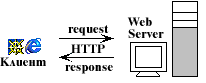
**Web сървър**

Web сървърът е програма, която използвайки модела клиент-сървър и протокола HTTP на World Wide Web, обслужва файловете, които формират Web страниците за Web потребителите (чиито компютри съдържат HTTP клиенти, които препращат заявките им).



Всеки компютър в Интернет, който предоставя Web сайт, трябва да има програма Web сървър.

|  |
| --- |
| Услуги |
| http://www-it.fmi.uni-sofia.bg/courses/BonI/images/bullet.gif  *MAIL (Computer Mail (E-Mail))*- електронната поща е услуга, може би най-популярната сред потребителите на Интернет. Услугата дава възможност за изпращане на съобщения до друг потребител от мрежата в ASCII или HTML формат. Съобщенията са придружени от адреси на подател и получател. Това на практика включва адресите на Mail сървъри, между които се осъществява обменът на съобщенията по мрежата. Всеки отделен потребител получава своята поща от пощенската кутия на своя Mail сървър. Подробно описание на Computer Mail се намира в документите[[RFC 821]](http://www.faqs.org/rfcs/rfc821.html),[[RFC 822]](http://www.faqs.org/rfcs/rfc822.html),[[RFC 937]](http://www.faqs.org/rfcs/rfc937.html). Simple Mail Transfer Protocol (SMTP) е наименованието на протокола на услугата електронната поща. |
| http://www-it.fmi.uni-sofia.bg/courses/BonI/images/bullet.gif  *FTP (File Transfer Protocol)*- обмен на файлове е услуга, позволяваща на потребителя да прехвърля файлове от своя компютър на друг компютър и обратно. Нивата на достъп на всеки потребител се определят от отсрещния компютър чрез задаване на потребителско име и парола. Най-честата употреба на FTP е свързана с копиране на файл или файлове от FTP сървър, включен в Интернет. Работата с полученото локално копие на файла не е свързана с ограничения. Подробно описание на FTP се намира в документа[[RFC 959]](http://www.faqs.org/rfcs/rfc959.html). |
| http://www-it.fmi.uni-sofia.bg/courses/BonI/images/bullet.gif  *TELNET (Network Terminal Protocol)*- отдалечена сесия (отдалечен терминал) е услуга, при която потребител може да се свърже с друг компютър от мрежата и да стартира процес в него. От този момент до края на сесията, всеки натиснат клавиш се изпраща на отдалечената машина и се интерпретира от нея. Обслужването се извършва от локалната машина, но Telnet програмата прави невидим вашият компютър. Първоначално връзката се осъществява чрез разпознаване на потребителя с потребителско име и парола. Telnet приложенията за микрокомпютри обикновено са придружени с терминални емулатори за определен тип терминали, подходящи за работа в среда UNIX или VMS. Подробно описание на Telnet спецификациите могат да се намерят в документите[[RFC 854]](http://www.faqs.org/rfcs/rfc854.html)и[[RFC 855]](http://www.faqs.org/rfcs/rfc855.html). |
| http://www-it.fmi.uni-sofia.bg/courses/BonI/images/bullet.gif  *USENET*- самостоятелна система, превърнала се в среда за дискусии и обмен на информация между хора с общи интереси, разделени по групи-"newsgroups". Обменът на новини по Интернет се обслужва от услугата NEWS, която се реализира чрез NNTP протокол. |
| http://www-it.fmi.uni-sofia.bg/courses/BonI/images/bullet.gif  *WEB или World Wide Web*- най-популярната услуга сред сърфистите по Интернет мрежата. Разпределената информационна система W3 дава достъп до документи по целия свят. Мултимедийната реализация на голяма част от тях ги прави особено атрактивни за преглед на нови филми, нова музика, графика, анимация и много други неща |
| http://www-it.fmi.uni-sofia.bg/courses/BonI/images/protocols.gif |
| Система за имена на домейни |
| Всеки възел в Интернет има уникален IP адрес. Поради факта, че IP адресите се запомнят трудно, вместо тях се използват имена на домейни. За повечето хора е по-лесно да се запомни името на домейна www.hp.com, вместо отговарящия на него IP адрес - 192.151.11.13. Името на домейна hp.com има повече от един IP адрес и посредством специален механизъм клиентите се изпращат към една от четирите машини, което се прави с цел постигане на еднакво натоварване на всички компютри. Всяко име на домейн отговаря на един или повече IP адреса и всеки IP адрес отговаря на едно или повече имена на домейн. В случай, че има повече от един IP адрес за едно име на домейн, това означава, че на едно и също място има няколко сървъра, които споделят входящите заявки и ако няколко имена на домейни отговарят на един IP адрес, тогава няколко клиента споделят един голям web сървър при доставчика на Интернет услуги. За да направи връзката между имената на домейни и IP адреси се изисква специализирана услуга, наречена DNS (Domain Name System). Йерархичното пространство с DNS имена се използва за свързване на имена на домейни с IP адреси и обратното. То се състои в последователност на имена, от най-общото до най-специфичното (в посока от ляво на дясно), отделени с точки, като например www.ferrari.it. Коренът на системата няма име. Под корена има набор от имена на домейни от високо ниво, които или се състоят от двубуквени кодове на отделните страни (както са описани в ISO-3166) или са по-общи като например ".edu", ".com", ".net", ".org". Повечето държави, като например Германия (".de") позволяват регистрирането на индивидуални организации директно под имената на домейни от високо ниво, което прави йерархията "плоска". В други държави, като например Великобритания (".uk") има допълнителен слой от общи категории под имената на домейни от високо ниво. Тези домейни от второ ниво могат да бъдат ".ac" за академични институции, като университети, ".co" за търговски организации, ".org" за всякакви видове организации и ".gov" за правителствени сайтове. |
| http://www-it.fmi.uni-sofia.bg/courses/BonI/images/domains.gif **Система за имена на домейни** |
| World Wide Web |
| През 1989 година изследователи от CERN (Eвропейска лаборатория за физика на частиците) в Женева си поставят за цел да разработят подходящо средство за предаване на текстова и графична информация на разпределените изследователски групи в средата на TCP/IP базирана мрежа. Изборът на документи или преглеждането на графика изисква търсене и намиране на машината, където е желаната информация, установяване на връзка с нея, прехвърляне на информацията до локална машина. Всяка подобна процедура налага стартиране на различни приложения (Telnet, FTP, Archie, или друга подходяща програма за визуализация на текст и графика). Поставената задача е създаване на система за достъп до произволен тип информация посредством унифициран интегриран интерфейс без необходимост от изпълнение на много стъпки при достъп и ползване на желания документ. През 1992 година CERN публикува проекта WWW (World Wide Web). Потребителите веднага оценяват рационалното в идеята и започват да създават свои WWW сървъри, за да направят своята информация достъпна по Интернет. Започна работа и по създаване на лесни за използване интерфейсни програми-WWW клиенти. В края на 1993 година WWW клиенти са разработени за различни компютърни системи, включително UNIX (X Windows), MacOS (Macintosh), MS Windows (PC). През лятото на 1994 година WWW е вече най-популярното средство за достъп до ресурсите на Интернет. Появяват се нови понятия - browser и navigator. Двете понятия отразяват функцията на един WWW клиент, предназначен да извлича, интерпретира и изобразява мултимедийни документи на екрана на локалната машина. *Какво представлява WWW* Информационната система World Wide Web (WWW или W3) е една от най-популярните услуги, достъпни чрез Интернет. Тя позволява да се комбинират текст, аудио, видео, графика и анимация в мултимедийни документи. Хипервръзки в тези документи правят възможен достъпа до други документи, свързани с първичния. Те от своя страна могат да сочат към други документи, намиращи се в други сървъри по мрежата без да имат директна връзка помежду си. По същество се оформя една паяжина от контекстно-ориентирани връзки. Информационната система World Wide Web е базирана на хипертекст (hypertext) технология. Една дума в хипертекст документ може да служи като указател (hyperlink) към друг документ, в който се намира информация свързана с думата - указател. В съвременните Web документи свободно се комбинират хипервръзки, аудио и видео фрагменти, графични икони и изображения, което ги превръща в хипермедийни. Информационната система WWW се състои от множество информационни сървъри (Web servers), които са постоянно достъпни по мрежата и непрекъснато се променят. Наблюдаваните промени са насочени към съдържанието на информацията, начина на нейното представяне и структуриране. Нови Web точки непрекъснато се появяват в Интернет и създават една общодостъпна информационна среда. За получаване на достъп до WWW е необходима връзка с мрежата и програма клиент (client, browser), която интерпретира и визуализира документите. Документите са хипермедийни и съдържат текст с команди за структуриране. По този начин WWW клиентът извършва форматиране с цел получаване на най-добрите възможни визуални резултати върху екрана на компютъра. |
| http://www-it.fmi.uni-sofia.bg/courses/BonI/images/comps.gif  **Обща архитектурна схема на информационната среда WWW** |
|  |

### Маршрутизатори

Маршрутизаторът е отправната точка за всички връзки на локалната мрежа с външния свят, което го прави особено уязвимо място в мрежата, ако не е снабдено с допълнителни средства за защита. По-старите [маршрутизатори](http://bg.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80) демонстрират ограничени способности на защитни стени. Те могат да бъдат надграждани с допълнителни софтуерни и [фирмуерни](http://bg.wikipedia.org/w/index.php?title=%D0%A4%D0%B8%D1%80%D0%BC%D1%83%D0%B5%D1%80&action=edit&redlink=1) възможности.

Пресяващият маршрутизатор (screening router) е най-евтиното, но и най-ненадеждно средство за мрежова защита. Способностите му се простират до мониторинг на достъпа до един или повече вътрешни сървъра и филтриране на входящите и изходящите пакети данни.

Предимствата на маршрутизатора с [пакетно филтриране](http://bg.wikipedia.org/w/index.php?title=%D0%9F%D0%B0%D0%BA%D0%B5%D1%82%D0%BD%D0%BE_%D1%84%D0%B8%D0%BB%D1%82%D1%80%D0%B8%D1%80%D0%B0%D0%BD%D0%B5&action=edit&redlink=1) в общи линии се изчерпват с неговата достъпност, лекота и ниска цена. Недостатъците са значително повече. Маршрутизаторът не позволява обстойни правила за филтриране, и следователно е предразположен към грешки и атаки. Още повече, че не дава възможност за [автентикация](http://bg.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) на пакетите. Почти е невъзможно да се скрие вътрешната структура и реалното адресиране на хостовете в мрежата.

Съвременните маршрутизатори на CISCO са и мощни защитни стени. Необходимо е да се купи и инсталира съответният софтуер, т.нар. „Cisco IOS“ и защитните функции почват да работят.

### Специализирани устройства от тип „защитна стена“

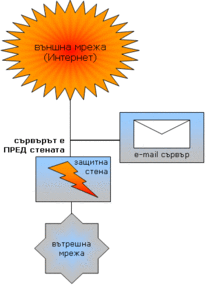
Продават се специализирани (dedicated) хардуерно-базирани системи за сигурност. Те работят под вградени [операционни системи](http://bg.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0), специално пригодени за нуждите на защитните стени, затова те са доста по-„безчувствени“ към много от слабостите със сигурността, присъщи на Windows NT и UNIX. Наличието на слабости в техния софтуер (firmware) обаче е потенциална опасност и поради тази причина трябва да бъдат специално проучвани преди инсталиране и софтуерът им своевременно обновяван.

### Разположения

[](http://bg.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Firewall-infrontof-server-bg.gif)

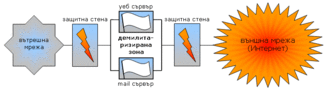
[http://bits.wikimedia.org/static-1.24wmf2/skins/common/images/magnify-clip.png](http://bg.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Firewall-infrontof-server-bg.gif)

Защитната стена е пред сървъра

[](http://bg.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Firewall-behind-server-bg.gif)

[http://bits.wikimedia.org/static-1.24wmf2/skins/common/images/magnify-clip.png](http://bg.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Firewall-behind-server-bg.gif)

Защитната стена е зад сървъра

[](http://bg.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Firewall-2-bg.gif)

[http://bits.wikimedia.org/static-1.24wmf2/skins/common/images/magnify-clip.png](http://bg.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Firewall-2-bg.gif)

Демилитаризирана зона

Защитната стена не само че няма да е от полза, но може и да е във вреда, ако не е разположена на правилното място. Следните фактори определят разположението на защитната стена:

* Броят на компютрите в локалната мрежа и нейната топология определят дали на всеки компютър ще се постави защитна стена или няколко компютъра могат да бъдат скрити зад една обща защитна стена. Освен това, тези параметри определят дали не е по-подходящо за защитна стена да се постави обикновен маршрутизатор или дори цял компютър, който да изпълнява защитни функции.
* Степента на необходимата защита и положението със защитата на съседните мрежи определят колко и какви защитни механизми едновременно ще работят за сигурността на локалната мрежа. Ако локалната мрежа съхранява критична по отношение на сигурността информация (например ако мрежата обслужва военна или финансова институция), то защитните механизми трябва да се прилагат както за цялата мрежа, така и за всеки хост поотделно.
* Характерът на информацията и услугите в локалната мрежа пък е фактор, който определя необходимостта и разположението на демилитаризирани зони в мрежата.
* Обемът и видът на трафика, генериран от защитаваната мрежа, определя начина, по който ще бъде конфигурирана защитната стена. Колкото е по-голям и разнообразен трафикът, толкова по-сложни ще са правилата, които стената ще съблюдава.

От значение е разположението на публичните сървъри, които не биха работели правилно, ако заради защитната стена хостовете от глобалната мрежа не могат да се свързват с тях. Ако e-mail сървърът, например, е разположен зад защитната стена на корпоративната локална мрежа, тогава в нея трябва да се “пробиват дупки”, за да се разреши електронната поща. Тези дупки обаче може да се използват от хакери. Ако e-mail сървъра е пред защитната стена и просто се наложат правила за електронна поща, то хем хостовете в локалната мрежа ще могат да използват тази услуга, хем ще бъде осигурена защита за мрежата. Защото, ако хакер все пак пробие защитата на e-mail сървъра, той все още няма да може да достигне до локалната мрежа, заради стоящата отзад защитна стена.

Затова е по-добре публичните сървъри (като e-mail сървъра) да стоят пред защитната стена на локалната мрежа. За да се обезопасят обаче и те, пред тях също се слага защитна стена. Това в крайна сметка е от полза за локалната мрежа, която така бива защитена двойно. Зоната между двете защитни стени обикновено се нарича демилитаризирана зона (demilitarized zone, DMZ).

Демилитаризираната зона представлява самостоятелен мрежови сегмент, в който информацията е под протекцията на защитни стени. Външните потребители имат достъп до DMZ, но не и до останалата част от корпоративната мрежа. Достъпът до данните и услугите от DMZ-сегмента се осъществява само през защитна стена. Комуникацията между DMZ и вътрешната мрежа също се осъществява чрез защитна стени със свои правила. DMZ е ефективен механизъм за онези компании, които очакват клиентите им да се свързват с техните мрежи по Интернет от външен за компанията източник, например при осъществяването на електронна търговия.

switch

Всички казвате по нещо вярно и по нещо грешно. Най-близко е Sertys - наистина в мрежите под хъб се разбира мултипортов повторител, а под суич се разбира мултипортов бридж. Така дефинирани, хъба работи на първо ниво от OSI модела и регенерира сигнала (разпознава 0 и 1 и съответно изпраща 0 и 1 на всичките си изходи)(същото прави и повторителя), а суича работи на второ ниво, "гледа" рамките (frames) и реализира следната функция (присъща и на бриджа): когато до него достигне рамка, суича (бриджа) поглежда, дали MAC адреса, за който е предназначена рамката, е записан в MAC таблицата му. Ако не е - изпраща рамката през всичките си портове (както би направил хъба). Хостът с въпросният MAC адрес вероятно ще отговори и ще изпрати рамка. Когато тази рамка мине през суича, той ще запише в MAC таблицата си, че хост с MAC адрес <еди кой си> се намира на порт <порта от който е дошла рамката>. От тук нататък, когато до суича дойде рамка, адресирана до MAC адрес, който е записан в MAC таблицата, той ще препрати тази рамка само през порта на който се намира въпросният хост (това го пише в MAC таблицата). Съществува механизъм за изтичане на давност на даден запис в MAC таблицата - по този начин ако даден хост се премести на друг порт, комуникацията ще се възтанови автоматично.

Основното предназначение на един суич (**switch**, комутатор) е да избере път, по който да изпрати данните от източника до тяхното местоназначение в дадена локална мрежа. Суичът работа с **МАС адреси** – това е уникален адрес на мрежовата карта на компютъра (нещо като ЕГН на компютъра).

Суичът има **вградена памет**. Тази памет се използва като междинен конектор между изпращащия и приемащия компютър. В нея се съхраняват МАС адресите на компютрите, които са включени към суича. Когато някой компютър изпрати сигнал, той съдържа в себе си и адресът на получателя. Суичът проверява в своята памет адреса, за който е предназначен сигналът и го изпраща само на необходимия порт.

Ethernet суичовете съчетават в едно устройство функциите на две по-стари Ethernet устройства – **хъба и моста**:

* свързват няколко мрежови сегмента, както прави това хъбът;
* управляват трафика между системите, така че да предотвратят конфликтите, подобно на работата на моста.

За разлика от хъба, **суичът не изпраща сигналът на всички компютри**, а само на този компютър, за който е предназначен сигналът. Поради това той може коректно да разпредели данните (сигналите), изпратени едновременно от няколко компютъра, без да задръства другите компютри с ненужни данни, както прави хъбът.

За разлика от моста, който  във всеки момент от време може да осъществи предаване на кадри само между една двойка портове, **суичът едновременно поддържа потоци от данни между всички свои портове**.

Повечето суичове поддържат пълнодуплексни операции (едновременно приемане и предаване на информация). Суичовете също така централизират кабелната система.

РАЗДЕЛЯНЕ НА ПОДМРЕЖИ