Доклад

По Интернет програмиране

Тема: Основни понятия и интернет протоколи

**1.Протокол**

Протоко̀лът най-общо представлява определено множество от правила в употребление при дадени обстоятелства.

Протокол в програмирането е множество от правила за комуникацията между обекти, програми или други програмни единици.

**2. Видове протоколи**

**TCP/IP (интернет протокол)**

Това са набор от стандартни правила, които позволяват на различни типове компютри да комуникират помежду си. IP протоколът гарантира, че всеки компютър, който е свързан към интернет, има специфичен сериен номер, наречен IP адрес. TCP указва как се обменят данни по интернет и как трябва да бъдат разбити на IP пакети. Той също така гарантира, че пакетите имат информация за източника на данните за съобщението, местоназначението на данните за съобщението, последователността, в която данните за съобщението трябва да бъдат събрани отново, и проверява дали съобщението е изпратено правилно до конкретната дестинация .

**SMTP (прост протокол за прехвърляне на поща)**

Тези протоколи са важни за изпращане и разпространение на изходящи имейли. Този протокол използва заглавката на пощата, за да получи имейл идентификатора на получателя и въвежда пощата в опашката на изходящата поща. И веднага след като достави пощата до имейл адреса на получателя, той премахва имейла от изходящия списък.

**PPP (протокол от точка до точка)**

Това е комуникационен протокол, който се използва за създаване на директна връзка между две комуникиращи устройства. Този протокол определя правилата, използвайки кои две устройства ще се удостоверяват едно с друго и ще обменят информация помежду си.

**FTP (протокол за прехвърляне на файлове)**

Този протокол се използва за прехвърляне на файлове от една система към друга. Това работи на модел клиент-сървър . Когато една машина поиска прехвърляне на файл от друга машина, FTO установява връзка между двете и се удостоверява взаимно, като използва техните ID и парола

**SFTP (протокол за защитено прехвърляне на файлове)**

SFTP, който също е известен като SSH FTP се отнася до протокола за прехвърляне на файлове (FTP) през Secure Shell (SSH) , тъй като криптира както команди, така и данни по време на предаване. SFTP действа като разширение на SSH и криптира файлове и данни, след което ги изпраща през защитен поток от данни на обвивката.

**HTTP (протокол за прехвърляне на хипертекст)**

Този протокол се използва за прехвърляне на хипертекстове по интернет и е дефиниран от www (световната мрежа) за пренос на информация. Този протокол определя как информацията трябва да бъде форматирана и предадена и също така определя различните действия, които уеб браузърите трябва да предприемат в отговор на повикванията, направени за достъп до определена уеб страница.

**HTTPS (HyperText Transfer Protocol Secure)**

HTTPS е разширение на Hypertext Transfer Protocol (HTTP). Използва се за защитена комуникация през компютърна мрежа с SSL/TLS протокол за криптиране и удостоверяване. Така че, като цяло, уебсайтът има HTTP протокол, но ако уебсайтът е такъв, че получава някаква чувствителна информация, като данни за кредитна карта, данни за дебитна карта, OTP и т.н., тогава той изисква инсталиран SSL сертификат, за да направи уебсайта по-сигурен.

**TELNET (терминална мрежа)**

TELNET е стандартен TCP/IP протокол, използван за виртуална терминална услуга, предоставена от ISO. Това позволява на една локална машина да се свърже с друга. Компютърът, който се свързва, се нарича отдалечен компютър, а който се свързва, се нарича локален компютър. Операцията TELNET ни позволява да показваме всичко, което се извършва на отдалечения компютър в локалния компютър.

**POP3 (Post Office Protocol 3)**

POP3 означава Post Office Protocol версия 3. Той има два агента за достъп до съобщения (MAA), като единият е MAA на клиента (агент за достъп до съобщения), а другият е MAA на сървъра (агент за достъп до съобщения) за достъп до съобщенията от пощенската кутия. Този протокол ни помага да извличаме и управляваме имейли от пощенската кутия на пощенския сървър на получателя към компютъра на получателя.

**IPv4**

Четвъртата и първоначално широко използвана версия на Интернет протокола се нарича IPv4 (Интернет протокол версия 4). Това е най-популярната версия на интернет протокола и отговаря за разпространението на пакети данни в цялата мрежа. Максималните уникални адреси за IPv4 са 4 294 967 296 (232), които са възможни поради използването на 32-битови адреси. Мрежовият адрес и адресът на хоста са двата компонента на всеки адрес. Адресът на хоста идентифицира конкретно устройство в мрежата, докато мрежовият адрес идентифицира мрежата, към която принадлежи хостът.

**IPv6**

Най-новата версия на интернет протокола, IPv6, е създадена за справяне с недостатъците на протокола IPv4. Максимум 4,3 милиарда уникални адреса са възможни с 32-битовите адреси на IPv4. Обратно, IPv6 използва 128-битови адреси, които позволяват значително по-голям брой уникални адреси. Това е важно, тъй като IPv4 адресите се изчерпваха и има все по-голям брой устройства, които изискват достъп до интернет. Освен това IPv6 предлага подобрени функции за сигурност като интегрирано удостоверяване и криптиране, както и по-добра поддръжка за мобилни устройства.

**ICMP**

ICMP (Internet Control Message Protocol) е мрежов протокол, който се използва за изпращане на съобщения за грешки и оперативна информация за мрежовите условия. Той е неразделна част от пакета за интернет протокол (IP) и се използва за помощ при диагностициране и отстраняване на проблеми с мрежовата свързаност.

Някои примери за ICMP съобщения включват:

* Echo Request и Echo Reply (ping)
* Дестинацията е недостъпна
* Времето е превишено
* Пренасочване

**UDP**

UDP (Протокол за потребителски дейтаграми) е протокол на транспортно ниво без връзка, ненадежден. За разлика от TCP, той не установява надеждна връзка между устройствата преди предаване на данни и не гарантира, че пакетите с данни ще бъдат получени в реда, в който са били изпратени или че изобщо ще бъдат получени. Вместо това UDP просто изпраща пакети от данни до дестинация без проверка за грешки или контрол на потока. UDP обикновено се използва за приложения в реално време, като поточно видео и аудио, онлайн игри и VoIP (глас през интернет протокол)където малко количество загубени данни е приемливо и ниското забавяне е важно.

**IMAP**

IMAP (Internet Message Access Protocol) е протокол, използван за извличане на имейли от пощенски сървър. Той позволява на потребителите да имат достъп и да управляват своите имейли на сървъра, вместо да ги изтеглят на локално устройство. Това означава, че потребителят има достъп до своите имейли от множество устройства и имейлите ще бъдат синхронизирани на всички устройства.

**SSH**

SSH (Secure Shell) е протокол, използван за защитено отдалечено влизане и други защитени мрежови услуги. Той осигурява сигурен и криптиран начин за отдалечен достъп и управление на сървъри, мрежови устройства и други компютърни системи. SSH използва криптография с публичен ключ за удостоверяване на потребителя и криптиране на предаваните данни, което го прави много по-сигурен от традиционните протоколи за отдалечено влизане като Telnet. SSH също така позволява защитено прехвърляне на файлове с помощта на протоколите SCP (сигурно копиране) и SFTP (протокол за защитено прехвърляне на файлове).

**3. Комуникация клиент – сървър**

1. Клиентите и сървърите обменят съобщения в модел на съобщения за отговор на заявка. Клиентът изпраща заявка, а сървърът връща отговор. Този обмен на съобщения е пример за комуникация между процесите.

2. За да комуникират, компютрите трябва да имат общ език и трябва да следват правила, така че и клиентът, и сървърът да знаят какво да очакват. Езикът и правилата за комуникация се определят в комуникацията.

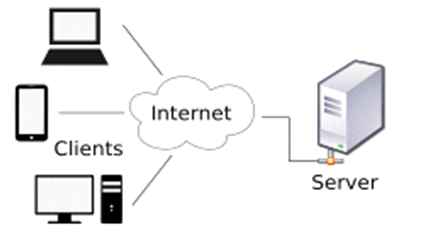
3. Всички протоколи клиент-сървър работят в приложния слой. Протоколът на приложния слой дефинира основните модели на диалога.

4. За да формализира още повече обмена на данни, сървърът може да внедри API (като уеб услуга). API е абстракционен слой за такива ресурси като бази данни и персонализиран софтуер. Чрез ограничаване на комуникацията до конкретен формат на съдържание. Като абстрахира достъпа, той улеснява междуплатформения обмен на данни.

5. Един сървър може да получава заявки от много различни клиенти за много кратък период от време. Тъй като компютърът може да изпълнява ограничен брой задачи във всеки момент, той разчита на система за планиране, за да приоритизира входящите заявки от клиенти, за да ги приспособи всички поред.

6. За да предотврати злоупотреба и да увеличи максимално времето за работа, софтуерът на сървъра ограничава начина, по който клиентът може да използва ресурсите на сървъра. Въпреки това сървърът не е имунизиран от злоупотреба.

7. Атаката за отказ на услуга експлоатира задължението на сървъра да обработва заявки, като го бомбардира със заявки непрекъснато. Това възпрепятства способността на сървъра да отговаря на законни заявки, които могат да улеснят комуникацията в мрежата.



8. Моделът клиент-сървър на изчисленията е структура на разпределено приложение, което разделя задачи или натоварвания между доставчици на услуги, наречени сървъри, и рикуестъри на услуги, наречени клиенти.

9. Често клиентите и сървърите комуникират през компютърна мрежа на отделен хардуер, но и клиентът, и сървърът могат да се намират в една и съща система.

10. Сървърната машина е хост, който изпълнява една или повече сървърни програми, които споделят своите ресурси с клиенти. Клиентът не споделя нито един от ресурсите си, но изисква съдържанието или услугата на сървъра. Следователно клиентите инициират комуникационни сесии със сървъри, които очакват (слушат) входящи заявки.

1.Протокол - <https://bg.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB>

2.Видове протоколи – <https://www.geeksforgeeks.org/types-of-internet-protocols/>

3.Комуникация клиент - сървър – <https://easyexamnotes.com/client-server-communication/>

Изготвил: Валентин Кьосев 12 ,,А‘‘ клас