



**ДЕПАРТМАН ЗА ПОСЛЕДИПЛОМСКЕ СТУДИЈЕ
БЕОГРАД**

**МАСТЕР СТУДИЈЕ
СТУДИЈСКИ ПРОГРАМ:
САВРЕМЕНЕ ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ**

МАСТЕР РАД

**КОМПАРАТИВНИ ПРИКАЗ САВРЕМЕНИХ
ТЕЛЕКОМУНИКАЦИОНИХ МРЕЖА СА ПРЕДЛОГОМ
ИМПЛЕМЕНТАЦИЈЕ МРЕЖЕ ЗА НАДЗОР И
УПРАВЉАЊЕ ЗА РАД У БЕЗБЕДНОМ ОКРУЖЕЊУ**

МЕНТОР:

Проф.др. Младен Веиновић

СТУДЕНТ:

Дејан Милошевић, дипл.инж.

БЕОГРАД, 2016.ГОДИНЕ

САЖЕТАК

Напредак технологија у савременим телекомуникацијама поставио је све сложеније и обимније захтеве корисника услуга. У циљу опслуживања крајњих корисника дошло је до убрзаног развоја уређаја, капацитета, услуга, што је са собом донело и потребу за централизовањем и обједињавањем надзора и управљања.

У овом раду извршен је кратак приказ телекомуникационих система са предлогом имплементације мреже за надзор и управљање за рад у безбедном окружењу. Концепт централизованог надзора и управљања разматран је на моделу предузећа или државног органа који поседује сопствену телекомуникациону инфраструктуру.

Радам је обухваћен кратак преглед тренутно перспективних произвођача комутационих, мултиплексних, радио-релејних и мрежних уређаја уз теоријско и практично разматрање могућности, потреба и захтева за увођењем мреже за надзор и управљање. Као део наведеног концепта указано је на значај и улогу безбедног окружења за рад коришћењем економичних и комерцијалних решења.

Циљ овог рада је упознавање са савременим телекомуникационим системима и основним принципима и могућностима за реализацију централизованог надзора и управљања у безбедном окружењу.

Кључне речи: телекомуникациони систем, комутациона мрежа, приступно-транспортни систем, радио-релејна мрежа, рачунарска мрежа, мрежа за надзор и управљање, IPSec.

СПИСАК СЛИКА

Слика 2.1 Основни модел телекомуникационог система.....	8
Слика 2.2. OSI референтни модел.....	12
Слика 2.3 TCP/IP референтни модел.....	14
Слика 2.4 Упоредни графички приказ OSI и TCP/IP референтног модела	15
Слика 3.1 Однос телекомуникационе мреже и <i>TMN</i>	20
Слика 3.2 Управљачки слојеви у оквиру <i>TMN</i> -а	26
Слика 4.1 Спољашњи изглед централе <i>MX-One</i>	28
Слика 4.2 Имплементација система преко групног степена.....	30
Слика 4.3 Пример увезивања елемената комутационе мреже у мрежу за надзор и управљање.....	31
Слика 4.4 Приступни PDH уређај ФМ 8x2 у радној станици	35
Слика 4.5 Транспортни мултиплексни уређај ОДС 622	36
Слика 4.6 Пример имплементације уређаја OTS/ODS 622 у сложеној телекомуникационој мрежи	38
Слика 4.7 Модел мреже за надзор и управљање телекомуникационом мрежом приступно-транспортних уређаја.....	41
Слика 4.8 Приказ радне површине у апликацији СУНЦЕ-М	42
Слика 4.9 Радио-релејни уређаји NERA фамилије са унутрашњом и спољном јединицом	43
Слика 4.10 Организација надзора и управљања PPMp.....	45
Слика 4.11 Графички приказ стања мреже у апликацији <i>Net Master</i>	47
Слика 4.12 Приказ грешака на уређају у мрежи	48
Слика 4.8 Пример радног графичког окружења софтвера „Dude“	50
Слика 5.1 Приказ рада мреже базиране на IPSec протоклу	55
Слика 5.2 Приказ заглавља АН пакета.....	56
Слика 5.3 Приказ заглавља ESP пакета.....	57
Слика 5.4 Приказ рада IKE протокола	58
Слика 6.1 Организација мреже за надзор и управљање телекомуникационом мрежом дигиталних централа.....	65
Слика 6.2 Организација мреже за надзор и управљање телекомуникационом мрежом приступних и транспортних мултиплексних система	66
Слика 6.3 Организација надзора и управљања радио-релејном мрежом	68
Слика 6.4 Организација надзора и управљања рачунарском мрежом	69
Слика 6.5 Предлог реализације заштите за рад у безбедном окружењу.....	71

САДРЖАЈ

СПИСАК СЛИКА	3
1.МЕТОДОЛОГИЈА НАУЧНОГ ИСТРАЖИВАЊА	6
1.1 Предмет истраживања	6
1.2 Циљеви и задаци.....	6
1.3 Истраживачке хипотезе	6
1.4 Методе истраживања и ток истраживачког процеса	7
2. ТЕЛЕКОМУНИКАЦИОНЕ МРЕЖЕ И МРЕЖЕ ЗА НАДЗОР И УПРАВАЊЕ	8
2.1 Телекомуникациона мрежа (систем)	10
2.2 Референтни модели заступљени у телекомуникационим мрежама за надзор и управљање.....	11
2.2.1 OSI (Open Systems Interconnection) референтни модел	12
2.2.2 TCP/IP (Transmission Control Protocol/Internet Protocol) референтни модел ..	13
2.2.3 Поређење OSI и TCP/IP референтног модела.....	15
3. ПЛАНИРАЊЕ МРЕЖА ЗА НАДЗОР И УПРАВЉАЊЕ.....	16
3.1 Процес планирања телекомуникационих мрежа.....	16
3.1.1 Чиниоци који утичу на планирање телекомуникационих мрежа.....	17
3.1.2 Функционално распоређивање организацијских целина	18
3.2 Мреже за надзор и управљање	19
3.2.1 Подела мрежа за надзор и управљање	21
3.2.2 Мреже за надзор и управљање јавним телекомуникационим мрежама	22
3.2.2 Мреже за надзор и управљање телекомуникационим мрежама посебне намене	23
3.2.3 Сагледавање чинилаца који описују мрежу за надзор и управљање	24
4. КОМПАРАТИВНИ ПРИКАЗ САВРЕМЕНИХ ТЕЛЕКОМУНИКАЦИОНИХ МРЕЖА СА МОГУЋНОСТИМА УДАЉЕНОГ ПРИСТУПА	27
4.1 Комутациони систем и могућност имплементације мреже за надзор и управљање	27
4.1.1 Комутациони систем	28
4.1.2 Могућност имплементације мреже за надзор и управљање у комутационој мрежи.....	31
4.2 Приступно-транспортни (мултиплексни) систем и могућност имплементације мреже за надзор и управљање	33
4.2.1 Приступни уређаји	34
4.2.2 Транспортни уређаји.....	36
4.2.3 Могућност имплементације мреже за надзор и управљање приступно-транспортним (мултиплексним) уређајима	39
4.3 Радио-релејни систем и могућност имплементације мреже за надзор и управљање	42
4.3.1 Радио-релејни уређаји.....	43
4.3.2 Могућност имплементације мреже за надзор и управљање у радио-релејној мрежи.....	45
4.4 Рачунарска мреже и могућност имплементације мреже за надзор и управљање ..	48
5. КРИПТОЛОШКИ ПРИСТУП АНАЛИЗИ ЗАШТИТЕ МРЕЖА ЗА НАДЗОР И УПРАВЉАЊЕ ТЕЛЕКОМУНИКАЦИОНИМ УРЕЂАЈИМА.....	51
5.1 Улога и значај заштите информација у телекомуникационим системима	51

5.2 Потенцијални начини угрожавања мрежа за надзор и управљање телекомуникационим мрежама	52
5.3 Могућност реализације заштићеног преноса података	53
5.4 IPSec протокол.....	54
5.4.1 AH протокол	55
5.4.2 ESP протокол	56
5.4.3 IKE протокол	57
5.5 Могуће имплементације IPSec решења за потребе мрежа за надзор и управљање телекомуникационим мрежама	58
6. ИМПЛЕМЕНТАЦИЈА МРЕЖЕ ЗА НАДЗОР И УПРАВЉАЊЕ ТЕЛЕКОМУНИКАЦИОНИМ УРЕЂАЈИМА У БЕЗБЕДНОМ ОКРУЖЕЊУ	60
6.1 Сагледавање стања у телекомуникационим мрежама са предлогом модела реализације мреже за надзор и управљање.....	63
6.2 Предлог надзора и управљања системом комутације	64
6.3 Предлог надзора и управљања системом приступно-транспортних (мултиплексних) уређаја.....	66
6.4 Предлог надзора и управљања мрежом радио-релејних уређаја.....	67
6.5 Предлог надзора и управљања рачунарском мрежом	68
6.6 Имплементација безбедног окружења за рад мрежа за надзор и управљање телекомуникационом мрежом.....	69
ЗАКЉУЧАК.....	72
ЛИТЕРАТУРА.....	73

1. МЕТОДОЛОГИЈА НАУЧНОГ ИСТРАЖИВАЊА

1.1 Предмет истраживања

Предмет истраживања у овом раду је анализа савремених телекомуникационих мрежа и система са акцентом на сагледавању могућности удаљеног приступа у циљу имплементације мреже за надзор и управљање за рад у безбедном окружењу.

1.2 Циљеви и задаци

Научни циљ овог рада је систематизација знања о телекомуникационим мрежама и мрежама за надзор и управљање телекомуникационим мрежама у сврху имплементације стечених знања у хетерогену телекомуникациону мрежу предузећа.

На нивоу научног описа могуће је сагледати основне појмове о савременим телекомуникационим мрежама и системима, мрежама за надзор и управљање, савременим криптолошким приступима заштити информација, процесима имплементације система за надзор и управљање телекомуникационим мрежама.

На нивоу научне класификације могуће је уочити: карактеристике телекомуникационих мрежа, захтеве које је неопходно сагледати и испунити у циљу стварања услова за имплементацију, модел система заштите информација који се може применити у мрежи за надзор и управљање телекомуникационим системима.

Друштвени циљ овог рада огледа се у практичној примени безбедне имплементације мреже надзора и управљања телекомуникационом мрежом у предузећима са хетерогеном организацијом целина.

1.3 Истраживачке хипотезе

Општа хипотеза при изради овог рада је била:

Анализом препорука за формирање мрежа за надзор и управљање и сагледавањем карактеристика савремених телекомуникационих система имплементираних у предузећу доћи до модела имплементације мреже за надзор и управљање уређајима у безбедном окружењу.

Радне хипотезе при изради овог рада су биле:

- стицање основних знања о процесу имплементације мрежа за надзор и управљање у телекомуникационим мрежама
- упознавање карактеристика комутационих, мултиплексних, радио-релејних, мрежних и шифарских система
- анализа могућности имплементације централизованог надзора и управљања уређајима хетерогених телекомуникационих система
- имплементација безбедног окружења за функционисање мреже за надзор и управљање

1.4 Методе истраживања и ток истраживачког процеса

Приликом израде овог рада коришћене су следеће методе:

- метода дескрипције у циљу описа чињеница и процеса везаних за телекомуникационе системе, мреже за надзор и управљање и шифарске приступе заштити информација
- метода анализе која се користила за извођење закључака разврставањем сложених појмова на просте коришћена је током објашњавања основних појмова о телекомуникационим мрежама и уређајима, мрежама за надзор и управљање и савременим шифарским методама заштите информација
- компаративна метода допринела је сагледавању сличности телекомуникационих система у погледу могућности имплементације централизованог надзора и управљања уређајима
- метода синтезе је коришћена у сврхе обједињавања чињеница и извођења закључака и објашњења у сврхе захтева и потреба за имплементацијом мреже за управљање

2. ТЕЛЕКОМУНИКАЦИОНЕ МРЕЖЕ И МРЕЖЕ ЗА НАДЗОР И УПРАВАЊЕ

Потреба за комуницирањем кроз историју људске врсте показала се као једна од основних потреба за разменом информација. Комуникација се одвија кроз три основна правца: садржај, форму и циљ. Садржај комуникације комбинован са формом те садржине ствара облик поруке, а циљ је да буде упућена одређеном лицу или организацији. Комуникација заснована на размени порука користити се и у размени информација између разних врста система, уређаја, машина са циљем задовољења основних функционалности и управљања истим.

Телекомуникациона мрежа представља скуп формиран од телекомуникационе опреме, спојних путева и сервиса са јединственим циљем размене садржаја порука према адекватним правилима и стандардима дефинисаним за ту мрежу. Телекомуникациони системи засновани су на основном моделу који се базира на процесима преноса, комутације и сигнализације, а универзални модел је приказан на слици 2.1



Слика 2.1 Основни модел телекомуникационог система

Процесом усложњавања телекомуникационих мрежа, потреба за управљањем над тим мрежама временом је постајала све израженија и захтевнија. У почетном периоду развоја првих дигиталних уређаја и система није постојала могућност даљинског надзора и управљања над истим са удаљене локације. Запослени који су се бавили инсталацијом и одржавањем ових система да би квалитетно извршавали задатке и обавезе које се пред њих постављају морали су да инсталирају одређене апликативне софтвере на рачунарима и да комуницирају са опремом у оквиру самих локација где је опрема била инсталирана. Како су се реализовала планска проширења система и повећавала количина инсталиране опреме, тако су се и повећавали захтеви за надзором и управљањем. Сложеност проблема резултовала је идејом за формирањем нове,

посебне мреже за управљање телекомуникационом опремом и сервисима за које је она била намењена.

Увођењем оптичких спојних путева ширина пропусног опсега постала је практично неограничена. Напретком технологија у области развоја оптичких комуникација створиле су се могућности за велико повећање капацитета у преносним системима. Појава синхроне дигиталне хијерархије – SDH хијерархије омогућила је формирање посебних мрежа за управљање (енг. “*Telecommunication Management Network- TMN*”) јер је рам синхроног трансфер модула (енг. “*Synchronous Transport Module – STM*”) сигнала имао резервисане капацитете за слање управљачких функција утиснутих у сам сигнал. Вишеструко увећање капацитета у преносним система омогућило је значајан комфор за пренос управљачких информација других уређаја, које су могле да се преносе у основном раму *STM* сигнала.

Сваки телекомуникациони систем, без обзира о каквом се решењу система ради, захтева постојање одређеног механизма који ће њиме да управља. То се може реализовати конфигурисањем посебне мреже за надзор и управљање потребног капацитета. Надзор опреме и система може вршити одређена организација која не мора да буде саставни део организације која је власник инфраструктуре. Оваква решења се у савременим телекомуникационим системима називају (енг. “*outsourcing*”) или издвајање процеса управљања над мрежом.

Функције мрежа за надзор и управљање су постале један од незаобилазних елемената у структури телекомуникационих система, што је временом постављало све новије и сложеније захтеве у структури тих мрежа. Људима који се баве пројектовањем савремених телекомуникационих мрежа наметнуло је обавезу да функције мрежа за надзор и управљање уврсте у обавезне елементе пројекта, као и да се баве унапређењем њихових функционалности. Такође, намеће се све више потреба да се изврши стандардизација функција управљања и компатибилности њихових интерфејса са самим телекомуникационим системима како би се сви процеси у мрежи аутоматизовали и утицај људског фактора у свакодневном раду свео на минимум.

Развој тржишта телекомуникационих услуга поставља нам увек нове захтеве за постојање стабилне, сигурне и поуздане мреже за управљање. Проширивањем како врста сервиса који се преносе до непосредних корисника, тако и мрежних ресурса који су им потребни, ствара се потреба за обједињеним центрима за управљање који би имали надређену апликацију (енг. „umbrella“) која би обједињавала све управљачке функције. Увођење оваквих система за надзор и управљање телекомуникационим мрежама представља врхунац достигнућа у аутоматизацији предметног проблема надзора и управљања, како са аспекта функционалности рада тако и са аспекта смањења броја запослених у процесу управљања системом.

Уколико узмемо у обзир све наведене чињенице процес формирања мреже за надзор и управљање би могли да дефинишемо кроз четири фазе имплементације:

- 1) Изучавање и опис телекомуникационе мреже
- 2) Пројектовање мреже за надзор и управљање
- 3) Избор потребног хардвера и софтвера
- 4) Имплементација мреже за надзор и управљање.

2.1 Телекомуникациона мрежа (систем)

Телекомуникациону мрежу чини више телекомуникационих уређаја различитог типа који су повезани преко одређеног медијума у циљу остваривања различитих телекомуникационих сервиса. Зависно од фактора који их дефинише и аспекта са ког се разматра могу да се поделе на неколико начина.

Сагледавањем старосне структуре, телекомуникационе системе можемо поделити на оне који имају уређаје исте генерације и оне који имају уређаје различитих генерација. Зависно од статуса власништва инфраструктуре, организационих принципа рада у мрежи и повезаности са другим системима, телекомуникационе системе можемо поделити на системе отвореног типа (конекције су отвореног типа и према другим корисницима) и затвореног типа (конекције су затвореног типа у оквиру организације). Разматрањем са аспекта величине, телекомуникационе мреже можемо поделити на велике мреже (са великим бројем група и фамилија телекомуникационе опреме) и мале мреже (са једном до две групе или фамилије уређаја). Уколико разматрамо са аспекта

разноврсности уређаја у мрежи можемо рећи да се телекомуникационе мреже деле на хомогене мреже (оне које имају заступљен претежно један тип опреме) и хетерогене мреже (оне које имају заступљено више типова опреме).

Глобално гледано телекомуникационе мреже можемо поделити на:

- 1) Јавне телекомуникационе мреже (системе) – представљају отворене системе за кориснике по раније дефинисаним условима за коришћење. Ове мреже чине мреже јавних оператора или провајдера услуга.
- 2) Приватне телекомуникационе мреже (системе) – представљају затворене системе за коришћење од стране запослених или сертификованих лица са циљем ограничавања приступа у циљу заштите података. У ове мреже можемо уврстити мреже државних органа као што су министарства, војска, полиција, банке, мреже приватних компанија и сл.

Напретком технологија у телекомуникацијама и убрзаним развојем интернета дошло је до интеграције разних сервиса и услуга у оквиру истих и различитих телекомуникационих мрежа са циљем унапређења функционалности и доступности.

2.2 Референтни модели заступљени у телекомуникационим мрежама за надзор и управљање

Функционалност једне мреже за надзор и управљање заснива се на скупу правила која дефинишу размену информација између учесника у мрежи. Скуп правила на којима се комуницирање заснива може се подвести под термин протокол.

У савременим *TMN* системима заступљена су два референтна модела која представљају функционални дијаграм како се одвија комуникација:

- 1) OSI (Open Systems Interconnection)
- 2) TCP/IP (Transmission Control Protocol/Internet Protocol)

Зависно од дела система на коме се комуникација одвија као и намене истог извршено је логичко груписање функција у тзв.слојеве. Слојеви имају улогу да податке са виших

нивоа приме, енкапсулирају и процесуирају у складу са својом функцијом и проследе нижем слоју, као и обратно, а зависно од тога у ком се смеру комуникација одвија. Разлике између поменута два референтна модела постоје, али се може рећи да се односе на функционалну организацију процеса на нивоима.

2.2.1 OSI (Open Systems Interconnection) референтни модел

Модел је развијен 1984.године од стране ISO (International System Interconnection) задужене за међународну стандардизацију. Логички и функционално је организован у седам различитих слојева са циљем да извршава додељени скуп функција у процесу комуницирања са нижим и вишим нивоима.



Слика 2.2. OSI референтни модел

Слојеви OSI референтног модела се деле по следећем:

1) Физички слој (Physical layer)

Протоколи физичког слоја описују механичке, електричне, функционалне и процедуралне процесе за активирање, одржавање и деактивирање физичке везе за битски пренос ка и од мрежног уређаја.

2) Слој података (Data Link layer)

Протоколи слоја за пренос података описују методу размене података на нивоу фрејма између уређаја, а преко заједничког медија.

3) Мрежни слој (Network layer)

Протоколи мрежног слоја служе да пружају услуге за пренос појединачних података преко мреже између идентификованих крајњих уређаја.

4) Транспортни слој (Transport layer)

Протоколи транспортног слоја дефинишу услуге сегментирања, преноса и десегментирања података између крајњих уређаја.

5) Слој сесије (Session layer)

Протоколи слоја сесије служе за контролу и организовање дијалога између слоја презентације крајњих корисника, а независно од дешавања на нижим нивоима референтног модела.

6) Слој презентације (Presentation layer)

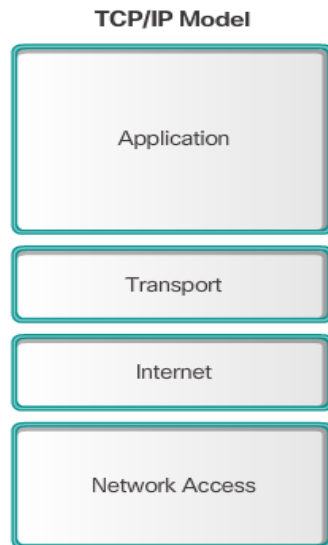
Протоколи слоја презентације намењени су да обраде податке у разумној форми за обе стране у комуникацији.

7) Слој апликације (Application layer)

Протоколи апликативног нивоа намењени су да омогуће приступ апликативним софтверима ка мрежи и представљају највиши ниво OSI референтног модела.

2.2.2 TCP/IP (Transmission Control Protocol/Internet Protocol) референтни модел

Модел је развијен од стране IETF (Internet Engineering Task Force) организације за развој, унапређење и одржавање интернет технологија. Конципиран је на скупу протокола за повезивање рачунарских мрежа. Овај референтни модел се такође бави проблематиком стандардизације за размену података. Логички и функционално је организован у 4 слоја.



Слика 2.3 TCP/IP референтни модел

1) Слој везе (Network Access layer)

Протоколи овог слоја задужени су за размену података, а представљају интерфејс између система и мреже и омогућавају пренос фрејмова коришћењем протокола слоја везе.

2) Мрежни слој (Internet layer)

Протоколи мрежног слоја служе за пакетски пренос података између изворишне и дестинационе адресе дефинисане у заглављу пакета.

3) Транспортни слој (Transport layer)

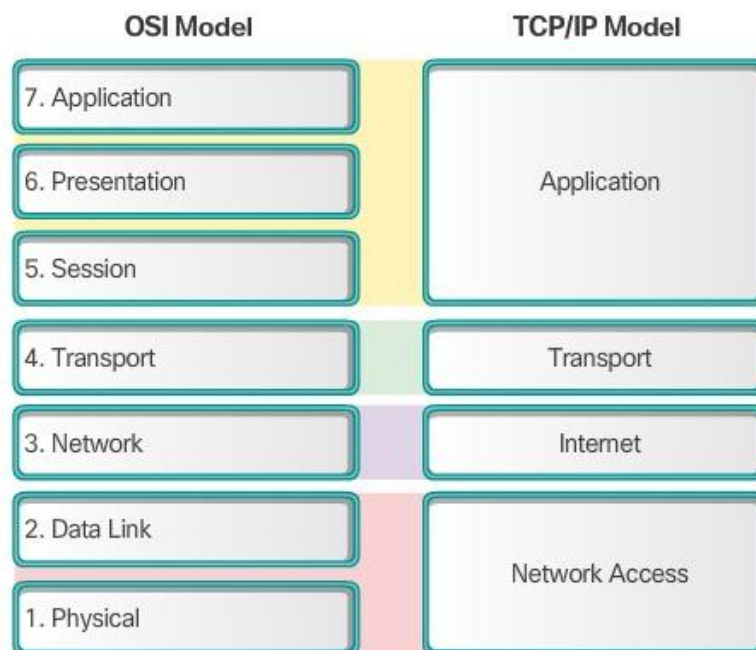
Протоколи транспортног слоја дефинишу услуге сегментирања, преноса и десегментирања података између крајњих уређаја.

4) Апликативни слој (Application layer)

Протоколи апликативног слоја обезбеђују комуникацију између апликативних софтвера учесника и представљају највиши ниво TCP/IP референтног модела.

2.2.3 Поређење OSI и TCP/IP референтног модела

Поређењем логичке и функционалне поделе горе дефинисаних модела може се доћи до закључка да модели, обављају исте функције кроз различити број слојева. У организацији TCP/IP референтног модела дошло је до обједињавања функција на нижим и вишим нивоима. На нижим нивоима физички слој и слој података код OSI референтног модела обједињен је у слој везе код TCP/IP референтног модела. Док је на вишим нивоима извршено обједињавање слојева сесије, презентације и апликације код OSI референтног модела у слој апликације код TCP/IP референтног модела. На слици 2.4 дат је упоредни графички приказ:



Слика 2.4 Упоредни графички приказ OSI и TCP/IP референтног модела

3. ПЛАНИРАЊЕ МРЕЖА ЗА НАДЗОР И УПРАВЉАЊЕ

Процес планирања мрежа за управљање телекомуникационим мрежама и системима обухвата сложену процедуру усаглашавања више различитих функција. Процес управљања телекомуникационом мрежом можемо образложити као збир одређених функција које служе за управљање опремом, контролу рада, лоцирање проблема, планирање капацитета, праћење перформанси, реализацију мерења саобраћаја, дистрибуцију кључева, контролу грешака и представљају основу за менаџмент наплате испоручених услуга.

3.1 Процес планирања телекомуникационих мрежа

Процес пројектовања телекомуникационих мрежа представља процес дугорочног планирања и разматрања њених намена и могућности. Може се рећи да је то сложени процес који нема прецизно дефинисан крај, већ прати рад и развој телекомуникационе мреже и одвија се током њеног животног века. Развој и унапређење услуга у мрежи дефинише и нове императиве за њену непрестану надоградњу. Престанак експлоатације мрежних и сервисних ресурса услед неисплативости дефинише и даљи циклус развоја и планирања система.

Планирање телекомуникационих мрежа се може разматрати по следећим фазама:

1) Сагледавање тренутног стања

Уколико мрежа функционише врши се сагледавање степена искоришћености мрежне инфраструктуре и њена функционалност. Анализом ових параметара могу се извршити основна поређења на основу којих се могу извести закључци и формирати полазна основа за процес планирања. Статистичком обрадом података о искоришћености ресурса, опреме, спојних путева, распореда мрежних уређаја можемо дефинисати даље смернице за боље искоришћење постојећих ресурса или проширење мреже. Правилним сагледавањем функционалног распореда мрежних елемената и њихове искоришћености може се избећи преоптерећеност опреме или неискоришћеност капацитета.

2) Сагледавање економске оправданости

Економска оправданост представља успоставу односа између планираних прихода и уложених расхода у рад телекомуникационе мреже. Анализа трошкова може бити изузетно важан фактор за праћење експлоатације мрежне опреме и планирање набавке нове опреме у циљу унапређења капацитета и сервиса у мрежи.

3) Планирање проширења и унапређења постојеће мреже

Уколико се са претходне две фазе изведу закључци да систем који је у раду треба занављати и унапређивати потребно је да се приступи пројектовању реализације. Пројектовање реализације обухвата хардверско и софтверско развијање мреже и сервиса, као и имплементацију нових, а у складу са претходно дефинисаним потребама и могућностима.

3.1.1 Чиниоци који утичу на планирање телекомуникационих мрежа

Анализом различитих услова који могу утицати на планирање телекомуникационих мрежа може се извршити њихова подела на организацијске, безбедносне, техничке и економске:

1) Технички услови

Обухватају анализу и одабир сервиса које желимо да имплементирамо у телекомуникационом систему. Након избора сервиса врши се одабир хардвера који ћемо инсталирати у постојећу инфраструктуру. Поред избора хардвера подразумева се и дефинисање неопходног софтвера за правилан рад инсталиране опреме.

2) Безбедносни услови

Имплементација политике безбедности се заснива на правилној и правовременој процени безбедносних услова за рад. Овим условима се између осталог дефинише потреба за заштитом комуникација између елемената

система, како на нивоу инфраструктуре тако и на нивоу сервиса, а у циљу спречавања отицања тајних података пословне природе.

3) Организацијски услови

У склопу организацијских услова приступа се пројектовању мрежне топологије, односно физичко-логичком имплементирању горе одабраног хардвера у постојећи телекомуникациони систем. Након извршења имплементације врши се физичко увезивање опреме и њено логичко умрежавање. Организацијски услови предвиђају и дефинисање мреже којом ће се управљати опремом као и избор људства и организацију њиховог рада.

4) Економски услови

Овим условима се формира упоредна анализа стања постојеће телекомуникационе мреже и анализа стања унапређења мреже и средстава која су потребна за њено одржавање. Приликом разматрања економских услова фактор безбедности у мрежи може значајно утицати на повећање цене система и његове исплативости, али се у тим ситуацијама врши процена вредности и значаја отицања тајних података и доноси адекватна одлука о исплативости. Економска оправданост значајног издвајања средстава за потребе безбедности телекомуникационих мрежа има посебну улогу у одбрамбено-безбедносном систему, систему јавне управе и банкарском систему једне државе. Сходно улози и значају који обезбеђује не можемо говорити о његовој економској исплативости, већ о потреби да буде што квалитетнији и функционалнији.

3.1.2 Функционално распоређивање организацијских целина

Уколико посматрамо телекомуникациони систем са глобалног аспекта долазимо до закључка да га не чини само једна организацијска целина, већ да се састоји од више међусобно зависно повезаних делова. Аспекти са којих се може извршити анализа фактора за поделу на функционалне подсистеме су:

1) Комплексност система

Зависно од структуре, организације могу бити организоване на принципу једне или више структурних целина. Самим тим оне имају разноврсне корисничке потребе, а у складу са пословима којима се баве, системи се могу посматрати као једноставни и сложени. Једноставни су они системи код којих је доминантна слична потреба за одређеном врстом сервиса и не представљају сложену корисничку структуру. Сложени системи представљају захтевну корисничку структуру па самим тим и веома сложену структуру сервиса.

2) Приоритет целина

У складу са наменом организацијских целина формира се и листа приоритета за сервисима. Делови организације који имају битну улогу у функционисању распоређују се у сам врх листе приоритета, па самим тим им се даје приоритет у свим функцијама сервиса у односу на друге кориснике.

3) Распоред корисника

У зависности од броја корисника дефинише се распоред мрежне опреме. Зависно од распореда корисника могу фигурирати изузетно мале целине са малим бројем корисника, али се могу појавити и целине које на једној локацији имају изузетно велики број корисника. Наведени проблеми са распоредом корисника могу значајно утицати на приступне мрежне ресурсе и распоред мрежних елемената.

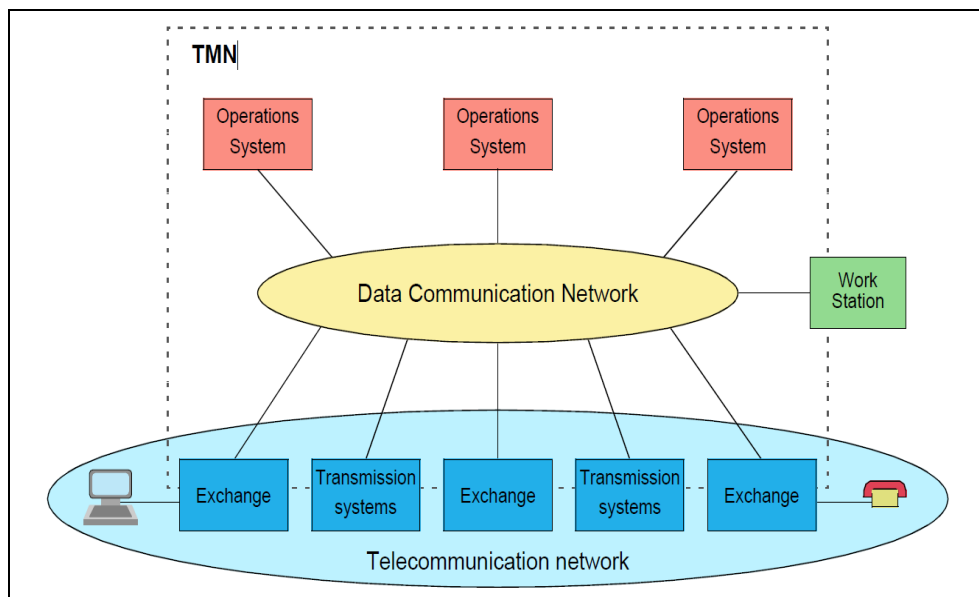
4) Број локација

Распоред и број локација дефинише и начин њиховог увезивања, као и избор технике која ће се користити. Избор технике се врши на основу дефинисаних параметара које процењујемо на основу приоритета целина које увезујемо.

3.2 Мреже за надзор и управљање

Мрежа за надзор и управљање представља функционално засебну мрежу, а која се путем стандардизованих интерфејса повезује са телекомуникационом мрежом, користи њене ресурсе и капацитете. За њу се може рећи да је архитектура за управљање мрежом

развијеном од ITU (енг.“International Telecommunication Union“) стандард M.3000. Намена мреже је да обезбеди комуникацију између интерфејса за надзор телекомуникационе опреме и апликативних софтвера који служе за надзор опреме имплементиране у телекомуникациони систем. Ова мрежа преноси податке и информације везане за надзор и управљање телекомуникационом опремом. Однос телекомуникационе мреже и мреже за надзор и управљање телекомуникационом мрежом приказан је на слици 3.1



Слика 3.1 Однос телекомуникационе мреже и TMN

Са слике 3.1 могуће је уочити да мрежа за надзор и управљање представља посебан систем који за пренос управљачких информација користи посебне телекомуникационе капацитете. Са аспекта коришћења саобраћајних ресурса не мора да буде посебна физичка мрежа, али је пожељно логичко одвајање од телекомуникационе мреже којом се управља. Сваки елемент мреже за надзор и управљање задужен је за надзор и управљање одређеном групацијом уређаја и сервиса. Разматрајући организацију дате мреже може се рећи да главни део мреже чини серверска јединица која сублимира управљачке функције, процесуира их и доставља их радној станици администратора мреже.

Основна улога мреже за надзор и управљање је да развије оквир за управљање телекомуникационим мрежама, обједињавањем функција управљања кроз планирање, инсталацију, администрацију и одржавање телекомуникационих мрежа и сервиса.

Функционалност мреже за надзор и управљање се базира на:

- могућности да поруке из елемента мреже пређу преко различитих интерфејса
- могућности конверзије тих порука из једног формата у други
- могућности преноса порука на разне локације
- способности анализе порука
- способности различитог облика презентовања ових порука
- сигурном и безбедном приступу овим порукама

Препоруке ITU дефинисане стандардом M.3010 дефинишу четири области које се разматрају посебно у процесу планирања и пројектовања мрежа за надзор и управљање, а односе се на:

- функционалну архитектуру
- физичку архитектуру
- информациону архитектуру
- логичку архитектуру

Администратор мреже за надзор и управљање има могућност да захваљујући доброј организацији скрати време реаговања на промене и догађаје у мрежи, да контролне функције проследи на жељене локације, да развије механизме за детекцију грешака у мрежи и унапреди сервисе и рад са корисницима система.

3.2.1 Подела мрежа за надзор и управљање

Дефинисање критеријума за поделу мрежа за надзор и управљање може се спровести на основу груписања и величине елемената којима се управља као и сложености и распореда мрежних елемената. У складу са наведеним критеријумима можемо извршити поделу мрежа за надзор и управљање телекомуникационим мрежама према:

1) Величини елемената

- мреже за јавне телекомуникационе системе
- мреже за телекомуникационе системе посебне намене

2) Груписању елемената

- хомогене
- хетерогене

3) Распореду елемената

- централизоване
- дистрибуиране

4) Сложености система

- просте
- сложене

3.2.2 Мреже за надзор и управљање јавним телекомуникационим мрежама

Јавне телекомуникационе мреже представљају сложене мреже које се састоје од бројних мрежних телекомуникационих уређаја различитих произвођача. Самим тим мреже пружају разноврсне услуге и сервисе користећи различите типове интерфејса. У склопу ових мрежа имплементирани су разни комутациони, преносни, приступни, транспортни системи као и мрежна опрема из разних рачунарских мрежа. Сложеност ове врсте мрежа посебно је изражена потребом да се имплементира мрежа за надзор и управљање телекомуникационом опремом различитих произвођача. Најчешће се дешава да овакве групе уређаја различитих произвођача користе и различите апликације за надзор и управљање које се интегришу у мрежу за надзор и управљање.

У јавним телекомуникационим мрежама тежи се централизованом архитектури надзора и управљања опремом. Узимајући у обзир наведену сложеност система овај процес централизације је јако тешко довести до краја, али се свакако постиже висок проценат искоришћења. Овај начин архитектуре има значајне предности у погледу економске оправданости у односу на дистрибуирану мрежу. Дистрибуирана мрежа захтева постојање мањих регионалних центара који се формирају на принципу расподеле нивоа приступа у процесу управљања мрежом.

Савремени трендови великих оператера у нашој држави базирају се на имплементацији централних системских софтвера за надзор телекомуникационих мрежа (енг. "umbrella"). Имплементација оваквих софтвера за потребе надзора и управљања доводи до поједностављења управљачких функција, а базира се на обједињавању апликација за надзор и управљање опремом различитих произвођача. Обједињавањем и оптимизацијом функција, правилним конфигурисањем мреже рад са овим типом софтвера у значајној мери се олакшава рад и смањује потреба за ангажовањем људства.

3.2.2 Мреже за надзор и управљање телекомуникационим мрежама посебне намене

Телекомуникационе мреже посебне намене представљају функционално и организационо мање системе од јавних телекомуникационих мрежа. Ове мреже су углавном затвореног типа, а намењене су углавном државним органима који имају потребу затвореног комуницирања са ограниченим ресурсима сервиса према јавним телекомуникационим мрежама. Мреже овог типа поседују телекомуникациону опрему за потребе реализације различитих сервиса, у много мањем обиму, а самим тим и са много мање разноврсности произвођача. Обим послова у оквиру мрежа за надзор и управљање оваквим мрежама је значајно једноставнији, базиран на имплементираним функцијама и сервисима који се динамички користе.

У већим организацијама које имају своје независне телекомуникационе системе, као што су електродистрибуција, банке, полиција, војска, постоји потреба за формирањем сопствене мреже за надзор и управљање. Обим послова и динамика промена у мрежама овог типа дефинишу и начин организације мрежа за надзор и управљање. У телекомуникационим мрежама овог типа може се формирати централизовани надзор и управљање, међутим имајући у виду да се углавном ради о типизираним произвођачима опреме, имплементација наведене мреже није превише захтевна и представља обично типски пример за реализацију оваквих система.

Пракса је показала да је у оваквим системима због дистрибуиране организације и аутономности услед отказа пожељно формирати дистрибуирану архитектуру мреже за надзор и управљање. Имајући у виду значај функција које државни органи обављају централизовани надзор и опоравак мреже услед квара може знатно отежати

функционисање крајњих корисника. Дистрибуирана архитектура се углавном заснива на формирању регионалних центара за надзор и управљање који се коришћењем опреме за заштиту информација интегришу са главном центру за надзор и управљање телекомуникационом мрежом.

3.2.3 Сагледавање чинилаца који описују мрежу за надзор и управљање

Током пројектовања мреже за надзор и управљање телекомуникационом опремом морају се узети у разматрање технички, безбедносни, организациони и економски аспекти.

Технички аспекти обухватају:

- врсту и типове елемената над којима се врши надзор, зависно од функције коју обављају. Узимајући у обзир функције које обављају најчешће можемо говорити о комутационим мрежама, преносним системима, радио-релејним мрежама и рачунарским мрежама. Зависно од квалитета и могућности опреме која се имплементира може се говорити о опреми различитих домаћих и страних произвођача.
- избор начина преноса управљачких порука. Разматрањем могућности преноса управљачких порука на опреми различитих произвођача можемо разматрати опције преноса порука саобраћајним телекомуникационим каналима у оквиру сигнала или организацијом логичких мрежа за надзор и управљање путем саобраћајних интерфејса у телекомуникационим мрежама.
- избор хардвера и софтвера. Избор хардвера и софтвера који се користи за формирање мреже за надзор и управљање телекомуникационом опремом директно је у вези са планираном архитектуром мреже. Избор централизоване или дистрибуиране архитектуре мреже, као и централизованих системских софтвера или произвођачких апликативних софтвера одређује количину и врсту хардвера.
- компатибилност хардвера и софтвера. Зависно од тога да ли се ради о типским интерфејсима или не мора се предвидети употреба конвертора интерфејса за поједине делове мреже.

- дефинисање сервиса и функција који ће се користити. Овај аспект зависи од намене и степена имплементације надзора мреже.

Безбедносни аспекти обухватају:

- избор поузданог начина управљања опремом. У циљу дефинисања политике безбедности у систему неопходно је при пројектовању мреже размотрити правилан распоред елемената за надзор и управљање мрежом, као и каснију имплементацију безбедносних решења.
- дефинисање опреме за заштиту информација. Приликом пројектовања мрежа за надзор и управљање телекомуникационим мрежама затвореног типа базираним на дистрибуираној архитектури са регионалним центрима за надзор и управљање, неопходно је дефинисати опрему за заштиту информација како не би дошло до отицања тајних података и управљачких информација.

Организацијски аспекти:

- избор архитектуре мреже за надзор и управљање. Подразумева доношење одлуке о избору топологије мреже зависно од потреба корисника.
- управљачки слојеви који се користе. У телекомуникационим мрежама обично се користе четири управљачка слоја који ће бити накнадно објашњена.
- скалабилност мреже. Подразумева могућност да се мрежа за надзор и управљање увек прошири имплементацијом нових елемената.

У склопу концепта мрежа за надзор и управљање користи се више управљачких слојева. Они су разврстани на следећи начин:

- слој управљања пословањем (енг. “*Bussines Management Layer-BML* “),
- слој управљања сервисима (енг. “*Service Management Layer-SML* “),
- слој управљања мрежом (енг. “*Network Management Layer-NML* “),
- слој управљања елементима мреже (енг. “*Element Management Layer-NEML* “)

Препорука ITU М.3010 дефинише управљачке слојеве мреже за надзор и управљање који су приказани на слици 3.2



Слика 3.2 Управљачки слојеви у оквиру TMN-а

Економски аспекти:

- цена неопходног хардвера и софтвера. Цена хардвера и софтвера дефинише најчешће и квалитет опреме имплементиране у систем, као и њену економску оправданост за наредна проширења и надоградње система новом опремом. У склопу овог аспекта потребно је обратити пажњу на трендове произвођача да ниском стартном ценом привуку набавку јефтиније опреме, а да почетне разлике касније надокнаде куповином разних врста лиценци.
- цена обуке људства за рад на одржавању мреже за надзор и управљање опремом. Овај аспект може значајно увећати цену система, како у периоду набавке, тако и касније у обучавању запослених. Са економског аспекта треба тежити системима који поседују GUI (енг. “Grafic User Interface”) апликације имајући у виду једноставнију и јефтинију обуку за рад са опремом.
- расположивост резервних делова. Приликом разматрања опреме за реализацију мреже за надзор и управљање морамо посебно обратити пажњу на фактор доступности и цене резервних делова, као и обавезама прописаним у гарантном року. Недоступност резервних делова може изазвати проблеме економске природе у каснијој експлоатацији мреже и компатибилности опреме.

4. КОМПАРАТИВНИ ПРИКАЗ САВРЕМЕНИХ ТЕЛЕКОМУНИКАЦИОНИХ МРЕЖА СА МОГУЋНОСТИМА УДАЉЕНОГ ПРИСТУПА

Анализирајући савремене телекомуникационе мреже јавних предузећа и државних органа може се извести закључак да оне представљају један функционалан систем имплементиран из више мањих подсистема. Подсистеми су међусобно независни у погледу пружања услуга, али су интегрисани у оквиру јединственог телекомуникационе мреже како у погледу опреме и сервиса које пружају, тако и у погледу логичке и тополошке архитектуре.

Телекомуникационе мреже које представљају предмет разматрања састављене су из четири функционална подсистема:

- комутациони систем који чине дигиталне телефонске централе последње генерације,
- приступно-преносни систем базиран на PDH приступним и SDH транспортним технологијама,
- радио-релејни преносни систем базиран на PDH приступним и SDH транспортним технологијама,
- рачунарска мрежа за управљање процесима и организационим пословима у предузећу.

4.1 Комутациони систем и могућност имплементације мреже за надзор и управљање

Запослени у предузећима имају свакодневне потребе за говорном комуникацијом путем телефона, како унутар предузећа тако и са пословним партнерима. За потребе комуникације најчешће се користе телефонски апарати који представљају терминални део комутационе мреже предузећа. У складу са функцијама које реализују запослени се често сусрећу са терминалима који захтевају имплементацију различитих типова сервиса заснованих на говорној и видео комуникацији.

Комутациони систем који ће се користити као пример за комутациону мрежу предузећа базира се на принципу већег броја телефонских централа новије генерације типа MX-One TSW, произвођача ASTRA (наследник шведског Ericssona).

4.1.1 Комутациони систем

Основне карактеристике ових система су дистрибуирана архитектура, флексибилност, модуларност и скалабилност. То омогућава задовољење различитих захтева који се односе на величину, функције, сигурност софтвера, капацитет саобраћаја и физички размештај код географски удаљених локација.

Две основне јединице у оквиру система су модул линијског интерфејса LIM (енг. "Line Interface Module") и модул групног степена GS (енг. "Group Switch"). У раду сваки LIM је аутономан и има свој управљачко-процесорски систем, сопствено комутационо поље, а по потреби и батеријску аутономију. Међусобно повезивање LIM-ова врши се путем GS, увезивањем саобраћајних интерфејса коришћењем G.703 стандарда, што омогућује дистрибуирану архитектуру. Спољашњи изглед централе MX-One приказан је на слици 4.1



Слика 4.1 Спољашњи изглед централе MX-One

Дистрибуирана архитектура комутационог система овог типа заснива се на:

- дистрибуираном хардверу који на свакој локацији функционише независно и поседује комплетан процесорско-комутацијски систем пружајући услуге крајњим корисницима у оквиру целине коју опслужује

- модуларности софтвера који омогућава аутономну контролу и управљање како у локалу тако и на нивоу регионалних и главних центра за надзор и управљање

У основне делове LIM-а се убрајају:

1) Управљачко-процесорски систем LIM-а

Управљачко-процесорски систем чине два процесора која се налазе у дуплираном режиму рада на нивоу LIM-а. У случају отказа једног од њих други аутоматски преузима функцију, без прекида у функционисању саобраћаја и надзора. Посебан значај систему даје могућност дуплирања и комутационог поља LIM-а, чиме се значајно доприноси стабилности и поузданости система.

2) Комутациони систем LIM-а

Сваки LIM се састоји од 1024 неблокирајућа временска одсечка којима се врши комутација у оквиру централе, док се сваки магацин LIM-а састоји од 256 неблокирајућа временска одсечка. Процес комутације имплементиран је путем плоче комутацијског поља LSU (енг. "Lim Switch Unit") и четири дистрибуцијске плоче DSU (енг. "Distribution Switch Unit"). Обрада говора и информација о комуникацији врши се на нивоу LSU плоче у специјалним меморијама.

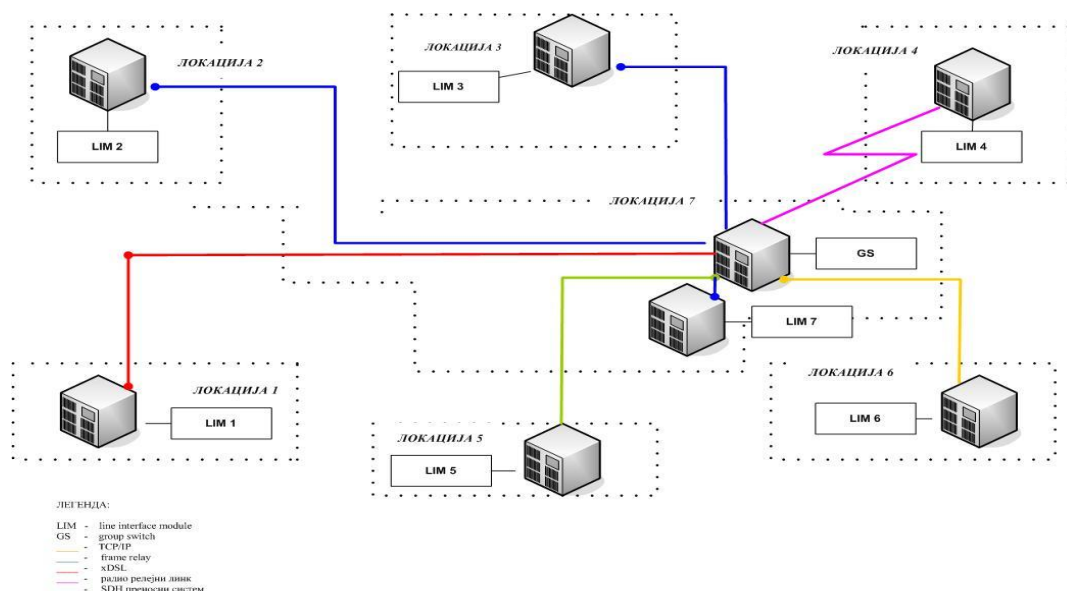
3) Плоче централе

Централа своју функционалност према корисницима постиже захваљујући корисничким интерфејсима који се у њу имплементирају путем учесничких плоча. За потребе коришћења и повезивања система најчешће су плоче улазно-излазних интерфејса за потребе комуникације са системом, плоче аналогних (класичних) телефонских прикључака, плоче дигиталних (ISDN) телефонских прикључака, плоче IP телефонских прикључака, плоча за дигиталне и IP преносничке групе као и плоче тонова које су неопходне за рад говорних сервиса.

Сваки LIM садржи најчешће комбинацију неких од модула са којима се може комплетирати кабинет у који се смешта опрема. Смештај опреме се може минимално реализовати са једним, а максимално са четири модула на располагању:

- PSM (енг. “*procesor switch module*”): модул процесора и комутацијског поља у који се обавезно смештају плоче PU5DC, LPU5, LSU и DSU,
- IFM (енг. “*interface module*”): модул линијских интерфејса обавезно садржи плочу за напајање, DSU и учесничке плоче,
- PWM (енг. “*power module*”): AC/DC са 2x12.5 А и батеријом за *back-up* од 26 Ah,
- PBM (енг. “*power backup module*”): модул додатног напајања за 2 x 26 Ah,
- PDM (енг. “*power distribution modul*”): модул дистрибуције напајања са простором за три плоче са електронским осигурачима 10x10A.

Групни степен централе представља дигитално комутационо поље које се бави успоставом и преносом временских одсецака, података и управљачких сигнала. Он није управљачки оријентисан елемент централе, већ се њиме управља путем осталих делова система (LIM-ова). Захваљујући групном степену систем је изузетно скалабилан и може подржати до 124 LIM-а у пуној конфигурацији. Уколико се ради о изузетно важним корисницима који се увезују преко групног степена пожељно је извршити дуплирање функције. На слици 4.2 приказан је пример система који је дистрибуиран на више различитих локација.



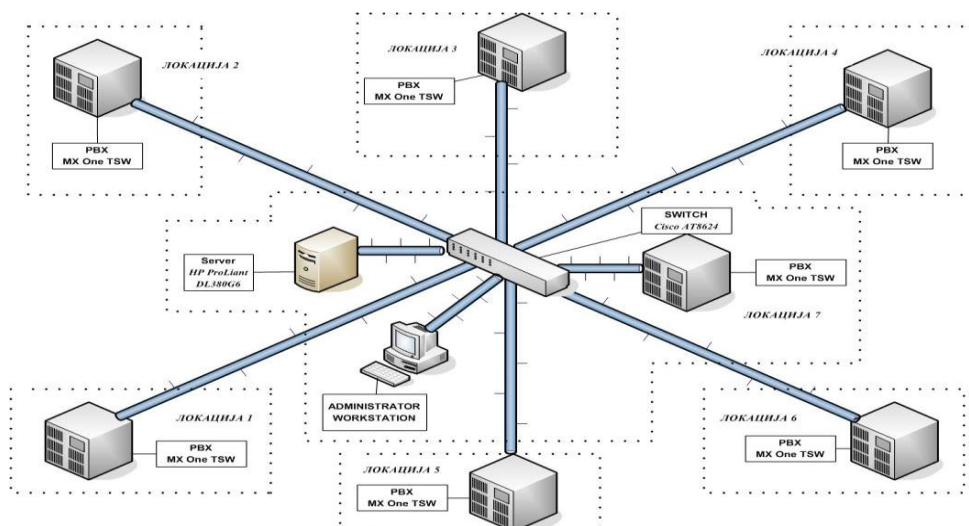
Слика 4.2 Имплементација система преко групног степена

У наведеном примеру реализовано је функционално увезивање дистрибуираних делова централе у једну целину. Увезивање делова система се најчешће врши употребом QSIG

сигнализације, док се за увезивање централа са другим централама у јавним мрежама користе и друге врсте сигнализације.

4.1.2 Могућност имплементације мреже за надзор и управљање у комутационој мрежи

Имајући у виду да се комуникација послуживоца са централом одвија на принципу MML језика (енг. "Man Machine Language") произвођач је предвидео и адекватне портове на улазно-излазној јединици за комуникацију са централом. Плоча NIU (енг. "Network Interface Unit") се користи за потребе приступа центри са неколико улазно-излазних интерфејса. Интерфејси плоче подржавају приступ већег броја апликација као што су улазно/излазни сервиси високог нивоа и мрежне апликације. За имплементацију мреже за надзор и управљање посебно је интересантан тип интерфејса „Ethernet“ 10/100 BaseT који нам пружа могућности сталне конекције централе у мрежи за надзор и управљање. Поред наведеног интерфејса постоје још три порта за синхроно/асинхрони приступ центри (тзв. V.24 интерфејса), који могу послужити за модемски приступ центри у случају да мрежни приступ није у функцији. Потенцијални модел мреже за надзор и управљање комутационом мрежом приказан је на слици 4.3, а базира се на увезивању локација у предузећу у циљу формирања централизоване архитектуре за управљање мрежом.



Слика 4.3 Пример увезивања елемената комутационе мреже у мрежу за надзор и управљање

Софтвер за надзор и управљање телекомуникационом мрежом централа „MarWatch“ може се користити за имплементацију и оваквим конфигурацијама. Одликује се могућношћу приступа мрежним уређајима двадесет четири часа дневно седам дана у недељи („24/7“) са било које локације. Анализом перформанси и могућности софтвера могу се истаћи његове предности:

1) заштићени удаљени приступ

Заштићени приступ се заснива се на безбедном приступу мрежи и елиминише могућности нарушавања система управљања. Он се може реализовати са било које локације. Запослени који се баве надзором и управљањем у мрежи могу ефикасно истраживати проблеме у мрежи и проналазити узроке непредвиђених стања.

2) надзор перформанси и доступност управљања „24/7“

Софтвер поседује могућност да даљински надгледа, управља и анализира статус мреже у реалном времену. У свом раду он не оставља никакве празнине у праћењу перформанси, што омогућава свеобухватну видљивост у мрежи и могућност да се преко приватних, а по потреби и јавних тачака приступа детектују и решавају проблеми.

3) алармирање у реалном времену

Могућност алармирања на надоласеће проблеме мреже у реалном времену помаже лицима која раде на пословима надзора и управљања да правовременим реаговањем избегну застој у систему. Он поседује скуп прилагодљивих упозорења, а најкориснији су статусни аларми доступних интерфејса и упозорења о приближавању максимално дефинисаним праговима вредности саобраћаја или прекорачењима.

4) детаљан рапорт о дешавањима у мрежи

Предефинисани извештаји и извештаји на захтев знатно убрзавају информисање запослених о учинку на нивоу мреже као и побољшање праћења нивоа услуга. Извештаји помажу у планирању и балансирању оптерећења, као и побољшању продуктивности.

5) прилагодљив кориснички интерфејс

Софтвер је оптимизован за приказ на мобилним телефонима, таблетима, мобилним уређајима. Обрађене и важне податке из рада на наведеној опреми може извозити у једноставном облику према потребама корисника.

Правилним увезивањем корисника у мрежи за надзор и управљање, подаци о надзору комутационе мреже се могу имплементирати до нивоа мобилности праћења корисника који управља самом мрежом.

4.2 Приступно-транспортни (мултиплексни) систем и могућност имплементације мреже за надзор и управљање

Приступно-транспортни систем или како се уобичајено назива мултиплексни систем представља централни систем у телекомуникационој мрежи организације. Његова улога и значај у једној телекомуникационој мрежи представљаја окосницу функционисања свих осталих телекомуникационих система. Улога наведеног система за формирање мреже за надзор и управљање телекомуникационим системом је од изузетног значаја имајући у виду да се саобраћајни капацитети за потребе ове мреже реализују преко овог система. Зависно од периода изградње приступно-транспортних система можемо говорити и о различитим врстама телекомуникационих технологија имплементираним у њихов рад везано за саобраћајне капацитете, као и о различитим врстама интерфејса за потребе њиховог надзора и управљања.

Уколико посматрамо приступно-транспортни систем из телекомуникационог угла уочавамо да се заправо ради о систему који се може лако поделити на две групе уређаја:

1) Приступни уређаји

Ову групу уређаја чине уређаји мањег капацитета намењени углавном за прихват или слање корисничких сервиса мањих капацитета и њихово мултиплексирање или демултиплексирање према крајњим корисницима.

2) Транспортни уређаји

Ову групу уређаја чине уређаји већег капацитета намењени углавном за потребе даљег мултиплексирања излазних капацитета приступних уређаја према уређајима из транспортне мреже.

Анализом тржишта и опреме која се користи у нашој земљи код јавних телекомуникационих оператера и корисника у затвореним системима за потребе приказа приступно-транспортне мреже користићемо два типска уређаја домаћег произвођача „ИРИТЕЛ а.д“. За потребе приступне равни користићемо уређај FM MSAN, а за потребе транспортних система уређај ОДС 622.

4.2.1 Приступни уређаји

Главна улога ових уређаја у приступном делу мреже базирана је на потребама да се поред класичних телефонских сервиса омогући корисницима одређени капацитет аналогних и дигиталних интерфејса за потребе функционисања сервиса у оквиру организације у којој се имплементира. Уређаји из ове фамилије су углавном конципирани на PDH технологији (енг. "Plesiochronous Digital Hierarchy") рада са могућношћу мултиплексирања улазних капацитета. Приликом реализације саобраћајних капацитета, на учесничке плоче уређаја могуће је повезати локалне кориснике или им довести саобраћај са удаљених локација. Излазни саобраћај уређаја базира се на мањим мултиплексним капацитетима.

Уређај који се користи као типичан пример ове фамилије је модел FM MSAN популарнији под називом FM 8x2. Уређај се заснива на следећим капацитетима:

- осам спољних линкова капацитета 2048 kb/s,
- 16 унутрашњих линкова капацитета 2048 kb/s искључиво намењених за потребе унутрашњег проспајања на учесничким плочама,
- капацитет уређаја износи до 800 локалних корисника или канала.



Слика 4.4 Приступни PDH уређај ФМ 8x2 у радној станици

Уређај подржава широк спектар учесничких плоча за потребе крајњих корисника како би омогућио што боље услове и интерфејсе за реализацију корисничких сервиса. У основној попуни уређај поседује кућиште, потребан сет делова за напајање и централну процесорско-управљачку плочу типа FMV. Зависно од потреба крајњих корисника могуће је имплементирати неке од следећих плоча водећи рачуна о капацитетима унутрашњих магистрала уређаја:

- PAT10 – 10 канала АТА интрфејс 2ж (корисничка страна),
- PAC10 – 10 канала АТА интрфејс 2ж (страна телефонске централе),
- PEM10 – 10 канала 2ж/4ж са Е/М сигнализацијом,
- PLB10 – 10 канала LB интрфејс 2ж,
- PN64 – 4 дигитална канала, типа n x 64 kb/s, интерфејс X.21/V.11,
- PIU (NT/LT) 4 дигитална ISDN прикључка са U интерфејсом,
- PET 3 10/100BaseTx I 3 100BaseFx Ethernet прикључка.

Уређај поседује више варијанти синхронизације које се базирају на сопственој синхронизацији или синхронизацији коју прима од референтног извора такта.

За потребе надзора уређаја у телекомуникационој мрежи уређај поседује неколико интерфејса који нам омогућавају приступ и реализацију функција надзора и управљања. Могућност директног приступа управљачкој FMV плочи заснива се преко серијског RS232 прикључка или путем интерфејса типа „Ethernet“, а који су искључиво намењени за комуникацију са опремом. Поред наведених интерфејса уређај има могућност повезивања са другим уређајима у станици исте или више равни из своје серије путем задње магистрале или тзв. „Q-busа“. Уколико нисмо у могућности да вршимо надзор и управљање на неки од наведених начина уређај поседује могућност даљинског

управљања путем управљачких DCC канала који су смештени у заглављу рама саобраћајних канала, а прослеђују се путем саобраћајног линка са друге станице са којом се сервис остварује. За реализацију изложених могућности увезивања потребно је извршити адекватно подешавање адреса и параметара интерфејса који ће се користити.

4.2.2 Транспортни уређаји

Транспортни уређаји представљају главне тачке транспортне мреже и пружају могућност преноса већих капацитета агрегираних у тим тачкама. Уређаји поседују могућности додавања-издвајања (енг., „add-drop“) мултиплексирања што представља изузетно повољне услове за прихват и одграђавање капацитета. По својим могућностима ова група уређаја представља веома финансијски исплативо решење у мрежама предузећа затвореног типа за потребе најразличитих варијанти умрежавања.

Уређај ODS/OTS622 представља нову фамилију уређаја за пренос дигиталних сигнала по оптичким влакнима, која је заснована на SDH (енг. „synchronous digital hierarchy“) техници мултиплексирања до нивоа STM-4 (622 Mbit/s).



Слика 4.5 Транспортни мултиплексни уређај ОДС 622

Уређај ODS/OTS622 је јединствена мултисервисна платформа за STM-4/STM-1 саобраћајне капацитете, проширива и до STM-16 нивоа. ODS/OTS622 представља економично решење за примену у градским (метро) и локалним мрежама у различитим конфигурацијама.

Овај уређај омогућава формирање:

- “тачка-тачка” комуникације,
- линеарне *SDH* мреже са могућношћу одграђавања капацитета,
- све врсте прстенова и других сложених структура на нивоу *STM-4* и *STM-1*,
- прикључење на *SDH* мреже истог или вишег хијерархијског нивоа,
- локално проспајање на нивоу *VC-12*, *VC-3* и *VC-4* контејнера.

Уређај омогућава пренос путем оптичких интерфејса имплементираних преко SFP модула по следећем:

- за оптички интерфејс 622 Mb/s по мономодном оптичком влакну у другом и трећем оптичком прозору на таласним дужинама 1310 nm или 1550 nm за растојања до 48 и 80 км,
- за оптички интерфејс 155 Mb/s по мономодном оптичком влакну у другом и трећем оптичком прозору на таласним дужинама 1310 nm или 1550 nm за растојања до 49 и 83 км.

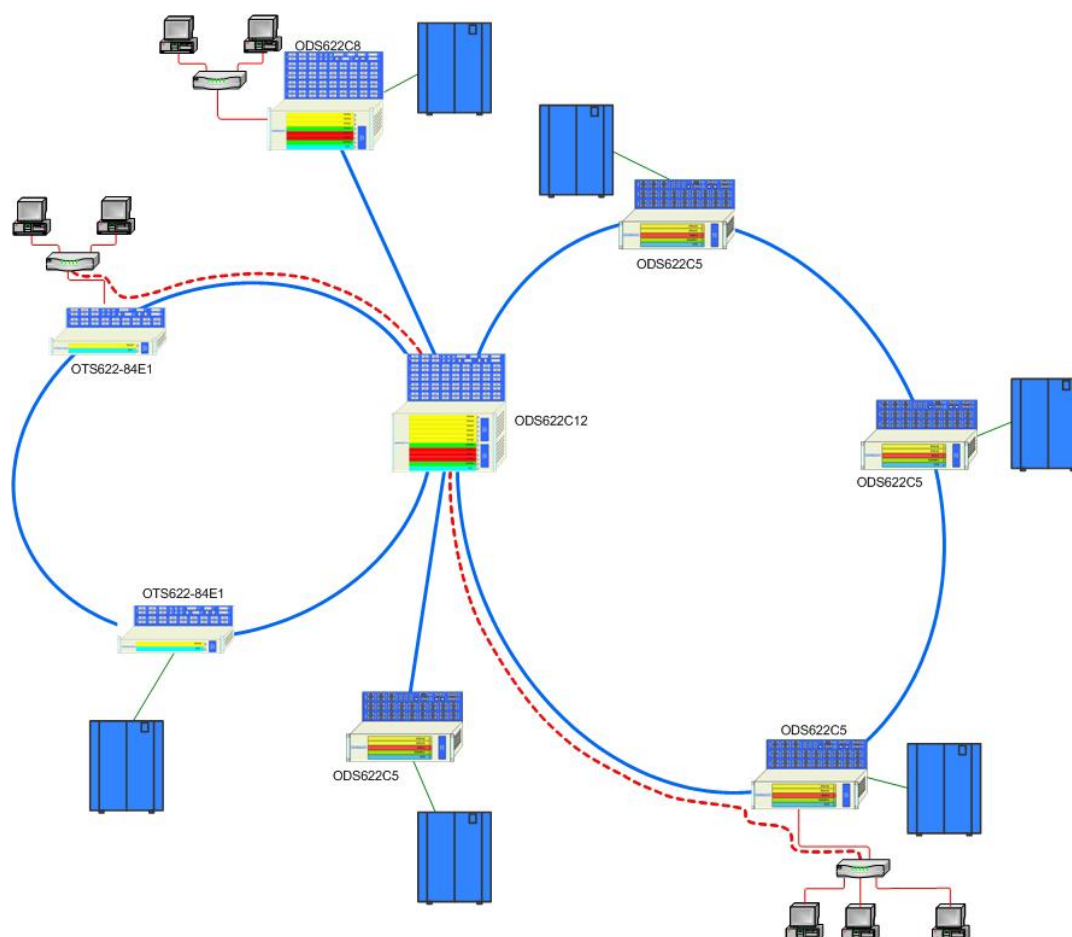
Имплементација уређаја у мрежи дефинише се у складу са проценама и потребама, а најчешће поседује три врсте плоча имплементираних у одређен тип кућишта и то:

- OTS картицу која поседује интерфејсе 21x2 Mb/s, 3 x 34 Mb/s, 4 x 10/100 Base TxEthernet , 1 x 100 Base Fx Fast Ethernet и два STM-4/STM-1,
- S4ADM-2 картицу која поседује интерфејсе 5 x 10/100 Base Tx Ethernet , 1 x 100 Base FxFast Ethernet, 1 x 1000 Base T/X Gigabit Ethernet и два STM-4/STM-1
- STI-63 картицу која поседује интерфејсе за 63 x 2 Mb/s.

За потребе заштите саобраћаја у случају прекида уређај поседује заштите на нивоу мултиплексне секције MSP 1+1 (енг.“Multiplex Section Protection“), заштиту на нивоу пута вишег или нижег реда (*VC12*, *VC3*, *VC4 path protection*), заштита на нивоу дела пута (*SNCP protection*) и 1:N заштита за притоке капацитета 2 Mb/s.

Синхронизација уређаја у мрежи се врши најчешће пријемом референтног такта синхронизације од извора синхронизације у мрежи или пријемом такта од других уређаја. Уређај поседује могућност да буде извор референтног такта, али се то избегава

Пример имплементације уређаја ODS/OTS622 у сложеној телекомуникационој мрежи представљен је на слици 4.6



телекомуникационој мрежи

Повезивање транспортних уређаја у мрежу за надзор и управљање телекомуникационим уређајима могуће је реализовати непосредно у телекомуникационој станици, ради заједничког управљања преко Q2 (RS 485) интерфејса или Q2Et (10/100BaseTx) интерфејса уз употребу адекватног свича. Уређај поседује и интерфејсе за надзор и управљање путем RS232 и „Ethernet“ порта на OTS картици који су такође намењени за увезивање у мрежу. Поред наведених интерфејса уређај поседује опцију надзора и управљања путем управљачких канала у заглављу

STM4/STM1 рама на саобраћајним интерфејсима који се најчешће користе за ове потребе.

4.2.3 Могућност имплементације мреже за надзор и управљање приступно-транспортним (мултиплексним) уређајима

Мрежу за надзор и управљање приступно-транспортним уређајима произвођача „ИРИТЕЛ а.д.“ могуће је реализовати како у затвореним предузећима тако и у јавним телекомуникационим мрежама. Уређаји поседују фабрички дефинисане интерфејсе за ове потребе па је на пројектанту мреже да изабере начин реализације и тип интерфејса који ће користити за формирање мреже. Произвођач је развио GUI (енг. “Graphic User Interface”) апликативни софтвер СУНЦЕ за потребе надзора телекомуникационе опреме, који омогућава функције контроле и надзора телекомуникационе опреме сопствене производње. Софтвер је наменски предвиђен за прикупљање и обраду управљачких информација, а путем истог могуће је реализовати функције:

- управљања грешкама (сметњама и кваровима)
- управљања перформансама
- управљања конфигурацијом и
- управљања сигурношћу.

4.2.3.1 Управљање грешкама

Управљање грешкама је група функција која омогућава детекцију, изолацију и корекцију неисправног рада телекомуникационе мреже. Управљање грешкама започиње детекцијом грешке. Израз “грешка” подразумева догађаје на уређају који га спречавају да нормално обавља своју функцију. Специјализована логика на уређају открива ове догађаје и прослеђује их рачунару. Уређаји су под сталним надзором. Аларми се приказују са ознакама нивоа озбиљности (приоритета) и локације. Поред надгледања аларма, омогућене су и различите врсте тестирања, којима се проверава рад система након отклањања грешке.

4.2.3.2 Управљање перформансама

Управљање перформансама подразумева надгледање перформанси уређаја. Ово је омогућено прикупљањем података о стању и понашању уређаја као целине. На основу добијених података врше се различите статистичке анализе и контрола квалитета служби. Надгледање перформанси се врши у интервалима трајања 15 минута и 24 сата. Уз надзор перформанси, софтвер омогућава приказивање историје аларма.

4.2.3.3 Управљање конфигурацијом

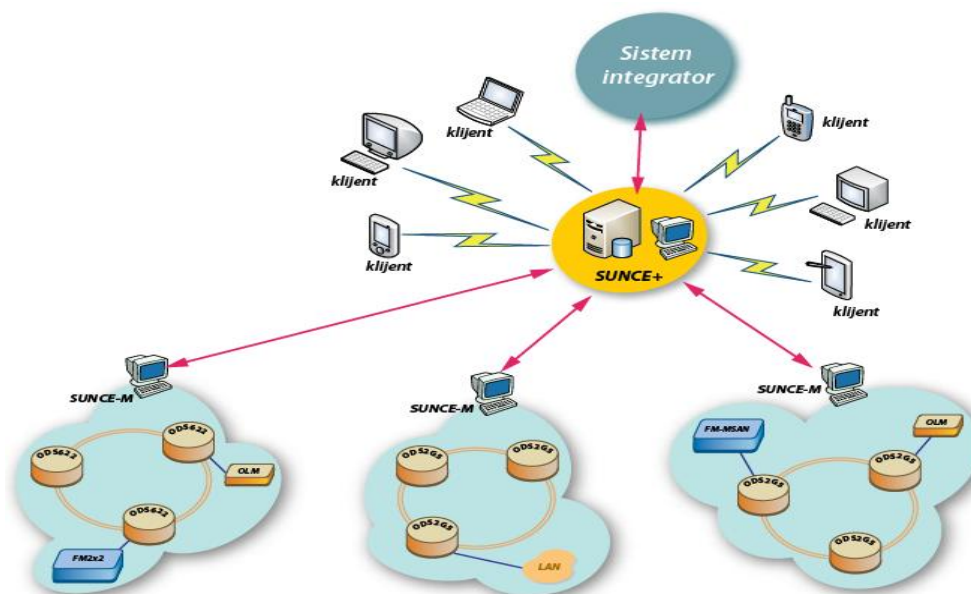
Управљање конфигурацијом обухвата функције које омогућавају обраду, прикупљање и прослеђивање података који се односе на конфигурацију и контролу статуса уређаја. Конфигурациони параметри се примају са уређаја, а рачунар може да шаље уређају податке о промени ових параметара, те на тај начин се мења начин рада уређаја, чиме могу да се отклоне и грешке које су се појавиле. Овим функцијама се проверава и задаје статус различитим параметрима који утичу на рад система.

4.2.3.4 Управљање сигурношћу

Сигурност приступа је омогућена ауторизацијом корисника приликом приступа софтверу. Постоје два начина приступа – администраторски и кориснички ниво.

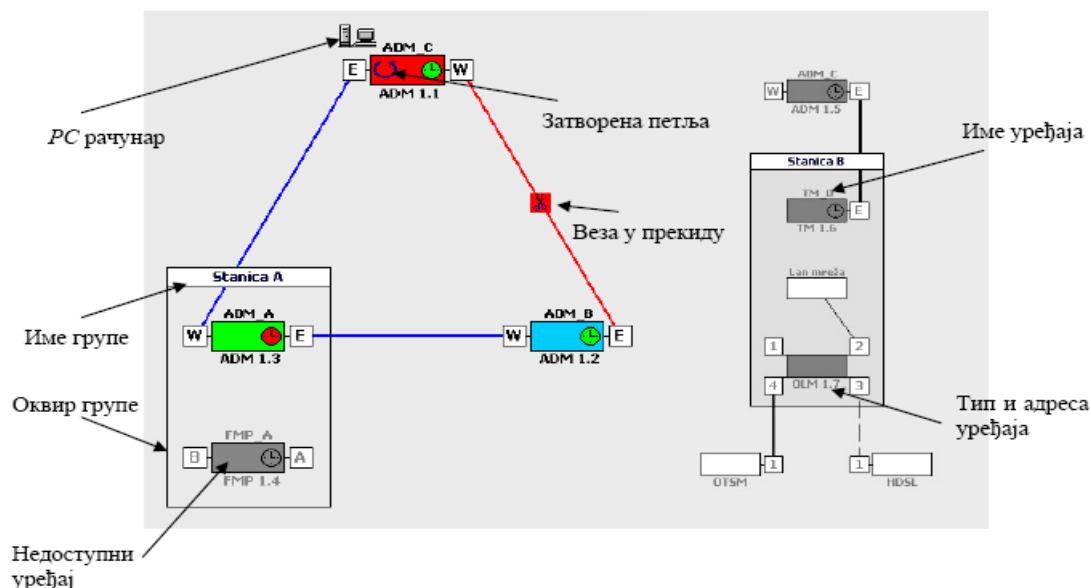
- кориснички ниво приступа омогућава преглед и надзор параметара система
- администраторски ниво приступа омогућава преглед и задавање опција система, као и креирање корисничких налога и измену права корисника.

Модел мреже за надзор и управљање телекомуникационом мрежом приступно-транспортних уређаја представљен је на слици 4.7 и илуструје реализацију мреже преко саобраћајних интерфејса телекомуникационе опреме.



Слика 4.7 Модел мреже за надзор и управљање телекомуникационом мрежом приступно-транспортних уређаја

Софтвер СУНЦЕ + за управљање мрежом телекомуникационих уређаја омогућава прегледан рад кориснику како у приступно-преносној мрежи тако и приликом конфигурисања самог уређаја. Намењен је за потребе надзора и управљања опремом на тзв. „острвском принципу организације“ путем регионалних центара за надзор и управљање опремом где се за потребе надзора користи софтвер СУНЦЕ-М. Апликација омогућава тренутно праћење стања у систему и динамичке промене удаљеним приступом. На слици 4.8 приказана је радна површина сегмента мреже приликом промена у телекомуникационој мрежи са појашњењима симбола и стања.



Слика 4.8 Приказ радне површине у апликацији СУНЦЕ-М

Поред апликације СУНЦЕ + и СУНЦЕ-М постоји и апликација СУНЦЕ-Л која служи за локални приступ уређају, али он није предмет тренутног разматрања.

4.3 Радио-релејни систем и могућност имплементације мреже за надзор и управљање

Радио-релејне комуникације представљају област телекомуникација која је посебну примену нашла у решавању проблема повезивања неприступачних локација или локација предузећа које не поседују развијену телекомуникациону инфраструктуру за увезивање у јавни телекомуникациони систем. Радио-релејни уређаји чине групу уређаја која омогућава пренос информација на даљину посредством електромагнетних таласа. За правилан рад и квалитетно одржавање комуникације неопходно је постојање оптичке видљивости и слободне I Френелове зоне између крајњих тачака између којих се комуникација успоставља. Изузетно велику примену имају код јавних емитера где се користе за пренос сигнала до неприступачних предајника за потребе емитовања програма.

4.3.1 Радио-релејни уређаји

За потребе приказа мреже за надзор и управљање телекомуникационим радио-релејним уређајима користе се уређаји произвођача Nera Networks (S) Pte Ltd из Норвешке чији су производи широко имплементирани у телекомуникационим мрежама у нашој земљи и свету. Савремени концепт радио-релејне опреме овог произвођача базиран је на IP технологији, али у циљу компатибилности коришћених технологија опреме у комутационим и приступно-транспортним системима користи се опрема базирана на TDM принципу рада, реализована у мрежама PDH и SDH технологија.

Радио-релејни уређај NERA EVOLUTION је елемент дигиталног система преноса и намењен је за изградњу сложених и разгранатих телекомуникационих мрежа и у зависности од примењене конфигурације Он може бити елемент транспортне или приступне равни радио-релејне мреже зависно од потреба. Под термином радио-релејни уређај NERA EVOLUTION се подразумева комплексна платформа фамилије радио-релејних уређаја. Погрешно је под именом NERA EVOLUTION подразумевати један заокружен и коначан производ. Ово значи да постоји велики број различитих конкретних изведби уређаја са могућношћу унутрашње и спољне монтаже, а самим тим и широк спектар могућности употребе истог.

Типични уређаји из фамилије ових уређаја приказани су на слици 4.9



Слика 4.9 Радио-релејни уређаји NERA фамилије са унутрашњом и спољном јединицом

Радио-релејни уређај NERA EVOLUTION који се користи за реализацију магистралних транспортних праваца великог капацитета и формирање окоснице (кичме) система преноса назива се NERA EVOLUTION – METRO LONG HAUL. Овај уређај је реализован као SDH радио-релејни уређај транспортног нивоа STM-1 (155 Mb/s) или STM-4 (622 Mb/s). METRO LONG HAUL варијанта се најчешће монтира у изведби интегрисане монтаже (енг., „*all indoor*“) због потребе да се употребе комплекснији склопови РФ мултиплекса и квалитетнији РФ филтри. Истовремено, за случајеве када је неопходна подељена монтажа (енг., „*split mount*“) омогућена је и њена изведба. У ту сврху се користи РФ мултиплекс малих губитака за спољашњу монтажу (енг., „*Branching box*“). Основни капацитет преноса по јединици примопредајника је 155 Mb/s, а постоји и верзија капацитета од 311 Mb/s који се може применити у одређеним варијантама. Једна од најзначајнијих карактеристика NERA EVOLUTION система је могућност реализације радио-релејних праваца на једном или на више канала. Под појмом канал подразумева се пуни дуплекс, фреквенцијски пар за истовремени пријем и предају. Различите конкретне изведбе називају се конфигурације. METRO LONG HAUL омогућава конфигурације почевши од основне 1+0 (један радни канал, плус „нула“ -нема заштитног канала) па све до максималне конфигурације од 7+1 и 10+0.

Радио-релејни уређај NERA EVOLUTION који се користи за реализацију приступних праваца различитог, променљивог капацитета и формирање приступне равни система преноса назива се NERA EVOLUTION – XPAND. Овај уређај је реализован као PDH радио-релејни уређај, скалабилног капацитета, нивоа до 75 x E1 (E1=2Mb/s према ITU G.703).

Радио-релејни уређај NERA EVOLUTION који се користи за реализацију приступних праваца релативно малог, непроменљивог капацитета и формирање приступне равни система преноса назива се NERA EVOLUTION – ACCESS. Овај уређај је реализован као PDH радио-релејни уређај нивоа од 4 x E1 или 16 x E1 (E1=2Mb/s према ITU G.703).

Платформа фамилије радиорелејних уређаја NERA EVOLUTION је осмишљена, дизајнирана и реализована на модуларном концепту. Модули, склопови су техничко технолошке целине које имају једнозначно одређену функцију. Исти модули се могу наћи у различитим конфигурацијама уређаја. Тако, примера ради, иста јединица

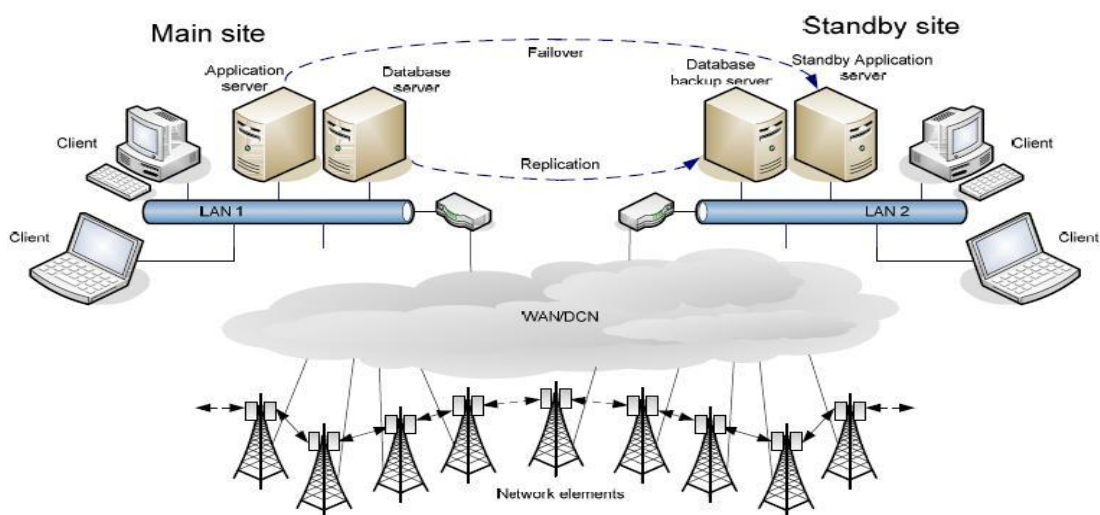
примопредајника се користи у NERA EVOLUTION – XPAND уређају капацитета 12 x E1 и у NERA EVOLUTION – METRO LONG HAUL уређају капацитета 155 Mb/s.

Основни механички елементи које се употребљавају за смештај модула и склопова су ормар и рам. Поред наведених основних постоје и други механички елементи који служе за формирање целине радио-релејног уређаја.

4.3.2 Могућност имплементације мреже за надзор и управљање у радио-релејној мрежи

Опрема произвођача NERA је дизајнирана да оптималне резултате рада постигне у мрежном окружењу, када се од више праваца формира мрежна топологија и када се сви уређаји спрегну кроз систем за надзор и управљање. За централизовани надзор и управљање користи се апликација „Net Master“ која је препоручена од произвођача. Могуће је под одређеним условима користити и друге апликације, али је то редак случај. Истовремено, могуће је функционисање једног или више праваца ван централног система за надзор и управљање.

Надзор и управљање радио-релејном опремом могуће је реализовати на више начина. Типичан начин реализације препоручен од стране произвођача базира се на формирању радне и резервне локације за менаџмент података што је и приказано на слици 4.10



Слика 4.10 Организација надзора и управљања PPMr

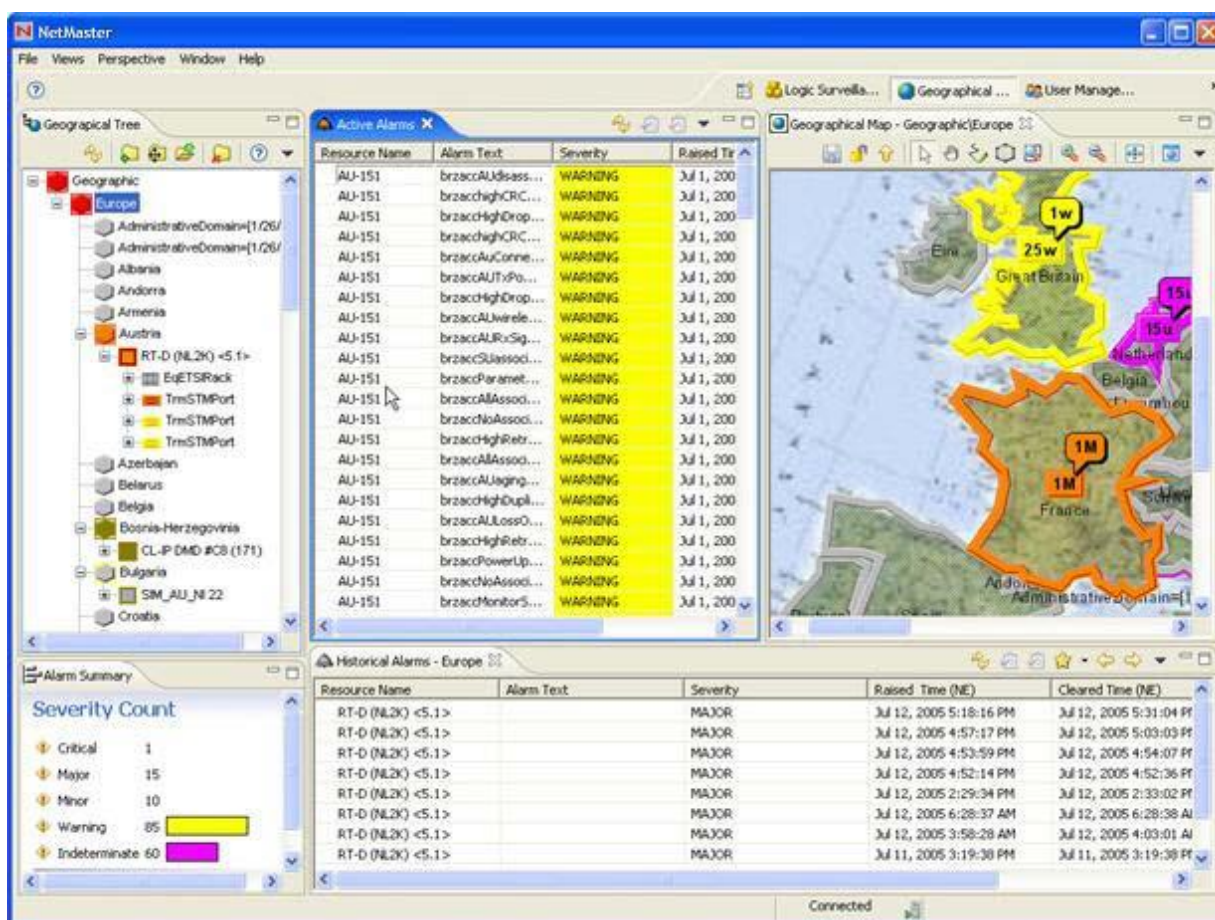
Интерфејси дефинисани од стране произвођача омогућавају повезивање уређаја преко независне мреже за надзор и управљање у јединствен систем надзора. Такође уређаји омогућавају повезивање у мрежу надзора и управљања путем контролних бита у заглављу STM-1/STM-4 сигнала. Одабир уређаја овог произвођача у сврхе приказа мреже за надзор и управљање базира се и на специјалној могућности уређаја да обрађује информације о статичким мрежним адресама суседних уређаја или уређаја у групи. Уређаји поседују интегрисани мини рутер у управљачкој јединици, што им даје посебне функционалности и нову димензију приступа надзору телекомуникационе опреме. Унутрашњи интегрисани рутер уређај подешава се за рад преко OSPF протокола, што значајно убрзава рад мреже за надзор и управљање овом врстом опреме. Размена управљачких информација се одвија у затвореним областима мреже које се дефинишу од стране пројектанта мреже, а податке о суседним областима поседују гранични рутери.

Анализирајући могућности и функционалности софтвера „NetMaster“ за надзор и управљање мрежом радио-релејних уређаја може се доћи до закључка да обезбеђује:

- управљање грешкама
- управљање перформансама
- управљање конфигурацијом
- управљање сигурношћу
- графички интерфејс
- мрежну топологију користећи домене
- аутоматску детекцију стања на уређајима
- анализу хардвера и софтвера на уређајима
- послове даљинске надоградње софтвера
- интерфејсе за управљачке системе више равни.

Апликација „Net Master“ представља свеобухватан систем за управљање мрежом и омогућава централизован рад и способност одржавања за све врсте и типове уређаја у мрежи ове фамилије уређаја. Помоћу овог софтвера може се управљати из „Web“ окружења свим елементима у мрежи. Софтвер је дизајниран са способностима конфигурисања, детекције кварова, праћења и управљања перформансама и

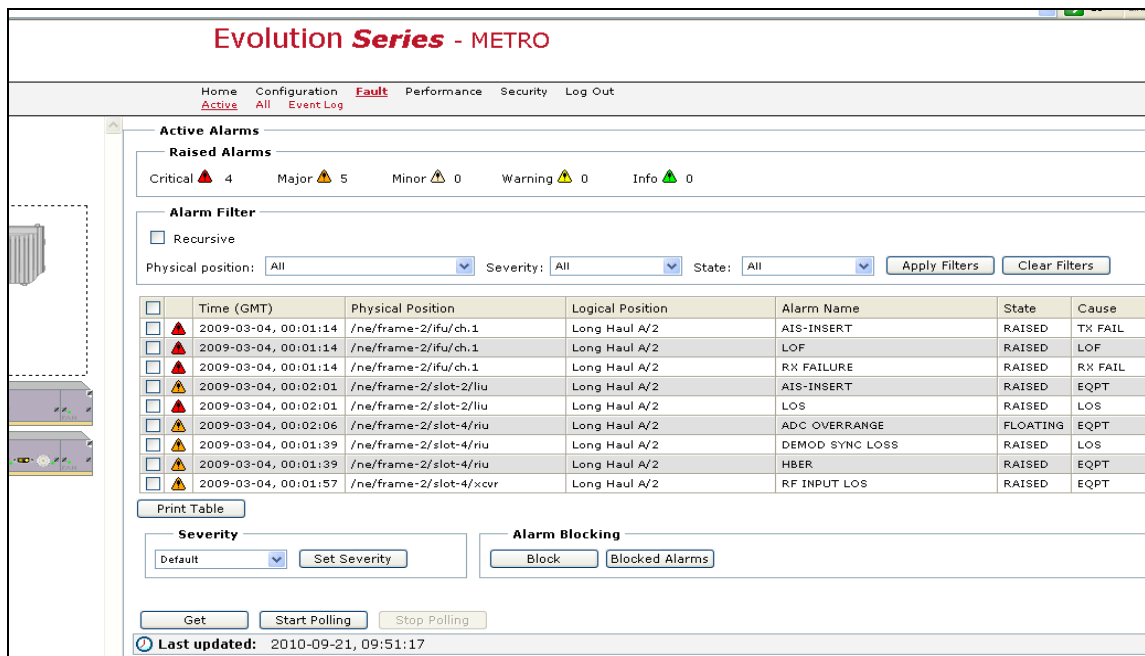
управљањем политикама безбедности. Главна намена софтвера је поједностављење комуникације путем мрежних интерфејса унутар и између преносних и транспортних уређаја, као и корисника или администратора мреже. У циљу реалног приказа стања у мрежи софтвер поседује „auto-discovery“ принцип рада и користи податке конфигурација у уређајима да аутоматски управља мрежом. Различитим уређајима и њиховим стањима може се приступити користећи графички приказ самог уређаја и његове попуне. Приказ графичког окружења елемената са приказом тренутног стања у мрежи представљен је на слици 4.11



Слика 4.11 Графички приказ стања мреже у апликацији Net Master

У току рада софтвер врши стално ослушкивање рада уређаја у мрежи и прикупљене податке обрађује и приказује у пољу за статус мреже и догађаје на уређајима. Извештавање корисника и администратора система реализује путем графичких обавештења приказаних на слици 4.12 док у самом уређају се могу прочитати конкретни подаци о насталој промени са свим параметрима битним за њену анализу.

Графички интерфејс уређаја коме се приступа након уочених промена стања приказан је на слици 4.12



Слика 4.12 Приказ грешака на уређају у мрежи

Широка база података доступна преко софтвера и добро организовано упутство у самом софтверу омогућавају кориснику сталну анализу дешавања у мрежи.

Посебне предности софтвера базирају се на могућностима формирања редувантних сервера и организовања безбедног складиштења података и конфигурација мрежних уређаја.

4.4 Рачунарска мреже и могућност имплементације мреже за надзор и управљање

Велики број предузећа за своју унутрашњу говорну и видео комуникацију као и размену података, користи локалне рачунарске мреже. Локалне рачунарске мреже базиране су на логичкој и најчешће организационој технологији предузећа и прате пословне процесе у њему.

Имајући у виду да се ради о најразличитијим типовима ЛАН мрежа са различитим бројем корисника за потребе приказа користиће се модел предузећа у којем постоји већи број ЛАН мрежа које се налазе на различитим локацијама, али су међусобно

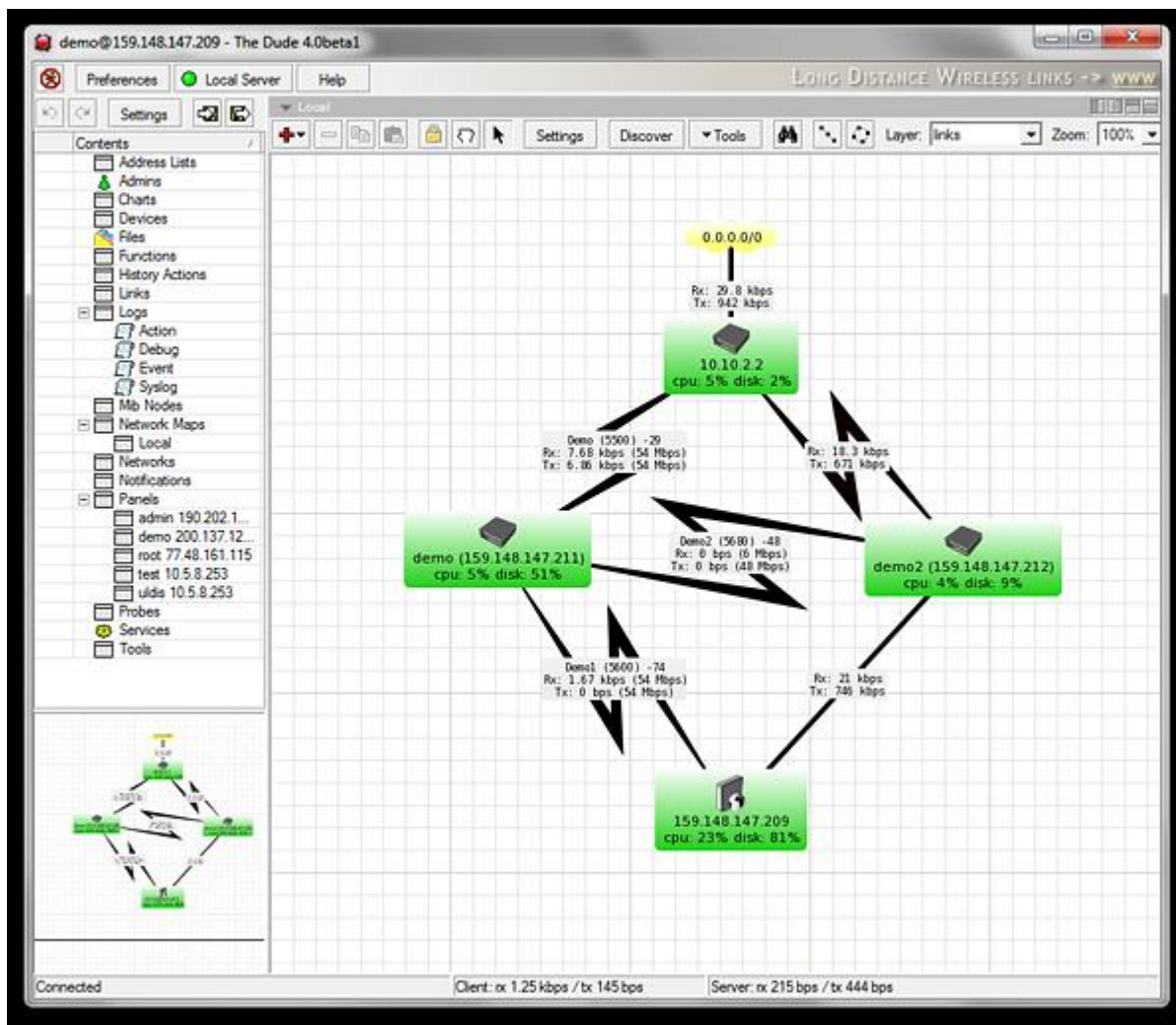
повезане WAN линковима у јединствену рачунарску мрежу организације. Локалне рачунарске мреже агрегирају пакетски саобраћај према телекомуникацим центрима предузећа, где се врши даље повезивање опреме према портовима преносно-транспортних система.

Сагледавањем тржишта мрежних уређаја и опреме може се рећи да тренутно у складу са односом цене и квалитета најбоље резултате у нижем ценовном рангу даје мрежна опрема произвођача „MicroTik” док у вишем ценовном рангу предњачи опрема произвођача CISCO. Мрежна опрема инсталирана у предузећима за потребе ЛАН мрежа захтева као и код јавних оператера удаљени начин управљања и надзора.

Као пример софтвера који се користи за надзор и управљање рачунарском мрежном опремом навешћемо „Dude” који се типично користи за управљање мрежном опремом произвођача „MicroTik”. Могућности наведеног софтвера заснивају се на константном праћењу следећих параметара:

- сервиса и промена везаним за напајање,
- поруке и обавештења,
- графичком приказу стања,
- праћењу функционалности уређаја,
- праћењу логовања,
- ажурирању података на „Syslog” серверу,
- управљање „MIB” тачкама у мрежи,
- тест параметрима опреме.

Софтвер пружа прегледну радну површину за приказ и рад што се може видети на слици 4.8



Слика 4.8 Пример радног графичког окружења софтвера „Dude“

Имајући у виду да се ради о имплементацији надзора у рачунарској мрежи, приказани софтвер је намењен за рад на независној станици у опсегу адреса мрежне опреме, дакле ван адресног опсега опреме у рачунарској мрежи.

5. КРИПТОЛОШКИ ПРИСТУП АНАЛИЗИ ЗАШТИТЕ МРЕЖА ЗА НАДЗОР И УПРАВЉАЊЕ ТЕЛЕКОМУНИКАЦИОНИМ УРЕЂАЈИМА

5.1 Улога и значај заштите информација у телекомуникационим системима

Актуелна дешавања у оквиру безбедности савремених информационо-комуникационих технологија постављају нове императиве како за примену раније усвојених решења у компанијама тако и за имплементацију нових. Пројектанти система суочени су са проблемима високе расположивости, поузданости и квалитета телекомуникационих услуга с једне и са величином и различитостима доступне опреме с друге стране. Савремени телекомуникациони системи омогућавају сигуран и безбедан пренос информација путем своје инфраструктуре. У савременом комерцијалном пословању постоји потреба за заштитом комуникација у циљу безбедног и сигурног преноса пословних информација. Улагања у опрему за заштиту информација у једном телекомуникационом систему представљаја значајну финансијску инвестицију, па се као један од основних елемената приликом планирања телекомуникационих мрежа разматра фактор безбедности о чему смо раније говорили. Питање економске исплативости оваквих комуникација има смисла за предузећа која размењују битне информације путем телекомуникационе мреже, а чијим би се пресретањем могло нарушити пословање или произвести велика материјална штета. Заштита информација на спојном путу нашла је посебну примену у мрежама државних органа где поверљивост информација има посебан значај за функционисање државних институција.

Узимајући у обзир улогу и значај једног телекомуникационог система, за предузеће које поседује све претходно разматране телекомуникационе системе, може се извести закључак да правилно, сигурно и безбедно функционисање мреже за надзор и управљање има непроцењиву вредност. Значај сигурног и безбедног функционисања овакве мреже телекомуникационих уређаја обезбеђује се сигурним и безбедним процесом управљања телекомуникационом опремом. Нарушавањем овог система може

се проузроковати велики губитак у пословању предузећа, угрозити радни процес, организација и довести до губитка значајних и поверљивих података.

5.2 Потенцијални начини угрожавања мрежа за надзор и управљање телекомуникационим мрежама

Анализом потенцијалних начина угрожавања мреже за надзор и управљање телекомуникационим системима може се доћи до закључка да потенцијални нападач може имати више разлога да нанесе штету систему како би дошао до осетљивих података ради уништења или промене или са циљем да онемогући приступ корисника систему. Основне мете напада представљају мрежни уређаји, приступно-транспортни системи и крајње корисничке апликације. Напади који су усмерени на податке који се преносе путем мреже за надзор и управљање телекомуникационим уређајима могу се класификовати у две групе:

1) пасивне нападе

Подразумевају нападе који су усмерени на прислушкивање и надгледање података без њихове измене. Пасивни напади представљају много једноставнији пут да се дође до података. Они су базирани на посредном принципу прибављања и теже их је открити у мрежи.

2) Активни напади

Подразумевају нападе који су усмерени на промену садржаја поруке. Реализација ових напада усмерена је на процес модификације пакета података који се крећу у мрежи, обично је у комбинацији са слањем лажних пакета и прекидима тока података. Ови напади су потенцијално опаснији, али су доста лакши за откривање.

5.3 Могућност реализације заштићеног преноса података

Савремене мреже за надзор и управљање телекомуникационим системима покушавају да својим корисницима и администраторима омогуће заштићени пренос података, порука и управљачких информација, а у циљу заштите података од неовлашћених лица о опреми, конфигурацијама, комуникацијама, пословним тајнама. Заштита информација се реализује на више начина, а базира се на:

1) заштити линкова (енг. "link encryption")

Овај вид заштите односи се на комплетан саобраћај на линковима успостављеним између две локације. Анализирајући слојеве OSI референтног модела можемо рећи да се овај вид заштите успоставља завршно са другим слојем и не омогућава потенцијалним нападачима да остваре увид у процес рутирања података.

Имајући у виду да се заштитом линкова суштински штите комуникације потребно је знатно више новца за реализацију оваквог начина заштите, с обзиром да се штити комплетна путања. Проблем овог начина реализације постаје посебно изражен уколико линкови имају више тачака одграђавања капацитета у мрежи. Ова врста заштите може бити деконспирирана уколико се на одређеним деоницама линка не користи адекватна заштита.

2) заштити са краја на крај (енг. "end-to-end encryption")

Ова врста заштите је реализована на комплетном спојном путу. Сагледавањем овог принципа рада на OSI референтном моделу долазимо до закључка да се она реализује преко више слојева модела. Овај вид заштите се реализује са краја на крај где се уједно врши и дешифровање. Проблем овог вида заштите података представљају сервисне информације и заглавља порука. Потенцијални нападач на основу ових елемената може да изврши лакши увид у рутирање и евентуално да лакше изврши декриптовање садржаја.

5.4 IPSec протокол

IPSec представља колекцију протокола који служе да обезбеде сигуран и заштићен пренос IP пакета кроз мрежу. Иако је сложен, овај модел се показао као врло успешан за заштиту TCP/IP врсте саобраћаја, а посебно је примењен у реализацији VPN-ова. Први пут је дизајниран током 1992.године, а зачетници идеје су били Johan Ioannidis, Phil Karn I William Allen Simpson. Они су за основу овог протокола користили SP3 сигурносни протокол на мрежном нивоу који је користила америчка влада и ISO-ов Network Layer Security Protokol - swIPe протокол. Развој овог протокола текао је у правцу IPv6 адресирања, са чиме је и паралелно развијан, али се у међувремену адаптирао и прилагодио IPv4 адресирању и успешно се користи за заштиту саобраћаја.

Овај протокол је дизајниран за рад на трећем слоју OSI референтног модела, такозваном мрежном слоју. Основни принципи на којима се овај протокол базира су:

- 1) контрола приступа подацима
- 2) аутентификација података
- 3) ауторизација корисника
- 4) заштита од преслушавања
- 5) тајност података (криптовање)

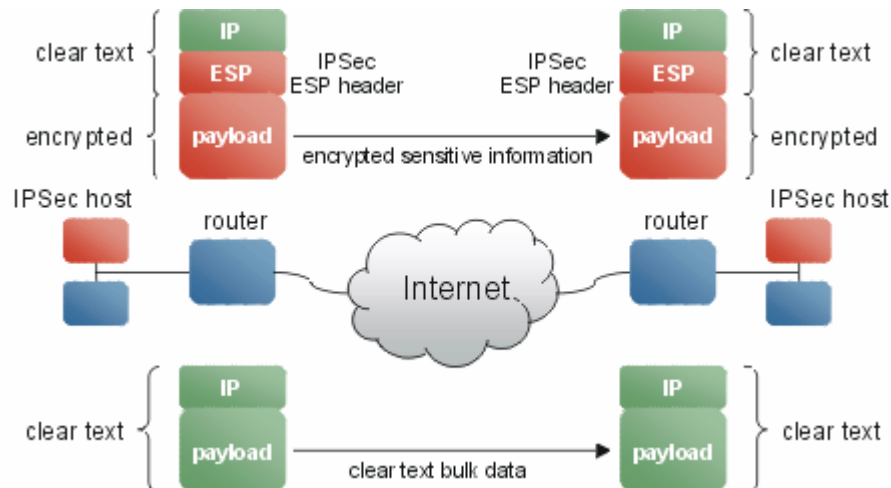
IPSec подржава два начина рада:

- 1) тунелирање пакета
- 2) транспортни начин рада

У првом начину реализације неколико рачунара (или цела LAN мрежа) скрива се иза једног чвора, па на тај начин постаје невидљив остатку мреже што је штити од напада.

У другом случају пакети се шаљу између два крајња рачунара на мрежи, при чему се рачунар који прима пакет реализује сигурносне провере пре испоруке пакета вишим слојевима OSI референтног модела.

Основни принцип рада овог протокола приказан је на слици 5.1



Слика 5.1 Приказ рада мреже базиране на IPsec протоклу

Протокол IPsec састоји од више протокола који служе да обезбеде заштићен и сигуран пренос пакета кроз мрежу. Постоје три најважнија протокола које IPsec користи, а то су:

- 1) AH – Authentication Header
- 2) ESP – Encapsulating Security Payload
- 3) IKE – Internet Key Exchange

Организационо гледано прва два протокола се могу сврстати у шифарске, док се трећи може сврстати у протоколе за размену кључева.

5.4.1 AH протокол

Authentication Header – AH протокол обезбеђује интегритет успостављене комуникације па проверава оргиналност података који се преносе у IP датаграмима. Опционо, овај протокол омогућава и заштиту од тзв. „replay“ напада за шта користи технику одбацавања старих пакета. Слика 5.2 илуструје заглавље AH пакета

0	1	2	3
0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Next Header	Payload Length	RESERVED	
Security Parameters Index (SPI)			
Sequence Number			
Authentication Data (variable)			

Слика 5.2 Приказ заглавља АН пакета

Слика илуструје следећа поља:

- **Next Header** – означава протокол података који се преносе (TCP или UDP)
- **Payload Length** – дужина АН пакета
- **RESERVED** – битови који се још не користе (вредност 0)
- **Security Parameters Index (SPI)** – комбинација сигурносних параметара и IP адресе
- **Sequence Number** – редни број пакета, користи се за заштиту од „replay“ напада
- **Authentication Data** – скуп података који се користи за аутентификацију пакета

5.4.2 ESP протокол

Encapsulating Security Payload (ESP) заглавље омогућава проверу оригиналности пакета, интегритет и тајност података који се преносе. Слика 5.3 илуструје заглавље ESP пакета

0								1								2								3								
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	
Security Parameters Index (SPI)																																
Sequence Number																																
Payload * (variable)																																
								Padding (0-255 bytes)																								
																Pad Length								Next Header								
Authentication Data (variable)																																

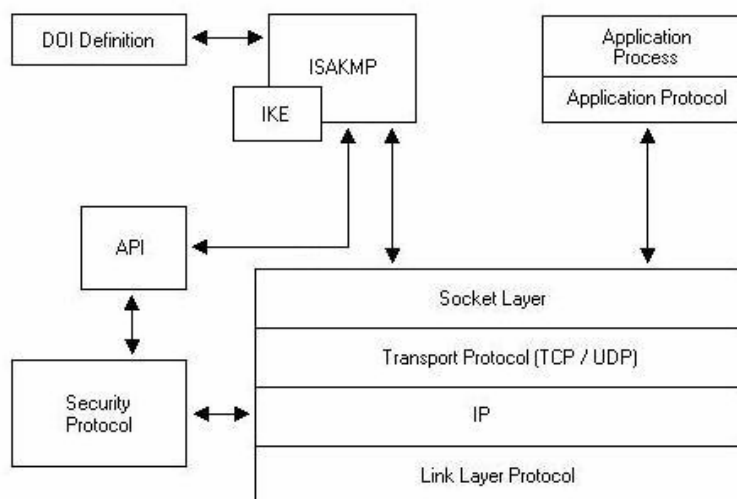
Слика 5.3 Приказ заглавља ESP пакета

Слика илуструје следећа поља:

- **Security Parameters Index (SPI)** – комбинација сигурносних параметара и IP адресе
- **Sequence Number** – редни број пакета, користи се за заштиту од „replay“ напада
- **Payload Data** – подаци који се шаљу
- **Padding** – користи се за пренос података који попуњавају цели блок
- **Pad Length** – дужина Padding поља
- **Next Header** – означава протокол података који се преносе (TCP или UDP)
- **Authentication Data** – скуп података који се користи за аутентификацију пакета

5.4.3 IKE протокол

IKE протокол извршава обострану аутентификацију корисника и успоставља SA (енг. “Security Association“) везу. Успостава ове везе подразумева прорачун „keying“ материјала као и договарање око скупа алгоритама и других параметара које ће SA штитити. Протокол функционише као иницијатор везе и нуди прихватљиве параметре за SA. Ако их друга страна прихвати остварује се SA веза. Пример успешног шифовања података за слање преко мреже од стране API (енг. “Application Programming Interface“) апликације помоћу IKE протокола приказан је на слици 5.4



Слика 5.4 Приказ рада IKE протокола

5.5 Могуће имплементације IPSec решења за потребе мрежа за надзор и управљање телекомуникационим мрежама

Досадашња пракса је показала да постоји све већа потреба за адекватном заштитом система. Анализом основних концепта заштите дошли смо до закључка да је у пракси најбоља заштита на што нижем слоју OSI референтног модела, чиме се побољшава сигурност преноса података у рачунарској мрежи. Разматрањем могућности зланомерних напада и функционалности IPSec протокола можемо закључити да фокус сигурности треба задржати на мрежном или тзв. трећем слоју OSI референтног модела. Заштита на овом слоју имала би изузетно велики значај и у мрежи за надзор и управљање телекомуникационим уређајима. IPSec протокол и уређаји који раде на бази овог протокола имали би централну улогу у заштити информација између главног центра за надзор и управљање и регионалних центара за надзор и управљање.

Заштита података за потребе преноса управљачких информација у мрежама за надзор и управљање телекомуникационим мрежама у пракси може се реализовати на два начина. Први и једноставнији начин реализације подразумевао би коришћење комерцијалних решења произвођача мрежне опреме где би се IPSec протокол применио на нивоу комуникације између мрежних уређаја коришћењем комерцијалних шифарских

алгоритама произвођача. Други начин заснивао би се на сопственом симетричном шифарском алгоритму који би се развио модификацијом AES алгоритма, са што већим могућностима утицаја на алгоритам и кључеве од стране крајњег корисника система.

Узимајући у обзир изнете варијанте заштите са аспекта безбедности најбољи модел би представљао други начин имајући у виду да се ради о поузданијем систему заштите информација.

6. ИМПЛЕМЕНТАЦИЈА МРЕЖЕ ЗА НАДЗОР И УПРАВЉАЊЕ ТЕЛЕКОМУНИКАЦИОНИМ УРЕЂАЈИМА У БЕЗБЕДНОМ ОКРУЖЕЊУ

Имплементација мреже за надзор и управљање телекомуникационим уређајима представља сложен процес који се реализује кроз планирање и пројектовање пре, у току или након успоставе телекомуникационе мреже. У процесу планирања неопходно је сагледати и прецизно дефинисати све претходно обрађене аспекте како би се извршило што квалитетнији приступ реализацији процеса увођења мреже у рад. У складу са сагледаним стањем следи процедура израде пројекта мреже и формирање неопходних тимова за реализацију пројекта.

У процесу планирања и израде пројекта неопходно је придржавати се проактивног приступа реализације пројекта. Под наведеним приступом подразумева се да се пројекат не реализује само у складу са садашњом ситуацијом, већ да представља основицу за будућа проширења и унапређења система, како у погледу дефинисања нових телекомуникационих мрежа, тако и у погледу примене нових система заштите информација. Сам проактивни приступ заснован је на далекосежном предвиђњу развоја телекомуникационе опреме и система, као и мрежа и софтвера за надзор и управљање истим.

Надзор и управљање телекомуникационом мрежом заснива се на реализацији функција из овог домена које су имплементирани за рад у безбедном окружењу. Управљачки подаци и конфигурације које се преносе кроз мрежу представљају веома интересантан материјал за потенцијалне нападачице како из спољног тако и из унутрашњег окружења. Применом активног или пасивног напада нападач може овладати подацима, ознакама, параметрима, конфигурацијама уређаја у мрежи па исте може злонамерно употребити за наредне акције са циљем нарушавања безбедности како мреже тако и функционисања целокупне организације за чије потребе је имплементирана. Стога се мора посветити велика пажња поступку имплементације система за заштиту информација у мрежи.

Модел мреже за надзор и управљање телекомуникационом мрежом практично је анализирати на примеру затвореног предузећа са разгранатом организационом структуром по територији. При анализи користимо начела која нам могу дати праву слику о функционисању једне сложене организације. Претпоставке ћемо базирати на постојању телекомуникационе опреме организоване у системе који се налазе у власништву предузећа, а размештени су на крајњим тачкама корисника, у телекомуникационим центрима. Инфраструктурни део мреже чине жични спојни путеви у власништву предузећа и јавних оператера услуга, као и бежични спојни путеви који су формирани путем радио-релејних уређаја у сопственом власништву. Рачунарке мреже су логички и топлошки организоване у складу са организационим целинама предузећа, а мрежна опрема се налази у телекомуникационим центрима предузећа.

Уколико извршимо анализу одговарајућих чинилаца у циљу планирања мреже за надзор и управљање телекомуникационом мрежом из претходног поглавља дошли би до почетних смерница за планирање.

У погледу техничких чинилаца неопходно је реализовати следеће:

- формирати логичку и тиополошку организацију независне рачунарске мреже за потребе надзора и управљања рачунарском и телекомуникационом опремом,
- у циљу реализације повезивања и формирања мреже за надзор и управљање неопходно је планирати и формирати саобраћајне ресурсе у телекомуникационој мрежи којом управљамо како би умањили цену пројектованог система,
- формирати регионалне центре за надзор и управљање у циљу повећања аутономности система и скраћења времена опоравка у случају отказа
- сагледати потенцијална агрегирања података и управљачких информација у мрежи за надзор и управљање на принципу архитектуре звезде као и прослеђење истих према главном надзорном центру,
- коришћењем рутера у регионалним центрима и главном центру за надзор извршити агрегирање и удруживање управљачких процеса на микролокацијама,

- за приступ телекомуникационим саобраћајним портовима користити саобраћајне интерфејсе засноване на стандарду G.703 или G.704/G.803 зависно од физичких ресурса опреме. На локацијама где постоје ограничени ресурси интерфејса користиће се конвертори интерфејса,
- извршити припрему и подешавање опреме у складу са физичком и логичком топологијом мреже,
- размену порука у мрежи и управљачких информација за надзор телекомуникационе опреме је заснивати на „Ethernet“ комуникацији,
- у циљу управљања телекомуникационом опремом и подсистемима користиће се апликативни софтвери MarWatch, Сунце М и Сунце +, NetMaster, Dude као и заштићени удаљени приступи помоћу VPN комуникација.

У погледу безбедносних чинилаца неопходно је реализовати следеће:

- сагледати распоред опреме и организациону структуру предузећа у циљу дефинисања политике безбедности за мрежу за надзор и управљање телекомуникационом мрежом,
- применом уређаја за заштиту информација формирати заштићене комуникације између регионалних центара за надзор и управљање и главног центра за надзор и управљање у циљу безбедног преноса информација преко инфраструктуре која није у власништву предузећа или је подложна отицању података,
- у складу са овлашћењима запослених дефинисати нивое приступа опреми, серверима и апликативним софтверима у мрежи за надзор и управљање,
- у циљу спречавања недозвољеног приступа и малициозних напада извршити превентивна подешавања опреме адекватним мерама заштите.

У погледу организацијских чинилаца неопходно је реализовати следеће:

- формирати регионалне центре за надзор и управљање телекомуникационом опремом како у погледу инфраструктуре, хардвера и софтвера, тако и у погледу запослених лица које ће се бавити пословима надзора и управљања опремом,
- придржавајући се препорука поменутог стандарда ITU M.3010 који дефинише управљачке слојеве мреже за надзор и управљање извршиће се имплементација

слојева NEML, NML и SML. Слој BML не користимо пошто се у овом систему не разматра управљање пословањем имајући у виду да се ради о мрежи затвореног предузећа, коме није основна намена пружање телекомуникационих услуга у циљу остваривања профита,

- створити услове за проширење система услед планираних и непланираних потреба.

6.1 Сагледавање стања у телекомуникационим мрежама са предлогом модела реализације мреже за надзор и управљање

Анализом досадашњих система јединствене телекомуникационе мреже која нам служи као полазна основа за планирање мреже за надзор и управљање можемо доћи до закључка да је имплементација исте изузетно сложен процес. Приступ проблему се разматра из угла сваког подсистема са предлогом увезивања, подешавања и адресирања опреме према организационом распореду целина предузећа.

У приступу реализацији проблема увођења мреже за надзор и управљање кренуће се са претпоставком да је предузеће у коме су имплементирани до сада разматране мреже распрострањено на већем делу територије државе. У циљу формирања јединственог (главног) центра за надзор и управљање неопходно је извршити претходно груписање управљачких информација. Процес груписања би се заснивао на агрегирању саобраћаја за потребе ове мреже на регионалном принципу, како би се избегли проблеми са већим хаваријама у мрежи, а уједно и допринело растерећености процеса надзора, управљања и реаговања на непредвиђене ситуације. Најбољи принцип разматрања регионализације телекомуникационе мреже је подела територије државе на основу географских страна света, како би се са што мање људских и финансијских ресурса савладала велика територија. Овај принцип није увек правилан имајући у виду да се у већим градовима обично налазе мреже већег капацитета са већом концентрацијом телекомуникационих центара.

Мрежу за надзор и управљање потребно је организовати путем шест центара за надзор и управљање (енг. "NOC-Network Operation Center") распоређених по следећем принципу:

- 1) Главни центар за надзор и управљање (NOC_A)
- 2) Резервни центар за надзор и управљање (NOC_B)
- 3) Центар за надзор и управљање север (NOC_N)
- 4) Центар за надзор и управљање исток (NOC_E)
- 5) Центар за надзор и управљање запад (NOC_W)
- 6) Центар за надзор и управљање југ (NOC_S)

Наведени регионални центри извршили би на својој опреми прихват надзора и управљања свих уређаја из своје зоне надлежности, обезбедили би локални приступ свим подсистемима телекомуникационе мреже у својој зони и прослеђење управљачких информација према NOC_A и NOC_B. За потребе формирања мреже на свакој локацији у зависности од обима опреме у телекомуникационој мрежи у својој зони надлежности и од сродности послова које запослени могу истовремено да извршавају потребно је извршити категоризацију радних места за запослене.

Имплементација мрежне опреме на територији за потребе мреже за надзор и управљање заснована је на постављању рутера CISCO 1841 допуњених са потребним бројем картица за прихват потребних саобраћајних капацитета. Повезивање опреме реализовало би се сопственим саобраћајним капацитетима. За потребе адресирања WAN линкова у мрежи за надзор и управљање коришћен је адресни опсег 10.10.10.0/30, имплементиран VLSM техником како би се добило максимално искоришћење корисног броја адреса.

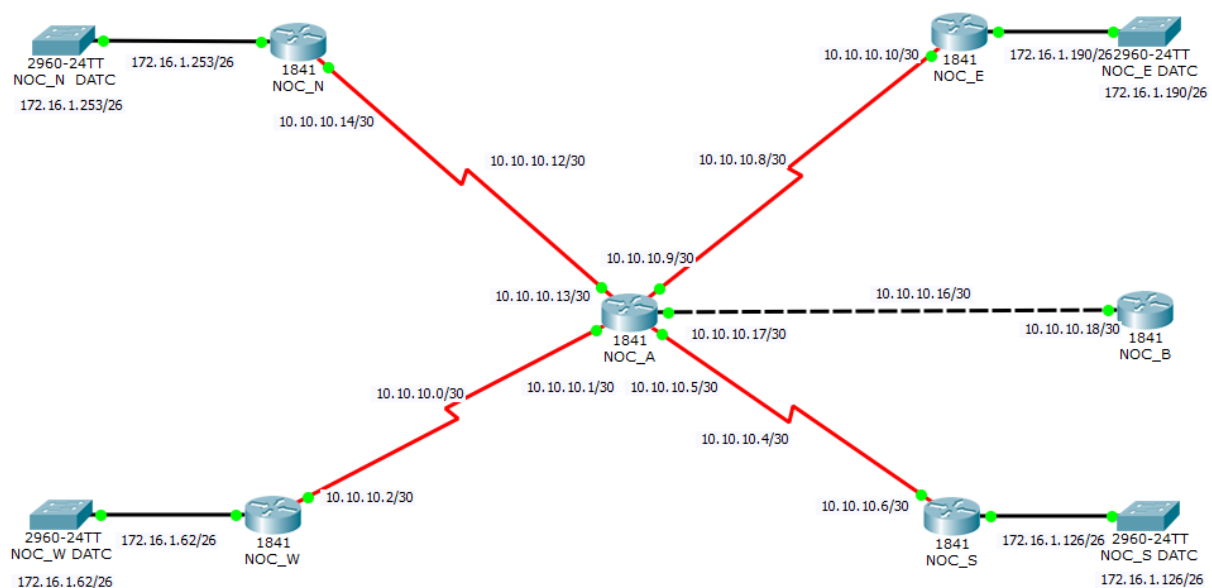
6.2 Предлог надзора и управљања системом комутације

Организација надзора и управљања централама заснива се на формирању рачунарске мреже централа како би се извршило повезивање истих са централном апликацијом за управљање. Повезивање и адресирање опреме на централну платформу мрежних уређаја реализује се на нивоу регионалних и главних центара за надзор и управљање.

Мрежу за надзор и управљање централама организовали би на територији по принципу:

- 1) централизованог надзора мреже централа апликацијом „MarWatch“ у NOC_A,
- 2) локалног надзора централа у зони из регионалних центара за надзор и управљање коришћењем наведене апликације
- 3) директног приступа централама на локацији на основу указане потребе

Организација мреже за надзор и управљање телекомуникационом мрежом централа представљена је на слици 6.1



Слика 6.1 Организација мреже за надзор и управљање телекомуникационом мрежом дигиталних централа

За потребе надзора мреже централа користи се мрежни опсег адреса 172.16.1.0/26 имплементиран коришћењем VLSM функционалности у 4 подмреже, за сваки регионални центар појединачно, како би се спречило ширење непотребних упита у мрежи и искористио што већи број корисних мрежних адреса.

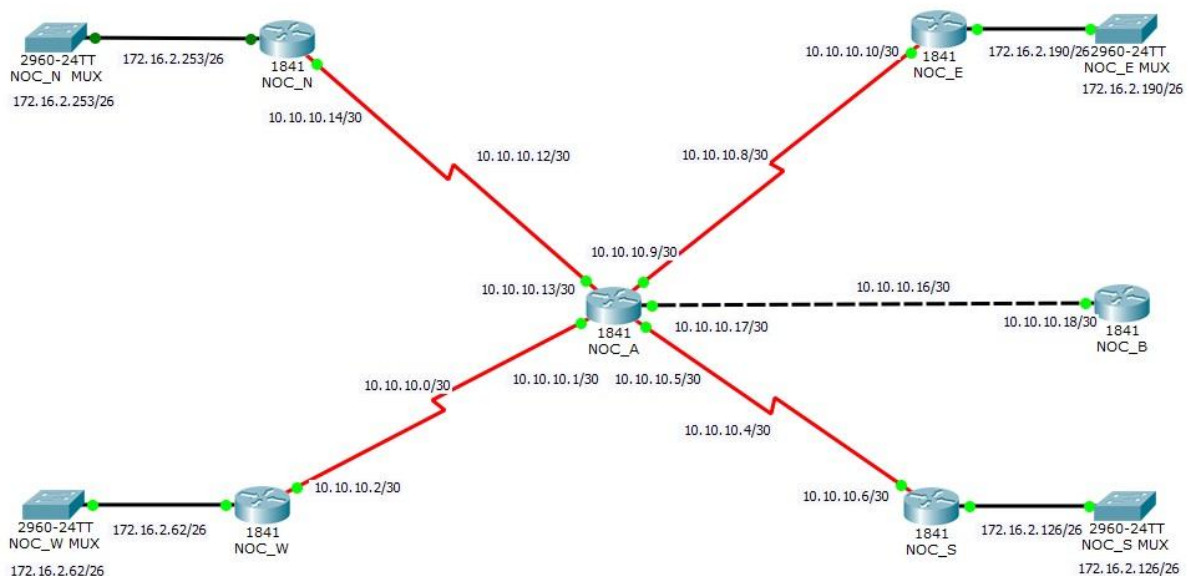
6.3 Предлог надзора и управљања системом приступно-транспортних (мультиплексних) уређаја

Имплементацију надзора и управљања у мрежама транспортних и приступних уређаја могуће је реализовати на истим принципима као што је претходно приказано за мрежу централа. За централизовано управљање мрежом користи се апликативни софтвер „СУНЦЕ +“ и „СУНЦЕ М“ који ради у мрежном окружењу у зависности од потреба и организације рада корисника о чему је раније било речи.

Мрежа за надзор и управљање мультиплексном опремом хијерархијски се организује на принципу:

- 1) централизованог надзора мреже помоћу апликације „СУНЦЕ +“ из NOC_A у синхронизацији са регионалним апликацијама „СУНЦЕ М“
- 2) локалног надзора мультиплексних уређаја у зони из регионалних центара за надзор и управљање коришћењем апликације „СУНЦЕ М“
- 3) директног приступа уређајима на локацији на основу указане потребе

Организација мреже за надзор и управљање телекомуникационом мрежом приступних и транспортних мультиплексних система представљена је на слици 6.2



Слика 6.2 Организација мреже за надзор и управљање телекомуникационом мрежом приступних и транспортних мультиплексних система

Као платформа за имплементацију мреже користи се исти распоред мрежних елемената. Мрежа надзора у управљања мултиплексном опремом организована је у опсегу адреса 172.16.2.0/26 уз коришћење VLSM технике адресирања.

6.4 Предлог надзора и управљања мрежом радио-релејних уређаја

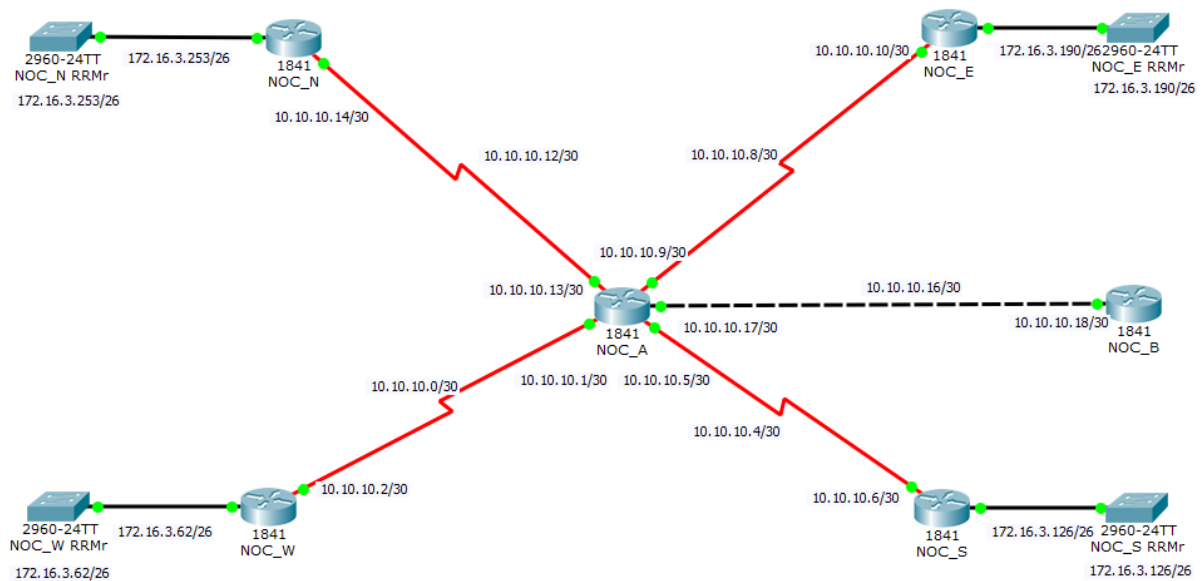
Надзор и управљање радио-релејним уређајима формира се правилним распоредом и адресирањем радио-релејних уређаја у зони функционисања. Имајући у виду да се наведени телекомуникациони систем у мрежи базира на размени управљачких информација на OSPF протоколу, неопходно је извршити правилно подешавање мрежне опреме за прихват и функционисање управљачких линкова. Протокол OSPF функционише разменом података о рутама, како у једној области, тако и између граничних рутера на границама зона па се неправилним подешавањима може узроковати погрешна размена информација.

Централни надзор мреже радио-релејних уређаја реализује се из NOC А коришћењем апликације „NetMaster”.

Мрежа за надзор и управљање радио-релејним уређајима хијерархијски се организује на принципу:

- 1) централизованог надзора мреже помоћу апликације „NetMaster”
- 2) директног приступа уређајима на локацији на основу указане потребе

Организација надзора и управљања радио-релејном мрежом представљена је на слици 6.3



Слика 6.3 Организација надзора и управљања радио-релејном мрежом

Мрежа за надзор и управљање радио-релејним уређајима имплементирана је у опсегу мрежних адреса 172.16.3.0/26 користећи распоред мрежних елемената за надзор и управљање у централној зони мреже.

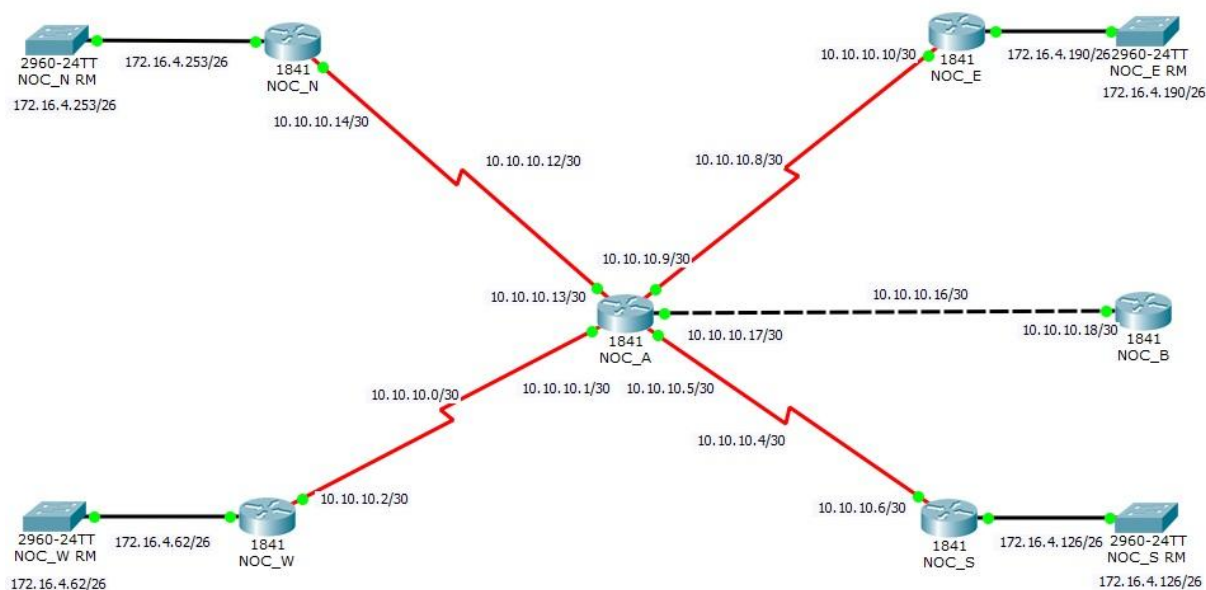
6.5 Предлог надзора и управљања рачунарском мрежом

Надзор и управљање рачунарском мрежом заснива се на надзору и управљању мрежним „L3“ уређајима који су имплементирани на демаркационим тачкама у рачунарској мрежи. Предмет ове врсте надзора нису крајњи сервери и рачунарска опрема, већ се подразумева да су они топлошки организовани како би се истим могло приступити преко уређаја „L3“ нивоа. У домену надзора и управљања уређајима „L3“ нивоа у рачунарској мрежи можемо говорити о централизованом приступу уређајима произвођача „Mikrotic“ које смо раније поставили као референтне.

Мрежа за надзор и управљање рачунарском мрежом се организује на принципу:

- 1) централизованог надзора мрежних „L3“ уређаја помоћу апликације „Dude“ из NOC_A
- 2) директног приступа „L3“ уређајима на локацији на основу указане потребе

Организација надзора и управљања рачунарском мрежом представљена је на слици 6.4



Слика 6.4 Организација надзора и управљања рачунарском мрежом

Мрежа за надзор и управљање рачунарском опремом имплементирана је у опсегу мрежних адреса 172.16.4.0/26 користећи распоред мрежних елементата за надзор и управљање у централној зони мреже.

6.6 Имплементација безбедног окружења за рад мрежа за надзор и управљање телекомуникационом мрежом

Савремене комуникације захтевају имплементацију безбедних услова за рад у циљу смањења могућности за отицање тајних података. Сагледавањем могућности потенцијалног нападача мрежа за надзор и управљање одређених телекомуникационим подсистемима, долазимо до закључка да последице напада могу бити несагледиве. Чињеница да немамо имплементиран систем заштите на спојном путу може довести до нелегалног прикупљања података, паралелног прикупљања и измене унетих података, лажних представљања у систему, планирања деструктивних напада у циљу урушавања телекомуникационих капацитета. Наведени потенцијални проблеми могу довести до несагледивих последица уколико се ради о мрежама државних органа једне земље, мада исте појаве могу нанети велике губитке и телекомуникационим оператерима услуга.

У циљу унапређења предложене имплементације мреже за надзор и управљање, као и анализирајући намену и могућности IPSec-а у претходним поглављима долази се до закључка да је неопходно обезбедити безбедан и сигуран пренос управљачких информација у мрежи за надзор и управљање. Стварањем таквих безбедносних услова за рад у једној мрежи ризик од нежењених напада и проблема у систему може се значајно умањити. Никада не можемо са потпуном сигурношћу рећи да је безбедност максимална имајући у виду да људски фактор може увек бити узрок нарушавања безбедности у једној мрежи.

Заштиту основних комуникационих праваца на нивоу мрежних уређаја између главног, резервног и регионалних центара за надзор и управљање телекомуникационим уређајима можемо реализовати на два начина:

- 1) коришћењем комерцијалних решења за успоставу IPSec VPN „site-to-site“ тунела између уређаја CISCO 1841
- 2) употребом посебних уређаја за шифровање који поседују сопствени алгоритам за имплементацију шифарског система

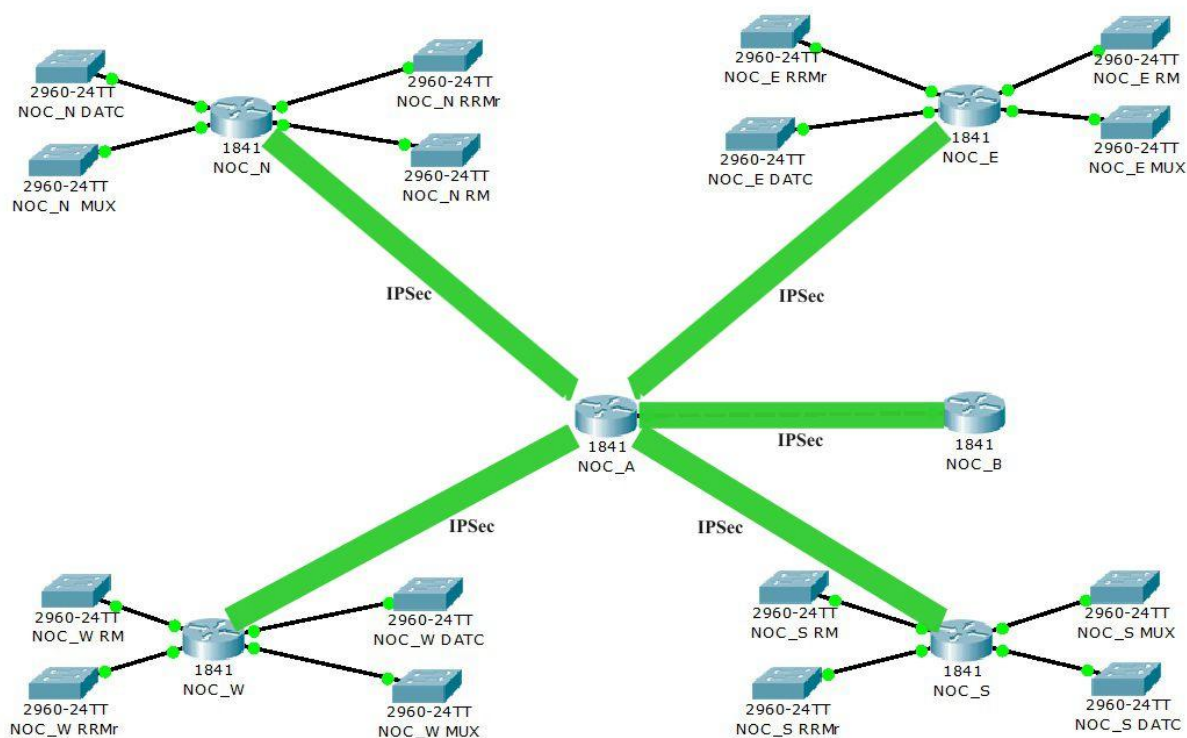
Први начин представља значајно јефтинију варијанту безбедносне заштите основних праваца комуникације, али у погледу безбедносне сигурности значајно је лошији од другог начина реализације. Узимајући у обзир да је предмет разматрања мрежа која се успоставља у затвореном телекомуникационом систему, без коришћења капацитета телекомуникационих оператера, за одабир модела заштите мреже користићемо први понуђени модел заштите. Овај начин заштите је доста једноставнији, јер не захтева имплементацију нових уређаја за криптозаштиту информација са свим пратећим трошковима.

Имплементација заштите информација извршила би се успоставом IPSec VPN „site-to-site“ тунела на следећим правцима:

- 1) Главни центар за надзор и управљање (NOC_A) - Центар за надзор и управљање север (NOC_N)
- 2) Главни центар за надзор и управљање (NOC_A) - Центар за надзор и управљање запад (NOC_W)

- 3) Главни центар за надзор и управљање (NOC_A) - Центар за надзор и управљање исток (NOC_E)
- 4) Главни центар за надзор и управљање (NOC_A) - Центар за надзор и управљање југ (NOC_S)
- 5) Главни центар за надзор и управљање (NOC_A) - Резервни центар за надзор и управљање (NOC_B)

Предлог реализације мреже за рад у безбедном окружењу приказан је на слици 6.5



Слика 6.5 Предлог реализације заштите за рад у безбедном окружењу

Подешавање рутера за рад у наведеном режиму рада представљало би пожељно оптерећење за експлоатацију њихових радних ресурса имајући у виду да се мрежа реализује на једноставнији начин без имплементирања додатних рутерских функција као што су NAT, PAT и слично. Поред предходно дефинисаних портова, приступних листа, рута, неопходно је извршити правилно подешавање рутера за рад успоставом IPSec тунела са суседима и подешавањима дужине кључа на минималних 256 бита.

ЗАКЉУЧАК

Савремене телекомуникационе мреже данас свој развој базирају на имплементацији најмодернијих информационих технологија. Пратећи захтеве и потребе корисника, телекомуникационе мреже се функционално развијају и имплементирају нове начине комуникације, користећи интеграцију са претходним технологијама и услугама. Прогресивни развој опреме, капацитета и услуга прати непрекидна интеграција разних технологија са циљем да се кориснику обезбеди висок степен доступности на било ком месту.

Телекомуникациони системи свој главни циљ фокусирају на квалитету и поузданости услуга корисницима, али се увек базирају на тзв. скалабилности система у циљу нових проширења, реализације нових сервиса и побољшању функционалности и економичности одржавања.

Експлоатација и управљање телекомуникационом мрежом представља сложен пословни процес, који се темељи на квалитетном планирању. Успешност надзора и управљања у једној телекомуникационој мрежи обезбеђена је правилном проценом скалабилности, флексибилности, поузданости, сигурности и безбедности.

Досадашња искуства и свакодневни безбедносни ризици у нашој земљи и свету захтевају подизање нивоа безбедносне културе у процесу надзора и управљања телекомуникационим системима. Осетљивост информација које се овом мрежом преносе захтевају квалитетну заштиту како не би дошло до нарушавања тајности. Зависно од намене, потреба, значаја и финансијских могућности можемо утицати на побољшање безбедносног окружења у коме је мрежа за надзор и управљање телекомуникационим системима имплементирана.

Тенденције даљег развоја телекомуникационих мрежа захтевају повећање нивоа безбедносне заштите управљачких информација у мрежама за надзор и управљање. За криптографске системе можемо рећи да су безбедни, у одређеном временском периоду. Као адекватан одговор на савремене ризике и претње можемо користити уређаје за криптозаштиту информација, а унапређења заштите реализовати праћењем савремених трендова и развојем криптографских алгоритама у циљу подизања нивоа безбедности информација.

ЛИТЕРАТУРА

- (1) Alex документација BC -13 за надзор и управљање PBX MXOne TSW
- (2) ITU-T препоруке M.3010, 3020, 3100, 3200, 3400 Telecommunication management network, Geneva,Switzerland, 2000
- (3) ITU-T препоруке M.3050.1, 3050.2, 3050.3, 3050.4 Enhanced telecommunication operation map, Geneva,Switzerland, 2000
- (4) ITU-T препорука M.3050 supplement 3 Enhanced telecommunication operation map, Geneva,Switzerland, 2004
- (5) Основни курс MX One TSW управљање и одржавање, Београд, Србија, Telegroup, 2007
- (6) Валентина Радојичић, Александра Костић-Љубисављевић, Горан Марковић: „Методологија планирања мреже“, PosTel 2008, Београд, Србија
- (7) „СУНЦЕ-М упутство за корисника“, Ирител, Београд, Србија, 2012
- (8) „NetMaster корисничко упутство за администраторе мреже“, Megalink, Београд, 2011
- (9) „Dude 4.0 корисничка документација“, MicroTik
- (10) „Дефинисање процеса увођења мреже за управљање телекомуникационим системима“, Владимир Суша, Наташа Госпић, YUINFO, Копаоник, 2010
- (11) Народна скупштина, Закон о електронским комуникацијама, Службени гласник Републике Србије, Београд
- (12) A.Menezes, P.van Oorschot, S.Vanstone, „Handbook of applied Criptography“, CRC Press Inc.USA
- (13) Младен Веиновић, Александар Јевремовић, „Рачунарске мреже“, Универзитет Сингидунум, Београд, Србија, 2016
- (14) Милан Милосављевић, Саша Адамовић, „Криптологија 2“ Универзитет Сингидунум, Београд, 2014
- (15) Дејан М. Гвоздић, „Трендови развоја оптичких телекомуникационих система, Електротехнички факултет, Београд, 2008
- (16) <http://www.icts.rs>
- (17) <http://www.ericsson.hr>
- (18) <http://www.iritel.com>
- (19) <http://www.itu.int>
- (20) <http://www.neratelecom.com>
- (21) <http://www.mikrotik.com>