

ТЕХНОЛОГИЧНО УЧИЛИЩЕ ЕЛЕКТРОННИ СИСТЕМИ КЪМ
ТЕХНИЧЕСКИ УНИВЕРСИТЕТ - СОФИЯ

ДИПЛОМНА РАБОТА

Тема: Мрежов анализатор с възможност за отдалечен анализ
посредством AngularJS 2 клиент

Дипломант: Ивайло Арнаудов

Научен ръководител: Стоил Стоилов

София, 2017

Списък на съкращения

VPN	Virtual Private Network
IP	Internet Protocol

Съдържание

0.1	Компютърни мрежи	4
0.2	Приложения на компютърните мрежи	4
0.2.1	Приложения на компютърните мрежи в бизнеса	4
0.2.2	Приложения на компютърните мрежи в дома	5
0.3	Изисквания към мрежов анализатор	5
1	Методи и технологии за реализация на мрежов анализатор	7
1.1	Основни принципи и технологии за реализиране на мрежови анализатор . .	7
1.1.1	Протоколи	7
1.1.2	Open Systems Interconnections (OSI) модел	8
1.2	Съществуващи решения и реализации	8
2	Проектиране на структурата на мрежов анализатор	9
2.1	Функционални изисквания към мрежов анализатор	9
2.2	Съображения за избор на програмни средства и развойна среда	9
2.3	Проектиране на структурата на базата от данни	9
3	Програмна реализация на мрежов анализатор	10
4	Ръководство на потребителя	11
5	Заклучение	12
A	Изходен код	13
	Библиография	14
	Списък на фигурите	15
	Списък на таблиците	16

Увод

0.1 Компютърни мрежи

Всеки от последните три века бива доминиран от някаква нова технология. Пример за това е ерата на механичните системи съпътстващи Индустриалната революция през XVIII век. За XIX век пък е характерен парния двигател. През XX век, ключовата технология е събирането, обработката и дистрибуцията на информация. С развитието ѝ човечеството става свидетел на инсталацията на глобални телефонни мрежи, изобретяването на радиото и телевизията, експоненциалния растеж на развитието на компютърната индустрия и, разбира се, Интернет. Като резултат от огромния технологичен прогрес в сферата на информационните технологии, през XXIV. разликите между съхраняване, транспортиране и обработка на информация изтъняват, а успоредно с това растат и изискванията на крайния потребител към комуникационните услуги.

Въпреки крехката възраст на компютърната индустрия (напр. в сравнение с автомобилната), тя прави значителен прогрес. През първите две десетилетия от съществуването им, компютърните системи са били силно централизирани. Университет или средно голяма фирма биха имали един или два компютъра, а по-големите институции - по няколко. Идеята за съществуването на малки устройства тип смартфон, които са взаимосвързани, е била по-скоро утопична.

Обединяването на компютрите и комуникациите оказва голямо влияние върху организацията на самите компютърни системи. Старият модел при който един компютър изпълнява заявките на цялата организация бива заменен от нов модел при който голямо количество отделни, но взаимосвързани компютри извършват обработка на дадена информация. Тези системи се наричат **компютърни мрежи**. Неформална дефиниция за компютърна мрежа е множество от автономни компютри, взаимосвързани (можещи да обменят информация помежду си) от една технология. [Tanenbaum and Wetherall \(2011\)](#)

0.2 Приложения на компютърните мрежи

0.2.1 Приложения на компютърните мрежи в бизнеса

Обикновено повечето компании имат голямо количество компютри, най-често по един за всеки служител. Изначално, те биха могли да работят в изолация един от друг, но в даден момент идва необходимост те да бъдат свързани с цел служителите да извършват работата си по-пълноценно чрез колаборация помежду си.

Един от основните проблеми, който решават компютърните мрежи е **споделянето на ресурси**. Целта е информацията да бъде достъпна от всеки в мрежата независимо от физическото му местоположение. Пример за това е група служители на организация, използващи един общ принтер — нито един от тях няма нужда от личен такъв, затова и решението е по-евтино, бързо и по-лесно за поддръжка от поддръжката на голямо количество принтери.

По-важен проблем, който решават компютърните мрежи е споделянето на

информация. Малките и средни компании са фундаментално зависими от дигиталната информация. Повечето компании имат записи за клиенти, за продукти, финансова информация и т.н. онлайн. По-малките компании са традиционно разположени в един офис, докато при по-големите интернационални компании компютрите и служителите са разпрострени в много държави. Това обикновено бива имплементирано чрез **Virtual Private Network (VPN)** с цел агрегация на индивидуалните мрежи на различни местоположения в една обща.

В допълнение, компютърните мрежи дават възможността да се използват вече изградената мрежова инфраструктура за телефонни разговори благодарение на технологията **Internet Protocol (IP) телефония**, или още известна като **Voice over IP (VoIP)**. Те също предоставят механизми за по-богати форми на виртуална комуникация – споделяне на екрана (**Desktop sharing**), видеоконференции, споделена обработка на документи, дори отдалечен мониторинг на пациенти. Компютърните мрежи отварят вратите и за нов бизнес модел, наречен електронна търговия (или **e-commerce**), който се развива с големи темпове в последните години и става де факто стандарт при търговията от всякакъв тип. [Tanenbaum and Wetherall \(2011\)](#)

0.2.2 Приложения на компютърните мрежи в дома

В началото на компютърната индустрия причините за покупка на компютър от крайния потребител са се свеждали до нужда от обработка на текст и игри. През ХХІ век, най-голямата причина човек да се сдобие с персонален компютър е достъп до Интернет. Аналогично на компаниите, крайните потребители могат да достъпят отдалечена информация, да комуникират посредством **социалните мрежи**, да купуват продукти и услуги чрез e-commerce системи, да използват електронно банкиране, да споделят мултимедия и софтуер, да колаборират посредством **wiki** сайтове (напр. Wikipedia). В перспектива, използването на компютърни мрежи за подобряване на интеракцията между хората може да се окаже най-важното приложение.

Друго напоследък развиващо се приложение на мрежите е концепцията за **Internet of Things (IoT)**. Основната ѝ характеристика е че електронните устройства на крайните потребители се включват в компютърните мрежи; напр. душа в банята, който традиционно не е компютър, би могъл да записва какво количество вода е използвано и да праща информацията на приложение, което изчислява как водата да бъде използвана възможно най-ефикасно. [Tanenbaum and Wetherall \(2011\)](#)

0.3 Изисквания към мрежов анализатор

Анализа на пакети (**packet analysis**), още известен като **packet sniffing** или **protocol analysis**, описва процеса на заснемане и интерпретиране на данни в реално време (т.е в момента на преминаване през преносвателната среда) с цел по-задълбочено разбиране на процесите в мрежата. Анализа на пакети типично се изпълнява от програма, наречена мрежов анализатор или пакетен анализатор (**packet sniffer**). [Sanders \(2011\)](#) Изискванията към един такъв мрежов анализатор е да може да помогне на мрежовия администратор със следните задачи:

- Идентифициране на участниците в мрежата
- Идентифициране на кой или какво използва (bandwidth на български?)
- Идентифициране на моментите на максимално използване (load) на мрежата
- Идентифициране на потенциални атаки или злонамерена активност

Глава 1

Методи и технологии за реализация на мрежов анализатор

1.1 Основни принципи и технологии за реализиране на мрежови анализатор

Процеса на анализ на пакети включва кооперация между софтуера и хардуера и може да бъде разделен в следните три стъпки:

- **Събиране** В началната фаза на работата си, анализатора събира 'сурови', неинтерпретирани данни в двоичен вид директно от проводника. Типично, това става като съответно избрания мрежови интерфейс за анализ бива превключен в т.нар. **promiscuous mode**. В този режим, мрежовата карта може да 'слуша' за всевъзможен тип трафик по дадения мрежови сегмент, а не просто такъв, адресиран до станцията.
- **Конвертиране** В следващата фаза на работата си, анализатора конвертира събраните данни в разбираем формат за крайния потребител. Тук е мястото, където повечето добри анализатори спират с анализа. След тази стъпка, данните събрани от преносвателната среда са във вид, който може да бъде интерпретиран на много основно ниво; останалата по-голяма част от анализа се оставя на крайния потребител.
- **Анализ** В третата и финална фаза, мрежовият анализатор извършва реалния анализ на събраната и конвертирана информация. Анализатора взема събраните данни, отчита използвания мрежови протокол базирайки се на извлечените до момента данни и започва да анализира конкретните свойства на протокола.

С цел да бъде разбран процеса на работа, а и съответно модела на реализация на мрежов анализатор, е необходимо дефиниране на основните принципи на комуникация между компютърните системи – основите на мрежовите протоколи, Open Systems Interconnections (OSI) модела, както и хардуера, поддържащ тази инфраструктура.

1.1.1 Протоколи

В състава на модерните компютърни мрежи има голямо множество от системи, които се изпълняват върху различни платформи. Осъществяването на комуникация между всяка от тези системи би било невъзможно без строго дефинирани правила, наречени **протоколи**. Тези протоколи, групирани на база логическото им взаимодействие, образуват т.нар. **протоколен стек**.

Популярна аналогия на протоколите са човешките езици — всеки един има конкретни правила за структура на изречението, за форми на глаголи, прилагателни и т.н. Както при езиците, с протоколите може формално да се дефинира маршрутизирането на пакети, инициране на връзка, потвърждаването на приети данни и др. Протоколите могат да бъдат прости или комплексни. Някои от общите черти, които традиционно споделят, макар и абстрактно представени, са:

- **Инициация на връзка** Дефинира кой иницира връзката, напр. клиентът или сървърът. При инициране на връзка може да е необходима и допълнителна служебна информация преди да протече обмена на полезна информация.
- **Договаряне на параметрите на връзката** Дефинира процес, в който двете страни се разбират — дали връзката е криптирана, как се пренасят ключовете за декриптиране, какъв тип е връзката (full/half duplex) и др.
- **Форматиране на данните** Дефинира подредбата на данните, в каква последователност се обработват от приемащата страна и др.
- **Откриване на грешки и корекция на грешки** Дефинира какво се случва при загуба на данни, как едната страна на връзката реагира при загуба на отговор от другата и др.
- **Терминиране на връзка** Дефинира как дадено крайно устройство сигнализира на друго че връзката е приключила, каква финална информация трябва да бъде предадена преди успешния край на връзката и др.

1.1.2 Open Systems Interconnections (OSI) модел

Open Systems Interconnections (OSI) моделът е оригинално публикуван през 1983г. от **International Organization for Standardization (ISO)** като документ под името *ISO 7498*. Моделът е нищо повече от препоръчителен. С оглед на това създателите на протоколи не са задължителни да го следват прецизно. OSI моделът също така не е единственият, чиято цел е да представи комуникационните процеси в компютърните мрежи — другият популярен модел е **Department of Defense (DoD)** модела, още познат като **TCP/IP** модел.

1.2 Съществуващи решения и реализации

wireshark etc.

Глава 2

Проектиране на структурата на мрежов анализатор

block diagrams?

2.1 Функционални изисквания към мрежов анализатор

what the analyzer should support

2.2 Съображения за избор на програмни средства и развойна среда

why c++ rocks, why angular rocks, show websocketpp benchmarks

2.3 Проектиране на структурата на базата от данни

??

explain orms / explain odb (if i integrate it) / show the db structure

Глава 3

Програмна реализация на мрежов анализатор

show sum code eh

Глава 4

Ръководство на потребителя

explaining how a sniffer works to noobs

Глава 5

Заключение

Приложение А

Исходен код

Библиография

- C. Sanders. *Practical packet analysis: using Wireshark to solve real-world network problems*. No Starch Press, San Francisco, Calif, 2. ed edition, 2011. ISBN 978-1-59327-266-1. OCLC: 755869776.
- A. S. Tanenbaum and D. Wetherall. *Computer networks*. Pearson Prentice Hall, Boston, 5th ed edition, 2011. ISBN 978-0-13-212695-3. OCLC: ocn660087726.

Списък на фигурите

Списък на таблиците