файл или сектора за зареждане на твърдия диск.

Заплахите за пълномощията (правата) са резултат от представянето на хакери като упълномощени потребители. Често срещана атака над правата е когато нарушителят открие мрежовата парола на потребител и влезе в системата.

Заплахата на приложенията може да бъде :

Превишаване на правата - когато нарушителят има възможност да повиши правата и привилегиите на неговата система до ниво, по-високо от нивото, на което трябва да бъдат;

Уязвимости на разработен от независим производител или персонализиран софтуер - доставчиците на услуги често използват софтуер, разработен от трети лица (third-party) и го преработват (персонализират) в зависимост от нуждите си. Може да има възможност за пробив.

Уязвимости на Web сървърите –недобре или в повече конфигурирани предлагани услуги, лошо написани CGI скриптове

Превземане на сесии-HTTP е несвързан протокол. Това означава, че при приключване на първоначалния обмен на съобщения между клиента и сървъра връзката прекъсва. С други думи, HTTP протоколът не запазва състоянието на сесията. Идентификаторът на сесиите (ID) е един вид заобикаляне на проблема със запазването на състоянието на сесията. Cookies осъществяват идентичността на сесиите. При превземането на сесии нарушителят превзема идентичността на сесията чрез достъп до данни на сървъри и мрежи

Атаки по e-mail:

e-mail бомбардиране-нарушителят изпраща на мишената идентични писма едно след друго, като по този начин препълва кутията му;

изпращане на спам (нежелани) съобщения-метод, при който атакуващите изпращат e-mailна стотици или хиляди потребители;

e-mail подслушване и измами-при e-mail подслушването атакуващите прихващат e-mail съобщения по мрежата, преди те да са пристигнали при получателя си. При e-mail измамата атакуващият прихваща e-mail съобщение по мрежата и променя информацията в него със злонамерена цел.

Мрежови заплахи: Тези уязвимости могат да се класифицират в следните три категории:

DoSатаки (Отказ на услуги/Denial of Service)-на упълномощени потребители се отказва достъп до мрежови услуги.

Разпределени DoS атаки (DDoS)–при атаката се използват по-голям брой компютри. DDoSатаките също целят отказа на мрежови услуги на легитимни потребители;

Атаки с измами с данни -включват прихващане, промяна и повреждане на данни, пътуващи по мрежата или намиращи се на хостовете.

Заплахи с измами на данни:

Атаките с измами на данни включват прихващане, промяна и повреждане на данни, пътуващи по мрежата или намиращи се на хостовете. Методи:

измами(spoofing) -компютърът на хакера се маскира като компютър от мрежата на компютъра-мишена

подслушване или слухтене (sniffing) -улавяне на мрежова информация

превземане на сесии

Защитна стена: Система или комбинация от системи, която подсилва границата между две или повече мрежи. Тя реализира правила за сигурност, които отделят две мрежи от нежелана комуникация. Мрежовите защитни стени пазят критична информация от опасности и в същото време позволяват преминаването на информация;

Функционалност на защитните стени

Филтриране на пакети - филтрирането на входящи и изходящи пакети на базата на информацията за протокола и адреса, въпреки че не се проверява съдържанието на пакета. Това е най-основната функция на една защитна стена.

Преобразуване на мрежов адрес- скрива хостове на вътрешни мрежи от хостове на външни мрежи чрез преобразуване адресите и портовете на вътрешни хостове до често срещани

външни адреси на защитната стена. Защитни стени, които действат по този начин, предотвратяват наблюдението на вътрешни хостове от злонамерени хостове на публична мрежа.

Прокси услуги - предоставят обмен на данни от страна на клиентските приложения с отдалечени системи. Така клиентският компютър се скрива зад защитната стена и за отдалечената система изглежда сякаш прокситo(proxy) взаимодейства с нея.

Потребителска автентикация. Тази функция е удобна, когато отдалечени потребители (в публична мрежа) използват динамични IP адреси, за да се свържат с частни мрежи. В този случай ограничение на базата на IP адреси не е практично, защото потребителят ще получи различен IP адрес, когато се свърже. Затова защитната стена ще поиска проверка на автентичността, преди да позволи влизане в частната мрежа.

Тунелиране(Tunneling). Чрез създаване на виртуален тунел се позволява на физически отделни мрежи да използват Интернет като среда за комуникация. Една такава реализация на защитните стени помага за създаване на виртуални частни мрежи (VirtualPiNetworking, VPN).

Криптография - механизъм, който защитава информацията чрез криптиране (шифриране) и декриптиране (дешифриране) на съобщения с таен код или шифър;

Видове криптиране:

Със симетричен ключ: използва един и същ ключ за криптиране н декриптиране на съобщението, Споделянето на ключа се извършва по сигурен и таен начин, за да се поддържа поверителността, Наричан още механизъм за криптиране с таен ключ, Протоколите на сигурността използват симетрични ключове като сесийни ключове за поддържане на поверителността на съобщения в онлайн комуникация

Например, протоколите Transport Layer Security(TLS) и Internet Protocol Security(IPSec) използват механизма на симетричния ключ, за да генерират сесийниключове със стандартни алгоритми за криптиране и декриптиране на съобщения.

Всяка сесия поддържа различен сесиен ключ и тези ключове се подновяват на определени интервали
Недостатъци :

Ключът трябва да се споделя между страните, които искат да взаимодействат. Това може да отслаби сигурността, тъй като повече от един човек знае за ключа.

Процесът на споделяне на ключа включва риска от пресрещане на ключа по мрежата от трето лице.

Рискът се повтаря всеки път, когато ключът се променя или между страните.

с несиметричен ключ:
криптирането с несиметричен ключ използва различни ключове за криптиране и декриптиране на съобщението; Изисква два ключа: публичен ключ и частен ключ; Наричано още криптиране с публичен ключ; частният ключ е известен само на собственика.

Публичният ключ се споделя и е достъпен за всички страни, които биха искали да взаимодействат със собственика на частния ключ. Криптиране на симетричните тайни ключове, за да ги защити по време на обмена им по мрежата или докато се използват, съхраняват или хешират в системи. Създаване на цифрови подписи, които предоставят автентикация и признаване за ресурси и цялостност на данни за електронни документи и съобщения.

Криптирането със симетричен ключ е от 100 до 1000 пъти по-бързо и натоварва процесорите по-малко, при криптирането с несиметричен ключ се използват по-тежки алгоритми в сравнение с криптирането със симетричен ключ, Алгоритмите, използвани в криптирането с публичен ключ, включват сложни математически функции, които подсигуряват, че веднъж изпълнен, процесът криптиране не може да се обърне лесно, Съобщението, криптирано с публичен ключ, може да се декриптира само със съответния му частен ключ и обратно, Ключовете са генерирани по такъв начин, че не е възможно да определите единия ключ, дори и да знаете другия.

Физическа сигурност

При планиране на политиката за мрежова сигурност трябва да се има предвид и ограничаване на физическия достъп на външни лица до данните в мрежата. Мероприятията могат да бъдат насочени в следните направления:

Защита на кабелите срещу директен физически достъп

Мрежовите кабели трябва да бъдат положени така, че да няма възможност за физически достъп до тях. Трябва да бъдат положени в специални канали или да бъдат скрити в окачени тавани или подови настилки. Кабелите с усукани двойки проводници са особено лесни за подслушване. При оптичните кабели това е възможно, но е значително по-трудно.

Защита на компютърната система

Важен момент от сигурността на мрежата е ограничаване на физическия достъп за външни лица до компютрите и другите мрежови компоненти. Може да се използват и технически средства за защита. При планиране на мрежовата сигурност трябва да се има предвид и възможността за загуба на информация поради природни бедствия, хардуерни повреди и технически грешки. Затова е необходимо да се планират мероприятия за защита на данните и възстановяване от сривове.

Съществуват три начина за предотвратяване на загубите на информация:

· Аварийно захранване – използват се непрекъсваеми устройства – **UPS** (Uninterruptible power supply). . *Те биват :*

Smart UPS системи- работят в режим он-лайн. и

Back UPS системи- работят в режим stand-by. При наличие на захранване, те осигуряват директна връзка на консуматорите към захранващата мрежа.

· Архивиране на данните

· Отказоустойчивост - предпазват данните от загуба чрез дублиране на самата хардуерна система. Например, много важни сървъри притежават по два захранващи блока, при авария на един от захранващите блокове, системата продължава своята работа като

алармира системния администратор. Важна особеност на системите за отказоустойчивост е възможността за замяна без изключване на системата (hot spare). Така, авариралият захранващ блок може да бъде демонтиран и сменен с изправен без изключване електрозахранването на компютърната система.

Съвременните операционни системи поддържат функция за горещо поправяне (hot fixing) на повредени дискови данни. При откриване на грешен сектор от диска, драйверът на отказоустойчивостта се опитва да премести данните в добър сектор и да отбележи повредения като лош – забранен за използване.

Най-често се използват системи за отказоустойчивост на данните реализирани чрез RAID технология за защита на данните, съхранявани на твърди дискове. За да има устойчивост, системата трябва да е преосигурена, да има излишък, дублиране на информацията (redundancy).

10. Обяснява криптирането на безжичната мрежа. Демонстрира знания за видовете нива на достъп до ресурсите на мрежа. – 10т.

Протоколи за криптиран достъп в безжичните мрежи.

WEP е съкращение за Wired Equivalent Privacy, това е протокол за сигурност за безжични локални мрежи (WLAN) защитени в IEEE 802.11b стандарт.

WPA, кратко от Wi-Fi® Protected Access, е специфично криптиране на данните за безжична мрежа. Подобрената функция на сигурността на WEP използващ Extensible Authentication Protocol (EAP) (разширен протокол за удостоверение) за сигурен достъп през мрежа и метод на криптиране за сигурен пренос на данни. WPA е проектиран за употреба с 802.1X сървър за удостоверяване, който разпределя различни ключове за всеки потребител. Може също и да се използва в режим с по-ниска сигурност с "Pre-Shared Key (PSK)" (предварително споделен ключ). PSK е проектиран за мрежи в дома или малкия офис, където всеки потребител има една и съща парола. WPA-PSK също се нарича и WPA-Personal.

WPA-PSK дава възможност на безжично устройство да се свързва с точка на достъп използвайки метод на криптиране TKIP или AES.

WPA2-PSK дава възможност на безжично устройство да се свързва с точка на достъп използвайки метод на криптиране AES.

TKIP (кратко от Temporal Key Integrity Protocol (Протокол за интеграция на временен ключ)) е метод на криптиране. TKIP предоставя смесване на ключовете за пакет, цялостна проверка на съобщение и механизъм за смяна на ключовете.

AES (кратко от Advanced Encryption Standard (Стандарт за разширено криптиране)) е Wi-Fi® одобреният силен стандарт на криптиране.

WPA-PSK/ WPA2-PSK и TKIP или AES използват предварително споделен ключ (Pre-Shared Key (PSK)), който е с дължина 8 или повече символа, максимум до 63 символа.

По света има голям брой компютри. Този висок брой компютри и уеб сайтове е труден за управление и е необходима някаква структура, за да може да се работи и да се управлява и поддържа Интернет и всичките му потребители. За това е измислен йерархичния дизайн на

компютърните мрежи, който разделя всички компютърни мрежи в 3 нива и всяко ниво има своите отговорности.

1. Ниво на достъп [access layer]
Това е най-ниското ниво и работи със самите компютри, като ги обединява в локална мрежа . В това ниво устройства работят с хъб и суич. Те работят с MAC адрес (Media Access Control адрес). Всички компютри локалната мрежа имат еднаква мрежова част в IP адреса си.

2. Дистрибуционно ниво[distribution layer]
Това е второто ниво. То управлява и свързва няколко нива на достъп. Отговаря за свързване на локални мрежи. Устройство, което работи на това ниво е рутер. Той работи с IP адреси

3. Основно ниво [core layer]
Това е най-високото трето ниво. То управлява и свързва няколко дистрибуционни нива. Отговаря за високо-скоростна връзка между устройствата от дистрибуционно ниво. Устройства, който работят на това ниво са мощни рутери и умни суичове. Рутерите от това ниво поддържат трафик с много висока скорост. Обикновено Интернет доставчиците разполагат с такива рутери, те са много скъпи. Устройствата от това ниво трябва да имат резервен път. Това се налага, защото това ниво отговаря за трафик между много компютри и не може да си позволим да спре. За това има резервни пътища, така че ако някой маршрут от това ниво стане невалиден (рутерът спре или кабелите се прекъснат), да може да се използва резервен маршрут.