ИЗГРАЖДАНЕ И КОНФИГУРИРАНЕ НА ХИБРИДНА МРЕЖОВА СВЪРЗАНОСТ ЗА ВИДЕОНАБЛЮДЕНИЕ МЕЖДУ СГРАДИ

Станимир Садинов

Технически университет Габрово, ул. Х. Димитър 4, Габрово, България

**кореспондиращ автор: murry@tugab.bg*

CONSTRUCTION AND CONFIGURING HYBRID NETWORK CONNECTIVITY FOR VIDEO SURVEILLANCE BETWEEN BUILDINGS

Stanimir Sadinov

Technical University of Gabrovo, H. Dimitar 4, Gabrovo, Bulgaria

**Corresponding author: murry@tugab.bg*

Abstract

The paper offers an example solution for the design and implementation of a hybrid communication network connectivity between three buildings. For this purpose, three different types of transmission media are used - wireless, optical and cable. The idea is to present a sample design and testing of a hybrid network with configuration of end devices and construction of a video server. Finally, sample tests and experimental work screens representing the capabilities of the selected equipment are presented.

Keywords: *PON, VLAN, NVR, video server*

ВЪВЕДЕНИЕ

Развитието на технологиите, широколентовият достъп, както и прогресът в телекомуникациите правят света, в който живеем постоянно променящ се. Резултатът от тази постоянна промяна на онлайн пространството е един нов вид свят – на дигитална система, продукт от сближаването на сфери като Интернет технологиите, телекомуникациите, медиите и забавната/развлекателната индустрия. Тези нови тенденции насочват вниманието към интензивна подкрепа за изграждане на хибридни мрежи, които с потенциала си, ще способстват за усъвършенстването на всички аспекти на широколентовата технология и широколентовите услуги. Хибридните мрежи могат да съдържат в себе си едновременно оптични, кабелни и безжични такива. В момента оптичните влакна се явяват най-съвършената и перспективна физична среда за пренасяне на информационни комуникационни сигнали. Предаването на информация с помощта на оптични влакна и влакнесто-оптични кабелни комуникационни линии и мрежи предоставя огромни предимства, в сравнение с класическите комуникационни преносни системи, използващи конвенционалните симетрични и коаксиални съобщителни кабели с медни проводници [1, 2, 3, 5, 6, 7, 9, 10, 11]. Все още обаче масово оптичните трасета не достигат изцяло до крайния клиент или дори да достигат – локалните мрежи – които са собственост и се поддържат от самия потребител, са изградени с медни кабелни трасета. Не са и редки случаите, в които към локалната мрежа трябва да се добави някое отделено работно място, до което няма как да стигне изцяло кабелна връзка – в тези случаи се използват и безжични мрежи [4, 8, 12].

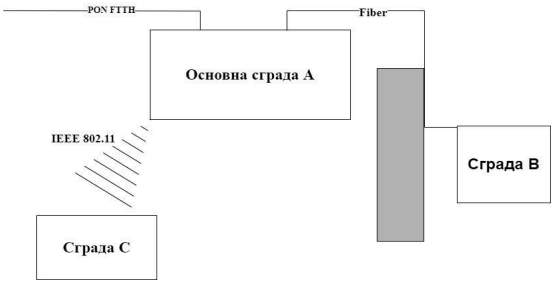
ИЗЛОЖЕНИЕ

В представена статия се разглежда проект на примерна хибридна мрежа, която ще трябва да осигури комуникация между мрежови устройства и камери за видеонаблюдение в три различни сгради, намиращи се на малко разстояние една от друга. Представения проект може да послужи при обучението на студенти с цел демонстрация на придобитите знания в реална среда на изпълнение на примерно задание. В разглеждания вариант основната сграда е на 3 етажа и в нея ще трябва да се конфигурират компютрите на служителите и камерите за видеонаблюдение. В проекта тя е записана като „Сграда А“. Останалите две сгради на компанията – „Сграда В“ и „Сграда С“ са по-малки складови помещения, в които не работят постоянно служители и в тях ще трябва да се конфигурират единствено камери. Също така видеонаблюдението в тях няма да се изгражда единствено локално, а трябва да има връзка с основната „сграда А“, тъй като в нея в отделено сървърно помещение ще бъде монтирана цялата апаратура на компанията, включително и записващите устройства.

Доставката на Интернет услугата до сградите ще се осъществява чрез Пасивна оптична мрежа (PON) технология, като вида на услугата е PON FTTH (Fiber To The Home) [5, 7, 9, 10, 11], тоест трасето ще е оптично от доставчика до самата сграда на компанията, и ще завършва в сървърното помещение.

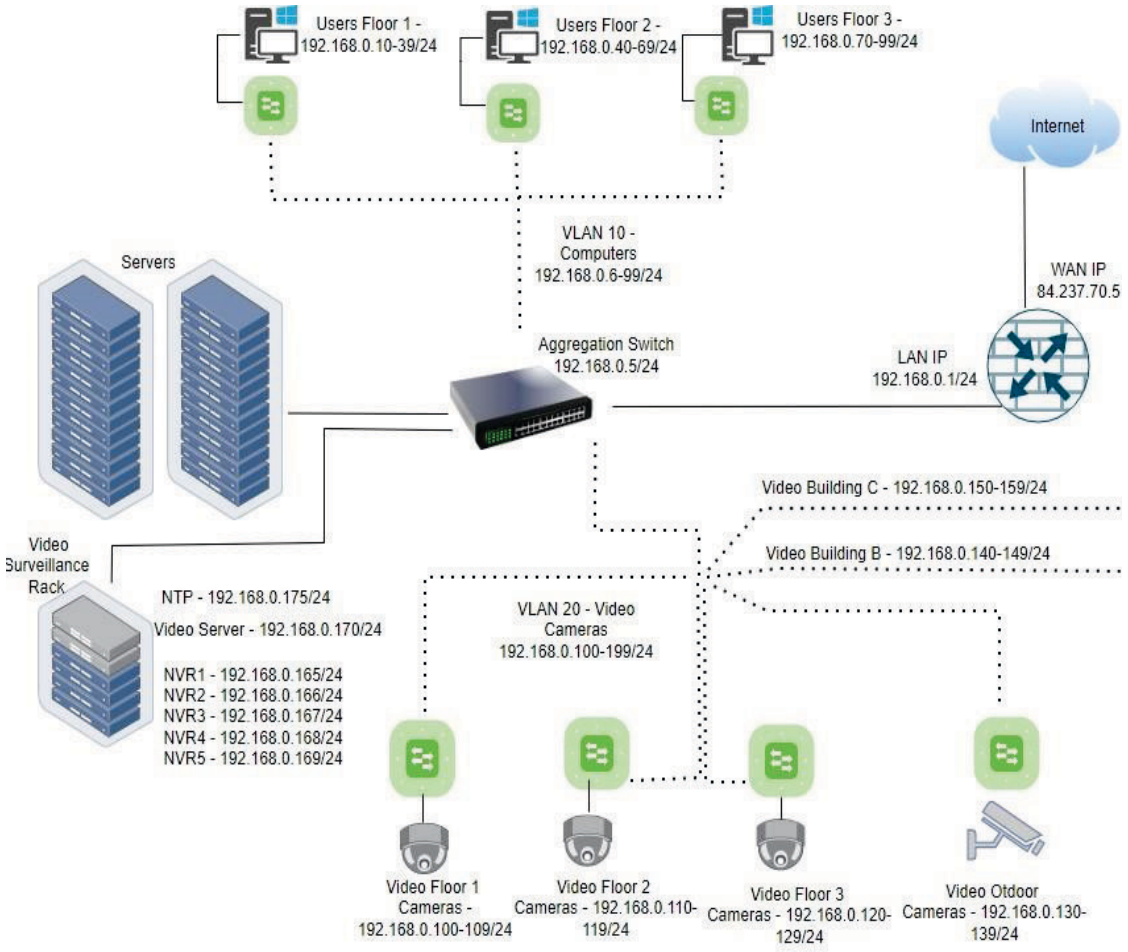
Между „Сграда А“ и „Сграда В“ няма пряка видимост, но има кабелен сноп стигащ от едната до другата сграда – в проекта на мрежата е заложено да се прекара оптичен кабел, с който да се осъществи връзката между двете сгради. (фиг.1) Въпреки, че тук скоростта на предаване на данни не е критична, е избрана оптична връзка заради следните й предимства в текущата ситуация:

- Разстоянието между двете крайни точки на трасето надвишава 100 метра и е много вероятно, ако комуникацията минава по меден кабел, да възниква затихване на сигнала;
- През по-голямата си част трасето ще минава през сноп пълен с кабели, провеждащи ниско и високо напрежение и оптичният кабел няма да се повлиява от електромагнитните излъчвания по маршрута си;
- Тъй като трасето е външно, оптичният кабел защитава апаратурата от повреди причинени от свръхнапрежение по комуникационната линия породено от гръмотевични бури.



Фиг. 1*.Разпределение на отделните сгради на компанията и връзките между тях*

Между „Сграда А“ и „Сграда С“ няма как да се прекара кабелно трасе, но има пряка видимост, затова сигналът между тях ще се прехвърли безжично. За целта ще се монтират външни антени на двете сгради, които ще преобразуват сигнала от медния кабел в локалната мрежа в основната сграда в безжичен и после обратно в кабелна връзка в „Сграда С“, за да се добавят устройствата към мрежата. Примерна схемна мрежова конфигурация е представена на фиг.2



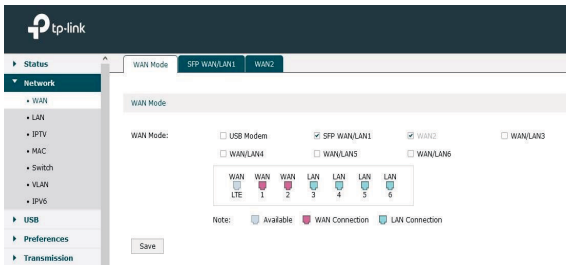
Фиг. 2. *Схема на компютърната локална мрежа в основната сграда – междинни, крайни устройства и апаратура в сървърното помещение*

За маршрутизатор на локалната мрежа и гейтуей към Интернет е избран TP-Link ER7206. Моделът е избран най-вече заради високоскоростните си интерфейси и вградения SFP WAN порт, който позволява оптичното трасе от доставчика да завърши директно в маршрутизатора избягвайки употребата на ONU устройства или медия конвертори. Също така има достатъчно на брой допълнителни функции, които подсигуряват лесното развитие и мащабируемост на мрежата на компанията в бъдеще – достатъчно на брой LAN портове, поддръжка на различни VPN тунели, протоколи за динамично рутиране, удобен web интерфейс за управление и мониторинг на мрежата и други.

Първоначалното достъпване до потребителския интерфейс на маршрутизатора става чрез въвеждането на IP адреса му по подразбиране (192.168.0.1) в браузър от компютър, който е в същата мрежа. След това системата изисква създаването на администраторска парола за достъп. След като маршрутизаторът е достъпен, първо се настройва WAN мрежата му – тоест входящия сигнал от доставчика.

От меню Netowrk-WAN-WAN Mode се задава кои физически интерфейси да са активни и кои не, също така кои да са WAN и кои да са LAN – фиг.3.

В частния случай на предложения проект за WAN са избрани задължителния WAN RJ45 порт и SFP порта, който ще приема сигнала от доставчика. Всички други свободни портове са конфигурирани в LAN режим.

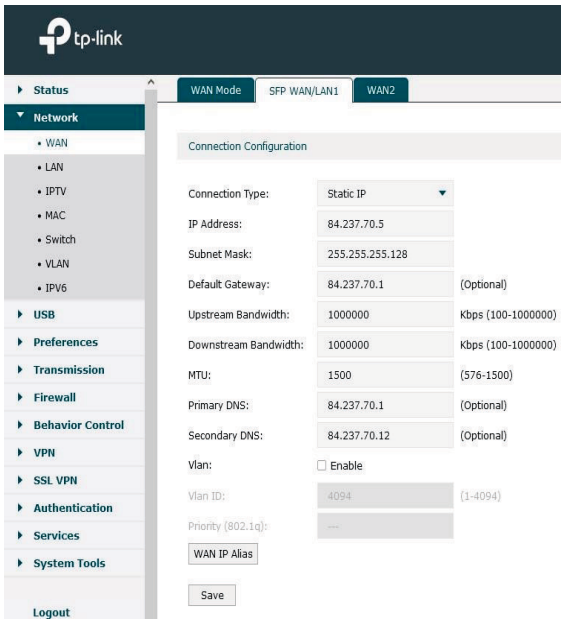


Фиг.3. *WAN mode избор*

Компанията има подписан договор с доставчика на Интернет той да предоставя 1 брой статичен външен реален IP адрес - 84.337.70.5 (фиг.4).

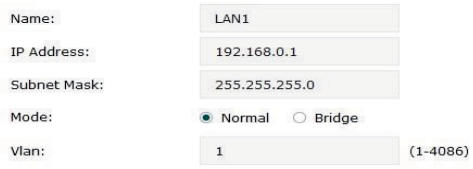
В меню Network-WAN-SFP WAN трябва да се зададе режим на WAN порта, като модела ER7206 предоставя следните възможности: Static IP, Dynamic IP, PPPoE, L2TP, PPTP

В случая се избира режим “Static IP” и се въвежда предоставеното от доставчика IP, както и допълнителните мрежови настройки като мрежова маска, шлюз, основен и вторичен DNS и други.



Фиг.4. *WAN конфигурация на маршрутизатора*

От меню Network-LAN се задава конфигурацията на локалната мрежа на маршрутизатора. За целите на проекта и по-лесното разбиране на мрежата ще бъде оставено адресирането по подразбиране в локалната мрежа – т.е. мрежата ще бъде с адрес 192.168.0.1. Маската ще бъде 255.255.255.0 т.е. в мрежата едновременно ще могат да се включат до 254 устройства – фиг.5.



Фиг. 5. *LAN конфигурация на маршрутизатора*

От същото меню се конфигурира (ако се налага) DHCP услугата на маршрутизатора. Трябва да се отбележи отметката за активиране на DHCP сървъра, да се настрои „pool“ с адреси, които да бъдат раздавани и за какво време да бъде един адрес „отдаван“ на устройство. От гледна точка на сигурност в мрежата, максималният брой на раздадените по DHCP адреси е ограничен до 21 (от 1-ви раздаван адрес 192.168.0.200 до последен – 192.168.0.220), тъй като всички устройства, които ще бъдат част от мрежата, ще бъдат с настроени статични адреси – фиг.6.

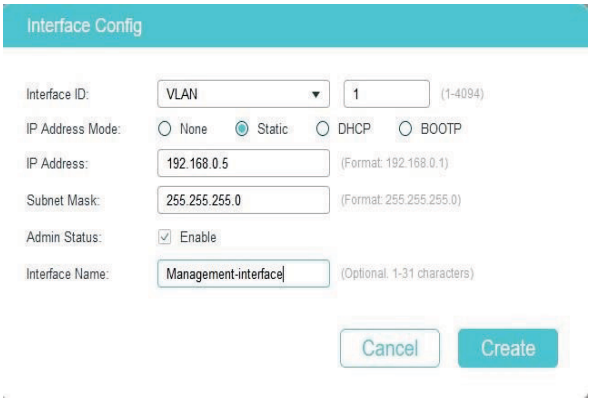
Фиг. 6*. DHCP конфигурация на маршрутизатора*

За избора на комутатор (aggregation switch), на който ще бъдат конфигурирани VLAN-и, които ще разделят трафика на клиентските компютри от този на видеонаблюдението е избран TP-Link TL-SG2218 със следните характеристики: 16 RJ45 гигабитови порта, 2 гигабитови SFP порта, L2/L3 функции, VLANs, Управление през web interface/ CLI.

Избран е управляем L2/L3 комутатор с висикоскоростни интерфейси. На него

ще се разчита да разпределя трафика между различни виртуални локални мрежи, да прави връзката между всички компютри на компанията и локалните сървъри, да обединява няколкото на брой суича, които разделят видеонаблюдението по зони, и да предава сигналите от видео камерите към записващите устройства, както и да предава целия изходящ трафик към маршрутизатора на мрежата.

Първоначалният достъп до комутатора е сходен с този на маршрутизатора. След като един път е достъпен, първо трябва да се конфигурира адреса му. Това става от секция L3 Features – меню Interface. Както е описано е схемата на мрежата, суичът ще е с адрес 192.168.0.5/24 – фиг. 7.

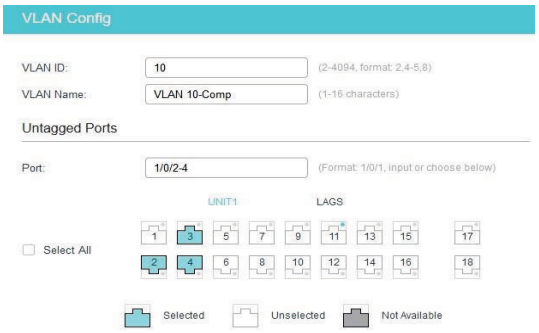


***Фиг. 7**. Мрежова настройка на комутатора*

След като устройството има валиден адрес от мрежата, трябва да се конфигурират 2 VLAN – един за компютърната техника в сградата и друг за видеонаблюдението. Компютърната мрежа има 3 „access“ комутатора – по 1 на всеки етаж. Тоест за начало в този VLAN ще трябва да се добавят 3 порта на суича. Този VLAN ще бъде с ID 10 и име VLAN 10-Computers.

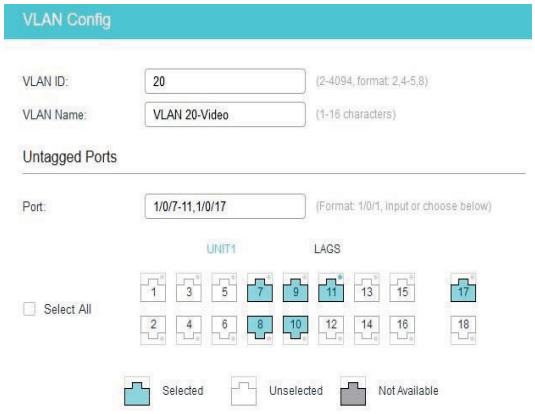
Видеонаблюдението общо разполага с 6 суича, които обединяват камерите по различните зони, следователно трябва да се отделят 6 порта във VLAN, който ще е с ID 20 и име VLAN 20-Video.

За конфигурация за виртуалните локални мрежи трябва да се влезе в секция L2 Features на комутатора и от там меню VLAN-VLAN Config – бутон „Add“. За VLAN, в който ще са компютрите, ще бъдат избрани портове 2,3 и 4 на комутатора – фиг.8.



***Фиг. 8**. VLAN 10 конфигурация*

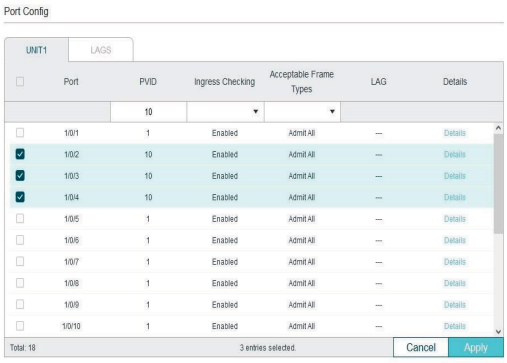
За VLAN, в който ще бъдат комутаторите обединяващи всички видео камери, ще бъдат избрани портове 7-11 и 17. 17ти порт е SFP – от него директно ще излиза оптичен кабел, който ще свързва видео мрежата в основната сграда с тази в „Сграда В“.



***Фиг. 9**. VLAN 20 конфигурация*

За да сработят правилно виртуалните локални мрежи, конфигурирани на комутатора, последната нужна стъпка е да се свържат физическите портове с номер (ID) на VLAN, в който са. Конфигурацията се изпълнява от VLAN – Port Config – фиг.10. Портове 2-4(VLAN за компютрите) се отбелязват със съответния номер на VLAN, в който са – 10 – в полето „PVID“.

Портове 7-11,17 се правят по същия начин, но съответно с „PVID“ – 20.



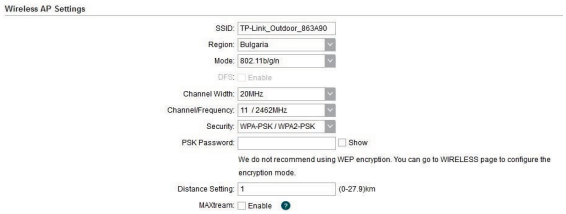
Фиг.10. *VLAN Port Config*

За комутатори (access switch), които ще обединяват всички компютри по отделните етажи са избрани TP-Link TL-SG3452X. Комутаторите са с гигабитови RJ45 портове, така че да отговарят на скоростта на мрежата и са 48-портови – разполагат с достатъчно на брой портове за устройствата на всеки един етаж, като е предвидено и място за бъдещо разширяване на мрежата.

За комутатор, който ще обединява видеокамерите по различните зони, е избран TP-Link TL-SL1218MP. Той е неуправляем модел, но всичките му портове поддържат PoE+. Технологията PoE ще се използва с цел по-лесна и бърза инсталация на цялата система за видеонаблюдение, както и за по практична поддръжка на системата в бъдеще.

За да се свърже основната сграда със „Сграда С“ ще бъдат използвани 2 броя антени (CPE устройства) TP-Link CPE 210,тъй като между сградите има пряка видимост, но няма как да се прекара кабелно трасе.

Устройството, което ще е на основната сграда (което физически ще е свързано с локалната мрежа и ще трябва да я разшири) ще е настроено в режим Access Point т.е. ще преобразува мрежата в безжична. Първоначално устройството се достъпва чрез адреса си по подразбиране, след което с настройките за режим, ще се конфигурира и статичен IP адрес от 192.168.0.180/24 – фиг. 11.



Фиг.11. *TP-Link CPE210 конфигурация*

Трябва да се настроят и SSID на мрежата, режим на 802.11, кой честотен канал да използва устройството, тип на криптиране и други.

При първоначалното си пускане отсрещното устройство трябва да се настрои в режим Client и всички настройки за безжичната мрежа трябва да са като на Access Point-а, в противен случай устройствата няма да успеят да се свържат успешно. То ще бъде с IP адрес 192.168.0.181/24. Неговият LAN порт ще бъде свързан с TP-Link TLSL1218MP PoE суича в „Сграда С“ и той ще се явява входна/изходна точка за тази безжична част на локалната мрежа.

Всички видеокамери в сградите на компанията ще са Hikvision DS-2CD1347G2-L (фиг.12) с основни характеристики: 4.0 Мегапиксела (2560x1440@20 кад/сек); Фиксиран обектив f=2.8 мм/F1.0; Вградена бяла LED светлина с обхват до 30м; Детекция на движение; Поддържа dual stream компресия H.265+, H.265, H.264+, H.26; Захранване: 12Vdc/PoE 4.5W. Тъй като моделът е с клас IP67 защита и също така може да работи в много широк температурен диапазон е подходящ както за вътрешен, така и за външен монтаж, всички кръгове на системата ще са изградени с него [14].

Фиг.12*. IP камера Hikvision DS-2CD1347G2-L*

След като устройството е захранено и добавено към мрежата, трябва да се достъпи чрез адреса си по подразбиране през браузър

След създаването на администраторска парола, ще зареди основната страница:

Тъй като камерата ще е с грешен час и дата, времето се настройва от меню Configuration-System-System Settings-Time Settings. Задава се времева зона. Времето може да се настрои ръчно, да се синхронизира с времето на компютъра, от който се настройва или да се зададе адрес на NTP server. Тъй като в мрежата на компанията е предвиден NTP сървър, се прави настройка с неговия IP адрес.

От меню Configuration-Network-Basic Setting-TCP/IP се настройва мрежовата карта на устройството. В случая това ще е първата камера от 1-ви етаж на основната сграда, следователно ще й се зададе адрес от 192.168.0.100/24.

По такъв начин се настройват всички камери от мрежата със съответните си IP адреси [13].

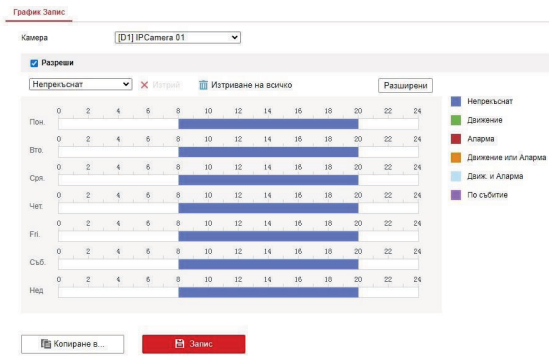
За записващи устройства ще се използват Hikvision DS-7616NI-K2 [14]. Общо ще са нужни 5 броя – по 1 бр. за всеки от 3-те етажа на основната сграда, 1 бр. за външния кръг на основната сграда и 1 бр., който ще обединява камерите в двата допълнителни склада, тъй като там камерите ще са по-малко на брой. На всички записващи устройства са предвидени да останат достатъчно на брой свободни канали за бъдещо разширение на мрежата. Както се вижда от логическото разпределение на мрежата на фиг. 2 – рекордерите ще заемат адресите от 192.168.0.65/24 до 192.168.0.69/24.

Основни характеристика на NVR: 16-канален мрежов рекордер, H.265/H.264+/H.264/MPEG4 компресия за видеонаблюдение, резолюция на запис до 8 MPx, до 4xSATA твърд диск (до 6TB/диск), HDMI + VGA мониторни изходи и 3 USB порта.

Рекордерът първоначално се достъпва по същия начин като камерите. Следват и същите настройки за време и мрежова карта.

От меню Configuration-System-Camera Management се вижда с кои камери в момента записващото устройство може да се свърже по мрежата. Избират се камерите, които трябва да се добавят към това устройство. За добавянето си всяка камера ще изисква да се въведат данните й за потребителско име и парола.

След като вече има добавени камери към рекордера се въвежда график на запис. Влиза се в меню Configuration-Storage-Schedule и за всеки канал (добавена камера) се избира тип на записа (непрекъснат, движение, аларма и др) и се задава часови график на запис – фиг.13.



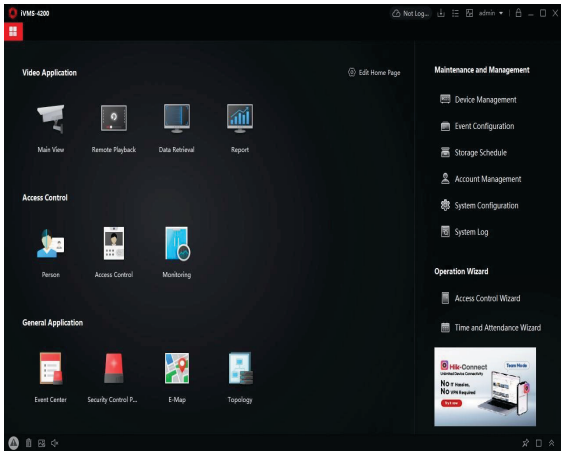
***Фиг. 13**. Примерен график на запис*

За изграждане на видео сървър е избрана софтуерната платформа iVMS 4200, която е безплатна за ползване и специално разработена за работа с различни по тип устройства и продукти с Hikvision марка.

iVMS-4200 е универсален софтуер за видео управление за DVR, NVR, IP камери, енкодери, устройства за контрол на достъп, охранителни контролни панели, видеодомофонни устройства, декодери, VCA устройства и др. Осигурява множество функционалности, включително преглед на живо в реално време, видеозапис, дистанционно търсене и

възпроизвеждане, архивиране на файлове, получаване на аларми и други.

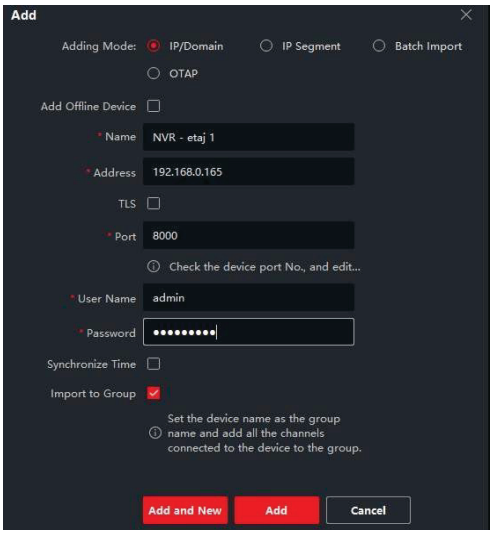
След инсталацията на софтуера iVMS 4200 и отварянето му, потребителят влиза на началната му страница – фиг. 14.



***Фиг. 14**. Начална страница на iVMS 4200*

Първата стъпка е да се добавят всички записващи устройства от мрежата към софтуера. За целта се влиза в меню Device Management-Device-бутон „Add“ и в появилия се прозорец се попълват мрежовите данни и данните за автентикация на устройството, което трябва да се добави – фиг. 15.

Тази стъпка се повтаря за всички NVR(DVR) устройства в мрежата. След това потребителят вече може да вижда всички камери от тях в реално време в меню „Main View“. В случая на клиента – IP адреси от 192.168.0.165 до 192.168.0.169. Не е проблем да се добави устройство, което не е в същата локална мрежа, стига то да е конфигурирано да „се вижда“ в Интернет и да е известен порта, по който то се достъпва. Също така ако в последствие към мрежата бъдат добавени IP видеокамери, които не са част от някой от рекордерите, също могат да бъдат изведени за наблюдение в софтуера.



***Фиг.15**. Добавяне на устройство към iVMS 4200*

***Фиг.16**. Меню „Main View“*

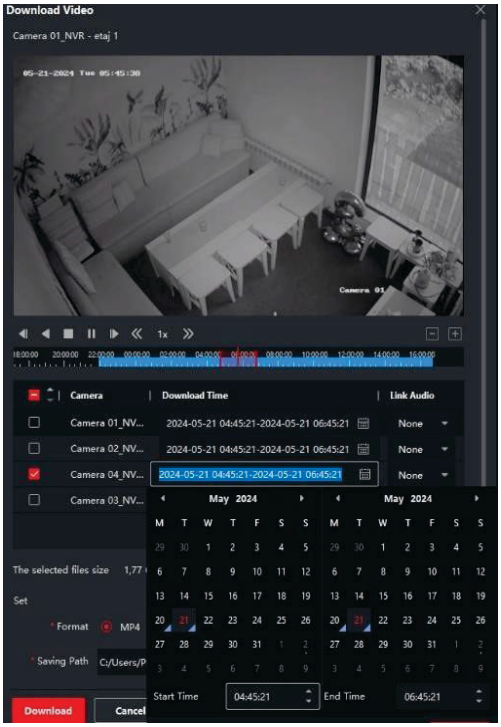
От долната лента с инструменти, натискайки иконката с дискета може да се запамети текущата подредба на камерите, за да не се пренареждат след всяко отваряне на програмата. Въвежда се име на изгледа и той вече стои най-горе в частта с избор на устройства в „Main View“.

Преглед на записи - от началната страница се избира меню „Remote Playback“ (фиг. 17). Избира се камера, чиито записи трябва да се проверят. След това от долната лента с инструменти се избира ден от календара, в който има направени записи и час. Натиска се „Play“ бутона и записът от посочената дата и час започва да се изпълнява. До изборът за дата и час има инструменти за пускане, пауза и спиране на видеозаписа, както и за намалява-

не/ускоряване на скоростта на преглед от 1x до 16x.

Фиг.17. *Меню „Remote Playback“*

Сваляне на запис – от същата лента с инструменти се натиска бутон „Download“. С натискането му се отваря прозорец, от който се избира период на запис, който трябва да бъде свален (фиг. 18). Избира се дали зададения период да се свали само за 1 камера или за няколко (всички).



Фиг. 18*. Инструмент „Download“*

Осигуряване на отдалечен достъп – За да може сървъра да се достъпва отдалечено, когато потрябва, а не да е нужен физически достъп до него, се позволява Windows функцията „Remote Desktop“, чрез която всеки оторизиран потребител в мрежата ще успява да достъпи сървъра, докато работи на друга машина.

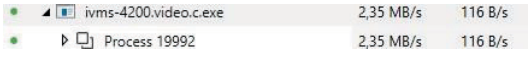
ПРОВЕДЕНИ ЕКСПЕРИМЕНТИ И ЗАКЛЮЧЕНИЕ

За експерименти с вече изградената и работеща мрежа се използва софтуерен инструмент „NetLimiter“, през който могат да се наблюдават отделните приложения и процеси, които са активни в даден момент в една Windows базирана машина. Инструментът следи какъв bandwidth (честотна лента) използва всяко приложение от локалната мрежа и с каква скорост качва/сваля данни в нея. В конкретния случай се следи активността на процеса създаден от iVMS4200.

Кликвайки върху 3-те точки до името на камерата излизат допълнителни функции. Кликвайки на Remote Configuration-Video се влиза директно във Видео настройките на конкретната камера. От бутон „Copy To“ конфигурацията на една камера може да се пренесе на всички други – фиг.19.

Фиг. 19*. Видео настройки на камера*

Тест 1 – Добавена е 1бр. камера от NVR в „Main View“. Конфигурирана е с 1280*720 резолюция, 2048 kbps Bitrate, 25Fps и H.264 компресиране . Получени са следните данни от инструмента NetLimiter:



След това от меню Remote Configuration-Video на камерата единствено е променен параметъра Bitrate от 2048Kbps на 3072Kbps. Download скоростта на iVMS 4200 се променя по следния начин:

Тест 2 – Направени са изчисления и за 10бр едновременно записващи се IP камери с резолюция от 4MPX (2560 x 1440), Bitrate 8192Kbps, 30Fps и H.264 компресиране в продължителност на 10 дни. Резултатът е (приблизително) заета честотна лента от 82Mbps и заето място (обем на записа) на твърдия диск на записващото устройство от 8.85TB т.е. NVR с твърд диск с обем от 6TB би записвал 6 до 7 дни.

Тест 3 – Направени са изчисления със същия брой и видео конфигурация на камерите с единствена разлика, че типа на компресията е променен от H.264 на H.265, съответно Bitrate = 4830. Резултатът е (приблизително) заета честотна лента от 48Mbps и заето място (обем на записа) на твърдия диск на записващото устройство от 5.2TB т.е.

NVR с твърд диск с обем от 6TB би записвал 10 до 11 дни.

Тест 4 – Направени са изчисления със същия брой камери, но тяхната видео конфигурация е променена на резолюция от 3MPX (2048 x 1536), Bitrate 2695Kbps, 20Fps и H.265 компресия. Резултатът е (приблизително) заета честотна лента от 27Mbps и заето място (обем на записа) на твърдия диск на записващото устройство от 2.9TB. С тази конфигурация е постигнат запис върху твърдия диск до 20 дни.

В заключение, предложеното примерно решение за проект на хибридна комуникационна мрежова свързаност между три сгради е реализирано и тествано. Чрез него се демонстрира възможността за използването на три различни видове преносна среда – безжична, оптична и кабелна. Подобна реализация е често срещана в практиката и може да послужи при обучението на студенти да проектират, реализират и тестват подобни примерни решения познавайки възможностите на хардуер, софтуер и различни комуникационни преносни среди.

Благодарности: Този доклад и изследванията в него са реализирани по проект „Разработка на IoT/4G/5G-базирани комуникационни решения за платформи, системи и услуги в "Интелигентен град"", договор 2403Е/2024 г. към УЦНИТ при ТУ – Габрово.

ЛИТЕРАТУРА

[1] Computer Networking: A System Administrator's Handbook, D.K. Academy, 2018.
[2] Macshmillan T., Cisco: Computer Networks. Basics, 2016.
[3] Lowe D., Computer Networks For Dummies, 2014.
[4] Milanov L., Networking Fundamentals. LAN Design, Switching, SoftUni, 2016
[5] Toshkov A., Design and construction of optical networks, 2011.
[6] Perros H., Connection-Oriented Networks, 2005.
[7] Steenbergen R., Everything You Always Wanted to Know About Optical Networking – But Were Afraid to Ask, 2013.
[8] Dankov P., Introduction to Wireless Communications, 2007.
[9] Gugova V., V. Pulkov Optical cable lines and networks, 2011.
[10] Ferdinandov E., K. Dimitrov, Optical communication systems, 2007.
[11] Ramaswami R., Optical Networks. A Practical Perspective, 2010.
[12] Communication-Systems-Engineering 2nd-Edition, John Proakis, Masoud Salehi, 2010.
[13] Simpson W., H. Greenfield IPTV and Internet Video, 2009.
[14] https://www.hikvision.com