

*ВИСША АТЕСТАЦИОННА КОМИСИЯ  
СПЕЦИАЛИЗИРАН НАУЧЕН СЪВЕТ ПО “ЕЛЕКТРОНИКА И  
КОМПЮТЪРНА ТЕХНИКА”*

*ИНЖ. НИКОЛАЙ РУМЕНОВ КАКАНАКОВ*

**МЕТОДИ И СРЕДСТВА ЗА РЕАЛИЗИРАНЕ НА  
ИНТЕРНЕТ БАЗИРАНИ РАЗПРЕДЕЛЕНИ  
ВГРАДЕНИ СИСТЕМИ**

*АВТОРЕФЕРАТ*

на дисертация за присъждане на образователна и научна  
степен „Доктор”

Научна специалност: 02.21.04, “Компютърни системи,  
комплекси и мрежи”

**Научен ръководител:**  
доц. д-р Гриша Валентинов Спасов

**Рецензенти:**

1: проф. д-р Рачо Иванов

2: ст.н.с. II ст. д-р Владимир Лазаров

## **ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД**

### ***Актуалност***

Развитието на компютърните и електронните технологии през последното десетилетие води до създаването на евтини едночипови компютри, периферни схеми, интелигентни сензори и изпълнителни устройства. Те дават възможност за реализиране на специализирани компютърни устройства за управление – ВМС. Паралелно с това, развитието на комуникационните технологии и моделите за разпределени информационни системи позволяват изграждането на разпределени системи за управление. Реализирането на Разпределени Вградени Системи (РВС) позволява извършването на теленаблюдение, телеконтрол, телеизмерване при използване на съществуващите апаратни и програмни средства. Разпределението на управлението между отделни компютърни системи позволява по-лесното им интегриране и администриране.

Много от въпросите при моделирането и изграждането на РВС още не са намерили задоволителни и утвърдени решения, особено в Интернет среда и затова изследванията в тази област са актуални. При съвременните локални мрежи се използват Fast/Gigabit Ethernet, топология звезда и връзки от тип пълен дуплекс и се прилагат технологии за разделяне на локалните мрежи на виртуални локални мрежи и приоритетна обработка. Това води до нови перспективи за изследване, а именно оценка на методите за приоритетна обработка, закъснение от обработка в комутатора, вариация на закъснението, детерминираност и определяне на границите, в които тези технологии са приложими за РВС.

### ***Цел и задачи на дисертационния труд***

Цел на дисертационния труд е изследването на методите и средствата за приложение на мрежови протоколи от стандартния TCP/IP стек в изграждането на Интернет базирани РВС и изследване на възможностите

за трансфер на технологии от бизнес информационните системи (по-конкретно многослойни клиент/сървър модели) в системите за отдалечено следене и контрол.

За постигане на тази цел в настоящия труд се поставят следните задачи:

1. Да се оценят възможностите за приложение на многослойни архитектури при реализацията на Интернет базирани РВС и да се предложи абстрактен модел за проектирането им, използващ стандартни Middleware технологии и обединяващ предимствата на йерархичните и разпределените системи.

2. Да се проектира протокол за извличане на данни в локални мрежи от контролери, съобразен с работата на многослойните клиент/сървър архитектури.

3. Да се дефинират основните потоци от данни при комуникация в РВС и да се предложи аналитичен модел за определяне на закъсненията в локална мрежа от контролери с управляем комутатор.

4. Да се предложи сценарий за симулационно изследване на приложението на Fast и Gigabit Ethernet при реализация на РВС и да се провери чрез симулация коректността на предложения аналитичен модел.

5. Да се проектира експериментална мрежа за изследване на Интернет базирани РВС и да се проведат насочени експерименти за проверка на коректността на предложените модели и протоколи.

### ***Метод на изследване***

Въз основа на сравнителен анализ са определени основните потоци от данни при комуникация в РВС. Теоретичните изследвания в дисертацията се базират на елементи от математическия апарат „Network Calculus” и симулационното моделиране. Приложните изследвания се базират на насочени експерименти, мрежово администриране и програмиране на езиците C/C++ и Java.

### ***Апробация***

Част от резултатите, представени в дисертационния труд са влезли в отчетите на научни и научно-приложни договори:

1. Проект към Фонд „Научни Изследвания”, договор номер: ВУ-МИ-108/2005, на тема: „Интегриране на Web услуги и данни в разпределени информационни системи в Интернет среда”.
2. Проект към Фонд „Научни Изследвания”, договор номер: МУ-МИ-1602/2006, на тема: „Анализ на атаките и методи за защита на Web услуги в глобални мрежи”.
3. Проект по НИС към ТУ-София, договор №992/НИ-17/2007, тема: “Web базирана експериментална мрежа от микроконтролери за изследване на информационното взаимодействие в разпределени системи за автоматизация”.

### ***Приложимост на резултатите***

Предложеният многослоен модел може да се използва за изграждане на разпределени системи за мониторинг и контрол в Интернет среда. Предложеният аналитичен модел за определяне на виртуалното закъснение и запаса в Интернет базирани РВС може да послужи за описание на закъсненията в мрежови автоматизационни системи. Проектираният приложен протокол може да се използва за извличане на данни в локални мрежи от контролери в рамките на системи за мониторинг и контрол.

### ***Публикации***

Основните теоретични и приложни резултати от дисертационния труд са представени в 13 публикации, както следва: една в списание “International Review on Computers and Software”, една в списание „Information Technology and Control”, една в списание „Електроника и Електротехника”, една в списание „Автоматика и Информатика”, в сборници на специализирани научни конференции с международно участие – девет.

### ***Обем и структура***

Дисертационният труд е изложен в 138 страници. Състои се от увод, речник на използваните термини, четири глави, заключение и библиографска справка от 145 литературни източника. Съдържа 56 фигури и 10 таблици.

## **КРАТКО СЪДЪРЖАНИЕ НА ДИСЕРТАЦИЯТА**

### ***Глава 1: Литературен Обзор***

В първа глава е направен преглед на Интернет базираните РВС. Разгледани са основните комуникационни технологии за реализацията им, заедно със специфичните им изисквания и сценариите за обмен. Разгледана е и принципната архитектура на Интернет базирана РВС, заедно с категориите Web сървъри и програмния модел на такава система и е направен кратък преглед на съществуващите платформи, които могат да се използват за реализиране на Интернет базирани РВС. Направен е преглед на съществуващите клиент/сървър модели, приложими за реализирането на Интернет базирани РВС и Middleware технологиите, които могат да се използват, заедно с техните предимства и недостатъци. Представени са основните механизми за сигурност при Интернет базираните РВС, в зависимост от това на кой слой от ISO/OSI работят. Представени са основните методи, използвани за проектиране на Интернет базирани РВС и са разгледани някои проблеми при използването на тези методи.

### ***Глава 2: Многослойни клиент/сървър архитектури за реализиране на Интернет базирани РВС***

В глава втора е направен анализ на приложението на многослойни архитектури клиент/сървър при реализацията на Интернет базирани РВС и е предложен референтен модел за реализация на такива архитектури. Прилагането им предоставя и възможност за използване на различни

стандартни и специално проектирани за RVC Middleware технологии.

### **2.1. Трислоен модел за изграждане на Интернет базирани RVC**

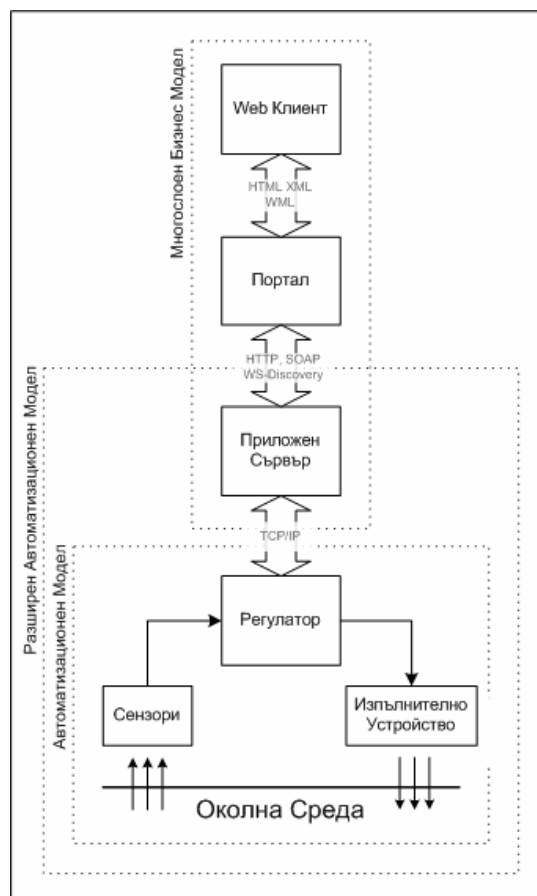
Прилагането на трислоен модел при RVC има за цел да раздели представителната от бизнес логиката и така да увеличи сигурността и надеждността на цялата система. Прилагат се идеите за използване на междинен слой, който да играе ролята на информационен портал към RVC. За разлика от традиционните бизнес трислойни архитектури, при RVC слой за данни е динамичен и има изисквания за работа в реално време. Контролерите изпращат на сървъра от междинния слой данните в момента, в който са готови. Въвежда се стандартен и популярен интерфейс за връзка с потребителя – Интернет браузер. Системата дава възможност за отдалечено администриране без да се увеличава много рискът за сигурността и надеждността и.

### **2.2. Многослоен модел за интеграция на Интернет базирани RVC**

Многослойните модели позволяват интегрирането на подсистемата за контрол и автоматизация с бизнес логиката на цялата система. В предложения модел може да има две проявления на подсистемата за контрол и автоматизация – локален мрежов контрол и разпределен контрол (фигура 2.2). Локалният контрол може да се разглежда като познатият в автоматизацията мрежов контрол. При него основната разлика с традиционните системи за управление е наличието на локална мрежа, по която се обменят данните. Разпределеният контрол включва една или повече подсистеми за локален контрол. Когато подсистемата за локален контрол е само една, може да се нарече отдалечен контрол.

При системите за разпределен контрол се наблюдава йерархично свързване – подсистемите за локален контрол включват контролер от ниско ниво и всички се свързват към контролер от високо ниво – фигура 2.3. Когато системата е силно разпределена, може да се въведе междинно ниво, което да е контролер от високо ниво за група от локални подсистеми.

Това йерархично разслояване позволява да се изолира влиянието между локалния и разпределения контрол и да се намали разпространението на деградацията от закъснението. Някои от решенията могат да се вземат от контролера от ниско ниво, когато те зависят само от параметри в локалната подсистема. Така се реализира филтриране и обобщаване на информацията на всяко ниво. Контролерът от междинно ниво служи за настройване на параметрите на контролерите от ниско ниво и модифициране на закона за управление спрямо измененията в характеристиките на физическата среда и управлявания обект. Ако няма контролер от междинно ниво, неговите функции се поемат от контролера от високо ниво. Контролерът от високо ниво служи за синхронизиране на работата на отделните групи от контролери. Той взема решения за промени в работата на контролерите от ниско и средно ниво, следвайки някаква глобална зависимост.



Фигура 2.2: Многослоен модел за разпределена автоматизация.

Предложеният модел има четири основни слоя – потребителски слой,

представителен слой, слой на услугите и слой за данни. В зависимост от реализацията на конкретните инстанции могат да бъдат имплементирани всичките четири слоя или само някои от тях.



Фигура 2.3: Многослойна мрежова система за управление.

### 2.2.1. Потребителски слой

Ролята на потребителския слой е да предостави на потребителите интерфейс за достъп до системата. Най-често се предоставя достъп чрез Web страници или чрез Web услуги. Използването на XSLT за трансформация от XML към желан формат, позволява да се използват голямо разнообразие от клиенти.

### 2.2.2. Представителен слой

На този слой се реализира входната точка към системата – Web портал и се описва начина на представяне на информацията на потребителя. Порталът приема заявките от потребителите и определя пътя им след това на базата на желаната услуга и сървъра от следващия слой, който може да я изпълни. Порталът е и мястото за регистрация на потребителите и проверка на правата им за достъп. За всеки потребител или група от потребители се съхранява описание на достъпните за него ресурси от системата. Те могат да бъдат дефинирани като „достъпни” и/или „видими”. За реализацията на този слой се предлага използването на JavaBeans и Apache Struts технологиите и възможностите им за реализиране на портали.



### *2.2.3. Слой на услугите*

На този слой се дефинира бизнес логиката и обектите в нея. Тук също така се проявява и разпределения характер на системата. За връзката между инстанциите на този слой се предлага използване на технологията на Web услугите. Някои от сървърите на този слой предоставят офис функционалността на системата и представляват части от стандартната информационна система. Останалите сървъри на този слой реализират разпределената автоматизация. В тази си част системата е реактивна, т.е. работи в зависимост от промените в средата и следените параметри и трябва да реагира със скоростта на тези промени. Работещите в тази част сървъри трябва да могат да определят кои заявки следва да бъдат обработени приоритетно и кои ще повлияят на работата на съответния им слой от данни. Използването на две отделни нишки като интерфейс позволява независимост на информационния обмен в слоя на услуги от реализацията на и протокола на комуникация в слоя от данни.

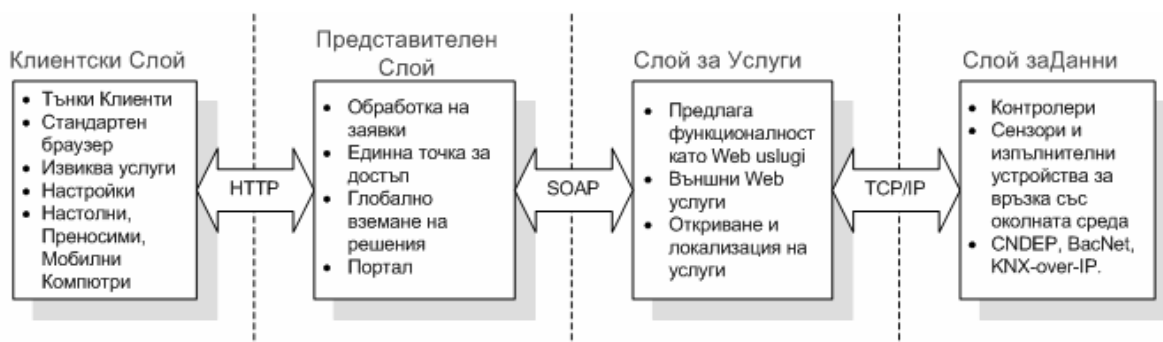
### *2.2.4. Слой за данни*

На слоя за данни се реализира съхранението на данните от работата на системата, реализира се събиране на журнална информация и се прави реалното извличане и продуциране на данни. На този слой се реализират и интегрират мрежите от контролери. В тези мрежи от контролери се извличат данни и се извършва контрол чрез специализиран протокол. За разлика от другите проявления на слоя за данни мрежата от контролери е динамична, както от гледна точка на устройствата, които продуцират данни и топологията им, така и от гледна точка на времето за продуциране на данните. Тук данните се извличат в реално време, което налага и някои особености, като нужда от бърза реакция, синхронизация. От гледна точка на автоматизацията този слой е слой на устройствата (device level). ВМС осъществяват същинската връзка с околната среда и следените/управляваните обекти. Наборът, типът и големината на

следените параметри определя изискванията към комуникационния протокол в мрежата от контролери.

### 2.2.5. Взаимодействие между слоевете

Взаимодействието между различните слоеве в модела и в рамките на отделните слоеве е базирано на различни комуникационни технологии и протоколи, съобразено с изискванията на работа на слоя, типа на обменяните данни и условията – фигура 2.7.



Фигура 2.7: Взаимодействие между слоевете.

## 2.3. Протокол за извличане на данни в мрежи от контролери (CNDP)

Протоколът CNDP (Controller Network Data Extracting Protocol) е асиметричен протокол, използван за извличане на данни от мрежата от контролери, която работи на слоя за данни в многослойни модели клиент/сървър. Обменът на данни е организиран по механизма заявка-отговор и съобщенията са байт-ориентирани върху UDP транспорт.

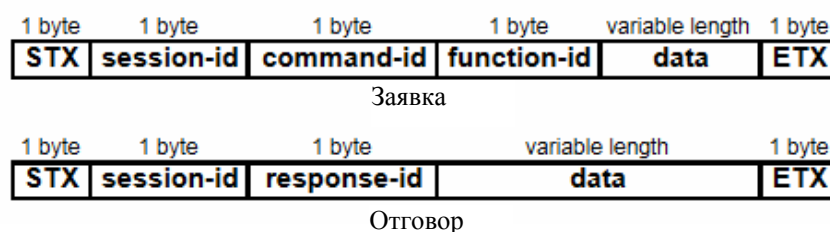


Фигура 2.9: Механизми на взаимодействие при CNDP.

Протоколът реализира три механизма на обмен на данни – фигура 2.9. Първият механизъм е извличане на данни: заявка за получаване на определен параметър и отговор, съдържащ параметъра. Вторият

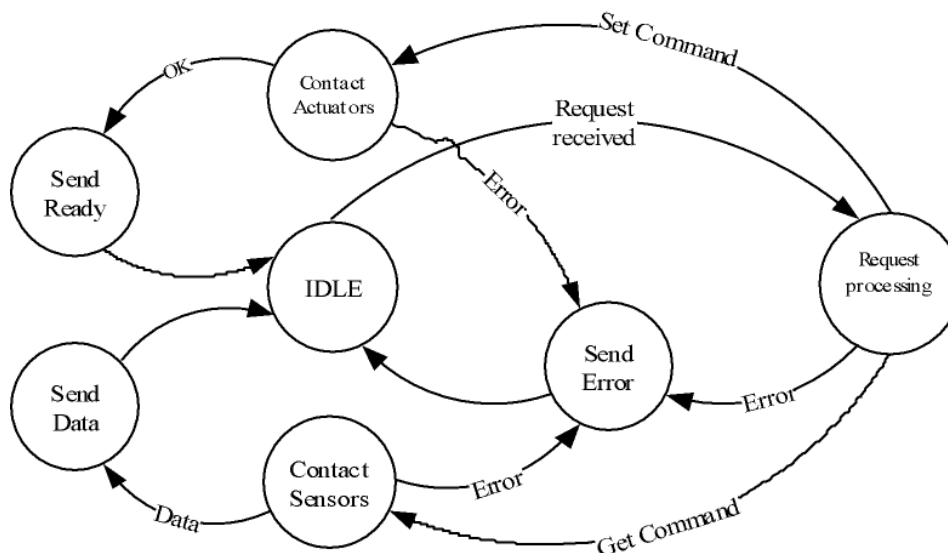
механизъм се използва за конфигуриране: изпраща се заявка с параметъра и новата му стойност, а отговорът е само потвърждение или грешка. При третия механизъм вградената система е инициатор – изпраща аларма, когато даден параметър излезе от определени граници.

Всяко съобщение се състои от стартов байт, байт за номер на сесия, байтове за данни и краен байт. Байтовете за данни може да присъстват в различен брой и проявления, които описват номер на команда, номер на функция, параметър за конфигуриране, стойност на параметър, код на грешка и други. Структурата на заявка и отговор е показана на фигура 2.10. Стартовият байт и байта за край на съобщение са ASCII кодирани – съответно 02 (STX) и 03 (ETX). Стойността в полето *session-id* автоматично се увеличава при всяка следваща заявка от страна на клиента и служи за уникално разпознаване на двойката заявка-отговор, заедно с IP адреса на подателя. Полето *command-id* съдържа идентификационен номер на CNDEP команда; команди с номера 0 и 255 са TEST, като първата винаги връща ОК, а втората ERROR. Команди с номера от 1 до 127 са GET заявки, а такива с номера от 128 до 254 – SET заявки. Това разделение е с цел по-лесно разграничаване на различните механизми за комуникация.



Фигура 2.10: Структура на CNDEP съобщенията.

Тъй като протоколът е асиметричен, сървърната и клиентската част изпълняват различни процедури. Клиентската част формира заявки, като следи за номер на сесия, изтичане на определено време за отговор и повторно изпращане при грешка. Сървърната част трябва да декодира получените заявки, да изпълни командата и да формира и изпрати съответния отговор – фигура 2.11.



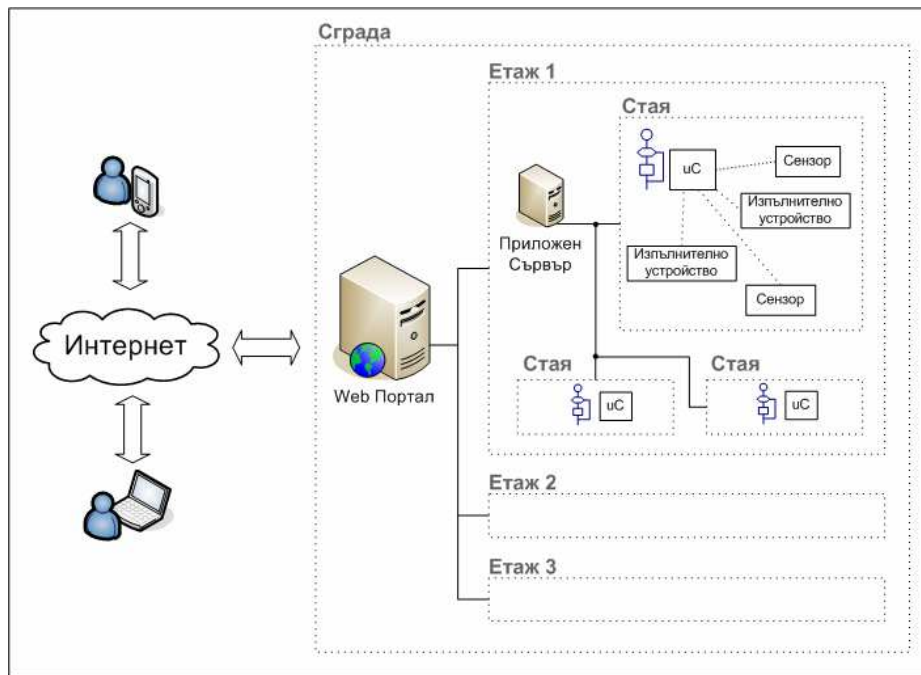
Фигура 2.11: Диаграма на състоянията на CNDP сървър.

## 2.4. Приложение на SNMP за реализация на PBC

Основните достойнства на протокола SNMP са бързата работа и наличието на програмни средства за събиране на информацията. Той е проектиран за следене на устройства и обратната връзка е само чрез промяна на вътрешни променливи, което го прави по-неудобен за приложение в Интернет базирани PBC. Недостатък е необходимостта да се обходи голяма част от дървото, за да се определи каква е заявката, а тъй като протоколът не е оптимизиран за PBC, дървото е сравнително голямо.

## 2.5. Приложение на многослойния клиент/сървър модел

Предложеният многослоен клиент/сървър модел е на достатъчно високо ниво на абстракция, че да може да бъде приложен в разнообразни реализации, като „умна къща”, персонално здравеопазване, управление аграрни обекти, енергийна ефективност. Архитектурата на представената система е проявление на предложения модел с ограничения, произтичащи от конкретното приложение – фигура 2.14. В нея се проявяват всички слоеве на модела и е налице интеграция с външни системи.



фигура 2.14: Архитектура на BMS за енергийната ефективност на сгради

Във всяка стая от сградата има сензори за следене на параметрите. Към всяко отоплително тяло има сензори за отчитане на консумираната мощност и за изпълнително устройство, което управлява работата му. Всички сензори и управляващи устройства, които работят заедно, се управляват от една ВМС. Групите от ВМС, работата на които зависи един от друг, представляват една мрежа от контролери (едно проявление на слоя за данни) и са свързани към един приложен сървър. Всички приложни сървъри са свързани към един Web портал, който синхронизира работата им и служи за входна точка към системата. Също така порталът може да се свързва към външни за системата климатични измервателни станции и услуги и да получава прогноза за времето или текущи данни. Тези данни се използват за донастройване на работата на системата с цел по ефективна работа на отоплителните и охладителните устройства и по-плавно регулиране на микроклимата. Приложните сървъри реализират слоя на услугите. Те обменят информация помежду си чрез Web услуги. Така промените в дадено помещение или регион се вземат предвид при регулирането на останалите помещения.

## **Изводи**

Предложен е абстрактен многослоен модел за реализиране на Интернет базирани РВС. Моделът позволява интегриране на бизнес информационни системи и РВС в една обща архитектура. Дадени са примерни реализации и приложими технологии за осъществяване на слоевете на модела.

Предложен е приложен протокол, базиран на UDP, който реализира информационното взаимодействие в слоя за данни. Този протокол използва просто структури от данни и кратки съобщения заявка/отговор за извличане на данни и предаване на управляваща информация в мрежи от контролери с управляващо устройство. Показани са и алтернативни протоколи за реализация на информационното взаимодействие на този слой.

Предложена е реализация на сървър за интеграция на слоевете за данни и услуги. Реализацията на сървъра позволява интегрирането на мрежата от контролери към архитектурата на Web услугите и позволява географското разпределение на системата.

### ***Глава 3: Изследване на протоколи за Интернет базирани РВС***

През последните години се наблюдава стремеж за адаптиране на стандартните протоколи за комуникация от TCP/IP стека и Интернет технологиите във всички информационни системи, включително и в РВС.

#### **3.1. Приложение на Ethernet за Интернет базирани РВС**

При изследването на Fast Ethernet трябва да се вземат под внимание основните различия спрямо базовия Ethernet: използването на комутатори, което предопределя липсата на колизии при предаване между независими станции, и използването на пълен дуплекс връзка.

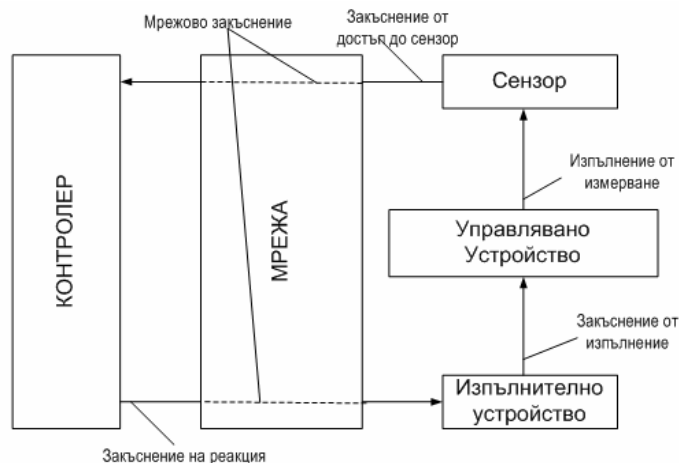
##### ***3.1.1. Типове трафик при Ethernet комуникация за РВС***

При изследване на РВС в локални мрежи е необходимо да се подбере типът трафик, който е най-близък до реалната ситуация. За РВС е характерен периодичен трафик, както и че размерът на пакетите почти не

се изменя във времето и е по-малък или близък до размера на минималния кадър. За реалистично представяне на трафика в РВС се използват комбинации от постоянен трафик (СВР) и Поасонов трафик, или постоянен трафик (СВР) и реални Ethernet трейсове. Прави впечатление, че трафикът е различен от офис мрежите, което налага друг тип експерименти и модели за описание на поведението на мрежата от типичните за Ethernet.

### 3.1.2. Основни параметри, влияещи на производителността на Ethernet за РВС

Системите за работа в реално време имат строги изисквания към времевите характеристики във всяка управлявана подсистема, която включва следене, изчисление по закон за управление, и реакция. В мрежовите системи за контрол, обратната връзка се затваря през мрежата. Закъснението от мрежата се проявява, когато сензорите, изпълнителните устройства и контролерът обменят данни помежду си – фигура 3.1.



Фигура 3.1: Мрежова система за управление и закъсненията в нея.

Закъсненията могат да бъдат постоянни, променливи или случайни, в зависимост от преносната среда, достъпа до нея и протокола за обмен.

### 3.1.3. Основни компоненти на закъснението при Ethernet комуникация за РВС

За по-точно анализиране на закъсненията при комуникация в РВС е

удобно те да се разделят на отделни компоненти, в зависимост от причините и характера на проявление. Закъснението в една локална мрежа може да се представи без отчитане на колизиите, като сума от следните компоненти: закъснението от обработка при изпращащата страна, при получаващата, времето за предаване на кадъра и времето за разпространение на сигнала по конкретната преносна среда.

*3.1.4. Аналитично определяне на запаса и виртуалното закъснение в система с Ethernet комутатор.*

За изследване на Ethernet като комуникационен протокол за Интернет базирани РВС се предлага аналитичен модел, основаващ се на математическия апарат „Network Calculus”. Този апарат се съсредоточава върху определяне на закъснението и запаса на системата, при което информацията в мрежата се разглежда като потоци, а мрежовите устройства като обслужващи възли, внасящи закъснение. Основните параметри, които се дефинират, са запас, виртуално закъснение, криви на пристигане и обслужване. Основната разлика с теорията на информацията е, че търсим границите на параметрите, а не средната им стойност.

### **3.2. Симулационна оценка на Ethernet за Интернет базирани РВС.**

За оценка на информационното взаимодействие и времезакъсненията в рамките на една РВС, използваща Ethernet като комуникационна среда, е предложен симулационен модел.

#### *3.2.1. Симулационна среда NS-2*

Предложеното симулационно изследване е реализирано на мрежовия симулатор NS (версия 2). Той представлява събитийно-ориентиран дискретен симулатор, разработен в университета Berkley.

#### *3.2.2. Сценарий на симулацията*

Предложеният сценарий за симулационно изследване е избран да съответства на често срещан модел на комуникация в РВС. Състои се от едно „главно” устройство и множество „подчинени”. Подчинените



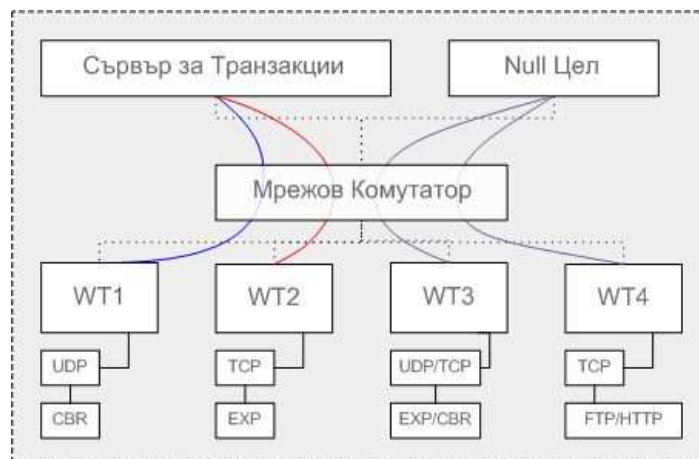
устройства представляват ВМС, които имат сензорни или изпълнителни устройства, включени към някои от техните интерфейси. Общо са наречени „мрежа от контролери”. Тъй като възлите в мрежата са свързани към комутатор, всеки обособен в свой микросегмент и работещ в режим на пълен дуплекс, то тогава броя на контролерите не е от значение. Техният брой има влияние само върху количеството на генерирания трафик и следователно в симулационния сценарий мрежата от контролери може да бъде представена от един единствен възел със съответния трафик. От друга страна, вследствие на модела на комуникация, изключваме възможността два контролера да комуникират помежду си и затова можем да ограничим броя на използваните възли до три – един за сървъра за транзакции, един за мрежовия комутатор и последния за мрежата от контролери. Комутаторът е програмируем и поддържа възможности за задаване на приоритет на класовете трафик и резервиране на пропускателна способност по схемата на стандарта 802.1p. В настоящата симулация е избрано в комутатора да се реализират четири опашки – една, която се обслужва с PQ и три, обслужвани по WRR. Пакетите от първата опашка се препредават без да се влияят от останалия трафик. Трите WRR опашки са с тегла 70/25/5%. (фигура 3.4).



Фигура 3.4: Физическа топология на симулационния модел.

В съответствие с избрания модел на симулация и с характерния за РВС трафик са избрани четири типа трафик – WT1, WT2, WT3, WT4. Първият

тип трафик (WT1) съответства на сценарии за комуникация, диагностика и мониторинг и контрол. Състои се от малки по размер, периодични съобщения. Той представлява 90% от целия трафик в настоящата симулация. Вторият тип трафик (WT2) съответства на сценарий за предаване на алармени съобщения. Представлява 4% от целия трафик. Разпределението му е случайно – може да се моделира като Поасонов процес. Третият тип трафик (WT3) съответства на сценария за конфигурация на устройствата в мрежата - използва малки по размер периодични съобщения и представлява 5% от целия трафик. Последният тип трафик (WT4) играе ролята на шум или фонов трафик. Обикновено се появява в началния момент на работа на мрежата и включва предаването на средни и големи по размер съобщения. Представлява 1% от целия трафик. Всеки от четирите типа трафик следва да се обвърже с подходящо приложение, което да го моделира с максимално подобие до реалния трафик – фигура 3.5.



Фигура 3.5: Логическа топология на симулационния модел.

### 3.2.3. Аналитично изчисление на резултатите

За изчисление на закъсненията и запаса в системата, се определят кривите на пристигане на всеки поток и параметрите на тези криви, съгласно предложения сценарий на комуникация. В изследването има четири потока с различни параметри – WT1, WT2, WT3 и WT4. Поток WT1 е периодичен, поради което неговата крива на пристигане може да се

опише с формула (3.18), където  $L$  – е размерът на кадъра, а  $T$  – периода:

$$(3.18) \quad \alpha_1(t) = L + \frac{L}{T} \cdot t$$

Останалите три потока (WT2, WT3 и WT4) могат да се моделират като TSPEC, описани с четиримерния вектор  $\{M_i, p_i, b_i, r_i\}$ , представящ максималния размер на кадъра –  $M$ , върховата скорост –  $p$ , максималния брой кадри, изпратени едновременно (burst) –  $b$ , и дългосрочната средна скорост –  $r$ . Кривите на пристигане се описват с формулата:

$$(3.19) \quad \alpha_i(t) = \min\{p_i \cdot t + M_i; r_i \cdot t + b_i\}$$

Обслужването, предоставено от комутатора на отделните потоци, зависи от дисциплината на обработка на заявките в опашката. Кривата на обслужване отново е RSPEC (rate-latency), но скоростта на препредаване и закъснението в комутатора се преизчисляват. За FIFO обработка скоростта на препредаването се изчислява по формула 3.21, а закъснението в комутатора по формула 3.22 за всеки поток. За PQ обслужване, съответно чрез формули 3.23 и 3.24. За обслужване с политика WRR – съответно с формули 3.25 и 3.26.

$$(3.21) \quad R_i = R - \sum_{i \neq j} r_j \quad (3.22) \quad S_i = S + \frac{\sum_{i \neq j} b_j}{R}$$

$$(3.23) \quad R_i = R - \sum_{j > i} r_j \quad (3.24) \quad S_i = \frac{\sum_{j > i} b_j}{R - \sum_{j > i} r_j} + \frac{\max(M_j : j < i)}{R}$$

$$(3.25) \quad R_i = R \cdot \frac{\varphi_i - M_i}{\sum_j \varphi_j - M_i} \quad (3.26) \quad S_i = \frac{\sum_{j \neq i} \varphi_j}{R}$$

Като се използват формулите за кривите на пристигане и обслужване, могат да бъдат определени максималното закъснение на всеки поток (формула 3.28) и необходимия запас в системата (формула 3.31).

$$(3.28) \quad D_i = S_i + \frac{M_i}{R_i} + \left( \frac{b_i - M_i}{p_i - r_i} \right) \cdot \frac{(p_i - R_i)^+}{R_i}$$

$$(3.31) \quad B_i = b_i + r_i \cdot \max\left(\frac{b_i - M_i}{p_i - r_i}; S_i\right) - R \left( \frac{b_i - M_i}{p_i - r_i} - S_i \right)^+$$

Използвайки формули 3.21-22 (FIFO), 3.23-24 (SP) и 3.25-26 (WRR) за описание на кривите на обслужване, могат да бъдат изчислени максималното закъснение по формула 3.28 и необходимият запас в системата по формула 3.31. Трябва само да се дефинират параметрите на отделните потоци (таблица 3.3).

**Таблица 3.3: Параметри на потоците и мрежовия комутатор**

SW		WT1		WT2		WT3		WT4	
R [bps]	1.0x10 <sup>8</sup>	L [bits]	576	b2 [bits]	4096	b3 [bits]	16384	b4 [bits]	48704
S [s]	4.5x10 <sup>-5</sup>	T [s]	1.0x10 <sup>-4</sup>	r2 [bps]	4.0x10 <sup>4</sup>	r3 [bps]	1.0x10 <sup>5</sup>	r4 [bps]	1.0x10 <sup>6</sup>
				M2 [bits]	2048	M3 [bits]	8192	M4 [bits]	12176
				p2 [bps]	1.0x10 <sup>8</sup>	p3 [bps]	1.0x10 <sup>8</sup>	p4 [bps]	1.0x10 <sup>8</sup>

Ако се вземе предвид сценарият с 1P3Q1T управление на опашките, могат да се направят изчисления за скоростта на препредаване и латентността, предоставена на всеки поток от комутатора, както и закъснението от престой в опашката. Важно е само да се подбере кой трафик в коя опашка да попадне. Има различни варианти за определяне на приоритета. Разликата между тях е основно в приоритета на трафика за конфигуриране на мрежата. Освен това може да варира приоритетът на периодичния трафик и алармите. При избрания вариант най-висок приоритет е присвоен на периодичния трафик, след това аларми, мрежова конфигурация и последно фонов. Трите нископриоритетни трафика получават „честно“ обслужване, ако приоритетната опашка обслужва неагресивен трафик – таблица 3.5.

**Таблица 3.5: Аналитични резултати за 1P3Q1T**

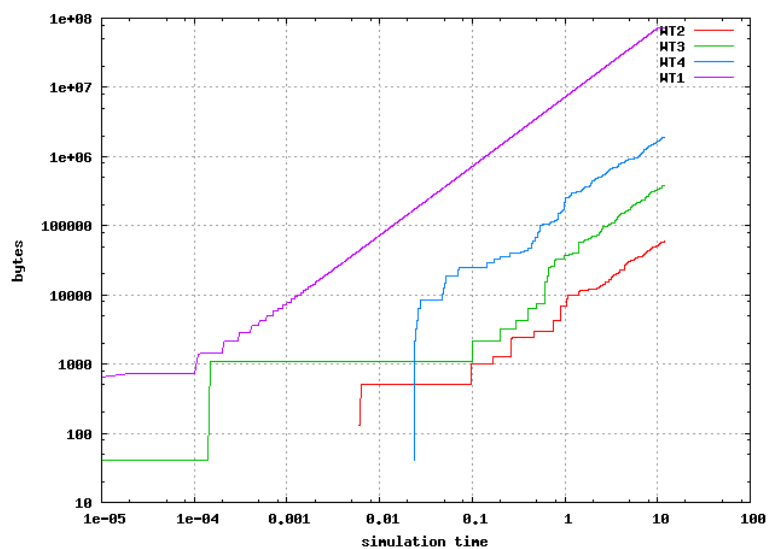
Flow	Backlog [Bytes]	Delay [μs]	Latency [μs]	Rate [Mbps]
WT1	729	37	11.3	1000
WT2	513	204	177	678
WT3	2054	470	443	242
WT4	6159	981	561	30

Полученото закъснение за WT1 е вследствие на необходимост от

изчакване на влязъл за обработка пакет от ниско-приоритетен поток. Максималната стойност е при изчакване на цял пакет с максимална големина от поток WT4 (1522 байта) – формула 3.24. Закъсненията за останалите потоци зависят от кривата на пристигане на WT1 и от теглата им в WRR обслужването. Максималното закъснение се получава, когато е необходимо да се изчакат пакетите от поток WT1 и пълно обхождане на останалите опашки (т.е. ако тъкмо е минал редът на съответния поток).

### 3.2.4. Резултати от симулацията

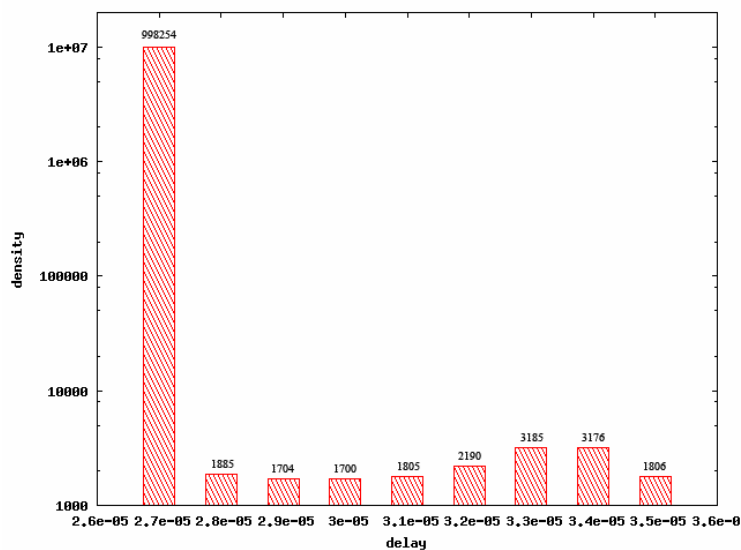
Както бе показано в предната секция, съществено е определянето на параметрите на потоците и мрежовия комутатор. Възможностите на използвания мрежов симулатор не позволяват дефиниране на трафик по зададените параметри, а същият се моделира чрез генератори. Параметрите на използвания в симулацията експоненциален трафик са съответно: packet size, burst time, idle time, rate. За привързването им към параметрите на аналитичния модел се използват специално изведени формули.



Фигура 3.9: Криви на пристигане на потоците в симулацията (логаритмичен мащаб)

Кривите на пристигане на всички потоци са стъпаловидни функции, като за периодичния поток стъпките са равномерни, а за останалите – неравномерни. Неравномерността на стъпките на потоците зависи от големината на пакетите и интервалите `idle_time` и `burst_time`. При промяна

на мащаба – за големи периоди от време, всички криви на пристигане се доближават по форма до линейна функция с наклон, равен на средната скорост на потока – фигура 3.9. Използваната пропускателна способност от поток WT1 е около 55 Мбит/сек. В частта от симулацията, където присъстват четирите потока, средната използвана пропускателна способност е 56 Мбит/сек, а максималната 94 Мбит/сек.

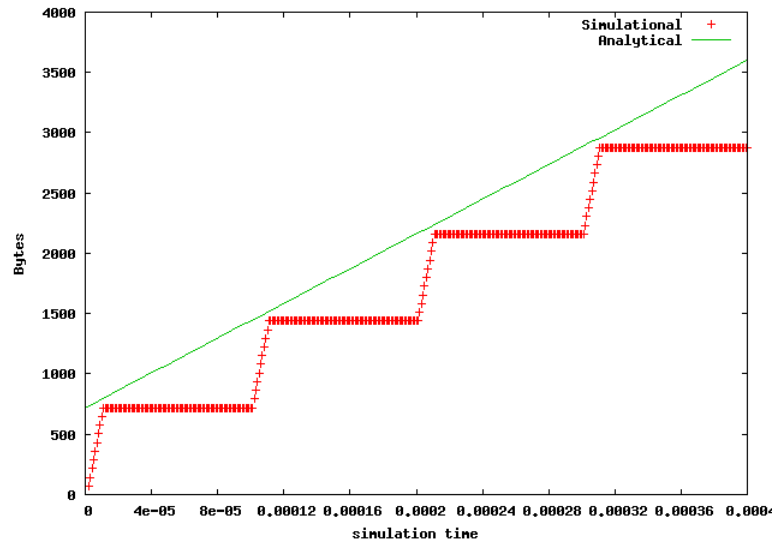


Фигура 3.12: Хистограма на закъснението на пакетите от поток WT1.

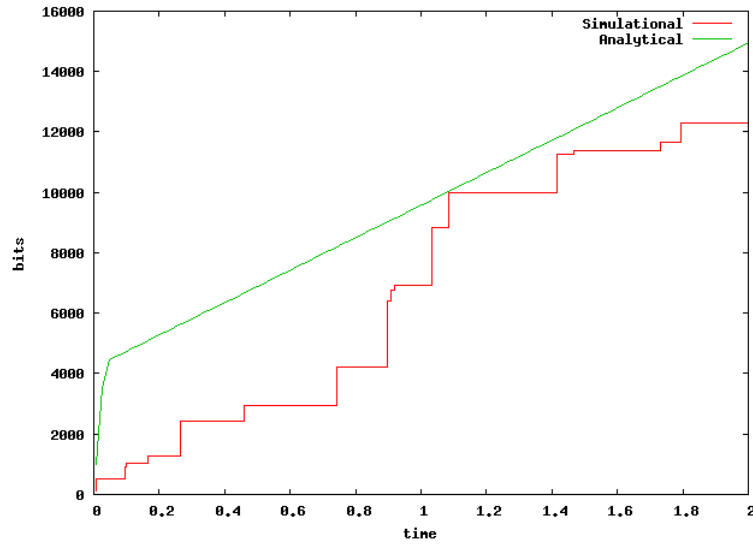
Основната част от пакетите – над 99.9%, от поток WT1 имат минимално закъснение, благодарение на приоритетното им обслужване в комутатора. На фигура 3.12 се наблюдава разпределението на броя пакети с различно закъснение. Това закъснение се генерира от необходимостта да бъде изчакано препращането на ниско-приоритетните пакети, което не може да бъде прекъснато.

### 3.2.5. Оценка на резултатите

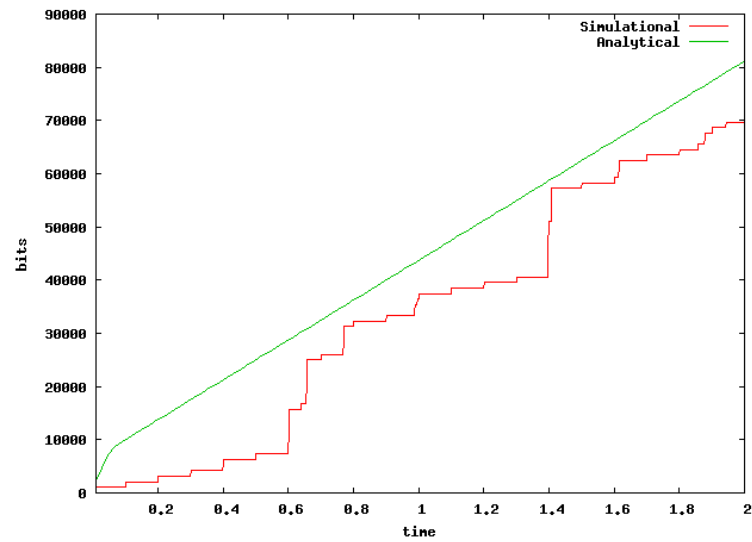
Сравнението на получените аналитични и симулационни резултати позволява проверката на достоверността на аналитичния модел и избора на параметри на отделните потоци. Интерес представлява съпоставянето на кривите на пристигане от симулацията и аналитично изчислените. Аналитичната и симулационната крива на пристигане за поток WT1 са показани на фигура 3.15, за WT2 – 3.16, за WT3 – 3.17, и за WT4 – 3.18.



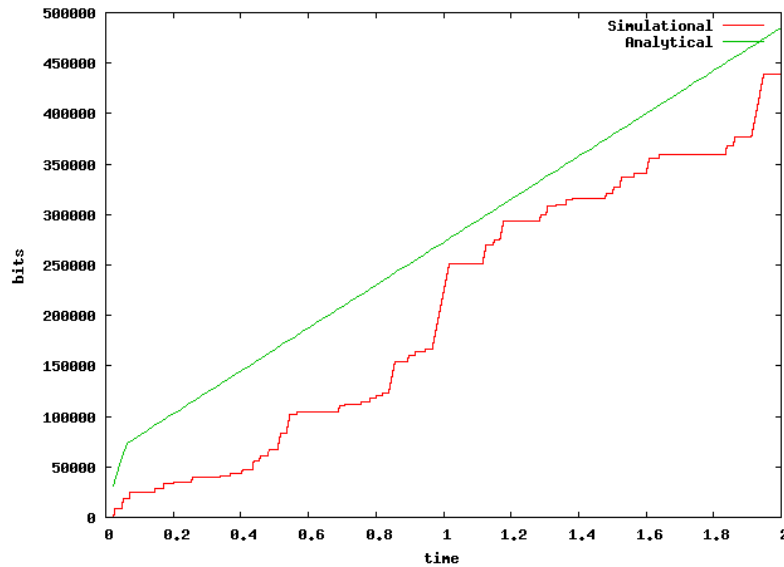
Фигура 3.15: Крива на пристигане на поток WT1.



Фигура 3.16: Крива на пристигане на поток WT2.



Фигура 3.17: Крива на пристигане на поток WT3.



Фигура 3.18: Крива на пристигане на поток WT4.

За поток WT1, в кривата на пристигане в симулацията се наблюдават равни участъци и участъци със стъпаловидно увеличаване на пристигащите пакети. Равните участъци са в периода на неактивност, а между тях се стартират няколко поредни периодични източника през малки интервали от време. Останалите потоци имат случаен характер на изпращане на пакетите, което е видно от графиките. На фигурите се вижда, че кривите на пристигане на всички потоци от симулацията са ограничени от аналитично определените, т.е. параметрите на всички потоци са подбрани коректно.

Другият параметър, по който се съпоставят аналитичните и симулационните резултати, и който е от основно значение за настоящето изследване, е закъснението на отделните потоци. Минималното, средното и максималното закъснение на всички потоци от симулацията, съпоставени с аналитично определеното ограничение на закъснението, са показани в таблица 3.6. Определените в симулационното изследване стойности за закъснението не надминават определените аналитично гранични стойности, а за потоците WT3 и WT4 симулационните резултати са значително по-ниски от граничните. Това може да се обясни с много малката вероятност да се прояви възможно най-лошият сценарий на



едновременно пристигане на пакети от трите ниско-приоритетни потока и съвпадение с периода на изпращане на периодичния поток.

Таблица 3.6: Закъснение на пакетите

Flow	Симуляционно определено закъснение, [ms] min / avg / max	Аналитично определено закъснение, [ms]
WT1	27 / 27 / 35	37
WT2	37 / 38 / 201	204
WT3	28 / 77 / 290	470
WT4	28 / 75 / 248	981

### Изводи

Предложен е аналитичен модел за определяне на виртуалното закъснение и запаса в Интернет базирани РВС, използващи Fast/Gigabit Ethernet и управляем комутатор с CoS. Моделът е базиран на математическия апарат на „Network Calculus” и определя граничните стойности на закъсненията и запаса.

Предложен е сценарий за симулационно изследване на закъснението и загубата на пакети в локална мрежа, използваща Fast/Gigabit Ethernet и управляем комутатор с Class-of-Service. Предложени са модели за генериране на типовете трафик в системата – периодичен, фонов, за инцидентен обмен на големи пакети и за администриране на мрежата.

Определени са аналитично максималните закъснения в система с управляем комутатор и четири информационни потока – един периодичен и три T-SPEC, при прилагане на приоритетна обработка в комутатора по схема 1P3Q1T, на базата на сценария за симулационно изследване.

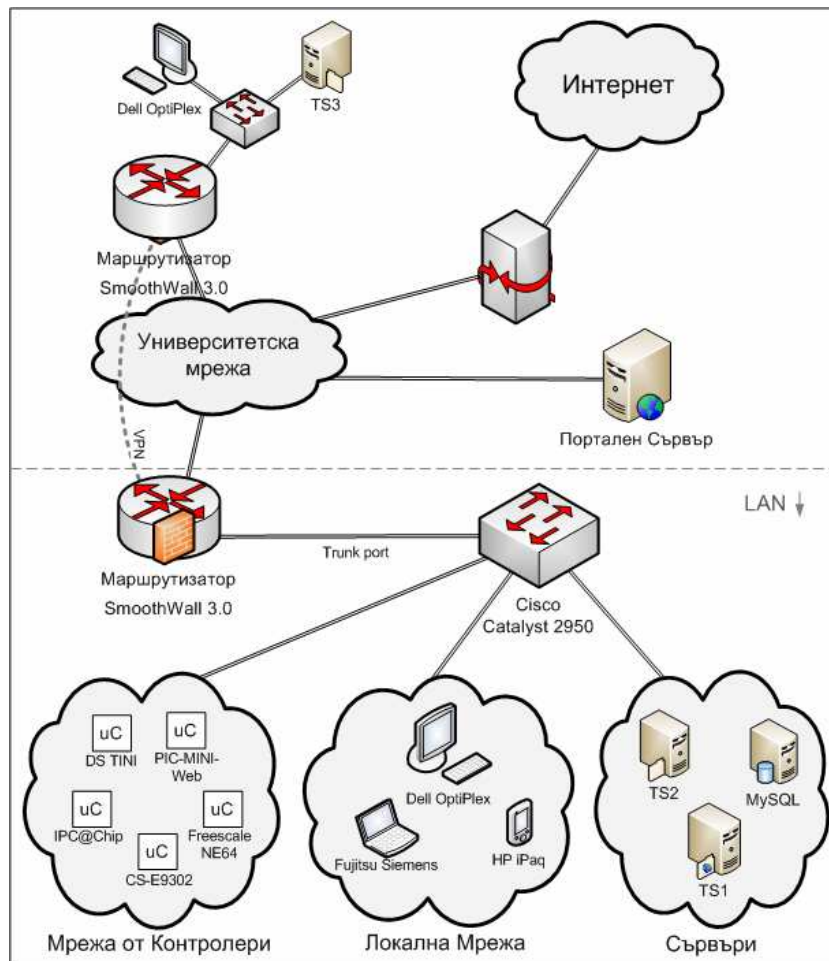
Предложени са резултати от симулационно изследване на закъснението и загубата на пакети в локална мрежа от контролери с фонов трафик, използваща Fast/Gigabit Ethernet и управляем комутатор. Резултатите са сравнени с аналитично определените за верификация на аналитичния модел.

## ***Глава 4: Експериментално изследване на реализации на Интернет базирани PBC***

В настоящата глава са представени направените насочени експериментални изследвания на комуникацията в мрежа от контролери, за да се проверят в лабораторна среда параметрите на комуникацията в локална мрежа от ВМС. Представени са, също така, и проведените насочени експерименти, доказващи работоспособността на предложената в глава 2 многослойна архитектура клиент-сървър за реализация на Интернет базирани PBC.

### **4.1. Експериментална разпределена вградена система за следене и контрол на отдалечени обекти.**

За провеждането на насочените експерименти е проектирана и изградена експериментална мрежа. В нея са включени различни по тип и функционалност ВМС, за да се оцени представянето на различните реализации на операционна система, TCP/IP стек, файлова система, Web сървър. Те са подбрани като представители на различни класове ВМС: висок клас системи, които имат сравнително голям изчислителен ресурс, 32 битов процесор и използват операционни системи с общо предназначение; среден клас системи, използващи 16 битов процесор и операционна система за работа в реално време; същият клас системи, но без операционна система за работа в реално време, а интегрирана Java виртуална машина; 8 битови ВМС, където няма операционна система, а приложенията и програмното осигуряване за работа с апаратната част и комуникацията са реализирани съвместно. Освен ВМС, в експерименталната мрежа са включени и сървъри за услуги, приложни сървъри, сървър за събиране на журнална информация, сървър с бази от данни, които работят на слоя за Услуги от многослойния модел.



Фигура 4.1: Топология на експерименталната мрежа.

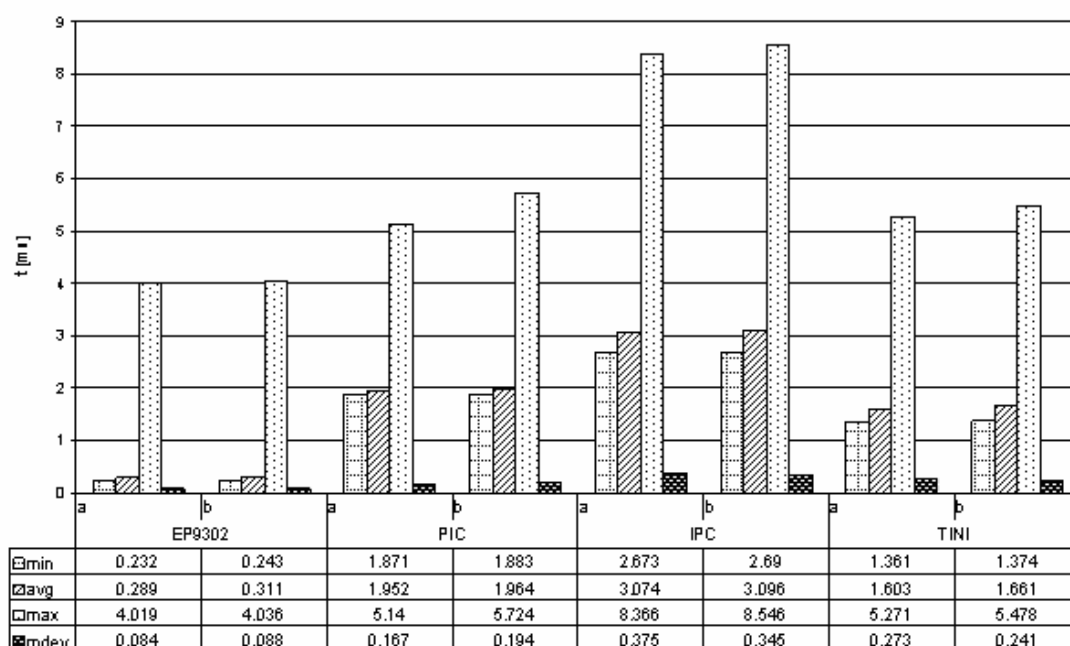
## 4.2. Експериментална оценка на параметрите на комуникацията в мрежа от ВМС.

В мрежата от контролери основната комуникация е от типа Master/Slave, като подчинените устройства са самите контролери. Те рядко са инициатори на предаване на данни. Основният тип комуникация, върху който може да се съсредоточи изследването, е Заявка/Отговор.

### 4.2.1. Оценка на клиент/сървър комуникацията на ВМС с вградени мрежови средства.

Първият предложен сценарий цели да се отчете времето за клиент/сървър комуникация на мрежово ниво при всяка от вградените системи в локалната мрежа. В този сценарий се използват възможностите на протокола ICMP и командата *ping*. При първия експеримент всяка от вградените системи е свързана директно към тестов компютър и от него

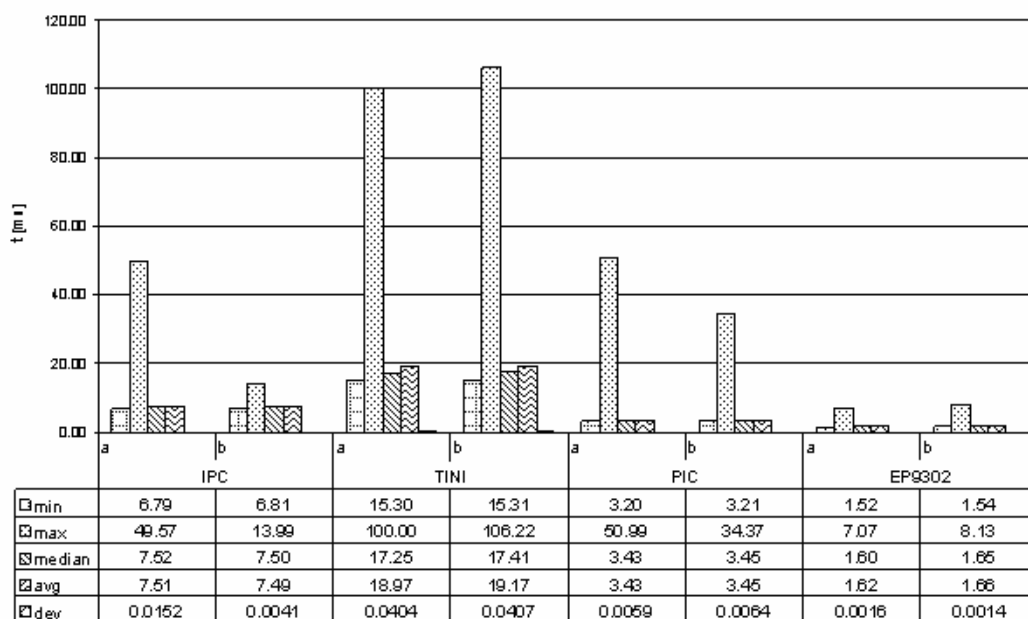
към вградената система се изпращат голям брой малки по размер ICMP заявки. Програмата (ping) отчита RTT за всеки пакет и след получаване на всички отговори определя минималната, максималната и средната стойност на този параметър и девиацията му. След това се повтаря същият експеримент, но вместо директно свързани, вградените системи и тестовият компютър са свързани към комутатора. Резултатите от двата експеримента са показани на фигура 4.2, означени съответно с буква „a” и буква „b”. Имайки предвид ниската натовареност на мрежата и комутатора, наличната пропускателна способност и липсата на загубени пакети, можем да заключим, че основното забавяне произтича от обработката в комуникационния стек на вградената система. Това е причина и за големите разлики в закъсненията при различните вградени системи. Тези разлики могат да се обяснят със специфичните характеристики на съответните вградени системи.



фигура 4.2: Измерени стойности за ICMP RTT за отделните контролери

За по-реална оценка на комуникацията трябва да се използват приложни протоколи, които работят в мрежи от контролери – CNDEP. С този протокол се провеждат няколко експеримента, за да се определи

забавянето в комуникацията на приложно ниво. Първо се свързват директно тестов компютър и вградена система, като на вградените системи се стартира CNDEP сървър, а на тестовия сървър се стартира клиент. Към контролерите в мрежата се изпраща CNDEP заявка и се изчаква отговорът, като се отчита времето от изпращане на заявката до получаване на отговор. Резултатите от двата експеримента са показани на фигура 4.3.

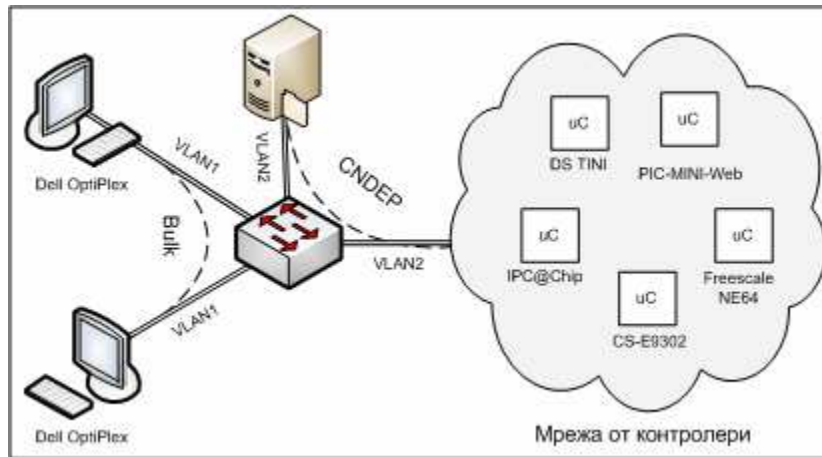


Фигура 4.3: Измерени стойности за CNDEP закъснението за контролерите

И при тези експерименти се наблюдава разлика между директното свързване и свързването през комутатор от порядъка на 0.01-0.0015 милисекунда, което е много близко до определеното при ICMP. От това може да се направи извод, че предположението, че комутаторът внася закъснение от порядъка на 0.01 милисекунди е достоверно.

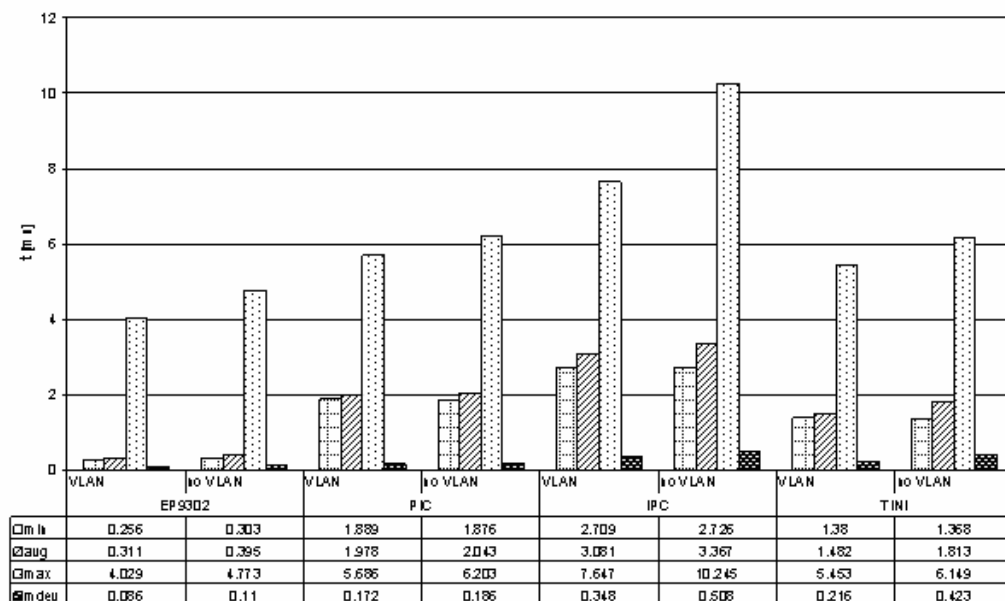
#### 4.2.2. Оценка на комуникацията при използването на виртуални локални мрежи.

Вградените системи и тестовият сървър са свързани към комутатора, като контролерите и сървърът са поставени в една и съща виртуална локална мрежа, а в друга виртуална локална мрежа са свързани компютри, обменящи фонов трафик. Топологията на мрежата за тези експерименти е показана на фигура 4.5.

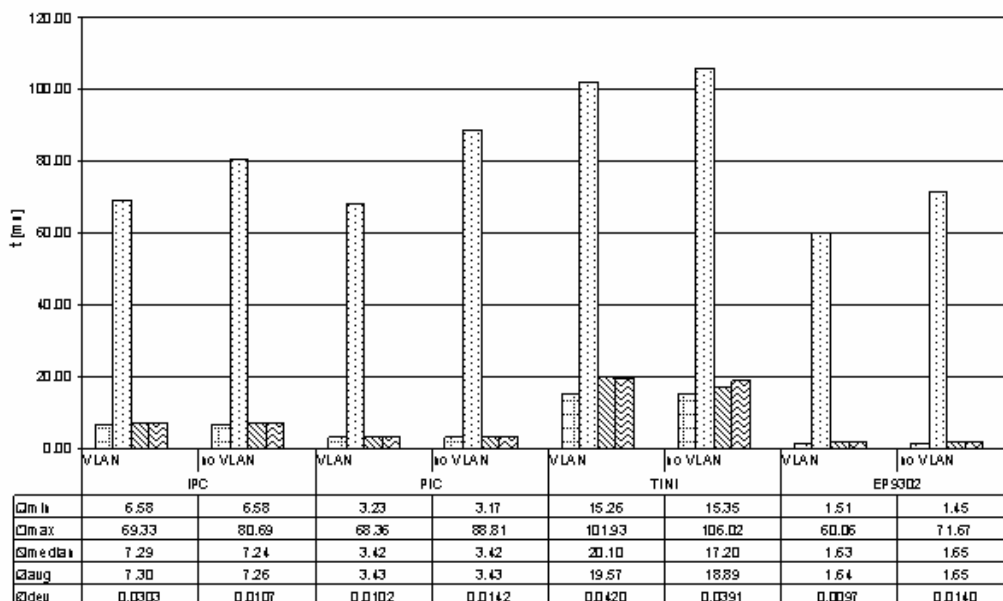


Фигура 4.5: Експериментална топология за оценка на интерференцията между виртуалните локални мрежи в комутатора.

Комутаторът се конфигурира така, че всичките му портове са в една виртуална локална мрежа с изключение на два. Към тези два порта се свързват тестовият компютър и съответната вградена система, с която се провеждат експерименти. След това тестовият компютър и вградената система се включват в други портове, които са в основната виртуална локална мрежа. Проведени са експерименти за определяне на ICMP RTT и на закъснението на клиент/сървър комуникацията с приложния протокол CNDEP, като резултатите са показани съответно на фигури 4.6 и 4.7.



Фигура 4.6: Стойности за ICMP RTT при използване на комутатор с виртуални локални мрежи.



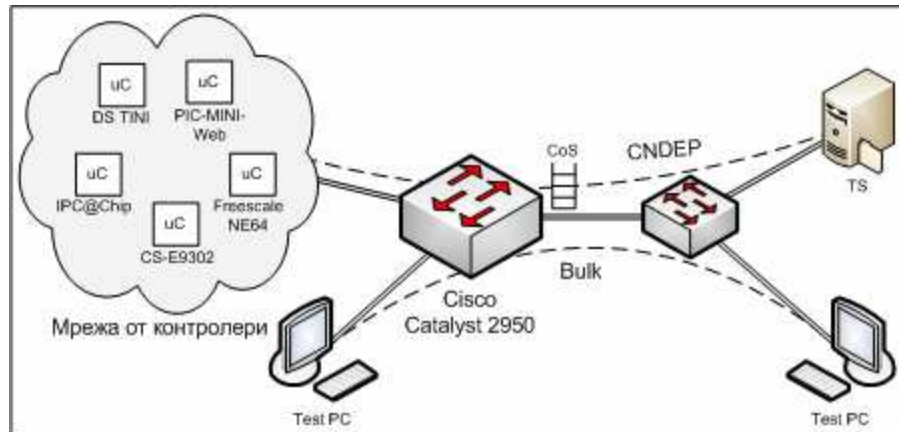
Фигура 4.7: Стойности за закъснението на клиент/сървър комуникация на протокола CNDEP при използване на комутатор с виртуални локални мрежи.

Експериментите се провеждат в условие на силно натоварване на комутатора. Забелязва се, че обособяването на контролерите в отделна виртуална мрежа не води до подобрене на параметрите, т.е. е налице интерференция между отделните виртуални мрежи. Резултатите са по-добре изразени за ICMP, отколкото за CNDEP, тъй като при приложния протокол вариацията на закъснението е по-висока и зависи повече от самите контролери, отколкото от комутатора.

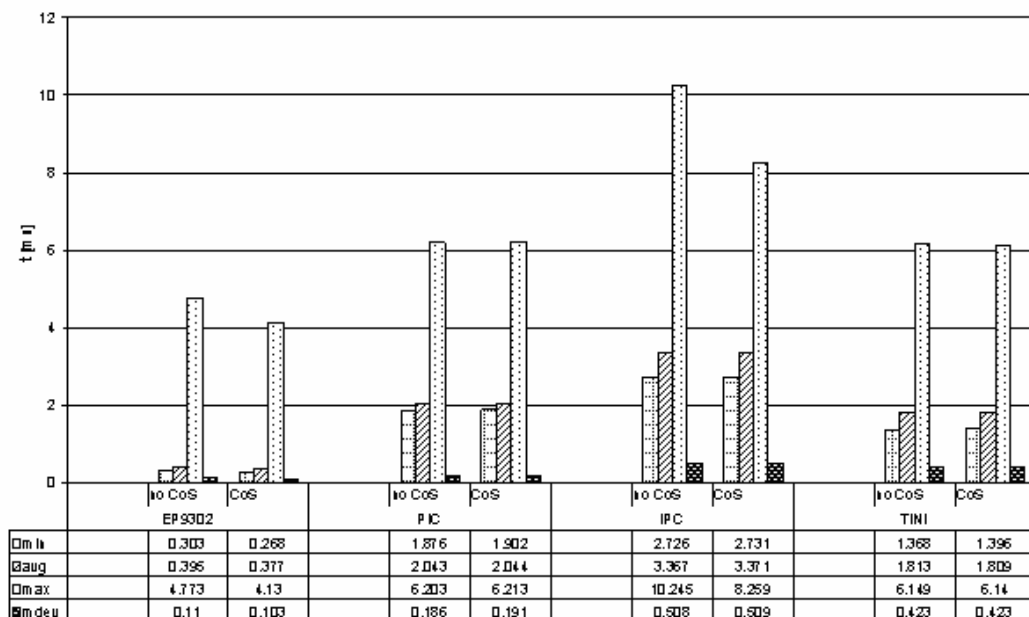
#### 4.2.3. Оценка на приложението на IEEE 802.1p за управление на трафика.

За да се наблюдава работата на IEEE 802.1p и приоритетното управление на опашките в комутатора, е предложен експериментален сценарий, който включва няколко трафика с различни приоритети и параметри. Изходящите портове на комутатора се конфигурират да реализират 1P3Q1T управление на опашките. Това включва една приоритетна опашка, която се обслужва винаги, когато има пакети. Останалите три опашки са конфигурирани в WRR с отношения 75:25:5. В комутатора се прилага маркиране на трафика, като фоновият трафик се

привързва към WRR опашките, а трафикът от контролерите – към приоритетната опашка. За да се наблюдава приоритетното обслужване, обаче, е необходимо и фоновият трафик, и трафикът от контролерите да бъдат насочени към един и същ изходящ порт на комутатора, тъй като има отделни опашки за всеки такъв – фигура 4.8.



Фигура 4.8: Експериментална топология за оценка на работата на CoS в комутатора.

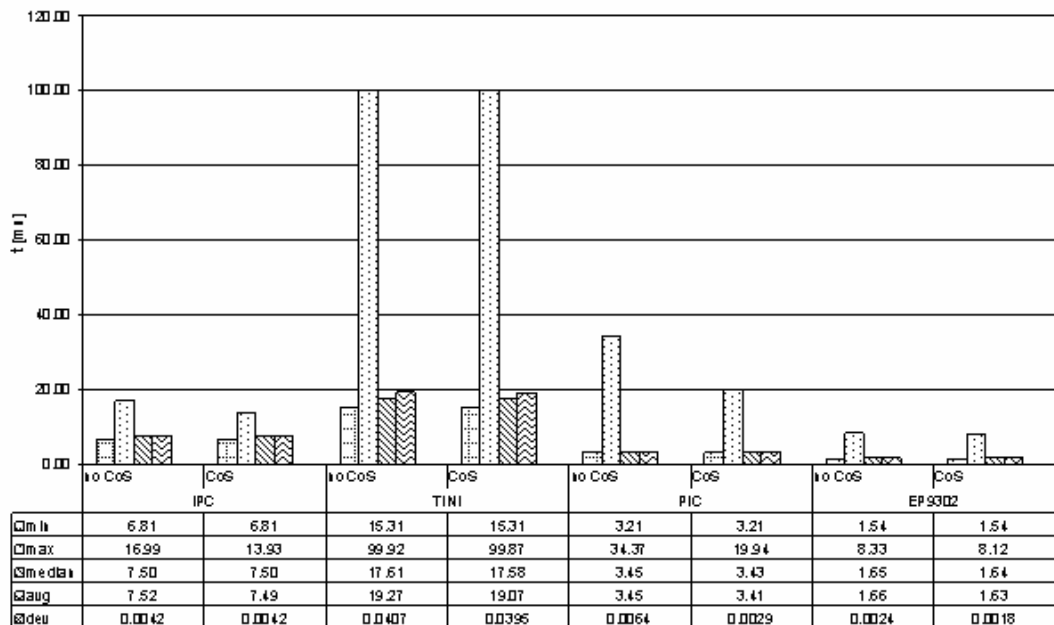


Фигура 4.9: Закъснение на ICMP при използване на CoS.

Резултатите за ICMP RTT (фигура 4.9) показват, че използването на приоритетно обслужване на трафика от контролерите не влияе върху минималните стойности. Наблюдава се леко понижаване на средните стойности в следствие на приоритетното обслужване. Поради факта, че



проведените експерименти с ICMP са адаптивни по отношение на периода на изпращане, резултатите не са силно изразени. Резултатите от експериментите с приложния протокол CNDEP (фигура 4.10) показват също стабилно ограничаване на максималното закъснение и леко намаляване на средното закъснение и вариацията му, като тези резултати са по-изразени, отколкото при ICMP.



Фигура 4.10: Закъснение на CNDEP при използване на CoS.

Може да се заключи, че прилагането на правилни политики за класифициране на услугите спомага за ограничението на максималните закъснения и колебанието на закъснението на високоприоритетния трафик, което е и важното при проектиране на РВС, работещи в реално време. Но това ограничаване не е силно изразено при експерименталните резултати, тъй като използваните ВМС внасят много случайни забавяния от комуникационния стек и достъпа до апаратната част.

#### 4.2.4. Обобщение на резултатите.

Използването на приложни протоколи, реализирани на Java, показват високи стойности на закъснението и вариацията му при силно натоварване, заради непредвидимия характер на освобождаване на ресурси от виртуалната машина и Garbage Collector. При вградените системи, където

няма операционна система, средните стойности за закъсненията от обработка са малки, но силно се влияят от другите приложения, работещи на системата, което води до силни вариации в закъснението. Най-добро представяне очаквано показват високият клас ВМС, с много изчислителни ресурси и мрежов контролер, работещ на 100 Мбит/сек.

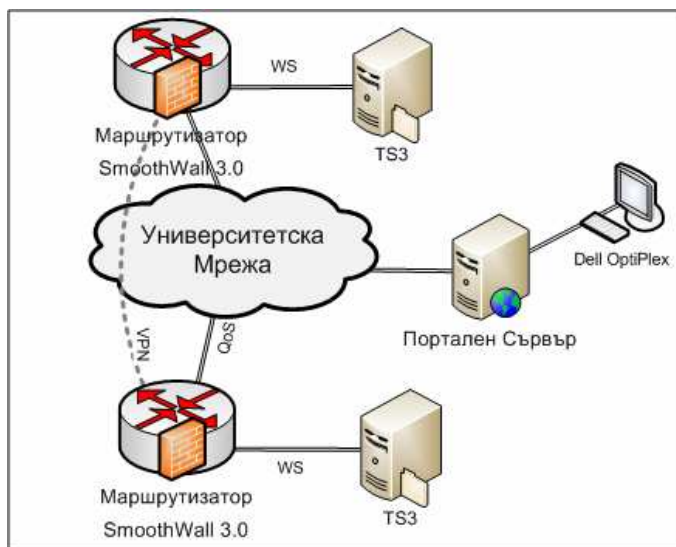
Използването на комутатор внася много малко, почти постоянно закъснение в комуникацията от порядъка на сто микросекунди при слабо натоварване. Разделянето на различните типове трафик в отделни виртуални локални мрежи не подобрява представянето при силно натоварване на мрежата. Използването на маркиране и приоритетно обслужване на трафика от контролерите позволява да се лимитират закъсненията на пакетите, като се ограничава до минимум загубата на пакети от нископриоритетния трафик. Прилагането на политики за CoS подобрява значително параметрите на локалната мрежа, но може да се използва за изграждане на РВС, само когато закъснението в самата ВМС е ниско. Когато основният източник на закъснение и нестабилност е комуникационният стек на използваната ВМС, комуникация в реално време не може да се осъществи със стандартни средства за оптимизация в комуникационната подсистема.

Отчетените закъснения за различните ВМС показват стойности, които позволяват прилагането им в системи за отдалечено следене на сензори и технологични обекти, където има забавяне в системата за отчитане (забавяния от стотици милисекунди). Само някои от представените ВМС, предимно от висок клас, имат максимални и средни закъснения, които позволяват приложението им в системи за отдалечен и разпределен контрол, но такива, работещи с не много висока скорост (забавяния от десетки милисекунди). Нито една от представените ВМС не позволява реализацията на системи в реално време със строги изисквания (като управление на многоосови мотори), които имат изисквания за закъснения

от порядъка на десетина микросекунди с вариация от микросекунда.

### 4.3. Оценка на Middleware технологията в слоя на услугите.

Оценката на Middleware технологиите и информационното взаимодействие в слоя за услуги изисква изграждането на специална опитна постановка. Предложената топология за провеждане на експериментите е показана на фигура 4.11.



Фигура 4.11: Топология за оценка на Middleware технологията.

#### 4.3.1. Оценка на XML базиран протокол за извличане на данни от контролери.

Предложено е експериментално изследване на версия на CNDEP, използваща XML кодиране на данните – xCNDEP. Следените параметри са размерът на заявката, размерът на отговора, времето за заявка/отговор и девиацията на това време. Резултатите са представени в таблица 4.1.

Таблица 4.1: Експериментална оценка на xCNDEP.

Controller	Command	Request size [byte]	Response size [byte]	Delay [ms]	$\sigma$ [ms]
IPC@CHIP	Test	234	200	12,847	0,121
	Get Temp	241	286	103,025	0,130
	Get Hum	238	286	141,691	0,139
DS TINI	Test	234	200	132,666	0,342
	Get Temp	241	286	103,025	0,130
	Get Hum	238	286	141,691	0,139

Забелязва се, че размерите на заявките и отговорите не се променят много за различните команди, както и времето за заявка/отговор. Може да се заключи, че основната част от забавянето се дължи на XML

кодиране/декодиране – около 80 милисекунди.

#### 4.3.2. Оценка на информационното взаимодействие при обмен на данни с Web услуги.

Когато са реализирани всички слоеве на многослойния модел, информационното взаимодействие в слоя за услуги трябва да има възможност за работа в Интернет среда. По тази причина следващите проведени експерименти оценяват предаването на двоични данни през XML кодирани Web услуги. Експерименталната постановка включва три сървъра с Web услуги. Основно се наблюдава закъснението и размера на пакетите при предаване на графики чрез Web услуги. За предаването на изображението са използвани два различни метода – SOAP with Attachments (DIME) и binary encoded XML..

#### 4.3.3. Оценка на методите за защита на Web услуги.

При изграждането на Интернет базирани РВС основно място заемат надеждността и сигурността. Интерес представлява забавянето, което се внася от прилагането на политики за сигурност. За целта се изследва забавянето от прилагане на различни политики за сигурност (фигура 4.12).



Фигура 4.12: Сценарии за изследване на методите за защита при Web услуги.

Основният проблем при използването на WS-Security е големият процент служебна информация. Размерът на служебната информация в съобщението за трите сценария с WS-Security е показано на таблица 4.2.

Таблица 4.2: Служебна информация на WS-Security за SOAP съобщенията

	SOAP size [bytes]	WSS header size [bytes]	Overhead [%]
scenario2	3370	1950	57.86
scenario3	2063	1207	58.51
scenario4	4907	3833	78.11

Служебната информация е около 50-60%, когато се използва само кодиране на XML съобщението или цифрово подписване, но при комбинацията от двете може да достигне до 80%. Тези стойности силно намаляват, когато се подписват или кодират само части от съобщението, което е и основното предимство на прилагането на WS-Security пред стандартните методи за мрежова сигурност.

#### 4.3.4. Обобщение на резултатите.

От проведените експерименти за оценка на Middleware технологията може да се заключи, че използването на Web услуги е подходящо за реализиране на информационното взаимодействие в Интернет базирани PBC, изградени по многослойни архитектури. Фактът, че технологията на Web услугите използва HTTP като преносен протокол, усложнява използването на политики за качество на услугите (QoS), но позволява гъвкави, платформено независими решения, работещи в Интернет среда. При необходимост от обмен на двоични данни чрез Web услуги трябва да се вземе предвид размера на тези данни и универсалността на решението. Използването на XML кодирани двоични данни е универсално и следва спецификациите на W3C, но внася значителни забавяния при предаване и обработка за големи по обем двоични данни. Използването на прикачени файлове към SOAP съобщението не увеличава размера на изпращаните данни и има по-малко забавяне, но не позволява прилагане на политики за мрежова сигурност като WS-Security. Прилагането на методи за защита на SOAP съобщението от подмяна и несанкциониран достъп внася голямо количество служебна информация, която може дори да надмине потребителските данни. За да се използва ефективно, трябва да се кодира

само конфиденциалната част от съобщението, но да се подпише цифрово цялото съобщение.

### **Изводи**

Предложена е експериментална мрежа за изследване на поведението на Интернет базирани РВС, реализирани на база на многослоен клиент-сървър модел и Fast/Gigabit Ethernet. Предложена е топология на мрежата, която да позволява провеждането на широк набор експерименти. Използвани са различни по тип и клас ВМС с различно количество памет, периферия и приложения.

Предложени са резултати от насочени експериментални изследвания на параметрите на комуникация в локална мрежа от контролери, използваща Fast/Gigabit Ethernet и управляем комутатор с 802.1p и 802.1Q.

Предложени са резултати от насочени експериментални изследвания на информационното взаимодействие в РВС, реализирана на базата на многослоен клиент-сървър модел. Изследванията включват оценка на приложението на архитектурата на Web услугите като Middleware технология в хетерогенни РВС с ниска степен на гранулярност.

### *Приноси на дисертационният труд*

Изследванията в настоящия дисертационен труд могат да се резюмират в следните научни, научно-приложни и приложни резултати:

Научни:

1. Предложен е абстрактен многослоен модел за реализиране на Интернет базирани РВС.

2. Предложен е аналитичен модел за определяне на виртуалното закъснение и запаса в Интернет базирани РВС, използващи Fast/Gigabit Ethernet и управляем комутатор с Class-of-Service.

Научно-приложни:

3. Проектиран е приложен протокол, базиран на UDP, който реализира информационното взаимодействие в слоя за данни.

4. Направено е симулационно изследване на закъснението и загубата на пакети в локална мрежа, използваща Fast/Gigabit Ethernet и управляем комутатор с Class-of-Service.

5. Проектирана е и изградена експериментална мрежа за изследване на поведението на Интернет базирани РВС, реализирани на база на многослоен клиент-сървър модел и Fast/Gigabit Ethernet.

6. Експериментално са определени времевите параметри на информационното взаимодействие в РВС, реализирана на базата на многослоен клиент/сървър модел.

*Публикации във връзка с дисертационния труд*

- [P1]. Spasov, G. , **N. Kakanakov**, „CGI-based applications for distributed embedded systems for monitoring temperature and humidity,” In Proc. CompSysTech'04, Ruse, Bulgaria, pp. I.6, 2004.
- [P2]. Спасов, Г., **Н. Каканакон**, “Разпределена вградена система за мониторинг на температура и влажност,” Списание “Електроника и Електротехника” бр. 3-4, стр. 38-44, 2005.
- [P3]. **Kakanakov, N.**, G. Spasov, „Adaptation of Web service architecture in distributed embedded systems,” In Proc. of CompSysTech'05, Varna, Bulgaria, pp. IIIB.10, 2005.
- [P4]. **Kakanakov, N.** “Experimental analysis of client/server applications in embedded systems,” In Proc. ELECTRONICS, book 4, pp. 97-102, 2005.
- [P5]. **Kakanakov, N.** “An application of web services for distributed measurement,” In Proc. ISMC (JVA) Youth Session, pp.55-60, 2006.
- [P6]. **Каканакон, Н.**, “Web базирани модели за Разпределена Автоматизация,” списание “Автоматика и Информатика”, бр. 3, стр. 44-48, 2006.
- [P7]. **Kakanakov, N.**, I. Stankov, M. Shopov, and G. Spasov, “Controller Network Data Extracting Protocol – design and implementation,” In Proc. CompSysTech'06, Veliko Tarnovo, Bulgaria, p. IIIA.14, 2006.
- [P8]. **Kakanakov, N.**, M. Shopov, and G. Spasov, „A new web based multi-tier model for distributed automation systems,” Journal “Information Technology and Control”, vol. 2, pp.44-48, 2006.
- [P9]. **Kakanakov, N.**, M. Shopov, I. Stankov, and G. Spasov, "Web Services and Data Integration in Distributed Automation and Information Systems in Internet Environment," Journal “International Review on Computers and Software”, vol. 1, no. 3, pp. 194-201, 2006.
- [P10]. **Kakanakov, N.** and M. Shopov, “Evaluating controller network data extracting protocol for embedded devices,” In Proc. Electronics ET'06, Sozopol, Bulgaria, b. 3, pp. 15-20, 2006.
- [P11]. **Kakanakov, N.**, M. Shopov, G. Spasov, H. Hristev, "Performance Evaluation of Switched Ethernet as Communication Media in Controller Networks," In Proc. CompSysTech'07, Russe, Bulgaria, p. IIIA.8, 2007.
- [P12]. **Kakanakov, N.**, M. Shopov, G. Spasov, “Time-Delay Simulation Analysis of Local Controller Networks,” In Proc. CompSysTech08, Gabrovo, Bulgaria, p. IIIA.12, 2008.
- [P13]. **Kakanakov, N.**, M. Shopov, G. Spasov, “Experimental Analysis of CoS Performance In Local Controller Networks,” In Proc. Electronics ET'08, Sozopol, Bulgaria, Book 1, pp. 81-86, 2008.