

**Univerzita Pardubice
Fakulta ekonomicko-správní**

Návrh komunikační infrastruktury počítačové sítě LAN pro firmu

Milan Feledík

**Bakalářská práce
2010**

Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky
Akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Milan FELEDÍK**
Studijní program: **B6209 Systémové inženýrství a informatika**
Studijní obor: **Informační a bezpečnostní systémy**

Název tématu: **Návrh komunikační infrastruktury sítě LAN pro firmu**

Z á s a d y p r o v y p r a c o v á n í :

Shromáždění požadavků konkrétního zadání
Vypracování návrhu řešení včetně alternativ
Ekonomický rozbor návrhu

Rozsah grafických prací:

Rozsah pracovní zprávy: **30 - 40 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

BIGELOW, Stephen J. Mistrovství v počítačových sítích : správa, konfigurace, diagnostika a řešení problémů. Brno. Computer Press, 2004. 990 s. ISBN 80-251-0178-9

DOSTÁLEK, Libor a kolektiv. Velký průvodce protokoly TCP/IP: Bezpečnost. 2. vyd. Praha. Computer Press, 2003. 571 s. ISBN 80-7226-849-X

DOSTÁLEK, Libor, KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS. 3. vyd. Brno. Computer Press, 2002. 542 s. ISBN 80-7226-675-6

PROSISE, Chris, MANDIA, Kevin. Počítačový útok : detekce, obrana a okamžitá náprava. Praha. Computer Press, 2002. 410 s. ISBN 80-7226-682-9

Vedoucí bakalářské práce:

Ing. Oldřich Horák

Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **5. října 2009**

Termín odevzdání bakalářské práce: **30. dubna 2010**

doc. Ing. Renáta Myšková, Ph.D.

děkanka

L.S.

doc. Ing. Jiří Křupka, Ph.D.

vedoucí ústavu

V Pardubicích dne 5. října 2009

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 30. 6. 2010

Milan Feledík

Poděkování:

Velice rád bych touto cestou poděkoval vedoucímu práce panu ing. Oldřichu Horákovi, pod jehož vedením tato práce vznikala.

Souhrn

Tato práce si klade za cíl návrh lokální počítačové sítě. V první části jsou uvedena technologická východiska návrhu počítačových sítí, příslušné normy, kritéria návrhu aktivních prvků a základní principy IP kamerového systému. Ve druhé části je na základě shromážděných požadavků konkrétního zadání vytvořen vlastní návrh komunikační infrastruktury s příslušnými variantami řešení a jejich ekonomickým zhodnocením.

Klíčová slova

LAN, Ethernet, TCP/IP, IP video

Title

Design of LAN communication infrastructure for the firm

Abstract

This work aims to design of Local Area Networks. The first section provides background techno-logical design of computer networks, the standards, design criteria of active elements and basic principles of IP camera system. The second part of the collec-specific entry requirements events created their own communication infrastructure design with the various solutions and their economic evaluation.

Keywords

LAN, Ethernet, TCP/IP, IP video

Obsah

1. TECHNOLOGICKÁ VÝCHODISKA PRO NÁVRH SÍTĚ.....	11
1.1 STRUKTUROVANÁ KABELÁŽ	11
1.1.1 <i>Horizontální sekce</i>	12
1.1.2 <i>Vertikální sekce</i>	13
1.2 SÍŤOVÉ KOMPONENTY.....	13
1.2.1 <i>Switch (Přepínač)</i>	13
1.2.2 <i>Router (Směrovač)</i>	15
2. KAMEROVÝ SYSTÉM IP CCTV	16
3. SHROMÁŽDĚNÍ POŽADAVKŮ.....	19
4. NÁVRH STRUKTUROVANÉ KABELÁŽE	22
4.1 NÁVRH ČÁSTI HORIZONTÁLNÍ ROZVODY	22
4.2 NÁVRH ČÁSTI VERTIKÁLNÍ A AREÁLOVÉ	23
5. NÁVRH BEZPEČNOSTNÍHO SYSTÉMU A WIFI SYSTÉMU	24
5.1 NÁVRH KAMEROVÉHO SYSTÉMU	24
5.2 NÁVRH PŘÍSTUPOVÉHO SYSTÉMU	31
5.3 NÁVRH PŘÍSTUPOVÝCH BODŮ WIFI	33
6. NÁVRH AKTIVNÍCH PRVKŮ	36
6.1 FAKTORY PRO VÝBĚR AKTIVNÍCH PRVKŮ	36
6.2 VOLBA AKTIVNÍCH PRVKŮ	37
6.2.1 <i>Volba aktivních prvků pro vrstvu přístupu</i>	39
6.2.2 <i>Volba aktivních prvků pro vrstvu jádra a distribuce</i>	40
6.2.3 <i>Volba směrovačů (router) pro přístup do Internetu</i>	42
ZÁVĚR.....	45
SEZNAM PŘÍLOH.....	49

Seznam obrázků

Obrázek 1 - Hierarchická struktura univerzální kabeláže	12
Obrázek 2 - Horizontální kanál	12
Obrázek 3 - Blokové schéma IP kamery	17
Obrázek 4 - Blokové schéma propojení rozvaděčů	23
Obrázek 5 - Rozmístění kamer v přízemí budovy	24
Obrázek 6 - Situace rozmístění venkovních kamer	26
Obrázek 7 - Fixní kamera 211M	26
Obrázek 8 - Fixed Dome 216MFD	27
Obrázek 9 - Záznamový server Dell T110	28
Obrázek 10 - Přístup uživatelů k záznamu videa	29
Obrázek 11 - IP systém s optickou sítí do jedné sběrnice	30
Obrázek 12 - Snímač REI-ST, externí hlavice H-PRO, H-PRO/K	32
Obrázek 13 - Schéma připojení WLC k LWAP	34
Obrázek 14 - Hierarchické uspořádání prvků v LAN	36
Obrázek 15 - Stackwise propojení mezi Catalysty 3750	41
Obrázek 16 - Mapování portů na routeru	44
Obrázek 17 - Návrh fyzické topologie	50
Obrázek 18 - Návrh fyzické topologie alternativní	51
Obrázek 19 - Schéma rozmístění IP kamer	52
Obrázek 20 - Situační schéma administrativa	53
Obrázek 21 - Situační schéma sklad	54
Obrázek 22 - Návrh logické topologie	55
Obrázek 23 - Návrh kalkulace propustnosti	57

Seznam tabulek

Tabulka 1 - Výkonnost kabelážních systémů	11
Tabulka 2 - Rozložení přípojných míst	20
Tabulka 3 - Kalkulace nákladů IP kamer	29
Tabulka 4 - Kalkulace nákladů přístupový systém	33
Tabulka 5 - Kalkulace nákladů WiFi	35
Tabulka 6 - Kalkulace nákladů aktivní prvky	44
Tabulka 7 - Ekonomické zhodnocení	56
Tabulka 8 - Ekonomické zhodnocení alternativa	56

Seznam zkratek

ACL	Acces Control List
AES	Advanced Encryption Standard
AP	Acces Point
CCTV	Closed Circuit Television System
CCD	Charge Coupled Device
CPU	Central Procesor Unit
DSP	Digital Signal Process
DVR	Digital Video Recorder
GBIC	Gigabit Interface Converter
HSRP	Hot Standby Router Protocol
IGRP	Interior Gateway Routing Protocol
IEEE	The Institute of Electrical and Electronics Engineers
IGMP	internet Group Management Protocol
IGRP	Interior Gateway Routing Protocol
IPsS	Intrusion Prevention Systems
ISP	Internet Service Provider
LAN	Local Area Network
LWAPP	Lightweight Acces Point Protocol
MAC	Media Access Control
MJPEG	Motion Joint Photographic Expert Group
MPEG	Moving Picures Experts Group
NAT	Network Adress Translation
OSPF	Open Shortest Path First
PoE	Power over Ethernet
RSTP	Rapid Spanning Tree Protocol
RPS	Redundant Power Supply
QoS	Quality of Services
RADIUS	Remote Authentization Dial-In User Service
RIP	Routing Information Protocol
RM-OSI	Reference Model-Open System Interconnection
SFP	Small Form Pluggable
STP	Spanning Tree Protocol
TCP/IP	Transmission Control Protocol/Internet Protokol
VoIP	Voice over Internet Protokol
VPN	Virtual Private Network
WAN	Wide Area Network
WiFi	Wireless Fidelity
WLC	Wireless LAN Controller

Úvod

Problematika návrhu komunikační infrastruktury je značně rozsáhlá a variabilní. Vše záleží na konkrétních podmínkách a na požadavcích jaké má výsledná síť splňovat. Záleží na typu koncových uzlů, použití přenosového média a geografického rozložení oblasti. Návrh takovéto sítě je pak možno realizovat několika možnými způsoby. Tato práce je zaměřena na návrh komunikační infrastruktury ve specifických podmínkách středně velké firmy.

Realizovaný návrh se týká sítě lokálního typu LAN (Local Area Network). LAN jsou budovány jako samostatné fyzické sítě regionálního rozsahu.

V návrhu LAN sítě je postupováno podle doporučení předních výrobců, jejichž zařízení jsou použita v samotném návrhu. Důraz je kladen na ochranu vynaložených prostředků a rozšiřitelnost infrastruktury v případě dalšího rozvoje firmy. Síťová zařízení jsou v práci navržena dle výkonnosti, dostupných fyzických rozhraní, podporovaných standardů a úrovně spravovatelnosti.

Používání počítačové sítě umožňuje velmi rychlý přístup k aktuálním datům a informacím spojený s minimálním zpožděním a administrativou. V současné době se prosazuje trend slučování všech typů komunikačních přenosů na digitální bázi a přenos v podobě dat v rámci jednoho typu přenosového protokolu - IP protokolu. Jde o konvergenci přenosu i sítě. Konvergovaná síť integruje zpracování datové, obrazové a hlasové komunikace využíváním společné síťové infrastruktury - kabelů, aktivních prvků a dalšího hardware.

Cílem této bakalářské práce je tedy na základě shromáždění požadavků konkrétního zadání vytvořit vlastní návrh komunikační infrastruktury včetně jeho ekonomického zhodnocení. Návrh se bude týkat strukturované kabeláže, kamerového systému, systému kontroly přístupu, bezdrátového systému a vlastní komunikační infrastruktury aktivních prvků. Dále jsou v práci ve stručnosti uvedena technologická východiska pro návrh technologií a základní principy IP kamerového systému.

1. Technologická východiska pro návrh sítě

Při návrhu zařízení v počítačových sítích se vychází z architektury pro komunikaci tzv. otevřených systémů RM-OSI. V návrhu komunikační infrastruktury budou navrženy prvky pro nejnižší tři vrstvy [8]:

1. Fyzickou vrstvu (Layer 1)
2. Linkovou vrstvu (Layer 2)
3. Síťovou vrstvu (Layer 3)

Návrh počítačové sítě je realizován pro dva typy normalizovaných lokálních sítí [13]:

- Ethernet/IEEE 802.3 - přenosové médium je optický a metalický kabel,
- WLAN/IEEE 802.11 - přenosovým médium jsou radiové vlny.

1.1 Strukturovaná kabeláž

Strukturovaná kabeláž je pasivní částí fyzické vrstvy. Jde o kabelážní systém pro přenos dat, hlasu a dalších služeb v rámci integrovaného provozu budov. Používá datové kabely se čtyřmi kroucenými páry a optický kabel. Největší výhody strukturované kabeláže jsou [8]:

- univerzálnost,
- modularita,
- flexibilita.

Univerzální kabelážní systémy ČSN EN 50173-1

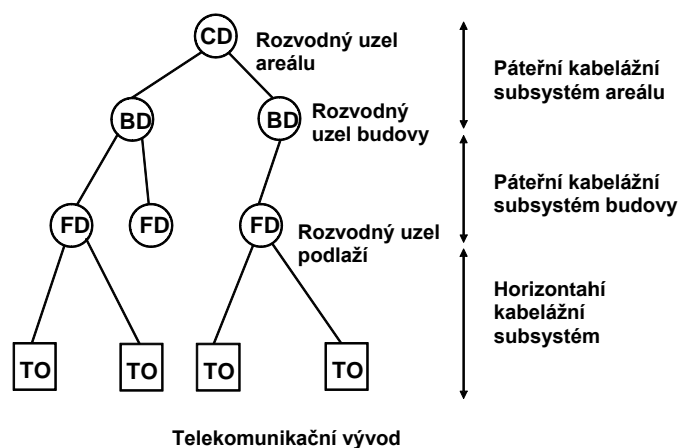
Tato norma definuje strukturu a nejmenší rozsah univerzálního kabelážního systému, požadavky na realizaci a výkonnostní požadavky na jednotlivé úseky kabeláže a jejich prvky [6]. Výkon těchto systémů je definován šířkou pásma, jak je uvedeno v tabulce 1.

Tabulka 1 - Výkonnost kabelážních systémů[6]

Třída	Šířka pásma	Kategorie	Přenosová rychlost
D	100 Hz	Cat.5/Cat. 5e	100 Mb/s
E	250 MHz	Cat. 6	1 Gb/s
E	500 Mhz	Cat. 6a	10 Gb/s
F	600 Mhz	Cat. 7	10 Gb/s

Univerzální kabeláž zahrnuje až tři kabelážní subsystemy znázorněné na obrázku 1 [6]:

- rozvodný uzel areálu (CD Campus),
- rozvodný uzel budovy (BD Building Distributor),
- rozvodný uzel podlaží (FD Floor Distributor).

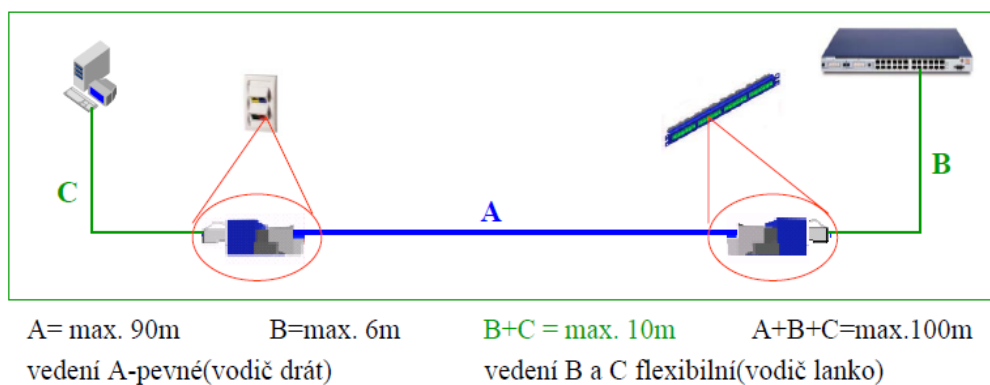


Obrázek 1 - Hierarchická struktura univerzální kabeláže[6]

1.1.1 Horizontální sekce

Fyzická topologie je vždy hvězda. Znázornění horizontální sekce je na obrázku 2. Nejpožívanějším přenosovým médiem v této části je metalický kabel. Jeho základní dělení je podle odolnosti vůči okolním vlivům [13]:

- nestíněný kroucený dvoupár - UTP (Unshielded Twisted Pair),
- stíněný kroucený dvoupár - FTP (Foiled Twisted Pair). Větší odolnost vůči okolním vlivům.



Obrázek 2 - Horizontální kanál[6]

1.1.2 Vertikální sekce

Přenosovým médiem pro páteří vertikální rozvody uvnitř budov může být metalický kabel, ale pro tzv. Campus rozvody (datové rozvody mezi budovami - trasy delší než 90 m) se používá optický kabel. Optický kabel se vyznačuje vyšší přenosovou rychlostí, šířkou pásma a odolností proti elektromagnetickému rušení. Jeho základní dělení je [13]:

- vlákna typu multimode (50/125 μ m, 62,5/125 μ m),
- vlákna typu singlemode (8 až 9/125 μ m).

1.2 Síťové komponenty

1.2.1 Switch (Přepínač)

Aktivním prvkem linkové vrstvy je přepínač - switch. Je to nejrozšířenější aktivní prvek v lokálních sítích. Slouží pro připojení koncových stanic (uživatelské počítače, IP telefony, IP kamery, WiFi přístupové body, servery). [2]

Kritéria výběru přepínače

Mezi typické parametry přepínačů malých LAN sítí patří [14]:

- absence managementu,
- s metalickými 5,8,12,16 porty s podporou rychlostí 10/100 Mb/s (Fast Ethernet) nebo 10/100/100 Mb/s (Gigabit Ethernet),
- základní funkcionality přepínání rámců,
- Auto-Sensing, Auto-Negotiation IEEE 802.3u - podpora automatického nastavení přenosové rychlosti a přenosového módu (Half/Full duplex),
- AutoMDI/MDI-X - automatická detekce a správné nastavení přijímacích a vysílacích pinů na metalickém portu.

Mezi základní parametry přepínačů středně velkých sítí LAN patří [14]:

- s managementem, konfigurace pomocí příkazů v příkazovém řádku přes sériovou konzoli (RS-232), vzdáleně přes Telnet či SSH, HTTP/HTTPS,
- SNMP v.3, v.2c (Simple Network Management Protocol) - správa jednotek z centrální SW aplikace (NMS, Network Management System),
- samostatné jednotky přizpůsobeny pro uchycení do 19“ rozvaděčů,

- metalické porty 24 nebo 48x 10/100 Mb/s nebo 10/100/1000 Mb/s pro připojení uživatelů,
- porty pro uplink (metalické nebo optické) - propojení přepínačů nebo pro připojení k centrálnímu prvku,
- stohovatelnost - vzájemným propojením přepínačů vzniká jednotka, která se chová jako jednotka s více porty. Celý stoh (Stack) má pouze jednu IP adresu a jediný konfigurační protokol. Možná je také agregace linek a zrcadlení portů přes jednotky ve stohu. Nabízí se dvě varianty stohování, pomocí speciálních kabelů (příslušenství, které je třeba koupit od stejného výrobce) nebo pomocí běžných metalických či optických portů.
- IGMP (Internet Group Management Protocol) - protokol pro skupinové vysílání videa v IP sítích (IP Multicast),
- Quality of Services (kvalita služeb) - funkce pro klasifikaci a prioritizaci dat. Vhodné především pro provoz konvergovaných služeb, tedy pro přenos dat, hlasu a videa.
- STP (Spanning Tree Protokol) IEEE 802.1d - podpora kruhové (redundantní) topologie. K bezchybné funkci sítě Ethernet je zapotřebí pouze jediná aktivní cesta mezi dvěma stanicemi. Zabraňuje vzniku smyček v přepínané síti. Doba zotavení v případě výpadku linky nebo některého z přepínačů v kruhu činí 30 až 40 sekund,
- sloty pro osazení moduly GBIC (Gigabit Interface Converter) nebo SFP (Small Form Pluggable, též MiniGBIC), ke kterým se připojují optická vlákna přímo přes konvertory SC nebo LC. Odpadá nutnost použití případných media konvertorů (další prvek v síti, u kterého může nastat případná porucha),
- zdvojené porty (Combo Porty nebo Dual Purpose Porty). Jeden port se skládá ze dvou rozhraní - metalického 10/100/1000base-T a optického 1000Base-X (SFP), přičemž aktivní může být pouze jedno rozhraní,
- podpora napájení Power over Ethernet (PoE). Předpoklad použití prvků disponujících podporou napájení po datovém kabelu Cat5 a vyšší (IP telefony, WiFi přístupové body, IP kamery),

- podpora VLAN 802.1q a podpora 802.1x protokolu s centralizovanou správou uživatelů na RADIUS server,
- vybavení redundantním napájecím zdrojem (RPS), nebo ke kterým lze RPS připojit (vysoká spolehlivost systému a zajištění úrovně služeb SLA).

1.2.2 Router (Směrovač)

Aktivním prvkem síťové vrstvy je směrovač (router), který definuje rozhraní mezi LAN a WAN. Umožňuje volbu směru přenášených paketů na základě směrovacích tabulek. V IP protokolu má každé rozhraní (uzel) tzv. IP adresu. [2]

Třídy adres

Adresa IP je rozdělena na dvě části: adresa sítě a adresa uzlu (počítače). Třídy adres dělíme do pěti tříd A, B, C, D, E. Adresace většiny LAN sítí se provádí v privátním rozsahu IP adres dle RFC 1918:

- Třída A - 10.0.0.0/8 až 10.255.255.255/8,
- Třída B - 172.16.0.0/16 až 172.31.255.255/16,
- Třída C - 192.168.0.0/24 až 192.168.255.255/24.

V třídě C první tři oktety identifikují adresu sítě, zbývající oktet identifikuje uzel. V podsíti se nesmí vyskytovat více zařízení se stejnou adresou. Sítě adresované privátním rozsahem dle RFC 1918 potřebují pro přístup na internet překlad adres na veřejné (NAT, PAT). [7]

Síťová bezpečnostní opatření

Mezi základní síťová bezpečnostní opatření patří [12]:

- instalace firewallů a IDS, IPS
- použití filtrů na směrovačích,
- vytvoření síťové topologie usnadňující monitorování,
- šifrování síťové komunikace,
- vyžadování autentizace.

2. Kamerový systém IP CCTV

Funguje na základě sady protokolů TCP/IP. V aplikaci využívající síťové video jsou digitalizované video streamy přenášeny na kterékoliv místo na síti pomocí běžné i bezdrátové IP sítě, což umožňuje monitorování videa a jeho záznam odkudkoliv v síti. Uživatel s příslušnými přístupovými právy tak může vzdáleně sledovat a nahrávat živé video záběry. K vybudování IP kamerového systému se používá systém strukturované kabeláže. [11]

IP síťová kamera

Základní charakteristiky jsou následující:

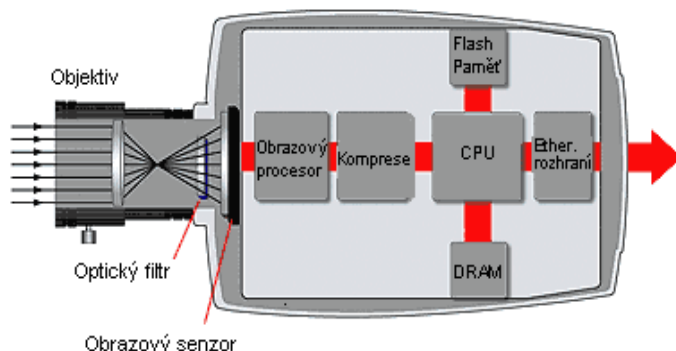
- kamera a počítač v jednom,
- má vlastní IP adresu, funguje samostatně jako koncový uzel sítě,
- umožňuje digitální záznam na server,
- možnost napájení po standardní kabeláži (PoE),
- kvalitní neprokládaný obraz (Progressive Scan) s více detaily a vyšším megapixelovým rozlišením,
- kvalita obrazu je definována počtem odeslaných snímků za vteřinu a rozlišením snímku,
- možnost centrálně spravovat distribuovaný systém.

Mezi základní pokročilé funkce patří:

- detekce rozpoznání pohybu. Přináší úsporu šířky pásma a kapacity disku (obraz z kamer může být přenášen pouze tehdy, když je před kamerou nějaký pohyb),
- snadná integrace přenosu hlasu přímo do videostreamu. Možnost obousměrné komunikace,
- propojení s dalšími systémy pomocí vstupních/výstupních portů (např. kontakt u dveří, detektor rozbití skla).

Technologie kamery

Vše potřebné pro sledování obrazu přes síť je zabudováno v jednotce, jak je znázorněno na obrázku 3. Kamera má vestavěný software pro web server, FTP server, FTP klienta a emailového klienta. Mezi další funkce patří alarmový vstup a výstup pro přenos. [11]



Obrázek 3 - Blokové schéma IP kamery[10]

Standardy pro kompresi videa

Digitální video se vždy komprimuje, aby se zvýšila přenosová rychlost a ušetřilo místo na disku. IP kamery obvykle používají tyto kompresní formáty [11]:

- Motion JPEG

Video ve formě sekvence JPEG obrázků. Kamera zachytí jednotlivé obrázky a zkomprimuje je do JPEG formátu. Frekvenci snímků okolo 16/s a více vnímá divák jako normální video (Motion JPEG). Každý snímek tvoří samostatný JPEG záběr (zaručená kvalita, určená úrovní komprese),

- MPEG

Základním principem formátu MPEG je porovnávání dvou komprimovaných záběrů, které mají být odeslány přes síť.

- H.264

Vytvořen ke snížení přenosových nároků a zvýšení celkové efektivity. Bez snížení kvality videa dosáhneme až 70% snížení velikosti videosouboru ve srovnání s M-JPEG až 40% úsporu velikosti souboru ve srovnání s MPEG-4.

Šířka pásma

Sít'ové kamery zasílají data po IP síti a spotřebovávají tak určitou část její kapacity. Šířka pásma potřebná pro přenos obrazu je jedním z nejdůležitějších kritérií při budování systému síťového videa. Zatížení sítě kamerami závisí na faktorech jako rozlišení obrazu, kompresní poměr, snímková frekvence či komplexnost scény. U kamerových systémů se používají dva způsoby přenosu obrazu v síti, které mají odlišné nároky na šířku pásma [3]:

- Unicast

Data jsou adresována pouze jednomu příjemci v počítačové síti.

- Multicast

Komunikace současně s několika příjemci v síti. Slouží ke snížení zatížení sítě (jeden videostream pro předem určenou skupinu uživatelů). Aktivní prvky v síti musejí v tomto případě podporovat multicastový přenos.

Kamery připojené do LAN sítě musejí mít k dispozici dostatečnou přenosovou kapacitu a na druhou stranu musejí ponechávat prostor další komunikaci v síti podle priority, aby nesnížili její výkon. Variantou je oddělit provoz kamer pomocí virtuálních sítí LAN, samostatných aktivních prvků nebo navýšit výkon sítě použitím výkonnějších aktivních prvků.

Požadavky na budování IP kamerových systémů

Při uvažování nad touto problematikou je nutno vzít v úvahu následující potřeby [3]:

- jaké oblasti chceme monitorovat,
- jaká je požadovaná snímková frekvence (stále nebo pouze v některých situacích),
- zda je třeba nahrávat obraz neustále nebo jen v případě, když dojde ve scéně k nějaké události,
- jak dlouho je třeba video archivovat,
- jaké je zapotřebí rozlišení a kvalita obrazu,
- zda je nutné kamerami otáčet nebo stačí nastavení jedním směrem,
- zda je třeba zajistit kvalitní obraz i v šeru nebo případně i ve tmě,
- jaká je požadovaná správa video záznamů.

3. Shromáždění požadavků

Budova je rozdělena na tři části - administrativní část, skladovou halu a expediční halu. Provoz budovy je určen, jak pro rozvoz zboží firemními vozy, tak pro výdej zboží zákazníkům. Obchodní sklad bude sloužit ke skladování zboží velkoobchodu a maloobchodu se sortimentem elektro-materiálu a elektro-osvětlení.

Administrativní budova je dvoupodlažní objekt. Její schematický plán je zobrazen v příloze 3a. V přízemí bude umístěno cca 60 přípojných míst. Nachází se zde obchodní oddělení, marketingové oddělení a bezpečnostní oddělení. Předpokládá se využití následujících aplikací:

- operační systémy (Windows 2007, Windows Vista, Windows XP),
- kancelářské aplikace (Microsoft Office, PDF Creator, atd.),
- aplikací firemního informačního systému,
- aplikací skladového systému,
- aplikací zaměřených na videokonference.

V prvním podlaží bude umístěno cca 45 přípojných míst. Nachází se zde projekční oddělení, ekonomické oddělení, vedení společnosti, zasedací místnost, technická podpora, oddělení nákupu a logistiky. Pro projekční oddělení budou provozovány aplikace pro 3D modelování podporující projekční činnost (např. AutoCad aj.).

Skladová hala a expediční hala, jejichž schematický plán je v příloze 3b tvoří dva spojené celky a navazují na administrativní budovu. V halách budou pracovníci skladu používat PDA zařízení a čtečky na příjem, kontrolu a výdej materiálu s požadavkem bezdrátového pokrytí.

Požadavky na kamerový systém

V zájmových prostorách budou umístěny barevné kamery, které budou připojeny na záznamové zařízení - digitální záznamový systém s výstupem Ethernet. Kamerami bude hlídán venkovní plášť celé budovy dále vstupní a vnitřní vytipované prostory objektu. Výstup záznamového systému bude zapojen do počítačové sítě, kde si oprávnění uživatelé (podle práv nastavených správcem počítačové sítě) budou moci prohlédnout záznam určité kamery v reálném čase, případně vytisknout materiál usvědčující viníka události. Po zapl-

nění záznamového disku (několik dní) se nejstarší data budou přepisovat novými. Základní požadavky na kamery jsou následující:

- nejméně jednomegapixelové rozlišení,
- centrální dohled a správa,
- funkce detekce pohybu,
- podpora autentizace IEEE 802.1x,
- podpora HTTPS.

Systém kontroly přístupu

U vstupního vchodu a dalších vytipovaných místností je požadována instalace přístupového systému. Přístupový systém je požadován včetně docházkového SW.

Požadavky na bezdrátové připojení WiFi

Je požadováno pro funkci e-skladu WiFi vykrytí prostoru expediční a skladové haly. Situační plán haly je znázorněn v příloze 3b. Základní požadavek na bezdrátové zařízení:

- podpora přenosových rychlostí dle norem IEEE 802.11 a,b,g,
- autentizace IEEE 802.1x.

Požadavky na aktivní prvky

Základní požadavky vyplývající z potřeb uživatelských zařízení a náročnosti provozu jsou následující:

- manažovatelnost prvků,
- podpora multicastu pro přenos videa,
- maximální redundance prvků.

Rekapitulace předpokládaného rozložení přípojných míst je uvedena v tabulce 2.

Tabulka 2 - Rozložení přípojných míst (Zdroj: autor)

Lokalita / Typ připojení	PC	IP kamery	Acces pointy	ACS kontrola vstupu	Server	Celkem
Administrace přízemí	48	7	4	1	6	66
Administrace I. NP	35	5	3	0	0	43
Sklad	4	7	4	0	0	15

Základní požadavky na budovanou infrastrukturu počítačové sítě LAN:

- rychlost a univerzálnost,
- schopnost dalšího růstu za předpokladu ochrany investic,
- schopnost integrace nových technologií,
- jednoduchá správa.

Resumé a metodika postupu návrhu systémů

Je požadováno zpracovat řešení návrhu infrastruktury aktivních prvků variantně a to s ohledem na možnost rozšíření administrativní budovy v budoucnosti o jedno patro a rozšíření skladové haly na dvojnásobnou velikost a s ohledem na stávající stav. Preferovat návrh na eventualitu rozšíření.

Vzhledem k požadavkům zapojení několika systémů a jejich rozmanitosti je vhodné při návrhu postupovat podle metodik předních výrobců jednotlivých systémů. Pro návrh kamerového systému to jsou základní doporučení uvedené v *AXIS Design guide* firmy Axis a pro aktivní prvky *Internetwork Design Guide* firmy Cisco [1][9].

4. Návrh strukturované kabeláže

Při návrhu této části se bude postupovat podle doporučení ČSN EN 50173-1, jejichž základní informace jsou uvedeny v kapitole 1.1.

4.1 Návrh části horizontální rozvody

V obou patrech kanceláří administrativní budovy bude provedena strukturovaná kabeláž pro rozvedení počítačové sítě. V komunikačních rozvaděčích budou kabely strukturované kabeláže zakončeny na panelech se 60-ti porty RJ45. Každé pracoviště bude vybaveno komunikační dvouzásuvkou, která obsahuje dva moduly RJ45. Do každého z těchto modulů RJ45 se může připojit jakékoliv zařízení, které podporuje odpovídající protokol (TCP/IP, Ethernet, telefon, aj.) tedy dva počítače, notebooky, síťové tiskárny, telefony, IP kamery, popřípadě jakákoliv jejich kombinace.

Hlavní rozvaděč bude umístěn v přízemí budovy v serverovně. Jedná se o centrální bod kabelážního systému. Odtud bude proveden po celém patře hvězdicový rozvod k účastnickým dvojjádrovým zásuvkám. Celkem 66 přípojných míst.

Podružný rozvaděč bude umístěn v I.NP. Odtud stejně jako v přízemí bude proveden po celém patře hvězdicový rozvod k účastnickým zásuvkám. Celkem 45 přípojných míst. Celkový situační plán rozmístění datových zásuvek administrativní budovy je znázorněn v příloze 3a. Rozvody budou realizovány stíněnými kabely U/FTP 4x2xAWG23 kategorie Cat 6A. K zásuvkám povedou vždy dva kabely v parapetním nebo podhledovém kanálu. V rozvaděčích budou následně umístěny aktivní zařízení počítačové sítě. Připojení kamer je navrženo prostřednictvím nestíněné kabeláže U/UTP Cat.5e, která je pro tuto potřebu dostačující.

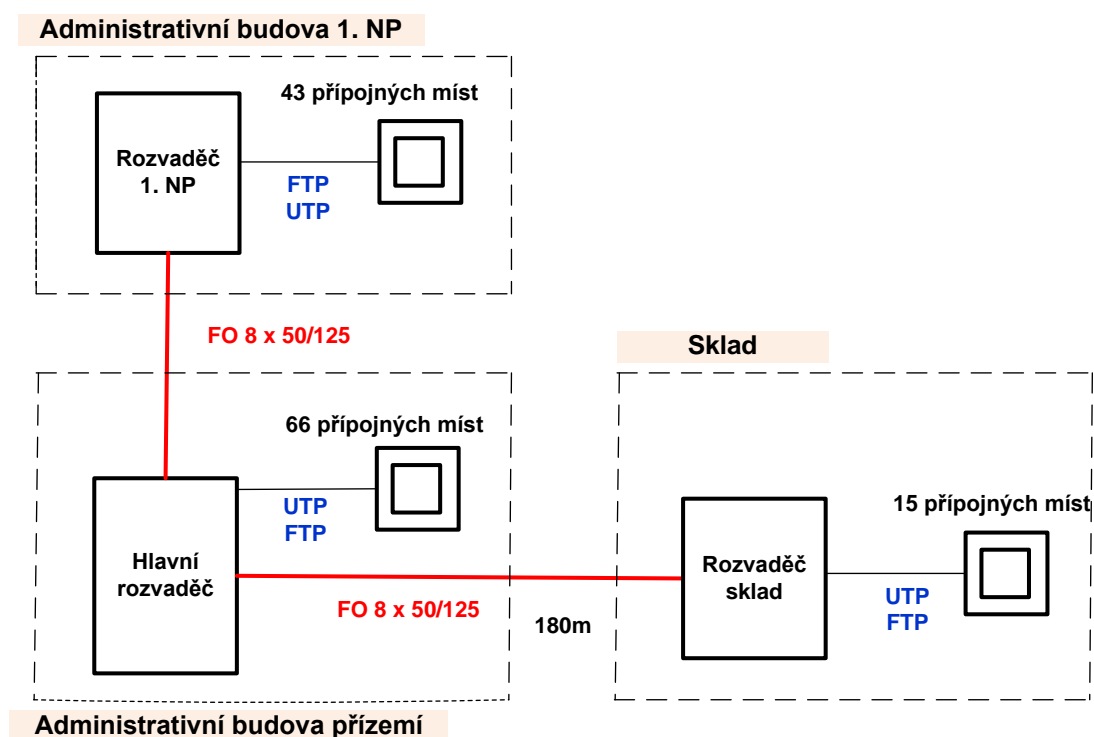
Parametry každého kabelu je nutné po montáži změřit, zda splňují požadavky kladené na síť s vysokou přenosovou rychlostí a vystavit protokol. Požadavkem je výstavba celého systému výhradně z komponent jednoho výrobce což umožňuje vyvážený přenos signálu v celé délce přenosového řetězce a dále následnou certifikací systému jako celku. Záruční doba na komponenty strukturované kabeláže je 20 let.

Výkonově tak kabeláž bude připravena na přenosovou rychlost 10Gb/s. Stávajícím požadavkům na přenos by vyhovovala i kategorie Cat.6, ale vzhledem k možným větším přenosovým nárokům do budoucna byla zvolena kabeláž Cat.6A.

4.2 Návrh části vertikální a areálové

Ve vertikální části bude hlavní rozvaděč v přízemí propojen s podružným rozvaděčem v I.NP optickými kabely (FO) 8vláken x 50/125 μ m (specifikace 1000BASE-SX). Důvodem použití optických kabelů je ochrana před rizikem vzniku potenciálových rozdílů, které mohou způsobit vážné poškození síťového hardwaru.

V areálové části bylo navrženo řešení připojení vzdáleného rozvaděče ve skladu ve vzdálenosti cca 180 m. Odtud budou připojeny kamery a bezdrátové body v části skladu. Pro připojení použijeme také optický kabel stejných parametrů tedy 8vláken x 50/125 μ m (1000Base-SX). Kabel bude uložen v drátěných žlabech pod stropem haly. Připojení bude tvořit dostatečnou kapacitu na plánované rozšíření skladu na dvojnásobnou kapacitu. Blokové schéma zapojení rozvaděčů je znázorněno na obrázku 4.

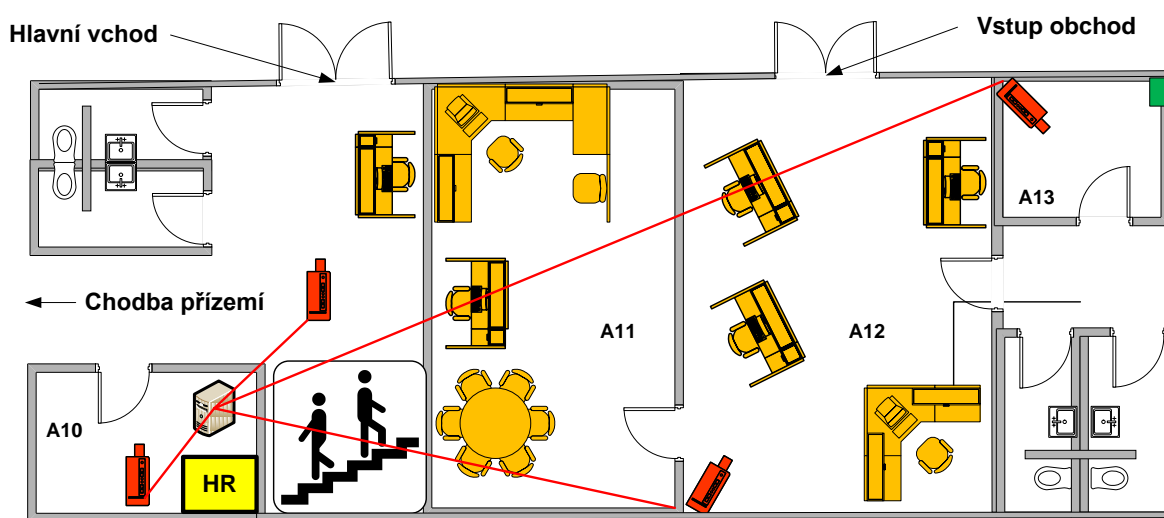


Obrázek 4 - Blokové schéma propojení rozvaděčů (Zdroj: autor)

5. Návrh bezpečnostního systému a WiFi systému

5.1 Návrh kamerového systému

Vzhledem k tomu, že jde o novou výstavbu ve které se počítá s kabelážním systémem ve formě strukturované kabeláže je budovaný kamerový systém zvolen na bázi IP kamer síťového videa. Kamerami bude hlídán venkovní plášť budovy a skladu, příjezd na rampu, vstupní prostory do objektu. Dále pak vnitřní vytipované prostory administrativní budovy tj. vstupní hala, serverovna, obchodní oddělení a pokladna jak je možno vidět na obrázku 5. V místnosti serveru bude umístěno barevné digitální záznamové zařízení a sledovací monitor LCD 21“ bude umístěn u bezpečnostního technika.



Obrázek 5 - Rozmístění kamer v přízemí budovy (Zdroj: autor)

Popis navrženého systému

Pro video přenos jsou navrženy videokamery s internetovým protokolem výrobce AXIS. Tyto kamery jsou navrženy a konstruovány pro splnění vysoké kvality a cenové dostupnosti. Systém Axis je vhodný pro aplikaci ve všech oblastech použití. Sortiment jednotlivých typů kamer umožňuje co nejlépe zvolit konkrétní typ kamery do určeného prostředí. Podpora formátů JPEG a MPEG4 s pěti stupni přednastavené komprese je významnou vlastností při konfiguraci síťového prostředí a výběru samotných aplikací. Pro další efektivitu, účinnost a zabezpečení v provozu tyto kamery nabízejí IP filtraci, simultánní přístup a ochranu hesly.

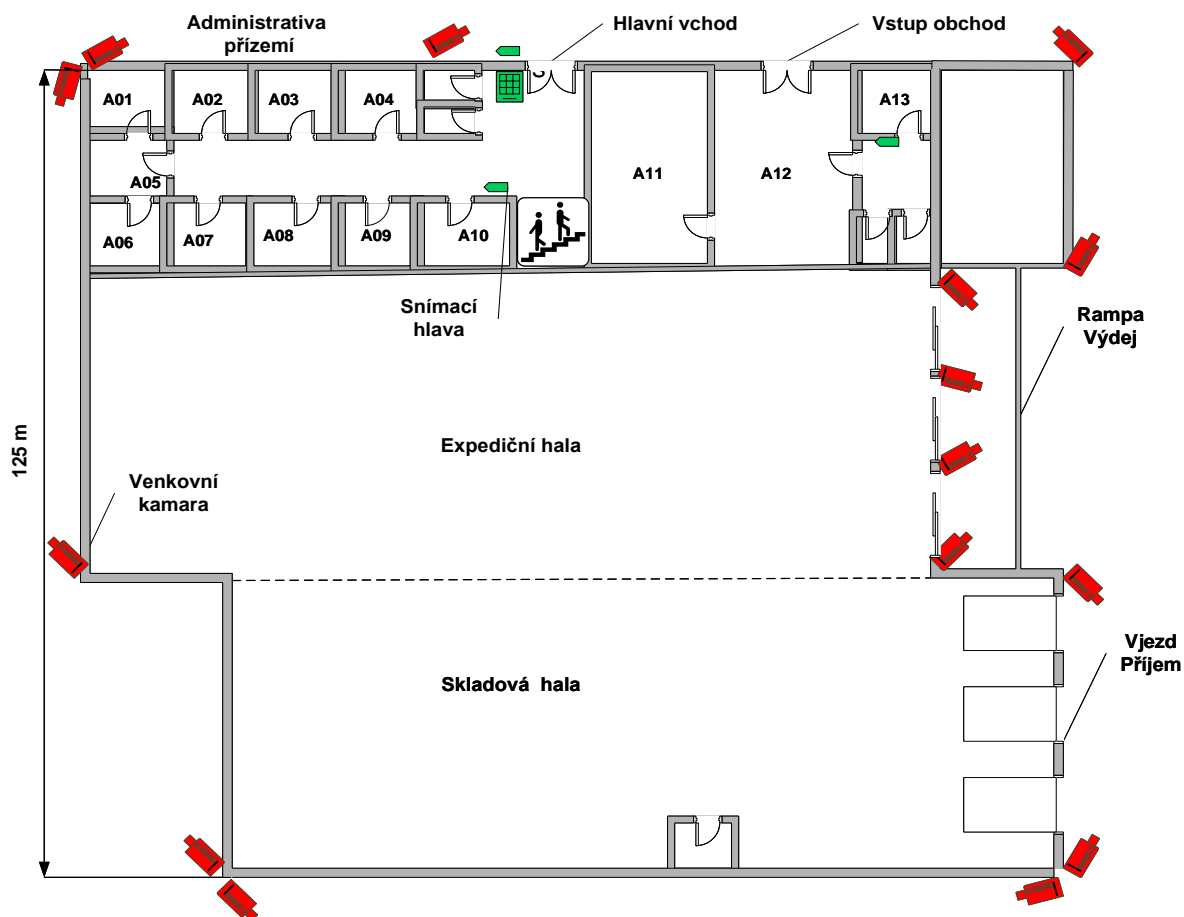
Umístění prvků systému

Pro tento objekt jsou navrženy dva typy kamer. Kamera Axis 211M typ fixní pro venkovní použití, která umožňuje vyšší kvalitu obrazu díky pokročilému zpracování videa a progresivnímu skenování pomocí CCD senzoru. Pracuje v maximálním rozlišení 1,3 Megapixelů při 12 snímcích za sekundu. Poskytuje ostrý a jasný obraz, ideální pro identifikaci jednotlivých osob a objektů. Veškeré venkovní kamery budou uvnitř venkovních krytů TPH, které obsahují vytápění s ventilací. Každá venkovní kamera bude mít své samostatné napájení 230V. Dvě kamery určené pro sledování vjezdu aut, budou navíc opatřeny jiným typem objektivu, který umožní lépe zachytit detaily aut a osob vjíždějících do tohoto prostoru. Druhým typem kamery je kamera Axis 216MFD typ Dome, která má podobné parametry, ale bude použita ve vnitřních prostorách.

Jde o IP kamery pracující v režimu „detekce pohybu“. Tato funkce umožňuje nahrávání záznamu pouze v případě, že kamera zaznamená ve sledované oblasti nějaký pohyb.

Kamery budou připojeny na příslušné aktivní prvky s technologií PoE. Napájení ethernetových zařízení prostřednictvím datových vodičů strukturované kabeláže, bez nutnosti použití přídavných napájecích zdrojů či síťových adaptérů na straně napájeného zařízení. Situace rozmístění venkovních kamer je znázorněna na obrázku 6. Fyzická topologie připojení kamer je znázorněna v příloze 3. Základní parametry použitých kamer jsou následující:

- videokomprese M-JPEG a MPEG-4,
- rozlišení až 1280x1024 při 12 fps, až 30 fps v rozlišení 800x600,
- plně duplexní audio se zabudovaným mikrofonom,
- podpora IEEE 802.1x.



Obrázek 6 - Situace rozmístění venkovních kamer (Zdroj: autor)

AXIS 211M

Tato fixní kamera se skládá z těla kamery a objektivu jak je možno vidět na obrázku 7. Je jasně rozpoznatelná včetně směru, který sleduje. Umožňuje výměnu objektivu, což dává možnost různé konfigurace kamery a pozorovacího úhlu.



Obrázek 7 - Fixní kamera 211M[11]

AXIS 216MFD

Tato kamera je typu Fixed Dome, jak je zobrazeno na obrázku 8 je polokulovitého tvaru a lze ji nasměrovat do požadovaného směru. Není možné rozpoznat do kterého směru je kamera natočena a odkud tedy obraz snímá. Není vybavena výměnnými objektivy.



Obrázek 8 - Fixed Dome 216MFD[11]

Požadavky na ukládací prostor

Pro stanovení požadavků na ukládací prostor je potřeba vzít v úvahu tyto parametry [1]:

- počet kamer,
- počet hodin za den, kdy kamera bude nahrávat,
- jak dlouho budou data uchovávána,
- zda záznam bude pouze při detekci pohybu nebo nepřetržitě,
- počet snímků za sekundu a komprese, kvalita obrazu.

Záznamový server

Pro stanovení vhodného typu byl použit kalkulátor propustnosti firmy Axis s navrženými parametry. Návrh výpočtu je v příloze 6. Základní návrh je určen pro celkem 19 kamer vybraného typu, délka archivace je 7 dní, komprese byla zvolena Motion JPEG, počet snímků za vteřinu je 6. Kapacitně je ukládací prostor dimenzován na cca 700 GB. Zvolené parametry je možno pro provozní potřeby případně upravit.

V návrhu systému IP CCTV je pro ukládání dat navržen záznamový server s datovým úložištěm přímo v serveru.

Byl vybrán typ Dell T110 X3460 znázorněný na obrázku 9. Lze ho přizpůsobit tak, že bude obsahovat až čtyři pevné disky pro důležitá data. Pole RAID zajistí zvýšenou ochranu

dat. Dále nabízí i nové možnosti konektivity pro externí úložiště pomocí portu e-SATA a základní správu systémů k jednoduchému monitorování systému.



Obrázek 9 - Záznamový server Dell T110 (zdroj: autor)

Základní parametry jsou následující:

- CPU: 1xIntel, XeonX3460 Processor (2.8GHz,8MCache,Turbo),
- RAM: 4GB(2x2GB)1333MHZ,
- Interní storage: 2x1TB SATA7200rpm,
- Řadič: SAS 6iR - RAID 0,1.

Bezpečnostní software

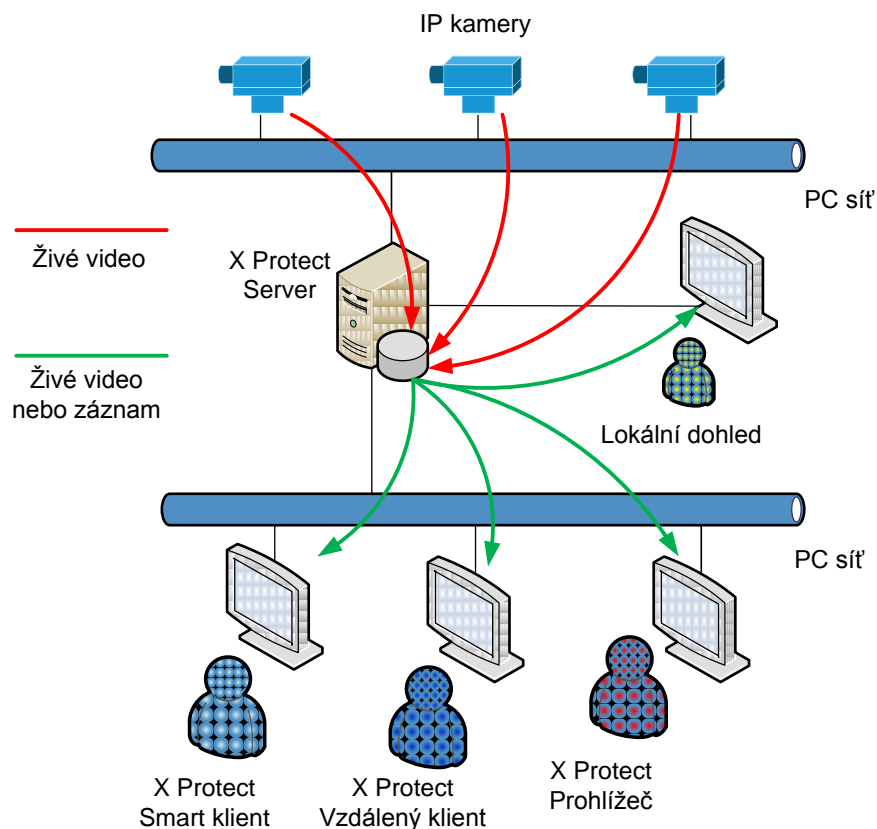
Vzhledem k většímu počtu kamer je pro správu, prohlížení a konfiguraci kamer vhodné zvolit specializovaný software správy videa.

Byl vybrán software XProtect Basis+ výrobce Milestone. Navržený software představuje vhodné řešení pro malé instalace, který poběží na jednom serveru. XProtect Basis+ podporuje až 25 kamer současně, tyto kamery mohou být navíc od různých výrobců.

Klíčové výhody jsou následující:

- pokročilá IP videotechnologie (ovládání kamery, detekce pohybu),
- snadná instalace, obsluha, rozhraní je intuitivní a přehledné,
- přístup k datům z jakéhokoliv počítače,
- rychlý export důkazního materiálu.

Přístup oprávněných uživatelů k záznamům na serveru je znázorněn na obrázku 10.



Obrázek 10 - Přístup uživatelů k záznamu videa (Zdroj: autor)

Základní vlastnosti:

- záznam videozáběrů z IP kamer ve formátu MJPEG, MPEG4,
- automatická detekce kamery,
- server modul, vzdálený klient, smart klient.

Kalkulaci nákladů na kamerový systém včetně dohledového softwaru je v tabulce 3.

Tabulka 3 - Kalkulace nákladů IP kamer (Zdroj: autor)

Technologie	Ks	Cena	Celkem
AXIS 211 M	15	15 500	232 500
AXIS 216 MFD	4	16 000	64 000
XProtect Basis+ pro 25 kamer	1	59 000	59 000
Záznam. server Dell T110	1	35 000	35 000
Celkem cena Kč bez DPH			390 500

Alternativní řešení návrhu připojení kamer

Vzdálenost připojení kamer k jednotlivým aktivním prvkům by neměla překročit 90 m. K připojení kamer zadní pláště budovy a rampy se počítá z podružného rozvaděče skladu, který je také navržen pro připojení zařízení pro budoucí rozšíření skladu.

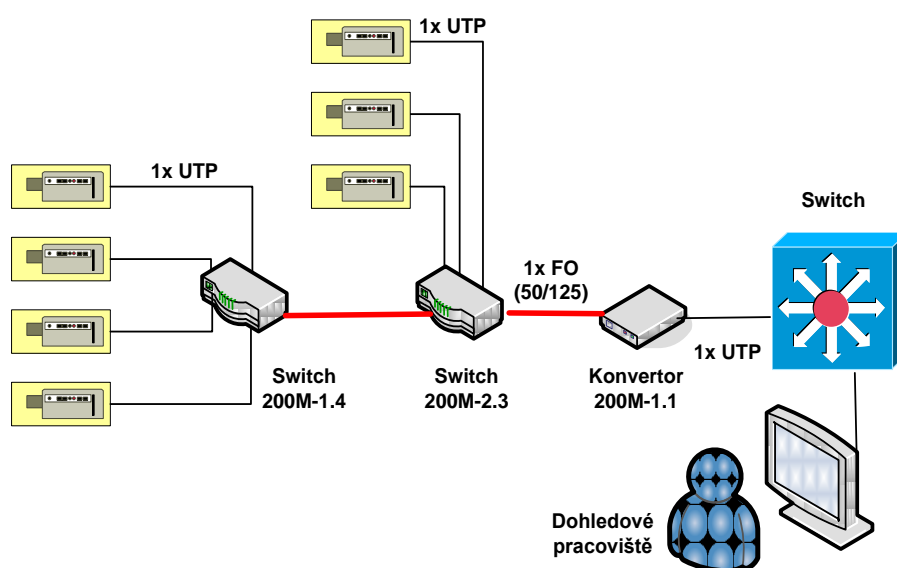
Jako alternativní řešení je připojení kamer z hlavního rozvaděče technologií WDM prostřednictvím optických konvertorů 200M pro převod z optického vedení na metalické.

Vlnový multiplexu WDM (Wavelength Division Multiplexing) základní vlastnosti [13]:

- zvyšuje přenosovou kapacitu optického vlákna,
- spojuje nebo rozděluje dvě vlnové délky do jediného vlákna a tak umožňuje přenos nezávislých aplikací po jednom vlákně.

Media konvertory 200M

200M je systém optických přepínačů, konvertorů a opakovačů s optickou sběrnicí 200 MB/s a 10/100 Mb/s Ethernet UTP porty. Sběrníkové řešení s implementovaným WDM v maximální možné míře redukuje nároky na cenu instalace systému. Jedním optickým vláknem tak lze připojit několik desítek IP kamer. Návrh zapojení standardního IP systému s optickou sítí optimalizovanou do jedné větvené sběrnice je znázorněn na obrázku 11. Možnost PoE rozšíření umožní napájet IP kamery přímo po datovém UTP kabelu. Vnitřní struktura přepínačů dovoluje směřovat multicastové pakety na požadovaný port.



Obrázek 11 - IP systém s optickou sítí do jedné sběrnice (Zdroj: autor)

Kamery mohou tak být alternativně připojeny optickým kabelem 4x50/125 pomocí médiakonvertorů a přepínačů prostřednictvím optické sběrnice 200 Mb/s. Jedná se o tyto typy výrobce METEL s.r.o.:

- 200M-1.1 = 1x optický port + 1x LAN UTP,
- 200M-2.3 = 2x optický port + 3x LAN UTP,
- 200M-1.4 = 1x optický port + 4x LAN UTP.

5.2 Návrh přístupového systému

V projektu je požadováno kontrolovat přístup osob pomocí kartového systému do vymezených prostor. Systém kontroly vstupu ACCESS umožňuje omezit vstup do určitých prostor pouze v určité době nebo určité skupině osob nebo jiných subjektů s vlastní identifikační kartou nebo znalostí vstupního kódu. Povolený pohyb osob se děje definováním přístupových oprávnění jednotlivých osob, které se vždy skládá z:

- určitého snímače nebo množiny snímačů,
- definované doby průchodu (časové zóny),
- volitelné speciální chování karty podle jejího typu.

Přístupový systém je pro potřeby tohoto projektu navržen jako systém ACCESS (výrobce COMINFO), který je určen pro řízení, kontrolu a zpracování definovaných pohybů osob uskutečněných pomocí identifikačních karet s využitím podpůrného hardware (různých typů snímačů identifikačních karet) a souboru programových modulů na příslušných počítačích.

Umístění prvků přístupového systému

Před hlavním vstupem do administrativní budovy bude umístěna snímací hlava v provedení s klávesnicí pro vstup číselných údajů (H-Pro/K). Ve vstupní hale bude umístěna další hlava v provedení bez klávesnice (H-Pro) společně se snímačem identifikačních karet REI-ST. Další snímací hlava bez klávesnice bude umístěna před vchodem do serverovny a pokladny. Umístění hlav je patrné ze situace na obrázku 6. Znázornění snímačů je zobrazeno na obrázku 12, zapojení fyzické topologie je v příloze 3.



Obrázek 12 - Snímač REI-ST, externí hlavice H-PRO, H-PRO/K (Zdroj: autor)

SW - Systém kontroly vstupu Acces

System se skládá z identifikačních karet (vždy určují konkrétního vlastníka), ze snímačů těchto identifikačních karet, komunikačních zařízení a počítačů a na nich provozovaného programového vybavení. Přístupový systém bude integrován s docházkovým systémem PASSPORT na úrovni společné databáze, shodných komunikací se snímači a předávání docházkových dat o průchodech pro zpracování v rámci evidence docházky.

Základní funkční vlastnosti systému ACCESS:

- definování práv jednotlivých ID karet pro vstup do zóny,
- zpřístupnění aktuálních stavů systému (kde se která identifikační karta nachází, stav zařízení) pomocí monitorovacích úloh,
- vzdálená správa snímačů,
- zavedení definice typů karet (skupiny osob) a k nim odpovídající chování,
- jednoduché přiřazování přístupových práv a možnost definovat vzory (šablony)

Celý přístupový systém je komunikačně propojen do jednoho funkčního celku. Snímací jednotka ve spojení s dalšími snímači a nadřazeným počítačem vytváří celek využívající všechny poskytované funkce. Tato komunikace bude realizována pomocí rozhraní ETHERNET 10BaseT. Každá jednotka docházkového systému je vybavena tímto rozhraním. Vlastní aplikaci správy přístupového systému lze spustit na kterékoliv pracovní stanici připojené k serveru. Kalkulace nákladů je uvedena v tabulce 4.

Tabulka 4 - Kalkulace nákladů přístupový systém (Zdroj: autor)

Technologie	Ks	Cena	Celkem
REI - ST snímač identifikačních karet	1	39 000	39 000
H - PRO/K externí snímací hlava	1	7 000	7 000
H - PRO externí snímací hlava	3	6 500	19 500
Docházkový SW komplet	1	58 400	58 400
Celkem cena Kč bez DPH			123 900

5.3 Návrh přístupových bodů WiFi

Aktivním prvkem návrhu této části je zařízení AP (Access Point). Jde o bezdrátový přístupový bod, který dovoluje bezdrátovým klientům přístup do bezdrátové sítě WLAN (Wireless LAN). V návrhu sítě je použito několik přístupových bodů pokrývajících požadované prostory v administrativě, jak je znázorněno v příloze 3a a halách znázorněné v příloze 3b:

- 1x vstupní hala,
- 1x obchodní oddělení,
- 1x zasedací místnost přízemí,
- 1x zasedací místnost I.NP,
- 7x pokrytí celého skladu (pro řešení e-skladu pro použití PDA s podporou WiFi 802.11g). V alternativním řešení pokryt jen expediční halu.

Existují dva způsoby řešení bezdrátové sítě:

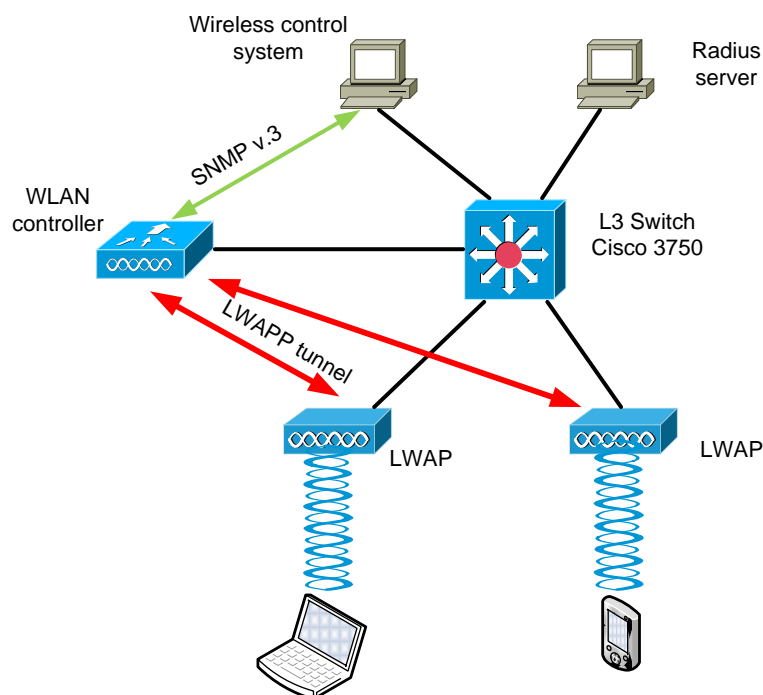
- **samostatná AP** - přístupové body jsou samostatně konfigurované a zapojené, místo připojení AP je i místem připojení klientů (složitá údržba a konfigurace na mnoha místech),
- **centrální řízení** - kdy AP představují pouze radiové a šifrovací rozhraní pro klienty, ostatní funkce přebírá kontroler (konfigurace na jednom místě).

Vzhledem k většímu počtu AP bylo navrženo centrální zařízení s lehkými AP prostřednictvím WLC (Wireless LAN Controller) od výrobce Cisco. Byl navržen typ Cisco AIR-WLC-2112-K9.

Funkce a výhody WLC:

- řídí AP prostřednictvím LWAPP (Lightweight Access Point Protocol) resp. CAPWAPP. Všechna AP jsou v LWAPP módu,
- pro komunikaci mezi WLC a AP se vytvoří bezpečný (šifrovaný) tunel,
- upravuje vysílací výkon sousedních AP (v případě výpadku fungování některého AP),
- centrální správa konfigurací jednotlivých AP,
- možnost připojení fyzicky (port) nebo virtuálně (VLAN) do různých sítí,
- autentizace uživatelů prostřednictvím RADIUS serveru,
- řízení výkonu vysílačů,
- sledování cizích AP v síti,
- roaming (přechod z jednoho bodu na druhý bez přerušení spojení).

Zobrazení schéma funkce WLC a připojení k jednotlivým LWAP je na obrázku 13.



Obrázek 13 - Schéma připojení WLC k LWAP (Zdroj: autor)

Pro vykrytí uvažovaných prostor byly navrženy přístupové body výrobce Cisco typ:

Cisco AIR –LAP1131AG-E-K9

Základní parametry přístupového bodu jsou následující:

- podpora přenosové rychlosti norem IEEE 802.11,
- napájení přímo po ethernet kabelu (PoE),
- autentizace - 802.1x, podpora VLAN.

Kalkulace nákladů na WiFi systém je v tabulce 5.

Tabulka 5 - Kalkulace nákladů WiFi (Zdroj: vlastní)

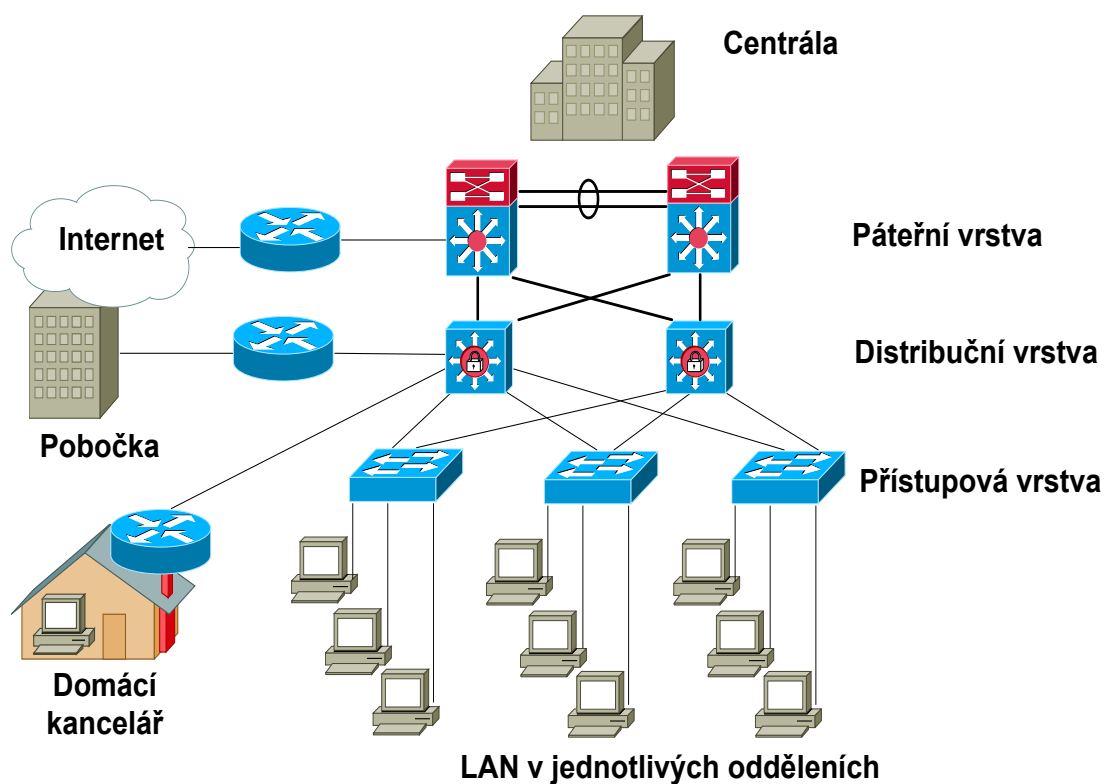
Technologie	Ks	Cena	Celkem
AIR-WLC-2112-K9	1	55 000	55 000
Cisco AIR.LAP1131AG	11	9 900	108 900
Celkem cena Kč bez DPH			163 900

6. Návrh aktivních prvků

Na základě požadavků na výkon a dostupnost je nejvhodnější použití hierarchické uspořádání s využitím směrovačů a různě výkonných přepínačů na třech úrovních jak je zobrazeno na obrázku 14 [9]:

- jádro sítě,
- distribuční síť,
- přístupová síť.

U méně rozsáhlých sítí dochází ke sloučení jádra (páteře) s distribucí v jednu vrstvu.



Obrázek 14 - Hierarchické uspořádání prvků v LAN[9]

6.1 Faktory pro výběr aktivních prvků

Mezi základní patří následující [12]:

- požadovaná šířka pásma závisící na maximálním objemu dat, které se budou přenášet (objem dat přenášených sítí za jednotku času),
- maximální dovolené přenosové zpoždění (doba mezi vysláním rámce a jeho přijetím jiným uzlem v síti),

- doba odezvy (doba, která uplyne mezi požadavkem na síťovou službu a odpovězí na požadavek),
- jednoduchost konfigurace a údržby,
- nepřetržitá vysoká dostupnost služeb.

6.2 Volba aktivních prvků

Z hlediska vlastností provozovaných aplikací, které budou tvořit: firemní informační systém, skladové aplikace, bezpečnostní aplikace (přenos videa), multimediální aplikace (marketingové prezentace), internetové aplikace (WWW, Email a přenos souborů) je nutné zvolit dostatečnou šířku pásma, minimální přenosové zpoždění, vysokou dostupnost, dostatečnou redundanci prvků sítě a kapacitní rezervu pro další vývoj.

Vysokou dostupnost získáme hierarchickým a modulárním designem s klíčovými prvky nasazenými redundantně. Navrhovaná síť bude realizována jako síť přepínaná, rozdělená do několika virtuálních sítí VLAN.

Z hlediska fyzického návrhu je navrženo rozdělení sítě do dvou vrstev:

- vrstvy přístupu,
- vrstvy jádra společně s distribucí.

Toto rozdělení do vrstev s sebou nese výhody jako rozčlenění jednotlivých částí sítě do menších domén, které přispívají k snadnější lokalizaci chyb a jejich odstraňování.

Ve vrstvě přístupu budou pro připojení koncových uživatelů a zařízení použity L2 přepínače.

Pro vrstvu jádra společně s distribucí, kde je agregace redundantních uplinků z přístupové vrstvy je žádoucí co nejrychleji přenášet data mezi jednotlivými částmi sítě budou použity sofistikovanější zařízení Layer 3 přepínače, které budou zajišťovat směrování paketů mezi jednotlivými VLANy.

Layer 3 Směrovací přepínač, Routing switch

Spojují výhody přepínačů a směrovačů. Základní vlastnosti:

- zařízení pracující na síťové vrstvě OSI modelu (Layer 3),
- softwarově implementované směrovací algoritmy, hardwarově implementované přepínání (odstranění velkého přenosového zpoždění, zvýšení propustnosti),
- možnost libovolné kombinace přepínacích a směrovacích funkcí na každém portu (směrování a přepínání jsou stejně rychlé),
- možnost implementace filtrů na bázi ACLs nebo použití QoS markování na každém paketu,
- aplikace standardních směrovacích protokolů (RIP, OSPF),
- oddělení (minimalizace) broadcastových domén,
- využití atributů IP protokolu (logické adresování, priority),
- rychlejší zpracování a vyšší propustnost paketů oproti směrovači - routeru.

Volba výrobce aktivních prvků

Hodnotu dostupnosti je možno navýšit volbou osvědčených přepínačů od spolehlivého dodavatele a nasmlouváním rychlého servisu. Pro vlastní návrh budou použity komponenty od jednoho výrobce splňující požadavky na úroveň služeb, spolehlivosti, managementu a servisní podpory. Na trhu jsou k dispozici produkty mnoha výrobců. Stanoveným kritériím nejlépe vyhovují aktivní prvky společnosti Cisco Systems. Výsledkem pak bude dostupná, odolná, flexibilní, snadno rozšiřovatelná a spravovatelná síť.

Cisco IOS - Internetworking Operating System

Je operační systém vyskytující se v síťových zařízeních výrobce Cisco. Jeho základní charakteristiky jsou:

- podporuje všechny dosud standardizované síťové protokoly na všech síťových technologiích a zároveň přináší další vlastní proprietární protokoly,
- má implementovány mechanismy, kterými je schopen překonávat různé nahodilé poruchové stavy vyskytující se v síti zajišťující vysokou stabilitu provozu.

6.2.1 Volba aktivních prvků pro vrstvu přístupu

Počtem přípojných míst cca 130 se navrhovaná LAN síť řadí do kategorie menších a středních podniků. Pro vrstvu přístupu byly navrženy přepínače 24 portové Cisco Catalyst řady 2960 místo 48 portových z důvodu zajištění alespoň částečné provozuschopnosti v případě HW poruchy zařízení. Obsahují všechny potřebné funkce přepínačů pro síť malého a středního rozsahu. Celkové zobrazení fyzické topologie je v příloze 1.

Cisco Catalyst WS-C2960-24 port switch - PC-L with PoE

Cisco Catalyst WS-C2960-24 port switch - TC-L

Přepínač je ve verzi s porty pro připojení zařízení pomocí PoE (kamery, přístupové body AP) nebo bez tohoto připojení (uživatelská PC). Základní parametry jsou následující:

- počet portů: 24 x Ethernet 10Base-T, Ethernet 100Base-TX,
- 2x10/100/1000Base-T/SFP, (mini-GBIC) uplink,
- Ethernet, Fast Ethernet, 2 Dual-Purpose Ports (10/100/1000 nebo SFP),
- VLAN podpora,
- Quality of Service (QoS),
- podpora technologie Cisco Cluster Management pomocí níž lze spravovat až 16 jednotek pomocí jedné IP adresy,
- Internet Group Management Protocol (IGMP) - řízení multicastů,
- Rapid Spanning Tree Protocol (RSTP) IEEE 802.1w - podpora redundantní topologie. Doba zotavení v případě výpadku linky nebo některého z přepínačů v kruhu činí 2 až 3 vteřiny (STP - 30 až 40 sekund). Zvýšená ochrana proti ztrátě konektivity z důvodu selhání jednoho prvku sítě (zvýšená dostupnost),
- Agregace portů (802.3ad LACP - Link Aggregation Control Protocol) - zdvojení přenosových cest do jedné logické. Zvýšení přenosové šířky pásma. (2x1Gb/s = 1x2Gb/s logický spoj).

Připojení serverů

Kritické servery doporučuji připojit přes dvě síťové karty ke dvěma různým přepínačům typ Cisco C2960G-24TC-L. Tento typ disponuje 20x 10/100/1000 porty (RJ-45) a 4x porty pro dvouúčelový uplink (10/100/1000BASE-T nebo SFP).

6.2.2 Volba aktivních prvků pro vrstvu jádra a distribuce

V oblasti jádra a distribuce použijeme dva redundantní přepínače na třetí vrstvě OSI modelu (Multilayer 3 Switch) propojeným do stohu pomocí Stack Wise technologie - produktová řada Cisco Catalyst 3750. Propojení přepínačů je možno vidět na obrázku 15.

Cisco WS-3750 G-12 S-S

Základní charakteristiky:

- 12 SFP-based Gigabit Ethernet portů,
- 32-Gbps, high-speed stacking bus,
- podpora směrovacích protokolů RIP1, RIP2, IGRP, EIGRP, OSPF, BGP,
- redundance prostřednictvím RSTP, STP,
- podpora Multicast VLAN Registrace (MVR) ,
- podpora IGMP, QoS, Cisco Cluster Management,
- správa prostřednictvím CLI (konzole), Telnetu, SNMP a HTTP,
- podpora HSRP (Hot Standby Router Protocol) - umožňuje dynamické vyvažování zátěže (spolupráce dvou směrovačů),
- nastavení pravidel komunikace pomocí Access listů.

Technologie Cisco StackWise

Slouží k tzv. stohování přepínačů propojením přepínačů na úrovni přepínací sběrnice. Určena pro přepínače Catalyst řady 3750. Základní charakteristiky [5]:

- pro propojení se používá speciální stohovací propojovací kabel,
- šířka sběrnice propojovacího spoje je 32 Gbps,
- společný operační systém, konfiguraci, MAC address tabulku a směrovací informace (vytváří jednu logickou jednotku),
- maximálně 9 přepínačů (lze přidávat i odebírat bezvýpadkově za provozu).

Při propojení do kruhu v případě jeho přerušení v jednom místě (např. při selhání některého propojovacího modulu) má za následek pouze pokles propustnosti stohovacího spoje na polovinu, nikoliv rozpad stohu. Stejně jako v případě plného propojení i v případě výpadku je stále veškerý datový provoz na všech portech obsluhován jednotně

a konzistentně na aktuální rychlosti stohovacího spoje. V případě poruchy kabelu nebo přepínače detekují sousední přepínače rozpojení kruhu a uzavřou kruh po obou stranách. V tomto režimu pak kruh má maximální kapacitu 16 Gbit/s. Stoh je řízen master switchem, kterým se stane jeden ze zapojených přepínačů.

Výhody stohování Stackwise:

- jednodušší správa - spravuje se pouze jedno zařízení místo dvou,
- vyšší odolnost proti výpadku,
- zjednodušení konfigurace sítě,
- rychlejší zotavení sítě při výpadku (při výpadku jednoho zařízení nedochází k přerušení provozu),
- zvýšení výkonu (možnost zapojení serverů současně do obou přepínačů).



Obrázek 15 - Stackwise propojení mezi Catalysty 3750[4]

Cisco Etherchannel Technology IEE 802.3 AD

Jde o technologii používanou v redundantní topologii na trunkových spojích při propojení distribuční vrstvy a vrstvy jádra a dále pak pro propojování serverů. Její výhody jsou [4]:

- větší šířka pásma,
- ihned detekuje chybu a odkloní provoz od nefunkční linky,
- deterministické automatické vyvažování zátěže mezi spoji (2x1Gb/s),
- snižuje riziko smyček,
- jedna logická přenosová cesta složená z více fyzických cest.

Propojení přepínačů přístupové vrstvy

Přepínače přístupové vrstvy budou propojeny gigabitovou páteří na optickém vlákně (vertikální rozvody). Fyzické rozhraní je 1000BaseSX prostřednictvím zásuvných konvertorů SFP typ GLC-SX-MM (LC konektor, vlákno multimode 50µm /125, dosah do 550m). Tyto transceiver moduly jsou "Hot-Swapable" s možností manipulace za běhu zařízení. Schéma fyzického připojení je zobrazeno v příloze 1.

Alternativní řešení

Jako alternativní řešení je ve vrstvě jádra použít jiného typu přepínače:

Cisco WS-C3560 G-24TS-S

Základní parametry:

- 24 Ethernet 10/100/1000 portů a 4 SFP-based Gigabit Ethernet portů,
- Multilayer switch,
- podpora multicastů.

Má podobné vlastnosti jako řada Cisco 3750, ale neumožňuje stohování pomocí Stackwise (nelze vytvořit jeden logický box). Dále má pouze 4 SFP sloty, ekonomicky je výhodnější. Pro snížení nákladů v této variantě budou core prvky zároveň sloužit pro připojení serverů. Fyzické připojení je zobrazeno v příloze 2.

6.2.3 Volba směrovačů (router) pro přístup do Internetu

Vybrán byl typ CISCO2911-SEC/K9. Jde o směrovač s přidavnými bezpečnostními funkcemi (firewall).

Cisco 2911 Security Bundle w/SEC license PAK

Základní parametry jsou:

- Intrusion Prevention Systems,
- firewall,
- filtrování obsahu (content filtering),
- VPN,
- 3 integrované WAN porty (Gigabit Ethernet),
- DSP procesory pro zpracování hlasu a videa.

IP adresace

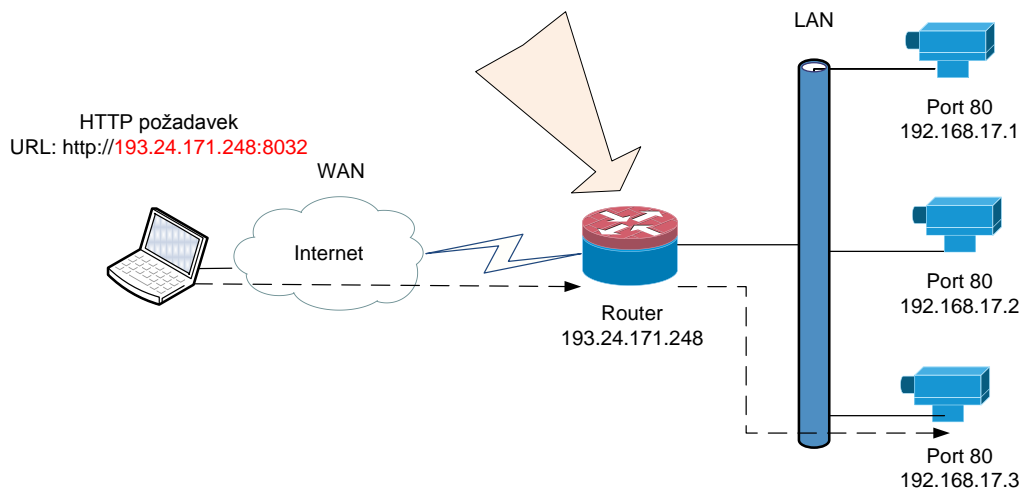
Adresní plán je velice důležitý pro konfiguraci zařízení (maskování sítě) pracujících na třetí vrstvě OSI modelu, tj. zařízení pracující s IP (síťovými) adresami.

Adresace uvnitř LAN

Jsou navrženy privátních adresy, které se mohou vyskytovat v lokálních počítačových sítích (nikoliv však ve veřejné síti Internet). Komunikace s jinými počítači skrze síť Internet je nutné tyto privátní adresy překládat pomocí NAT (Network Address Translation) resp. PAT (Port Address Translation) na veřejné (přidělené od poskytovatele připojení k Internetu ISP (Internet Service Provider)). Mapování portu na směrovači je znázorněno na obrázku 16. V navrhované síti použijeme adresy v rozsahu privátních adres třídy C, kde první tři oktety IP adresy jsou vyhrazeny pro adresu sítě a zbývající oktet představuje adresu uzlu.

Podniková síť LAN bude rozdělena do tzv. virtuálních sítí VLAN odpovídajících jednotlivým oddělením s vyhrazením dalších VLAN sítí pro management aktivních prvků, serverů a přístupu do Internetu. Komunikace mezi jednotlivými VLAN sítěmi bude probíhat na Layer 3 přepínačích Catalyst 3750. Návrh rozdělení a adresaci VLAN je zobrazeno v grafické podobě v příloze 4. Kalkulace nákladů na aktivní prvky je uvedena v tabulce 6.

Mapování portů na routeru			
Externí IP adresa routeru	Externí port	Interní adresa kamery	Interní port
193.24.171.248	8028	192.168.17.1	80
193.24.171.248	8060	192.168.17.2	80
193.24.171.248	8032	192.168.17.3	80



Obrázek 16 - Mapování portů na routeru (Zdroj: autor)

Tabulka 6 - Kalkulace nákladů aktivní prvky (Zdroj: autor)

Technologie	Ks	Cena	Celkem
WS-C2960-24-PC-L	3	37 000	111 000
WS-C2960-24-TC-L	3	30 000	90 000
WS-C2960G-24TC-L	2	42 000	84 000
WS-3750 G-12 S-S	2	101 000	202 000
CISCO2911-SEC/K9	1	49 000	49 000
Celkem cena Kč bez DPH			536 000

Závěr

Cílem této práce byl návrh komunikační infrastruktury malé až středně velké firmy s připojením do internetu. V první části práce byly popsány základní technologická východiska návrhu LAN. Dále byly popsány prvky, základní principy a výhody IP kamerového systému. Stěžejním úkolem bylo vytvoření návrhu infrastruktury dle konkrétních požadavků zákazníka.

V části návrhu strukturované kabeláže byla navržena instalace kabeláže kategorie 6A s přenosovou rychlostí až 10 Gb/s, která zajistí dostatečnou přenosovou kapacitu do budoucnosti.

V návrhu kamerového systému se jednalo o návrh celkem 19 kamer pro vnitřní nebo venkovní použití s požadovanými parametry. Pro dohled a správu kamer byl navržen dohledový software. Jako variantní řešení bylo zvoleno připojení některých venkovních kamer po optickém kabelu s použitím technologie vlnového multiplexu.

V rámci přístupového systému byly navrženy čtyři snímací hlavy s kontrolou přístupu do vymezených prostor a jeden vnitřní snímač identifikačních karet umístěný u hlavního vchodu. Celý systém je integrován se SW docházkového systému pro evidenci průchodů a správy docházky.

V návrhu bezdrátové sítě bylo pro řízení a správu 11 přístupových bodů navrženo nasazení přístupového kontroleru, který zajišťuje komunikaci a snadnější správu přístupových bodů. V alternativním řešení není s tímto prvkem v návrhu počítáno, ale toto řešení nedoporučuji. Dále alternativní řešení počítá v návaznosti na zadání s pokrytím pouze expediční haly.

V návrhu aktivních prvků byl velký důraz kladen na zajištění dostupnosti připojení resp. na její redundanci. Redundance je řešena v prvním případě zdvojením přenosových cest, kde jsou aktivní prvky přístupové části tj. switche Cisco 2960 připojeny k centrálnímu uzlu Catalyst 3750 pomocí tzv. uplinků. V druhém případě jde o samotnou redundanci centrálního uzlu, kde byly použity dva identické L3 switche Catalyst 3750 propojené prostřednictvím StackWise sběrnice.

Pro vrstvu jádra a distribuce byl navržen prepínač produktové řady Catalyst 3750, který se svými 12x SFP optickými porty zajišťuje nezávislost na přenosovém médiu a disponuje dostatečnou kapacitou při rozšiřování sítě o další přístupové prvky. Stackwise stoh zajišťu-

je chování obou boxů jakožto jednoho logického celku, kdy routing informace jsou sdíleny mezi oběma switchi ve stacku, primárně však routing zajišťuje master switch a v případě jeho výpadku jednoho je druhý switch schopen převzít L3 funkce s minimálním výpadkem. Switching se odehrává lokálně na jednotlivých boxech ve stacku a na stackwise sběrnici. Výhodou tohoto řešení je možnost cross-box etherchannel trunků vůči jednotlivým přístupovým switchům a v podstatě vytvoření 2Gbit/s páteře (2x1Gbit/s) loop-free hvězdicové topologie. Zároveň je zajištěna redundance přenosových cest, pro případ jejich poruchy, kdy se pouze „rozpadne“ etherchannel.

Pro připojení serverů jsou navrženy dva dedikované switche Catalyst C2960G-24TC poskytující 20x 10/100/1000Mbit/s porty, tzn. připojení všech serverů lze realizovat 1Gbit/s. Připojení serverů je v obou případech plánované multihoming ve fault-tolerant modu.

Alternativní řešení přináší ekonomicky výhodnější variantu ovšem se ztrátou klíčových vlastností primárního řešení. Výměnou core prvků Catalyst 3750 za Catalyst 3560, přicházíme o možnost stackwise stohu, a tím možnost logického sdružení v jeden box. Nelze tak sdílet L3 funkcionalitu mezi core prvky. Pro případ výpadku aktivního z core prvků musíme zajistit převzetí L3 funkcionalit (routingu) záložním core prvkem, to znamená využití HSRP protokolu. Další nevýhodou je ztráta možnosti cross-box etherchannel trunků, místo toho máme redundantní kruhovou topologii, s STP/RSTP protokolem, kdy redundantní přenosová cesta je zablokována a nepřenáší data. Páteří rychlost je tak 1Gbit/s. Dále je zde počítáno s připojováním serverů do core prvků, a ne do dedikovaných serverových switchů. Core switche Catalyst 3560 poskytují každý pouze 4SFP porty, tj. dohromady 8 na médiu nezávislých rozhraní, což je v současném návrhu postačující, ale v případě budoucího rozšiřování sítě by mohlo být nedostatečné (nutnost používání media-konvertorů).

Směrovač pro přístup do internetu byl vybrán typ Cisco 2911 s přídatnými bezpečnostními funkcemi firewallu zajišťujícího navíc další síťové služby - překlad síťových adres. Samotný návrh obsahuje nákresy topologie sítě, kde je znázorněno jednotlivé propojení síťových prvků.

Ekonomická kalkulace je uvedena vždy u konce jednotlivých částí návrhu. Celková rekapitulace nákladů s variantním řešením je v příloze 5. Zde se vycházelo z katalogových cen jednotlivých výrobců.

Literatura

- [1] AXIS Design guide [Online]. IPSECURITY, 2010 [cit. 2010-04-20]. Dostupný z WWW: <http://www.ipsecurity.cz/_axis/_dnld/gd_ipsurv_design.pdf/>.
- [2] BIGELOW, J., *Mistrovství v počítačových sítích : správa, konfigurace, diagnostika a řešení problémů*. 1. vyd. Brno : Computer Press, 2004. 990 s. ISBN 80-251-0178-9.
- [3] BUIGL, P., *IP kamerové systémy*, Security World, září, 3/2008, IDG Czech,a.s., Praha ISSN 1802-4505.
- [4] *Cisco Etherchannel Technology* [Online]. © Cisco Systems, 1992-2010 [cit. 2010-04-20]. Dostupný z WWW. <http://www.cisco.com/en/US/tech/tk389/tk213/technologies_white_paper09186a0080092944.shtml>.
- [5] *Cisco StackWise Technology White Paper* [Online]. © Cisco Systems, 1992-2010 [cit.2010-04-20]. Dostupný z WWW:<http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5023/prod_white_paper09186a00801b096a.html>.
- [6] ČSN EN 50173-1, *Informační technologie - Univerzální kabelážní systémy . Část 1: Všeobecné požadavky na kancelářské prostředí*. Praha : Český normalizační institut, 2003, 108 s.
- [7] DOSTÁLEK, L., a kol., *Velký průvodce protokoly TCP/IP: Bezpečnost*. 2. vyd.. Praha : Computer Press, 2003., 571 s. ISBN 80-7226-849-X.
- [8] DOSTÁLEK, L., KABELOVÁ, A., *Velký průvodce protokoly TCP/IP a systémem DNS* 3. vyd. Brno : Computer Press, 2002., 542 s. ISBN 80-7226-675-6.
- [9] *Internetwork Design Guide, Internetworking Design Basics* [online]. © Cisco Systems, 1992-2010 [cit. 2010-04-20]. Dostupný z WWW: <<http://www.cisco.com/en/US/docs/internetworking/design/guide/nd2002.html>>.
- [10] KÁLLAY, F., PENIAK, P., *Počítačové sítě LAN/MAN/WAN a jejich aplikace*. 2. vyd. Praha : Grada, 2003. 356 s. ISBN 80-247-0545-1.

- [11] NETCAM: Síťové video [online]. [cit. 2010-04-10]. Dostupný z WWW:<<http://www.netcam.cz/encyklopedie-ip-zabezpeceni/co-je-sitove-video.php/>>.
- [12] PROSISE, Ch., MANDIA, K., *Počítačový útok : detekce, obrana a okamžitá náprava* . 1. vyd. Praha : Computer Press, 2002. 410 s. ISBN 80-7226-682-9.
- [13] PUŽMANOVÁ, R., *TCP/IP v kostce*. 1. vyd. České Budějovice : Kopp, 2004. 607 s. ISBN 80-7232-236-2.
- [14] VYKLICKÝ, M., *Switch - základ podnikové sítě* [online]. c2008: [cit. 2010-04-05]. Dostupný z WWW: <<http://connect.zive.cz/node/611/>>.

Seznam příloh

Příloha 1: Návrh fyzické topologie, aktivní prvky

Příloha 2: Návrh fyzické topologie alternativní

Příloha 3: Schéma rozmístění IP kamer

Příloha 3a: Situační schéma administrativa

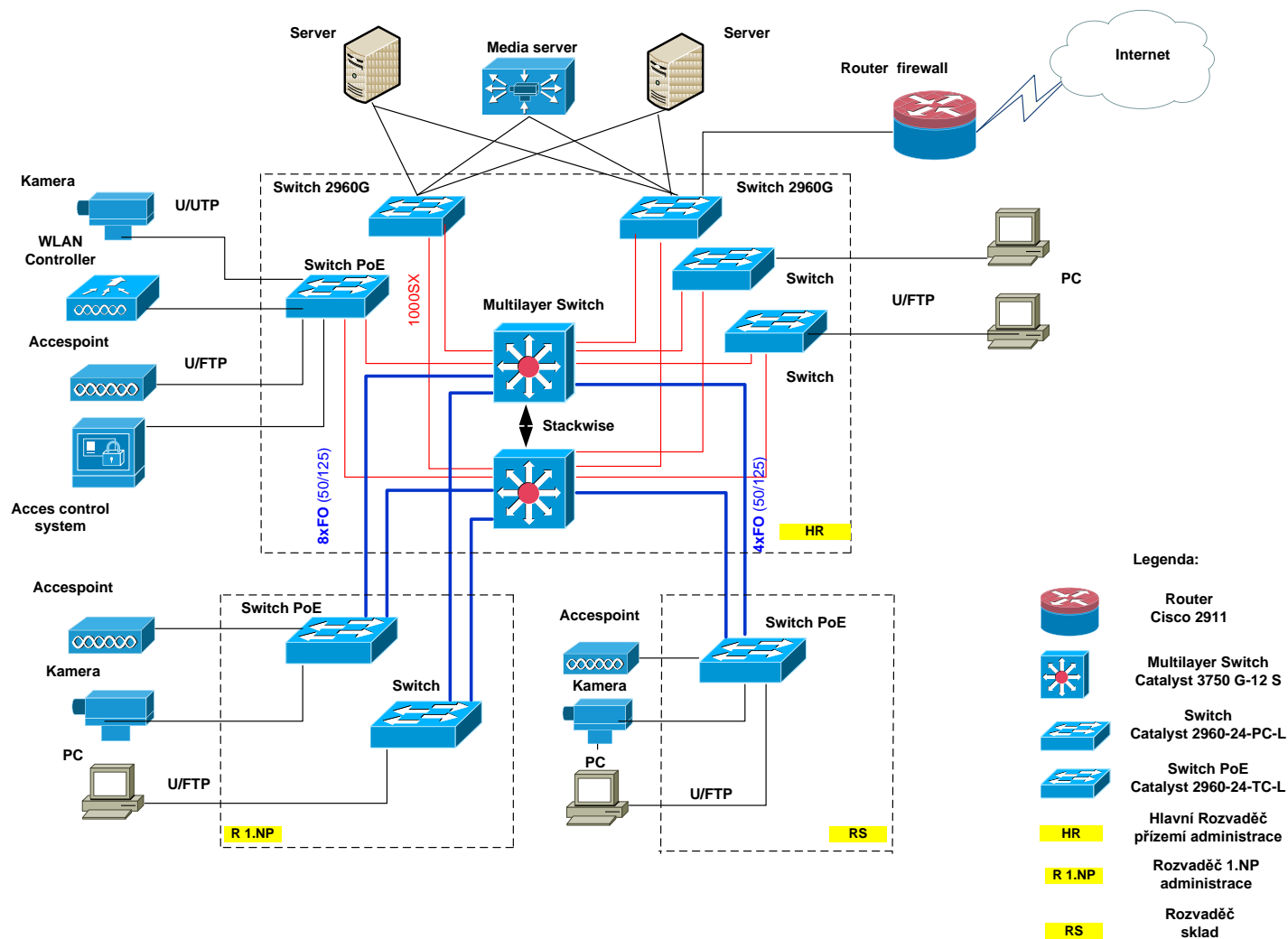
Příloha 3b: Situační schéma sklad

Příloha 4: Návrh logické topologie, virtuální síť

Příloha 5: Ekonomické zhodnocení

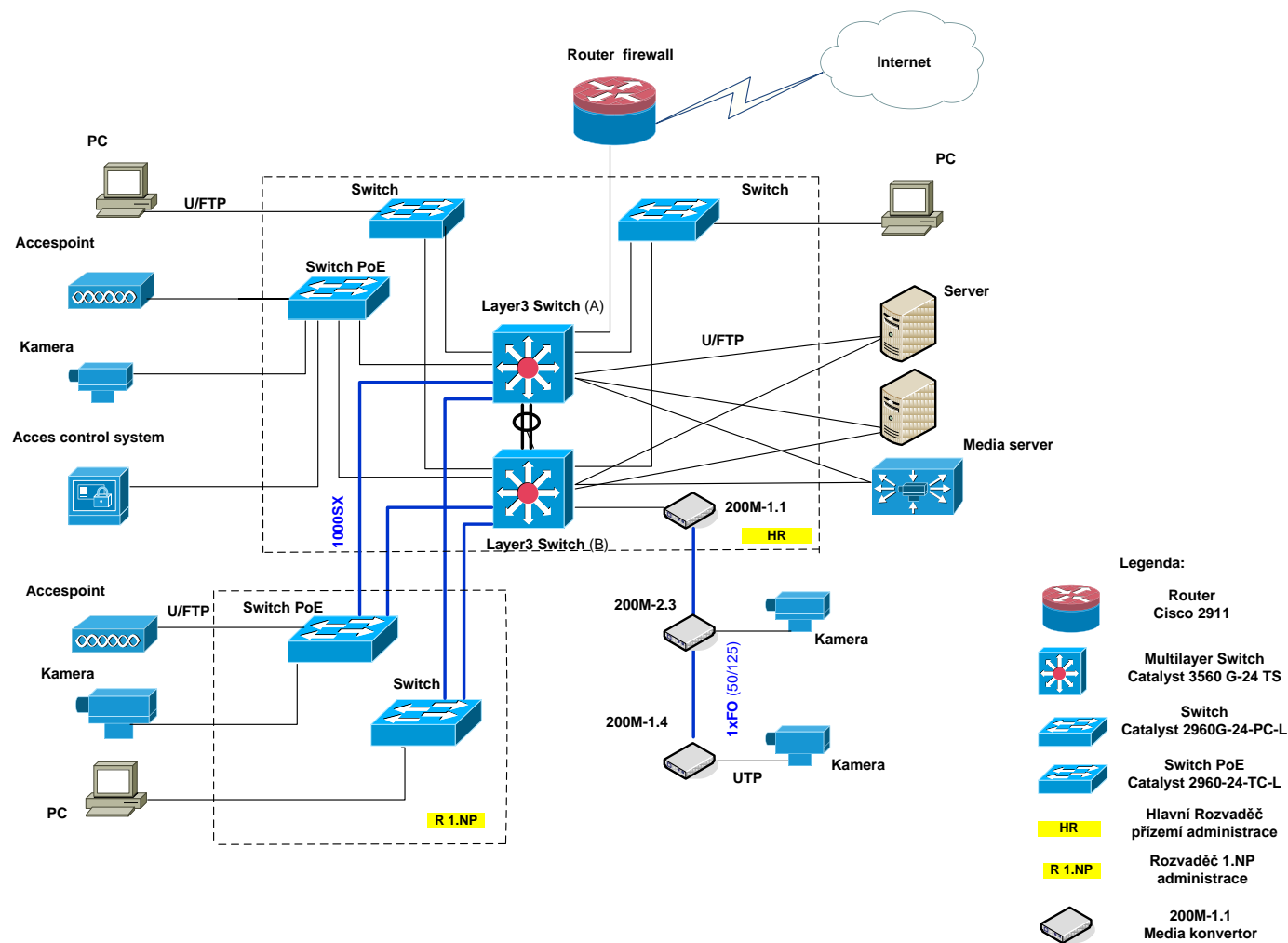
Příloha 6: Návrh kalkulace propustnosti

Příloha 1 - Návrh fyzické topologie, aktivní prvky



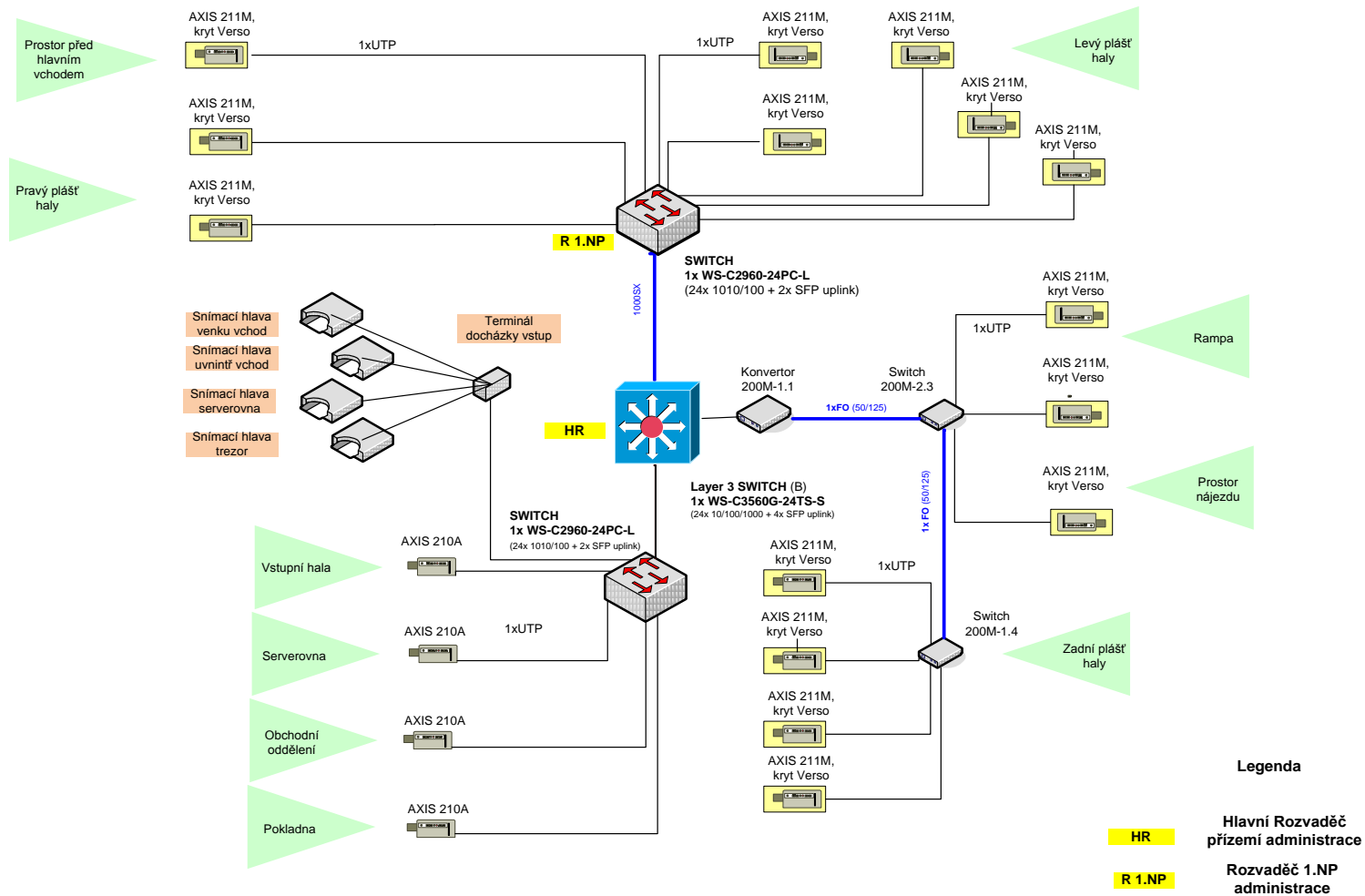
Obrázek 17 - Návrh fyzické topologie (Zdroj: autor)

Příloha 2 - Návrh fyzické topologie alternativní



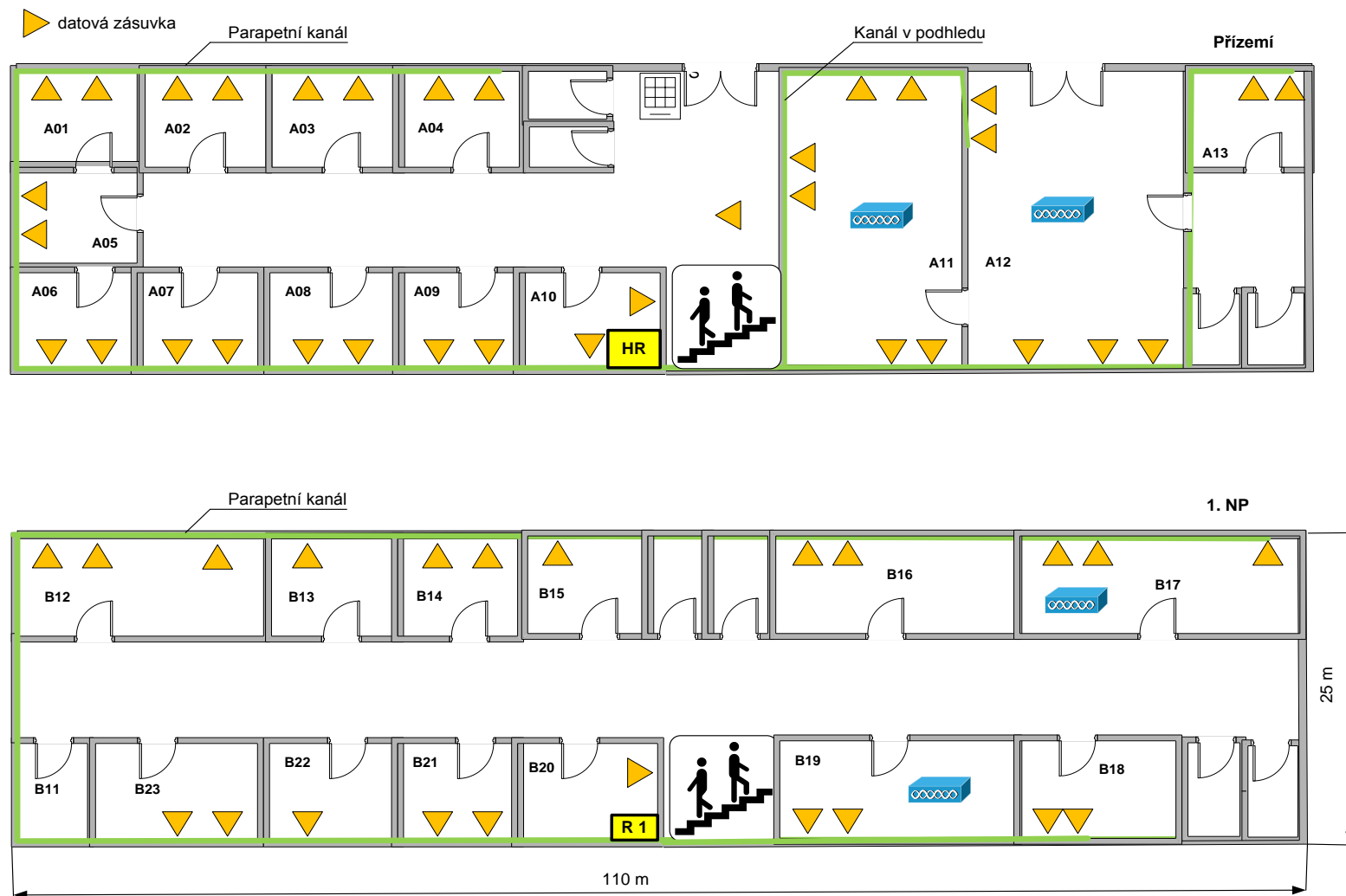
Obrázek 18 - Návrh fyzické topologie alternativní (Zdroj: autor)

Příloha 3 - Schéma rozmístění IP kamer



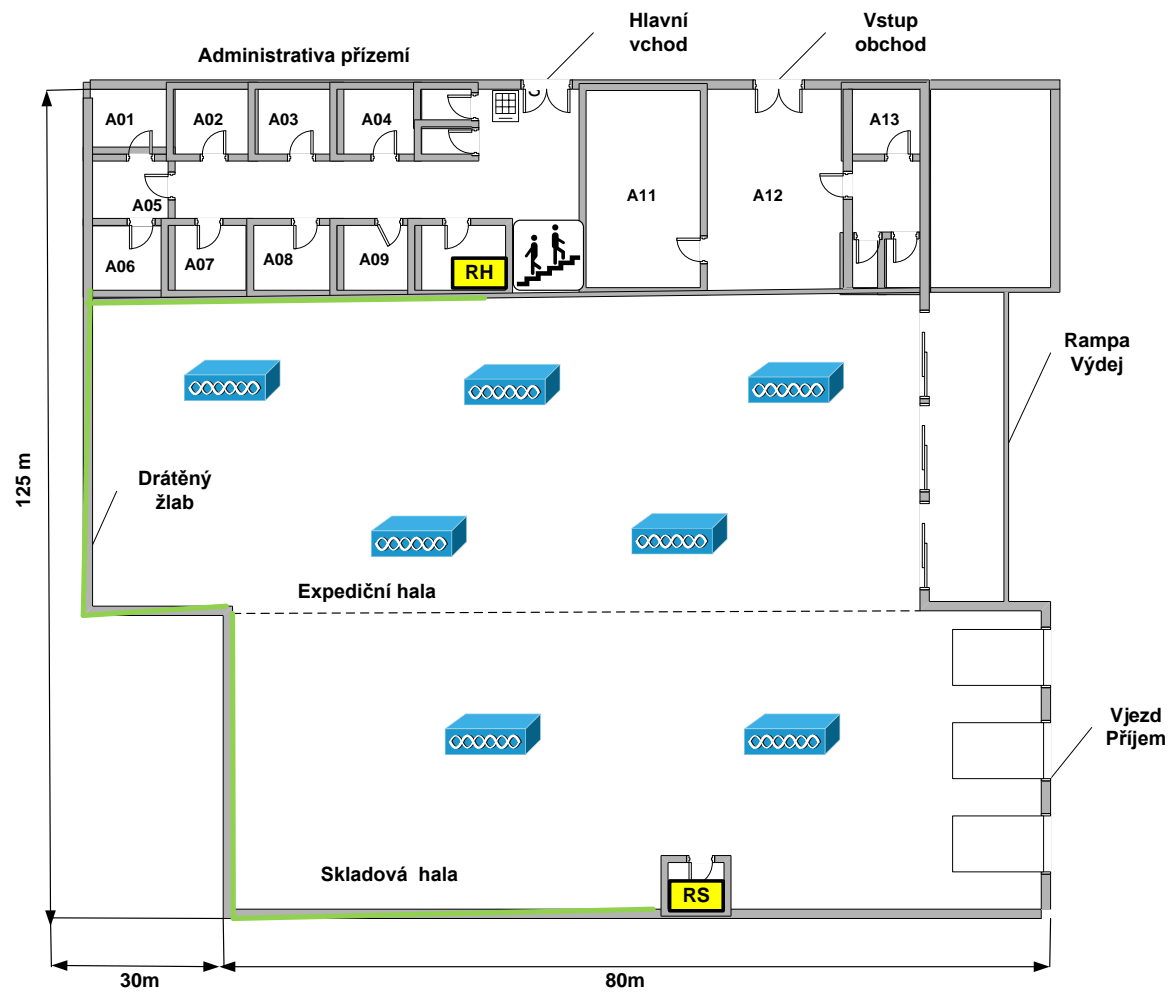
Obrázek 19 - Schéma rozmístění IP kamer (Zdroj: autor)

Příloha 3a - situační schéma administrativa



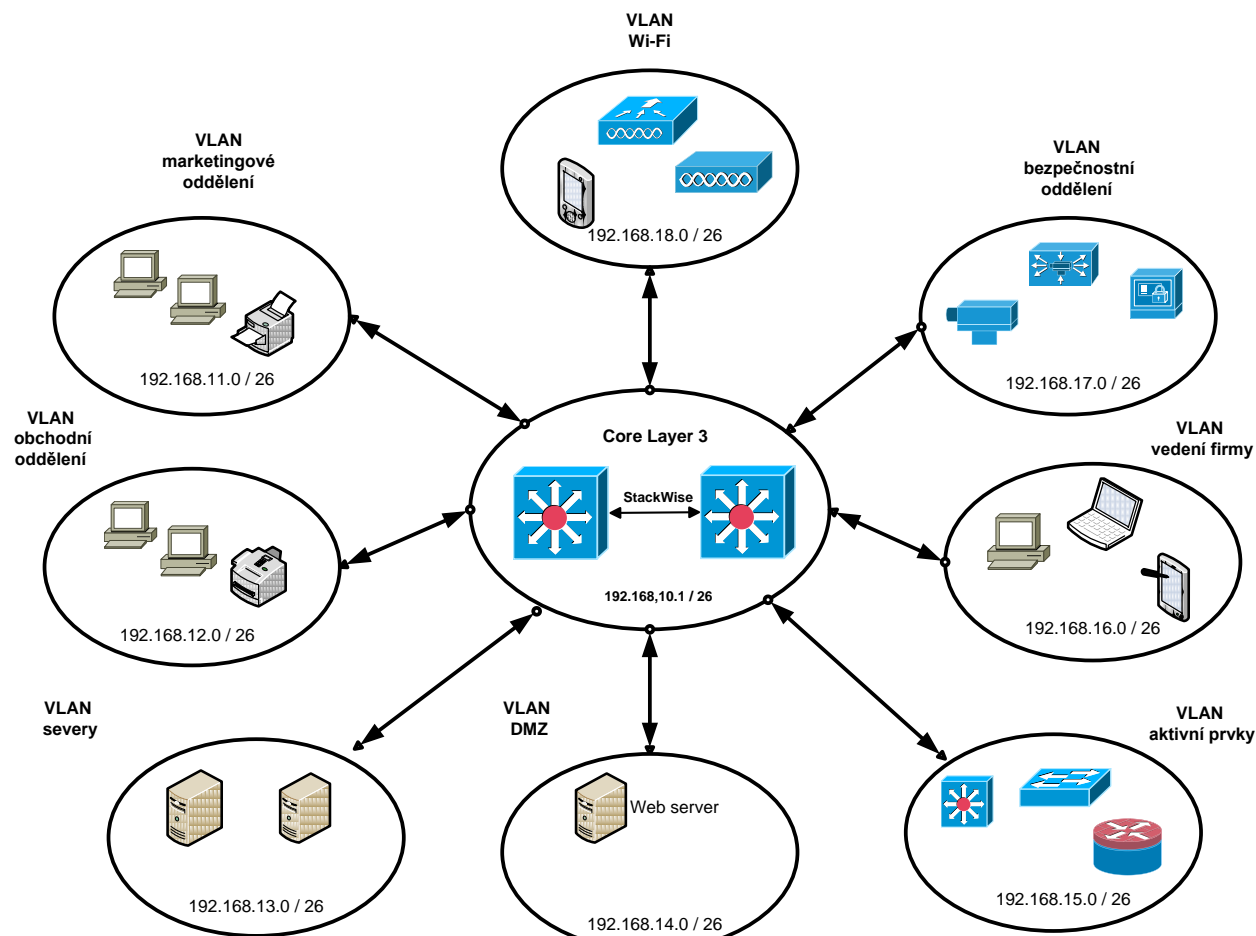
Obrázek 20 - Situační schéma administrativa (Zdroj: autor)

Příloha 3b - Situační schéma sklad



Obrázek 21 - Situační schéma sklad (Zdroj: autor)

Příloha 4 - Návrh logické topologie, virtuální sítě



Obrázek 22 - Návrh logické topologie (Zdroj: autor)

Příloha 5 - Ekonomické zhodnocení

Tabulka 7 - Ekonomické zhodnocení (Zdroj: autor)

Technologie	Ks	Cena	Celkem
WS-C2960-24-PC-L	3	37 800	113 400
WS-C2960-24-TC-L	3	30 800	92 400
WS-C2960G-24TC-L	2	42 000	84 000
WS-3750 G-12 S-S	2	99 000	198 000
AIR-WLC-2112-K9	1	55 000	55 000
Cisco AIR.LAP1131AG	11	9 900	108 900
AXIS 211 M	15	15 500	232 500
AXIS 216 MFD	4	16 000	64 000
XProtect Basis+ pro 25 kamer	1	59 000	59 000
CISCO2911-SEC/K9	1	49 000	49 000
Dell T110 X3460	1	35 000	35 000
REI - ST snímač identifikačních karet	1	39 000	39 000
H - PRO/K externí snímací hlava	1	7 000	7 000
H - PRO externí snímací hlava	3	6 500	19 500
Docházkový SW komplet	1	58 400	58 400
Celkem návrh Kč bez DPH			1 215 100

Tabulka 8 - Ekonomické zhodnocení alternativa (Zdroj: autor)

Technologie	Ks	Cena	Celkem
WS-C2960-24-PC-L	2	37 800	75 600
WS-C2960-24-TC-L	3	30 800	92 400
WS-C3560 G-24TS-S	2	60 200	120 400
Media konv. 200M	3	5 600	16 800
Cisco AIR.LAP1131AG	9	9 900	89 100
AXIS 211 M	15	15 500	232 500
AXIS 216 MFD	4	16 000	64 000
XProtect Basis+ pro 25 kamer	1	59 000	59 000
Dell T110 X3460	1	35 000	35 000
CISCO2911-SEC/K9	1	49 000	49 000
AIR-WLC-2112-K9	0	55 000	0
REI - ST snímač identifikačních karet	1	39 000	39 000
H - PRO/K externí snímací hlava	1	7 000	7 000
H - PRO externí snímací hlava	3	6 500	19 500
Docházkový SW komplet	1	58 400	58 400
Celkem alternativa Kč bez DPH			957 700

Příloha 6 - Návrh kalkulace propustnosti



Name	Model	No. of cams	Bandwidth (View, Rec, Event)	Storage (7 days)
1 Venkovní kamery	AXIS 211M	15	79.1 Mbit/s, 9.4 Mbit/s, 67.5 Kbit/s	492.3 GB
2 Vnitřní kamery	AXIS 216MFD	4	32.1 Mbit/s, 3.3 Mbit/s, 12 Kbit/s	196.9 GB
Project celkem			111.2 Mbit/s, 12.7 Mbit/s, 79.5 Kbit/s	689.3 GB

Camera

Name [Image scenario](#) [Audio](#) [Model](#) No. of channels

Vnitřní kamery Intersection AXIS 216MFD 4

Viewing [Play example](#)

[Frame rate](#) [Resolution](#) [Compression type](#) [Compression](#) Bandwidth

6 fps 1280x1024 MotionJPEG 10 8228 Kbit/s

Continuous recording [Play example](#)

Record for [Frame rate](#) [Resolution](#) [Compression type](#) [Compression](#) Bandwidth

24 h 6 fps 640x480 MotionJPEG 70 850 Kbit/s

Event recording [Play example](#)

Alarm [Frame rate](#) [Resolution](#) [Compression type](#) [Compression](#) Bandwidth

20 % 6 fps 1280x1024 MotionJPEG 50 15 Kbit/s

Obrázek 23 - Návrh kalkulace propustnosti (Zdroj: autor - upraveno na základě [1])