

1.4.14 Analogový převodník pro Uzlový objekt typu 1, 2 a Konc. objekt typu 1

Tabulka 29 Funkční požadavky na analogový převodník pro Uzlový objekt typu 1, 2 a Koncový objekt typu 1

Požadovaná funkcionality/vlastnosti	Způsob splnění požadované funkcionality/vlastnosti	Doplň Uchazeč dle nabízeného zařízení
Výrobce zařízení	Uvedení výrobce	CISCO
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	VG310
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	http://www.cisco.com/c/en/us/products/collateral/unified-communications/vg-series-gateways/product_data_sheet09186a00801d87f6.html
Napájení přes externí zdroj	ANO	ANO
VLAN 802.1q, možnost tagování rámců dle 802.1p	ANO	ANO
Dva porty Ethernet 10/100 pro možnost redundantního připojení k síti LAN	OBSAHUJE	ANO
Signalizační protokol	SIP, H.323	ANO
Audio kodeky	G.711, G.722, G.729, iLBC	ANO
Přenos faxu přes protokol IP	Standard T.38	ANO
Plnohodnotný port FXS včetně podpory signalizace Loop-Start a Ground-Start	ANO	ANO
Minimální počet analogových portů FXS	24	ANO
In-Band DTMF	ANO	ANO
Konferenční hovory	ANO	ANO
Funkce přidržení/pokračování hovoru	ANO	ANO
Funkce přímého nebo konzultačního přepojení hovoru	ANO	ANO
Funkce přesměrování hovoru	ANO	ANO
Identifikace volajícího	ANO	ANO
Music-on-Hold pro analogové telefony	ANO	ANO

Výrobce	Produktové číslo výrobce	Popis KOMPONENTY	Počet kusů KOMPONENTY
CISCO	VG310	Cisco VG310 - Modular 24 FXS Port Voice over IP Gateway	1
CISCO	CON-PSRT-VG310ICV	PRTNR SS 8X5XNBD Cisco VG310 - Modular 24 FXS Port Voice	3
CISCO	SVG3XUK9-15403M	Cisco VG3X0 UNIVERSAL	1

CISCO	MEM-CF-256MB	256MB Compact Flash for Cisco 1900 2900 3900 ISR	1
CISCO	CAB-ACE	AC Power Cord (Europe) C13 CEE 7 1.5M	1
CISCO	HWIC-BLANK	Blank faceplate for HWIC slot on Cisco ISR	1
CISCO	SL-VG3X0-IPB-K9	Cisco VG3X0 IP Base License	1
CISCO	SL-VG3X0-UC-K9	Cisco VG3X0 Unified Communications License	
CISCO	LIC-CUCM-10X-ESS-B	UC Manager-10.x Essential User License-1K to 10K	24

1.4.15 Analogový převodník pro Koncový objekt typu 2

Tabulka 30 Funkční požadavky na analogový převodník pro Koncový objekt typu 2

Požadovaná funkcionality/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplň Uchazeč dle nabízeného zařízení
Výrobce zařízení	Uvedení výrobce	CISCO
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	ATA190
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	http://www.cisco.com/c/en/us/products/collateral/unified-communications/ata190-2-port-adapter/datasheet-c78-731473.html
Napájení přes externí zdroj	ANO	ANO
VLAN 802.1q, možnost tagování rámců dle 802.1p	ANO	ANO
Dva porty Ethernet 10/100 pro možnost redundantního připojení k síti LAN	OBSAHUJE	ANO
Signalizační protokol	SIP, H.323	ANO
Audio kodeky	G.711, G722, G.729, iLBC	ANO
Přenos faxu přes protokol IP	Standard T.38	ANO
Plnohodnotný port FXS včetně podpory signalizace Loop-Start a Ground-Start	ANO	ANO
Minimální počet analogových portů FXS	4	ANO
In-Band DTMF	ANO	ANO
Konferenční hovory	ANO	ANO
Funkce přidržení/pokračování hovoru	ANO	ANO

Požadovaná funkcionality/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplňující Uchazeč dle nabízeného zařízení
Funkce přímého nebo konzultačního přepojení hovoru	ANO	ANO
Funkce přesměrování hovoru	ANO	ANO
Identifikace volajícího	ANO	ANO
Music-on-Hold pro analogové telefony	ANO	ANO

Výrobce	Produktové číslo výrobce	Popis KOMPONENTY	Počet kusů KOMPONENTY
CISCO	ATA190	UC 2 Port Analog Telephone Adapter	1
CISCO	CON-PSRT-ATA190	PRTNR SS 8X5XNBD UC 2 Port Analog Telephone Adapter	1
CISCO	SPA-CLIP-EU	SPA Power Clip for Europe/Asia	1
CISCO	LIC-CUCM-10X-ESS-B	UC Manager-10.x Essential User License-1K to 10K	4

1.4.16 Server interoperability MS Lync

Server je součástí "Serveru pro IP telefonii (IP PBX)"

1.4.17 Licence interoperability MS Lync

Výrobce	Produktové číslo výrobce	Popis KOMPONENTY	Počet kusů KOMPONENTY
CISCO	LIC-EXP-RMS	Expressway Rich Media Session	3
CISCO	CON-PSBU-LICEXPRM	PSS SWSS UPGRADES Expressway Rich Media Session	9

1.4.18 Systém nahrávání hovorů

Výrobce	Produktové číslo výrobce	Popis KOMPONENTY	Počet kusů KOMPONENTY
---------	--------------------------	------------------	-----------------------

RETIA		ReDat® eXperience 1	1
RETIA		ReDat® eXperience Basic - Catalog	1
RETIA	REX BASIC LICB	Základní produktová licence	1
RETIA	REX BASIC LIC1	Licence pro aktivaci 1 kanálu	15
RETIA		ReDat® CTI (Integrační moduly pro CTI, CDR, integrace se SW CC)	1
RETIA	REX CTI CI CM/CC LICB	CTI Cisco CUCC (IPCC) nebo CTI CUCM (CallManager), SPAN nebo SPANLESS	1
RETIA	REX CTI CI CM/CC LIC1	Licence pro aktivaci 1 současně nahrávaného kanálu CTI Cisco CUCC / CUCM	15

Výrobce	Produktové číslo výrobce	Popis KOMPONENTY	Počet kusů KOMPONENTY
CISCO	TCS-C220-5RP-K9	TelePresence Content Server: 5 Recording Ports 2 Live Ouput	1
CISCO	CON-PSRN-C5RPK9	PRTNR TP VID 8X5XNBD TelePresContSrvr:5 RecPorts2 LiveOuput	3
CISCO	MXE-UCS-HDD-BLKP	MXE UCS Server HDD blank cover	6
CISCO	MXE-UCS-PSU-BLKP	MXE UCS Server power supply filler (blanking)	1
CISCO	LIC-TCS-2L	2 Live Output Calls License	1
CISCO	LIC-TCS-6.0-K9	CTCS Version 6.0 software - license	1
CISCO	LIC-TCS-5R	5 Recording Call License	1
CISCO	SW-TCS-6.0-K9	TelePresence Content Server Version 6.0 software	1
CISCO	MXE-UCS-1GE-N2XX	MXE UCS Server 1Gb Ethernet Quad Port NIC	1
CISCO	CAB-9K10A-EU	Power Cord 250VAC 10A CEE 7/7 Plug EU	1

CISCO	MXE-UCS-RAID-MZ	MXE UCS RAID SAS 2008M-8i Mezzanine Card	1
CISCO	MXE-UCS-HDD-600G	MXE UCS Server Hard Disk 600 GB 10K RPM	2
CISCO	R2XX-RAID1	Enable RAID 1 Setting	1
CISCO	MXE-UCS-MR-8GB-R	MXE UCS Server DRAM - 8GB DDR3	4
CISCO	MXE-UCS-E5-2640	MXE UCS Server CPU E5-2640	2
CISCO	MXE-UCS-PSU-650W	MXE UCS Server 650W power supply	1
CISCO	BE7M-M4-K9	Cisco Business Edition 7000M Svr (M4), Export Restricted SW	1
CISCO	CON-PSRT-BE7MM4K9	PRTNR SS 8X5XNBD Cisco Business Edition 7000M Server, Exp	3
CISCO	VMW-VS5-HYP-K9	Cisco UC Virt. Hypervisor 5.x (2-socket)	1
CISCO	VMW-VS5-SNS	Cisco UC Virt. Hypervisor 5.x - SnS	1
CISCO	BE7K-SW-9X10X	Media (no lic) for Cisco Collaboration 9.x 10.x	8
CISCO	R2XX-RAID5	Enable RAID 5 Setting	2
CISCO	CIT2-A03-D300GA2	300GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive sled mounted	1
CISCO	CIT2-CPU-E52680D	2.50 GHz E5-2680 v3/120W 12C/30MB Cache/DDR4 2133MHz	12
CISCO	CIT2-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v	2
CISCO	CIT2-MRAID12G	Cisco 12G SAS Modular Raid Controller	2
CISCO	CIT2-MRAID12G-1GB	Cisco 12Gbps SAS 1GB FBWC Cache module (Raid 0/1/5/6)	1
CISCO	CIT2-PCI-1B-240M4	Right PCIe Riser Board (Riser 1) (3 x8) for 6 PCI slots	1
CISCO	CIT2-PCIE-IRJ45	Intel i350 Quad Port 1Gb Adapter	1
CISCO	CIT2-PSU2V2-1200W	1200W V2 AC Power Supply for 2U C-Series Servers	1
CISCO	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	1
CISCO	VMW-VS5-HYP-USEL	Cisco UC Virt. Hypervisor Entitlements	1

CISCO	CON-PSBU- VMWVS5HL	PSS SWSS UPGRADES Cisco UC Virt. Hypervisor Entitlements	6
-------	-----------------------	---	---

1.4.19 Tarifikační systém

- Řešení telefonního systému obsahuje i systém pro tarifikaci hovorů pro všechny telefony nového telefonního systému.

Výrobce	Produktové číslo výrobce	Popis KOMPONENTY	Počet kusů KOMPONENTY
2RING	2Ring-CA-CDR-CISCO	2Ring CA Add On License for 1 additional Cisco connector	3
2RING	2Ring-CA-Ext2817	2Ring CA Add On License for 2817 users	1
2RING	2Ring-SUP-CA-CDR-CISCO	2Ring CA Cisco connector - EPU Support	9
2RING	2Ring-SUP-CA-Ext2817	2Ring CA Add On License for 2817 users - EPU Support	3

1.4.20 Pomocný drobný materiál

Komponenta	Produktové číslo výrobce	Popis KOMPONENTY	Počet kusů KOMPONENTY
Kabel FTP, cat.6, drát, 1m	sutpd6ac3	PremiumCord CAT6A FTP Kabel 4x2,drát AWG23,čistá měď 305m	46
Kabel FTP, cat.6, drát, 1m, včetně uložení	INSTKAB	Instalace včetně materiálu	1
Patch kabel FTP, cat.6, 2m	sp6ftp020	PremiumCord FTP 2m CAT.6 patch kabel awg26 šedá	1
Patch kabel UTP, cat.6, 2m	sp6utp02	PremiumCord Patch kabel UTP RJ45-RJ45 CAT6 2m šedá	1
Patch kabel UTP, cat.6, 3m	sp6utp03	PremiumCord Patch kabel UTP RJ45-RJ45 CAT6 3m šedá	1
Patch panel 24 port FTP cat.6, 1U	A-PAN6-24S	DIGITUS Patch panel, Cat6 19" 24xSTP RJ45	1
Stíněný konektor FTP, drát, 8pc, cat. 6, RJ45	srj45s-c6s	PremiumCord Konektor RJ 45 stíněný, Cat6, na silný vodič AWG23	1
Držák na zeď pro zobrazovací jednotku videokonference	Držák pro zobrazovací jednotku videokonference E,F	pro připojení zobrazovacích jednotek	1

E,F			
Montážní kit pro videokonferenci a kameru	Montážní kit pro videokonferenci a kameru	pro připojení kamery	1
Octopus Cable 24 port	OCT-CABLE	Octopus Cable 24 port	1

2. Návrh řešení

Očekáváme následující součinnost zadavatele.

2.1. Dokumentace

Očekáváme kompletní dokumentaci komunikační infrastruktury, odpovídající jejímu aktuálnímu stavu v době zahájení migrace. Zejména očekáváme následující dokumenty, pokud jsou relevantní:

- Detailní popis aktuální topologie LAN/WAN,
- Aktuální konfigurace stávajících prvků LAN/WAN,
- Specifikace funkcionalit LAN/WAN prvků, které mají být implementovány nad rámec stávající konfigurace,
- Aktuální dokumentace zapojení rozhraní jednotlivých prvků v elektronické formě,
- Kabelová kniha mapující fyzické propoje v rámci instalovaných lokalit,
- Seznam používaných VLAN a jejich parametrů (Spanning-tree, VTP),
- IP adresní schéma.

2.2. Součinnost při instalaci

- Seznam lokalit a kontaktů na osoby zodpovědné za migraci v dané lokalitě,
- Prostor pro instalaci dodávaných prvků
- Napájení odpovídající požadavkům výrobce (jističe),
- Chlazení odpovídající požadavkům výrobce,
- Výpočetní zdroje podle požadavků výrobce v případě virtualizovaných komponent,
- Provozní odstávka po dobu migrace na novou infrastrukturu
- Vzdálený přístup na instalovanou infrastrukturu za účelem úpravy konfigurace dodávaných komponent.

2.3. Součinnost při definici akceptačních testů

Specifikace funkčních požadavků (provoz kritických aplikací, způsob aplikačního testování)

2.4. Požadované kapacity stávající infrastruktury Karlovy Vary

Pro instalace sekundárních serverů IP telefonie na VMware infrastrukturu v Karlových Varech jsou požadovány min. tyto zdroje:

10x	vCPU
48GB	RAM
6x	vNIC

2.5. Řešení nově budované komunikační infrastruktury

2.5.1 Certifikát IPv6 funkčnosti a interoperability

Navrhovaná zařízení splňují požadavek na certifikát IPv6 funkčnosti a interoperability od nezávislé testovací organizace, jako je certifikát IPv6 Ready Logo Phase II nebo ekvivalentní.

2.5.2 Modulární L3 přepínač pro páteř Uzlového objektu typu 1

Jako přepínač pro páteř uzlového objektu typu 1 navrhujeme použít modulární chassis Cisco Catalyst 6807 s řídicími moduly Supervisor-2T a linkovými kartami disponujícími rozhraními typu GE/10GE/40GE pro připojení navazující infrastruktury. Navrhovaná zařízení podporují sdružení dvou prvků do jednoho logického celku – clusteru přepínačů (Virtual Switching System – VSS).

Navrhované L3 přepínače pro objekty UO1 splňují požadovanou funkční specifikaci pro L3 přepínače. Zejména se jedná o následující funkce:

- Směrovací funkce L2-L4,
- Podpora standardních směrovacích protokolů - OSPFv2/v3, BGP a MP-BGP.
- Podpora vytváření oddělených IP VPN sítí prostřednictvím virtualizace směrovacích tabulek (VRF-lite) a virtualizace síťových služeb.
- Směrování IP multicast provozu pomocí protokolů PIM SM a PIM SSM,
- Ochrana proti podvržení zdrojové MAC a IP adresy a ochranu proti neautorizovaným službám DHCP.
- Řízení kvality služeb (QoS) s možností definice frontování, klasifikace provozu, markování provozu (DSCP, COS) s možností omezení a vyčlenění šířky pásma provozu v jednotlivých kategoriích a definici prioritní fronty pro provoz IP telefonie.
- Podpora současného IPv4 a IPv6 provozu – DualStack, IPv6 služby DNS, Telnet/SSH, DHCP, Multicast a QoS.
- Monitorování aplikačních toků s využitím technologie NetFlow.
- Podpora MultiChassis portchannel v případě zapojení L3 přepínačů do VSS clusteru.

L3 přepínače budou nasazeny s použitím výše uvedených vlastností.

2.5.3 L3 přepínač pro páteř Uzlového objektu typu 2

Jako L3 přepínač pro páteř uzlového objektu typu 2 navrhujeme použít zařízení Cisco Catalyst 4500-X. Jedná se o semimodulární přepínač s integrovaným řídicím modulem a podporou GE/10GE SFP transceiverů pro připojení navazující infrastruktury. Tato zařízení podporují sdružení dvou

prvků do jednoho logického celku – clusteru přepínačů (Virtual Switching System – VSS).

Navrhované L3 přepínače pro objekty UO2 splňují požadovanou funkční specifikaci pro L3 přepínače. Zejména se jedná o následující funkce:

- Směrovací funkce L2-L4,
- Podpora standardních směrovacích protokolů OSPFv2/v3, BGP a MP-BGP,
- Podpora vytváření oddělených IP VPN sítí prostřednictvím virtualizace směrovacích tabulek (VRF-lite) a virtualizace síťových služeb,
- Směrování IP multicast provozu pomocí protokolů PIM SM a PIM SSM a to jak pro protokol IPv4,
- Ochrana proti podvržení zdrojové MAC a IP adresy a ochranu proti neautorizovaným službám DHCP,
- Řízení kvality služeb (QoS) s možností definice frontování, klasifikace provozu, markování provozu (DSCP, COS) s možností omezení a vyčlenění šířky pásma provozu v jednotlivých kategoriích a definici prioritní fronty pro provoz IP telefonie,
- Podpora současného IPv4 a IPv6 provozu – DualStack, IPv6 služby DNS, Telnet/SSH, DHCP, Multicast a QoS,
- Monitorování aplikačních toků s využitím technologie NetFlow,
- Podpora MultiChassis portchannel v případě zapojení L3 přepínačů do VSS clusteru.

L3 přepínače budou nasazeny s použitím výše uvedených vlastností.

2.5.4 DC přepínač s vysokou dostupností pro datové centrum

Jako přepínač pro datové centrum budované infrastruktury navrhujeme použít přepínač Cisco Nexus 5672UP. Jedná se o datacentrový přepínač s rozhraními typu GE/10/40GE a Fibre Channel. Tato zařízení podporují tradiční LAN a SAN, ale i konvergovanou infrastrukturu. Navrhované DC přepínače s vysokou dostupností pro datové splňují požadovanou funkční specifikaci. Zejména se jedná o následující funkce:

- Bezeztrátová architektura přepínače (lossless fabric architecture),
- Připojení koncových zařízení – porty s přenosovou technologií 1GE/10GE/FCoE, nativní FC,
- Podpora agregace portů do virtuálních trunků napříč fyzickými šasi (multichassis etherchannel), podpora port channelingu,
- Podpora virtualizace serverové infrastruktury včetně možnosti aplikovat síťové politiky (VLAN, QoS, rate-limiting) pro připojené virtuální servery,
- Podpora VSAN (Virtual SAN) a NPIV (N-Port ID Virtualization),

- Podpora bezeztrátového přenosu a datacentrových technologií definovaných standardy IEEE 802.1Qaz (Data Center Bridging Exchange protocol a Enhanced Transmission Selection), IEEE 802.1Qbb (Priority-based Flow Control) a FC-BB-5 (FCoE),
- Řízení kvality služeb (QoS) s možností definice frontování, klasifikace provozu, markování provozu (DSCP, COS), s možností omezení a vyčlenění šířky pásma provozu v jednotlivých kategoriích a definici tzv. non-drop QoS politiky pro FCoE provoz.

DC přepínače budou nasazeny s použitím výše uvedených vlastností.

Datacentrový přepínač je založen na bezeztrátové architektuře (lossless fabric architecture) a plně podporuje datacentrové technologie definované standardy IEEE 802.1Qaz (Data Center Bridging Exchange protocol a Enhanced Transmission Selection), IEEE 802.1Qbb (Priority-based Flow Control) a FC-BB-5 (FCoE).

Datacentrový přepínač také podporuje funkcionalitu, která umožňuje sloučit dva fyzické přepínače do jednoho virtuálního, který se vůči okolním systémům (přepínače, servery, atd.) chová jako jeden logický přepínač a který podporuje agregaci portů do virtuálních trunků napříč fyzickými šasi (multichassis etherchannel).

Datacentrový přepínač disponuje porty s přenosovou technologií 1GE/10GE/FCoE, nativní FC a podporuje technologie Port channeling, VSAN (Virtual SAN) a NPIV (N-Port ID Virtualization).

Datacentrový přepínač rovněž disponuje efektivní podporou virtualizace serverové infrastruktury včetně možnosti aplikovat síťové politiky (VLAN, QoS, rate-limiting) pro připojené virtuální servery.

Datacentrový přepínač plně podporuje řízení kvality služeb (QoS) s možností definice frontování, klasifikace provozu, markování provozu (DSCP, COS), s možností omezení a vyčlenění šířky pásma provozu v jednotlivých kategoriích a definici tzv. non-drop QoS politiky pro FCoE provoz.

2.5.5 Přístupový LAN přepínač pro Uzlové objekty typ 1 a 2

Jako LAN přepínače pro uzlové objekty typu 1 a 2 navrhujeme použít zařízení Cisco Catalyst 3650. Jedná se o fixní stohovatelné přepínače s porty typu 10/100/1000 ethernet a fixními SFP uplink porty typu GE nebo 10GE. Kapacita sběrnice stohu těchto zařízení je 160 Gbps. Přepínače obsahují zabudovaný kontrolér bezdrátových sítí.

Očekáváme, že přístupové L2 přepínače pro objekty typu UO1 a UO2 budou sloužit pro připojení koncových zařízení. Navrhované prvky splňují

požadovanou funkční specifikaci pro přístupové přepínače. Zejména se jedná o následující funkce:

- Připojení koncových zařízení pomocí FE/GE,
- Připojení na návaznou infrastrukturu pomocí GE/10GE uplinků s případným sdružením linek do Portchannel rozhraní,
- Napájení zařízení přes Ethernetové rozhraní,
- QOS klasifikace, markování a zařazení do výstupních front s prioritizací hlasového provozu,
- Ochrana proti podvržení zdrojové MAC a IP adresy a ochranu proti neautorizovaným službám DHCP,
- Optimalizace IP Multicast provozu,
- Monitoring aplikačních toků prostřednictvím technologie Netflow.

Přístupové přepínače budou nasazeny s použitím výše uvedených vlastností.

2.5.6 LAN přepínač pro Koncové objekty typ 1 a 2

Jako LAN přepínače pro objekty typu KO1 a KO2 navrhujeme použít zařízení Cisco Catalyst 2960X. Jedná se o fixní stohovatelné přepínače s porty typu 10/100/1000 ethernet a fixními SFP uplink porty typu GE nebo 10GE. Kapacita sběrnice stohu těchto zařízení je 20 Gbps. Očekáváme, že přístupové L2 přepínače pro objekty typu KO1 a KO2 budou sloužit pro připojení koncových zařízení. Navrhovaná zařízení splňují požadovanou funkční specifikaci pro přístupové přepínače. Zejména se jedná o následující funkce:

- Připojení koncových zařízení pomocí FE/GE podle typu lokality,
- Připojení na návaznou infrastrukturu pomocí GE/10GE uplinků s případným sdružením linek do Portchannel rozhraní,
- Napájení zařízení přes Ethernetové rozhraní,
- QOS klasifikace, markování a zařazení do výstupních front s prioritizací hlasového provozu,
- Ochrana proti podvržení zdrojové MAC a IP adresy a ochranu proti neautorizovaným službám DHCP,
- Optimalizace IP Multicast provozu,
- Monitoring aplikačních toků prostřednictvím technologie Netflow.

Přístupové přepínače budou nasazeny s použitím výše uvedených vlastností.

2.5.7 LAN přepínač s integrovaným WLAN kontrolerem pro Koncové objekty typu 1

Jako LAN přepínače s integrovaným WLAN kontrolerem pro koncové objekty typu 1 navrhujeme použít zařízení Cisco Catalyst 3650. Jedná se o fixní stohovatelné přepínače s porty typu 10/100/1000 ethernet a fixními SFP

uplink porty typu GE nebo 10GE. Kapacita sběrnice stohu těchto zařízení je 160 Gbps. Přepínače obsahují zabudovaný kontrolér bezdrátových sítí.

Očekáváme, že přístupové L2 přepínače s integrovaným WLAN kontrolerem pro objekty typu KO1 budou ve fázi implementace sloužit pro připojení koncových zařízení pomocí LAN. Navrhované prvky splňují požadovanou funkční specifikaci pro přístupové přepínače. Zejména se jedná o následující funkce:

- Připojení koncových zařízení pomocí FE/GE,
- Připojení na návaznou infrastrukturu pomocí GE/10GE uplinků s případným sdružením linek do Portchannel rozhraní,
- Napájení zařízení přes Ethernetové rozhraní,
- QOS klasifikace, markování a zařazení do výstupních front s prioritizací hlasového provozu,
- Ochrana proti podvržení zdrojové MAC a IP adresy a ochranu proti neautorizovaným službám DHCP,
- Optimalizace IP Multicast provozu,
- Monitoring aplikačních toků prostřednictvím technologie Netflow.

Přístupové přepínače budou nasazeny s použitím výše uvedených vlastností.

2.5.8 Centrální VoIP hlasová brána

Navržené zařízení Cisco 2911 pro centrální Voip hlasovou bránu má modulární architekturu s možností přidávat hlasové moduly rozhraní dle budoucí potřeby. V současnosti je dle požadavků zadavatele zařízení vybaveno potřebnými moduly pro připojení brány k VTS a síti LAN včetně potřebného množství DSP procesorů. Zařízení může komunikovat za pomoci protokolů H.323v4, SIPv2 nebo MGCP.

Hlasová brána podporuje rozhraní ISDN PRI, ISDN BRI ve formě modulů, včetně integrovaných DSP procesorů pro zpracování a kódování hlasu a možnosti vytvoření konferenčního mostu s podporou kodeků G.722, G.711, G.729 a iLBC.

Zařízení obsahuje interpreter TCL skriptů a lokální úložiště o dostatečné kapacitě pro lokální přehrávání oznamovacích hlášení volajícím. Za pomoci TCL skriptů je umožněno modifikovat algoritmus zpracování signalizace včetně změn identifikace.

Výkon zařízení umožňuje přenášet požadované množství současných hovorů včetně přenosu faxů standardizovaným protokolem T. 38. Zařízení podporuje šifrování pro hlas (SRTP) i signalizaci pro definovaný počet hovorů. Hlasová brána Cisco obsahuje nástroje pro on-line měření kvality přenosové infrastruktury z pohledu VoIP za pomoci simulace VoIP provozu.

Z pohledu IP protokolu SW zařízení obsahuje plnou podporu IP adresace a směrovacích protokolů pro Ipv4 a Ipv6 a rovněž možnost použití směrovacích unicast resp. multicast protokolů OSPFv2/v3, BGPv4 a MP-BGP, PIM SM a PIM SSM pro Ipv4 i Ipv6. Hlasová brána podporuje technologii DualStack (Ipv4 a Ipv6) s plnou podporou Ipv6 služeb DNS, Telnet/SSH, DHCP, Multicast a QoS. Zařízení je certifikováno certifikátem Ipv6 Ready Logo Phase II.

2.5.9 Multiservisní WAN směrovač pro Uzlový objekt typu 1

Jako WAN směrovač pro objekty typu UO1 navrhujeme použít zařízení Cisco ASR 1001-X. Jedná se o modulární směrovače s integrovanými GE a 10GE porty a pozicí pro rozšiřující modul. Navrhovaná zařízení splňují požadovanou funkční specifikaci pro WAN směrovače. Zejména se jedná o následující funkce:

- Zajištění IPv4 konektivity s podporou dynamickým směrovacím protokolem OSPF/BGP/MP-BGP,
- Podpora vytváření oddělených IP VPN sítí prostřednictvím virtualizace směrovacích tabulek (např. technologie VRF-lite) a podpora virtualizace síťových služeb,
- Směrování IPv4 multicast provozu,
- Hardwarová podpora šifrování aplikačního provozu s využitím technologie IPsec,
- Služby Quality of Service (QoS) včetně Hierarchical Queuing Function, klasifikace provozu, markování provozu pomocí DSCP a vyčlenění šířky pásma provozu v jednotlivých aplikačních kategoriích a definici prioritní fronty pro provoz IP telefonie,
- Podpora současného IPv4 a IPv6 provozu – DualStack, IPv6 služby DNS, Telnet/SSH, DHCP, Multicast a QoS,
- Monitorování aplikačních toků s využitím technologie NetFlow.

Předpokládáme nasazení WAN směrovačů s použitím výše uvedených vlastností.

2.5.10 Multiservisní WAN směrovač pro Uzlový objekt typu 2

Jako WAN směrovač pro objekty typu UO2, KO1 a KO2 navrhujeme použít zařízení Cisco řady 4000. Pro objekty typu UO2 navrhujeme použít směrovače Cisco 4451.

Směrovače Cisco řady 4000 jsou modulární s různým počtem a typem integrovaných GE portů a pozic pro rozšiřující moduly. Jednotlivé modely se dále liší celkovou propustností směrovaného provozu a šifrovacím výkonem.

Navrhovaná zařízení splňují požadovanou funkční specifikaci pro WAN směrovače. Zejména se jedná o následující funkce:

- Zajištění IPv4 konektivity s podporou dynamickým směrovacím protokolem OSPF/BGP/MP-BGP,
- Podpora vytváření oddělených IP VPN sítí prostřednictvím virtualizace směrovacích tabulek (např. technologie VRF-lite) a podpora virtualizace síťových služeb,
- Směrování IPv4 multicast provozu,
- Hardwarová podpora šifrování aplikačního provozu s využitím technologie IPSec,
- Služby Quality of Service (QoS) včetně Hierarchical Queuing Function, klasifikace provozu, markování provozu pomocí DSCP a vyčlenění šířky pásma provozu v jednotlivých aplikačních kategoriích a definici prioritní fronty pro provoz IP telefonie,
- Podpora současného IPv4 a IPv6 provozu – DualStack, IPv6 služby DNS, Telnet/SSH, DHCP, Multicast a QoS,
- Monitorování aplikačních toků s využitím technologie NetFlow,
- Integrovaná hlasová brána s rozhraním typu ISDN PRI/BRI, podporou požadovaných kodeků, VoIP signalizace SIPv2 a H.323v4, šifrování VoIP provozu, lokálního přehrávání oznamovacích hlášení a skriptingu.

Předpokládáme nasazení WAN směrovačů s použitím výše uvedených vlastností.

WAN směrovač bude mimo jiné plnit funkci hlasové brány. Primárním úkolem je zajistit komunikaci IP telefonní sítě s tradičními telefonními systémy, tedy např. s veřejnou telefonní sítí telekomunikačních operátorů, pobočkovými ústřednami a analogovými telefonními přístroji či faxy. Řešení IP telefonie plně podporuje připojení jakýchkoliv analogových zařízení telefonů pomocí převodníků nebo portů v hlasových bránách.

Významnou funkcionalitou je SRST (Survivable Remote Site Telephony). Zprostředkuje IP telefonům na pobočkách registraci a sestavení hovorů v případě výpadku WAN linky k centrálnímu Callmanageru.

2.5.11 Multiservisní WAN směrovač pro Koncový objekt typu 1

Jako WAN směrovač pro objekty typu UO2, KO1 a KO2 navrhujeme použít zařízení Cisco řady 4000. Objekty typu KO1 navrhujeme osadit směrovači Cisco 4331.

Navrhovaná zařízení splňují požadovanou funkční specifikaci pro WAN směrovače. Výčet vlastností je shodný s multiservisními WAN směrovači pro objekt typu UO2.

WAN směrovač bude mimo jiné plnit funkci hlasové brány. Primárním úkolem je zajistit komunikaci IP telefonní sítě s tradičními telefonními systémy, tedy např. s veřejnou telefonní sítí telekomunikačních operátorů, pobočkovými ústřednami a analogovými telefonními přístroji či faxy. Řešení

IP telefonie plně podporuje připojení jakýchkoliv analogových zařízení telefonů pomocí převodníků nebo portů v hlasových bránách.

Významnou funkcionalitou je SRST (Survivable Remote Site Telephony). Zprostředkuje IP telefonům na pobočkách registraci a sestavení hovorů v případě výpadku WAN linky k centrálnímu Callmanageru.

2.5.12 Multiservisní WAN směrovač pro Koncový objekt typu 2

Jako WAN směrovač pro objekty typu UO2, KO1 a KO2 navrhujeme použít zařízení Cisco řady 4000. Objekty typu KO2 navrhujeme osadit směrovači Cisco 4321.

Navrhovaná zařízení splňují požadovanou funkční specifikaci pro WAN směrovače. Výčet vlastností je shodný s multiservisními WAN směrovači pro objekt typu UO2.

WAN směrovač bude mimo jiné plnit funkci hlasové brány. Primárním úkolem je zajistit komunikaci IP telefonní sítě s tradičními telefonními systémy, tedy např. s veřejnou telefonní sítí telekomunikačních operátorů, pobočkovými ústřednami a analogovými telefonními přístroji či faxy. Řešení IP telefonie plně podporuje připojení jakýchkoliv analogových zařízení telefonů pomocí převodníků nebo portů v hlasových bránách.

Významnou funkcionalitou je SRST (Survivable Remote Site Telephony). Zprostředkuje IP telefonům na pobočkách registraci a sestavení hovorů v případě výpadku WAN linky k centrálnímu Callmanageru.

2.5.13 WLAN kontrolér pro řízení přístup. bodů WLAN sítě v Koncových objektech

Wireless LAN kontrolér Cisco WiSM2 je servisní modul do přepínače Cisco Catalyst 6500. Propojení mezi WiSM2 a sběrnici přepínače je 2x 10Gbit/s, kontrolér splňuje požadovanou propustnost 16 Gbit/s. WiSM2 v navrhované konfiguraci umožňuje řízení 200 přístupových bodů, které mohou být zapojeny přímo v LAN nebo umístěny v jiných objektech připojených přes WAN. AP komunikují s kontrolérem přes protokolem CAPWAP, který zapouzdřuje jak uživatelská data, tak řídicí provoz. Řídicí provoz je šifrován automaticky, datový provoz je možné šifrovat volitelně po doplnění příslušné licence (je součástí nabídky).

Pro zajištění vysoké dostupnosti navrhujeme k primárnímu kontroléru použít druhý do páru. Oba kontroléry pak budou konfigurovány do tzv. HA páru (High Availability Pair). V tomto případě pár vystupuje vůči AP jako jediný kontrolér. Mezi oběma jsou soustavně synchronizována jak konfigurační data, tak stavové informace o připojených AP a klientských stanicích. V případě výpadku primárního WLC převezme sekundární jeho funkci bez odregistrování AP tak, že je zajištěn trvalý provoz bez přerušení. Pokud jde o licence pro AP, ty se pro celý HA pár pořizují jen jednou.

Management wireless kontroléru je možný prostřednictvím příkazové řádky, HTML rozhraní nebo SNMP aplikací. Příkazová řádka je dostupná přes přímou sériovou konzoli (RJ-45 i USB), prostřednictvím interního sezení přes šasi 6500 a přes síťový terminál SSH nebo Telnet. HTML rozhraní je dostupné protokolem HTTP a/nebo HTTPS.

Wireless kontrolér jako centrum bezdrátové sítě plní zejména následující funkce.

- **Registrace a management přístupových bodů**

WLC podporuje AP zapojené jak v LAN, tak přes WAN. Podporuje současně AP v režimu local, MESH a FlexConnect. V režimu FlexConnect mohou být data bridgována lokálně na přepínači bez transportu CAPWAP tunelem do kontroléru. WLC detekuje cizí (rough) AP.

- **Řízení přístupu a roaming wireless klientů**

WLC provádí autentizaci klientů podle všech existujících WiFi standardů včetně 802.1i (WPA, WPA2), provádí řízení přístupu prostřednictvím protokolu 802.1x/EAP v provedení PEAP, EAP-FAST, EAP-TLS a dalších, řídí použití šifrování metodami AES, TKIP a WEP.

Je podporován roaming v rámci jednoho WLC nebo mezi různými WLC a to na 2. i 3. vrstvě OSI modelu.

- **Řízení radiové sítě (Radio Resource Management)**

Všechny AP plní současně funkce WiFi obsluhy klientů, detekce kvality radiového spektra a detekce chybných a útočných datových rámců. Řídící rámce jsou označovány kontrolním polem, které je soustavně průběžně kontrolováno. Tím jsou detekovány cizí nežádoucí a útočné AP a stanice - funkce Management Frame Protection a 802.11w. WLC automaticky řídí pro každý AP použitý radiový kanál a vysílací výkon. Tyto hodnoty jsou periodicky optimalizovány na základě průběžného měření úrovně a kvality signálu. WLC může výpadek některého z AP korigovat automatickým zvýšením vysílacího výkonu sousedních AP. Prahové hodnoty rozhodovacího procesu RRM je možné korigovat.

RRM je proces, který se provádí pro všechny WLC konfigurované v jedné RRM skupině (clusteru).

- **Spektrální analýza**

Kromě monitoringu WiFi zařízení a WiFi frekvencí, dokáže WLC ve spojení s nabízenými AP provádět spektrální analýzu celého frekvenčního pásma a detekovat tak ne-wifi rušení a útoky. Na základě

signatur je možné identifikovat řadu typických zařízení jako jsou Blue Tooth, kamery, mikrovlnné trouby, X-box konzole a mnoho dalších.

Je možné definovat alarmy, které se touto detekcí spouští.

- **Detekce útoků**

Navrhovaný kontrolér Cisco WiSM2 má vestavěny funkce IDS/IPS. A je schopen integrace s externím IPS zařízením.

WLC může bránit komunikaci klientům připojeným k cizím nežádoucím AP tak, že opakovaně vysílá deautentizační rámce s adresou dotčené stanice.

- **Další funkce - QoS, multimédia, mDNS, AVC**

WLC podporuje diferenciaci kvality služby do čtyř kategorií (front) podle specifikace 802.11e a WMM. Podporuje Call Admission Control pro hlasové a video služby. WLC obsahuje funkce video streamingu použitím IP multicastů.

WLC má vestavěny funkce mDNS pro podporu Apple zařízení. Je možné nastavovat pro různé služby.

WLC monitoruje uživatelský provoz na aplikační vrstvě a podle nastavených hodnot může různým službám nastavovat různé priority v přenášeném provozu.

- **Web-based Guest Access**

Navrhované wireless kontroléry mají integrovanou funkce pro oddělení návštěvnického provozu - Guest Access. Návštěvníci se po připojení do WiFi sítě musí nejprve přihlásit na web portálu prostřednictvím krátkodobého uživatelského účtu. Správa účtů je možná přímo v management rozhraní kontroléru nebo v management software Cisco Prime Infrastructure.

2.5.14 WLAN access point

Předpokládáme nasazení přístupových bodů (dále AP) typu Cisco Aironet 2702. Přesné číslo produktu je AIR-CAP2702I-E-K9, což specifikuje AP s vestavěnými všesměrovými anténami homologovaný pro použití v regulační doméně ETSI, jejíž součástí je Česká republika.

AP má kovovou hermeticky uzavřenou konstrukci s plastovým radomem, který chrání antény. Má dva RJ-45 porty 10/100/1000 Mbit/s a port RJ-45 pro sériovou konzoli. K napájení se typicky používá přepínač podporující 802.3at (PoE+) nebo 802.3af (PoE). Možné je také napájení přes power injektor nebo přímým připojením napájecího adaptéru 48V. AP má možnost zajištění zámkem k montážní podložce (držáku).

AP podporuje provoz protokoly 802.11b/g/n v pásmu 2,4 GHz a protokoly 802.11a/ac/n v pásmu 5 GHz. AP je schopen pracovat v režimu 3x4 MIMO se třemi prostorovými toky (spatial streams) a podporuje optimalizaci fáze signálu - beamforming. Přes WLC je na těchto AP možné aktivovat funkci Band Select, která manipuluje s management rámcí tak, že klienti upřednostní pásmo 5 GHz před pásmem 2,4 GHz.

AP obsahují výrobcem vestavěný certifikát X.509, kterým se ověřují při registraci na WLC.

Kromě standardních funkcí spojených s obsluhou wireless klientů disponují AP Cisco Aironet 2702 řadou přídavných technologií. Za všechny zmíníme zejména možnost fungovat jako wireless sniffer. V tomto režimu AP monitoruje kanál, odchytává všechny WiFi rámce a přes síť LAN je odesílá do vzdáleného analyzátoru - OmniPeak, Wireshark.

AP Cisco Aironet 2702 mají vestavěný hardware pro spektrální analýzu ve všech podporovaných pásmech. Ve spojení s WLC může identifikovat typické zdroje rušivých signálů a vyhodnocovat závažnost dopadu rušení na kvalitu signálu.

2.5.15 Firewall a IPS systém pro datové centrum

Předmětem dodávky jsou dvě redundantní firewall (FW) systémy typu Cisco ASA 5585-X SSP20. Oba FW systémy jsou modulární a jsou osazeny SourcePOWER IPS modulem typu SSP20. Firewall zařízení s IPS moduly jsou navrženy pro účel ochrany datového centra zadavatele.

Nabídka na FW a IPS systém pro datové centrum zařízení zahrnuje následující licence:

- FW - 5 Security Contexts License (5x virtuálních FW kontextů),
- FW - Botnet Traffic Filter License (ochrana před Botnet sítěmi na 3 roky),
- IPS modul – FirePOWER IPS and Apps Licenses (licence pro funkci IPS a Apps - AVC na 3 roky).

Navrhované redundantní FW a IPS systémy pro datové centrum splňují požadované funkční specifikace. Jedná se především o následující funkce:

- Stavový firewall
- FW podporuje L2 (transparentního) módu s podporou NAT a PAT
- FW podporuje L3 (routovaného) módu s podporou NAT a PAT
- FW podporuje rozdělení na tzv. virtuální firewally včetně možnosti definovat QoS politiky pro jednotlivé kontrolované datové toky včetně podpory Low Latency Queuing
- FW nabízí vysokou dostupnost jednotlivých virtuálních FW v režimu Active – Active (tzn. pro virtuální FW „Aa“ je aktivní pouze na jednom fyzickém FW, jeho pasivní záloha „Ap“ je umístěna na druhém

fyzickém FW, stejný mechanismus lze uplatnit pro další virtuální FW, pro každý virtuální FW lze definovat na kterém fyzickém FW má být daný virtuální FW aktivní)

- Současný provoz L2 a L3 módů v rámci různých virtuálních FW
- FW nabízí podporu stavové inspekce protokolů IPv4, IPv6 a dále aplikačních protokolů (HTTP, FTP, DNS, SMTP, CIFS a další)
- FW odpora stavové inspekce pro IP telefonních protokolů (SIP, SIP/TLS, H.323v1-4, RTP, RTCP a SRTP)
- IPS systém umožňuje nasazení v Inline režimu nebo v IDS režimu
- IPS systém obsahuje signatury, které jsou v pravidelném intervalu aktualizovány a distribuovány výrobcem a dále umožňuje definování vlastních signatur
- IPS systém je schopen detekovat anomální provoz, provádí inspekci protokolu IPv4 a IPv6
- IPS systém je schopen provádět pomocí funkce AVC (Application Visibility Control) funkce aplikační kontrolu pro více jak 3000 typů aplikací, provádí jejich detekci a je schopný určit jejich rizika a bezpečnostní dopad.

Navrhované firewally a IPS systémy splňují výše uvedenou funkční specifikaci a dále další funkční specifikace uvedené ve funkční specifikaci zadávací dokumentace – „Příloha č. 4 – Technická specifikace“.

Součástí dodávky je kontrola dodávky, upgrade softwaru FW a IPS systémů, fyzická instalace do rozvaděče - připojení na napájení, základní konfigurace 1x virtuálního firewallu – nastavení IP, max. 5 interface, 5 ACL typu permit IP any any.

2.5.16 Hraniční (PE) směrovač sítě ITS pro Uzlový objekt typu 2

2.5.17 Zabezpečení komunikační WAN infrastruktury

Navrhovaná komunikační WAN infrastruktura zajistí zabezpečení WAN linek mezi jednotlivými objekty prostřednictvím šifrovací technologie IPSec. Všechny navrhované WAN směrovače splňují všechny funkční požadavky zadavatele. Jedná se zejména o následující funkce:

- Podpora technologií AES 256, IKEv2 a SHA-2,
- Hardwarová podpora šifrování na celtrálních multiservisních směrovačích,
- Hardwarová podpora šifrování na pobočkových směrovačích,
- Podpora selektivního šifrování provozu per IP VPN,
- Podpora vytváření šifrovaných VPN dle RFC 3547 (GDOI based VPN) s centrální správou
- šifrovacích klíčů,

- Podpora autentizace směrovačů pomocí certifikátů X.509 a infrastruktury PKI (s certifikační
- autoritou),
- Podpora výměny bezpečnostních informací (certifikáty, šifrovací klíče) mezi směrovači
- prostřednictvím privátní radiové sítě Pegas.

2.6. Řešení platformy pro síťové služby

2.6.1 NMS systém (dohled sítě)

Navržené řešení dohledového systému Cisco Prime poskytuje spolehlivé informace o aktuálním stavu komunikačního prostředí. NMS systém současně umožňuje konfigurovat a monitorovat celou komunikační infrastrukturu z jednoho místa.

Jsou podporovány následující funkcionality

- Komplexní správa životního cyklu LAN i WLAN infrastruktury (nasazení, administrace, monitoring, odstraňování problémů)
- Automatická archivace konfigurací, porovnávání konfigurací, porovnávání konfigurací vůči šablonám.
- Konfigurační šablony dle "best practice" a designových příruček
- Inventarizace nasazeného HW v síti
- Inventarizace, nasazení, správa firmware do síťových zařízení
- Monitorování výskytu koncových zařízení, IP telefonů a uživatelů v síti
- Generování reportů bezpečnostních problémů infrastruktury
- Monitoring připojení koncových zařízení napříč pevnou i bezdrátovou sítí
- Hierarchické mapy zobrazující umístění AP, šíření signálu a aktuální pozice wifi klientů (notebooků, PDA, WiFi telefonů, WiFi RFID tagů apod.)
- Centrální konfigurace bezdrátových sítí včetně bezpečnostních politik, QoS profilů
- Nástroje pro detekci a řešení problémů v bezdrátové síti (grafy obsazenosti kanálů, grafy odpovídající provozu klientů, atd.)
- Zobrazování alarmů týkajících se kvality signálu
- Technologický dashboard pro zobrazování výsledků měření kvality signálu bezdrátové sítě

- Automatické dohledání portu pevné sítě s připojeným falešným Access Pointem

2.6.2 Monitoring provozních toků - NetFlow kolektor, NBA

Předmětem dodávky je Netflow kolektor FlowMon kolektor (IFC-R5-6000PRO) od výrobce INVEA-TECH. Tento typ kolektoru nabízí 6TB (HW RAID 5) úložiště pro ukládání netflow dat. Kolektor zahrnuje nástroj pro sběr, analýzu a vizualizaci NetFlow/sFlow/IPFIX dat - FlowMon monitorovací centrum (FMC). Kolektor je licencován per zařízení a neobsahuje žádná omezení typu počet zdrojů dat, množství monitorovaných toků či počet uživatelů systému. Maximální výkon tohoto kolektoru je 150.000 toků/s, výkon se může lišit v závislosti na nastavení zařízení a instalovaných pluginech.

- Pro realizaci NBA zadavatele je navržen plugin FlowMon ADS Standard (FPC-ADS-S), který má následující technické parametry: počet toků/s max. 1000 bez agregace, profilování chování max. 1000 IP.

- Navrhovaný Netflow kolektor včetně modulu pro NBA splňuje všechny funkční specifikace uvedené ve funkční specifikaci zadávací dokumentace – „Příloha č. 4 – Technická specifikace“.

- Součástí dodávky je kontrola dodávky, upgrade softwaru systémů, fyzická instalace do rozvaděče - připojení na napájení, základní konfigurace – nastavení management IP, nastavení max. 5 zdrojů dat pro sběr netflow statistic z koncových zařízení.

2.6.2.1 Řešení systému detekce anomálií a nežádoucího chování v síti (ADS)

- FlowMon ADS plug-in nabízí dva základní postupy pro efektivní detekci anomálií a nežádoucího chování v síti.
- První postup spočívá ve vyhledávání nežádoucích vzorů v komunikaci na síti. Avšak na rozdíl od jiných nástrojů není analyzován obsah jednotlivých paketů, ale komunikace jako celek (zdrojové a cílové IP adresy, použité porty, příznaky spojení, mezipaketové mezery, délka komunikace a mnoho dalšího). Díky tomu je možné snadno detekovat události, jakými jsou např. útoky (skenování portů, slovníkové útoky), nežádoucí aplikace (P2P sítě, anonymizační služby), infikované počítače (viry, spyware) a řada dalších.
- Druhý postup je založen na vyhodnocování chování jednotlivých zařízení v síti a změně chování oproti jejich obvyklému stavu. Jedná se o moderní metodu označovanou jako behaviorální analýza. Hlavní výhoda spočívá v možnosti detekovat události, které jsou jinými systémy nezjistitelné a mohou se jevit jako legitimní – např. zcizená identita a hromadné kopírování

důležitých firemních dat, nakažené zařízení (rozesílání spamu, snaha infikovat další stanice), provozní problémy (nefunkční aktualizace, nadměrná zátěž) a další.

2.6.2.2 Hlavní přínosy ADS

- Zvýšení nejen vnější ale zejména vnitřní bezpečnosti sítě
- Detekce skenování sítí, slovníkových útoků, útoků zahlcením typu denial of service (DoS, DDoS), útoků na aplikační protokoly, P2P aktivit, spyware, spamů, virů nebo botnet sítí
- Identifikace nežádoucích služeb (např. podvodných web serverů)
- Odhalení specifických i dosud neznámých hrozeb, pro které neexistují signatury (a IPS ani antiviry je neodhalí)
- Budování profilů chování jednotlivých zařízení a detekce změn komunikačních partnerů, objemů provozu či struktury provozu
- Obrana proti sociálnímu inženýrství a úniky informací z organizace
- Účinné i pro šifrovaný provoz
- Detailní přehled o struktuře síťového provozu v síti
- Kontrola dodržování bezpečnostních směrnic
- Odhalování vnitřních i vnějších útoků
- Monitoring kvality služeb
- Eliminace nežádoucích aplikací
- Odhalování infikovaných zařízení v síti
- Prevence používání nežádoucího software a sdílení nelegálního obsahu
- Kontrola nad odchozím provozem sítě, ochrana dobrého jména
- Rychlá diagnostika zpoždění sítě, služeb a aplikací
- Odhalování špatných konfigurací sítě a síťových zařízení

Na základě dlouhodobých statistik o provozu jednotlivých zařízení na síti plug-in FlowMon ADS automaticky sleduje a informuje o jakékoliv změně v jejich chování nebo v chování celé sítě. Profily chování vytvářené pluginem FlowMon ADS zahrnují:

- Schopnost detekce nežádoucích vzorů chování
 - vnitřní i vnější útoky
 - nežádoucí služby a aplikace
- Behaviorální analýza
 - profily chování
 - detekce anomálií, podezřelého chování
- Stoprocentní znalost a přehled o komunikacích v síti – síť přestane být blackbox ve které jsou přenášeny nějaké pakety
- Řádové snížení času nutného k řešení problémů

- Vyšší efektivita správců sítě – efektivní troubleshooting
- Kompletní reporting o dění na síti
- Přehled o využití síťových služeb a šířek pásem aplikacemi
- Optimalizace síťové infrastruktury
- Předcházení incidentům a výpadkům sítě
- Moderní „nadstavba“ nad monitorováním datových toků
- Automatická pokročilá detailní analýza NetFlow dat
- Účinné i pro moderní útoky psané na míru
- Vzrůstající požadavky na monitoring a bezpečnost, budování CSIRT týmů na mnoha úrovních
- Nástroj pro podporu implementace a kontroly dodržování bezpečnostních politik a norem (ISO, ISMS)
- Splnění požadavků externích auditorů na monitoring sítě
 - záznam o každé komunikaci, která proběhla po síti
 - finanční instituce, státní organizace a další

2.6.3 Autentizační systém (Protokol 802.1x)

Předmětem dodávky jsou dva centrální autentizační systémy Cisco ISE 3415 (AAA nebo RADIUS servery). Oba systémy budou nasazeny v HA režimu. Cisco ISE servery budou použity zadavatelem pro nasazení 802.1x ověřování koncových zařízení a další Network Access Control (NAC) služeb přístupové vrstvy v LAN a bezdrátových sítích zadavatele.

Nabídka zahrnuje následující licence:

- Basic licenci pro 2500 koncových zařízení, licence obsahuje následující funkcionality:
 - 802.1x a MAB funkce, základní funkce AAA (Authentication, Authorization, Accounting),
 - Webovou autentizaci (lokální, centrální a registraci zařízení),
 - MACsec,
 - Webový portál pro „guest“ uživatele a služby pro sponzory,
 - Cisco TrustSec® SGT (Security Group Tagging),
- Plus licenci pro 2500 koncových zařízení, licence obsahuje následující funkcionality:
 - Profiling – automatické rozpoznání OS nebo typ koncového zařízení,
 - Profiler feed service - synchronizace pravidel pro profiling,
 - Registrace a provisioning zařízení pro BYOD (Bring Your Own Device),

- Context sharing (Cisco pxGrid),
- Endpoint Protection Services (EPS).
- Apex licenci pro 2500 koncových zařízení, licence obsahuje následující funkcionality:
 - Posture – kontrola stavu stanice,
 - Podpora pro Enterprise mobility management (EMM) a Mobile device management (MDM) – možnost integrace s EMM a MDM systémy,
 - Cisco AnyConnect Unified Agent verze 4.0 (pozn.: pokud budete chtít použít AnyConnect Posture modul pro kontrolu stavu stanice, v tomto případě je nutná Cisco AnyConnect Apex licence, tato licence není součástí dodávky).

Navrhovaný autentizační systém splňuje všechny funkční specifikace uvedené ve funkční specifikaci zadávací dokumentace – „Příloha č. 4 – Technická specifikace“.

Součástí dodávky je kontrola dodávky, upgrade softwaru systémů, fyzická instalace do rozvaděče - připojení na napájení, základní konfigurace – nastavení management IP, konfigurace HA.

Následující kapitoly popisují základní funkce a principy 802.1x a MAB ověřování.

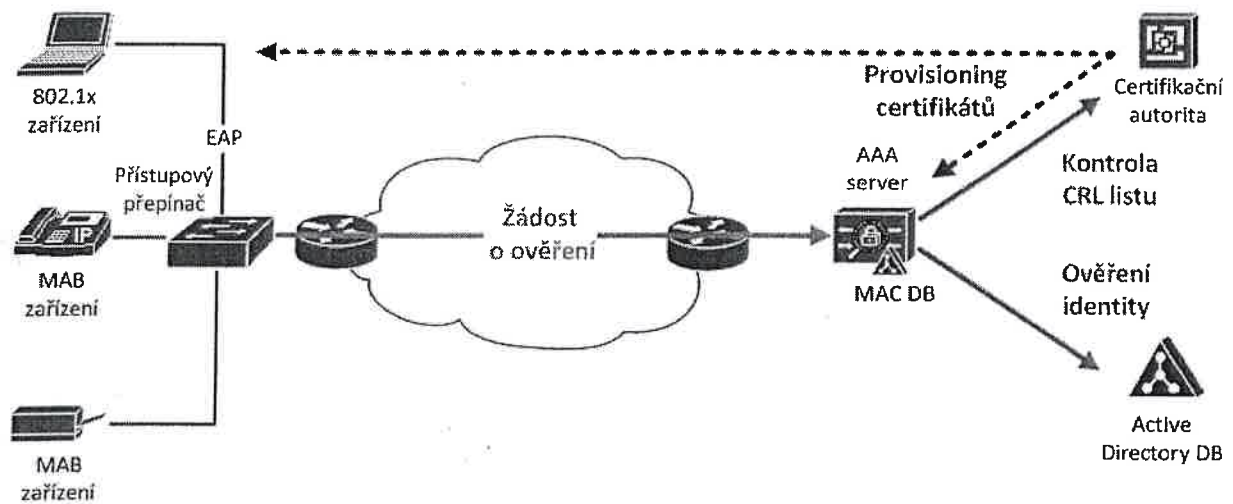
2.6.3.1 Obecný popis jednotlivých komponent

Ověřování přístupu pomocí 802.1x se skládá z následujících komponent:

- přepínače Cisco Catalyst a bezdrátové WLC kontroléry v roli autentizátorů přístupu,
- Cisco Identity Service Engine (ISE) v roli AAA serveru,
- Cisco ISE databáze MAC adres – pro zařízení, která nepodporují 802.1x je nutné použít MAC adresu zařízení, která je ověřena pomocí metody MAB,
- stávající AD nebo PKI infrastruktura,
- koncová zařízení, která podporují 802.1x, pokud tomu tak není je nutné použít metodu MAB, dále mohou být zařízení nebo uživatelé rozděleny do skupiny podle typu (PC, tiskárny, ip kamery, ip telefonní přístroje, atd.).

S centrálními AAA servery mohou spolupracovat další části infrastruktury, jako je např. navazující síťová infrastruktura, doménové kontroléry nebo certifikační autorita.

Obecnou logickou topologií pro ověřování přístupu pomocí 802.1x a MAB metod a další související komponenty znázorňuje následující obrázek.



Obrázek 1 - Logická topologie 802.1x

Přístupové přepínače

Přístupový přepínač zaregistruje pokus o připojení koncového zařízení. Detekuje, zda zařízení podporuje ověření identity pomocí protokolu 802.1x nebo zda bude ověřována MAC adresa daného zařízení. Údaje o identitě zašle pomocí RADIUS požadavku na AAA server, který v odpovědi rozhodne o povolení přístupu a nastavení přístupových parametrů portu, na který se zařízení připojilo.

Bezdrátové kontroléry

Bezdrátový kontrolér zaregistruje pokus o připojení do bezdrátové sítě. Požadavek na přístup ověří pomocí metody 802.1x na AAA serveru, který v odpovědi rozhodne o povolení přístupu a nastavení přístupového oprávnění (VLAN, dACL).

AAA servery

AAA servery přijímají od přístupových přepínačů pomocí protokolu Radius žádosti o ověření koncového zařízení. V případě zařízení s podporou 802.1x ověří údaje a platnost jeho certifikátu. V případě, že zařízení 802.1x nepodporuje, je proveden dotaz do MAB databáze ohledně povolení přístupu na základě MAC adresy. V případě povolení přístupu mohou být na přístupové přepínače zaslány další parametry pro přístup (VLAN, dACL).

AAA servery jsou klíčové pro fungování 802.1x a je tedy nutné řešit jejich vysokou dostupnost.

PKI infrastruktura

PKI infrastruktura zajišťuje vydávání certifikátů pro ověření identity pomocí 802.1x. Zároveň zajišťují vydávání informací o neplatných certifikátech například pro ukradená nebo vyřazená zařízení. Pro tento účel v rámci tohoto projektu očekáváme použití pravidelně vydávaných CRL. V případě požadavků na on-line kontrolu lze použít OCSP protokol. V takovém případě je nutné řešit vysokou dostupnost PKI infrastruktury.

MAB databáze

MAB databáze obsahuje MAC adresy všech zařízení, tedy včetně těch, jež podporují 802.1x, kterým má být umožněn přístup do komunikační infrastruktury. Pro MAB databázi je použita interní databáze AAA serveru.

2.6.3.2 Obecný postup připojení pomocí 802.1x

Obecný postup připojení k přístupovému rozhraní přepínače v LAN prostředí pomocí 802.1x bude následující:

- Koncové zařízení je fyzicky připojeno na rozhraní přístupového přepínače LAN infrastruktury.
- Přístupový přepínač se pokusí zjistit identitu koncového zařízení pomocí protokolu 802.1x nebo je jako identita použita MAC adresa tohoto zařízení.
- Informace o identitě jsou zaslány na AAA server.
- AAA server ověří identitu připojovaného zařízení nebo uživatele, identitou se rozumí následující možnosti:
 - doménové heslo nebo certifikát stanice (EAP-MSCHAPv2, EAP-TLS),
 - doménové heslo nebo certifikát uživatele (EAP-MSCHAPv2, EAP-TLS).
- Na základě ověřené identity AAA server zašle povolení nebo zamítnutí přístupu do LAN infrastruktury a doplňkové parametry připojení.

Obecný postup připojení v bezdrátovém prostředí ke korporátnímu SSID pomocí 802.1x bude následující:

- Koncové zařízení se začne připojovat k bezdrátovému SSID, které je centrálně řízeno (vysíláno) pomocí bezdrátového kontroléru.
- Bezdrátový kontrolér se pokusí zjistit identitu koncového zařízení pomocí protokolu 802.1x.
- Informace o identitě jsou zaslány na AAA server.
- AAA server ověří identitu připojovaného zařízení.
- Na základě ověřené identity AAA server zašle povolení nebo zamítnutí přístupu do LAN infrastruktury a doplňkové parametry připojení.

2.6.4 Diskové pole s FC rozhraním

Nabízené diskové pole disponuje dvěma redundantními řidiči a hrubou diskovou kapacitou 48TB. Tato disková kapacita je složena z celkem dvaceti SAS disků, každý o kapacitě 4TB. Celkově je diskové pole rozšiřitelné až na celkový počet 150 disků což odpovídá hrubé kapacitě 600TB. Každý řadič je osazen 12GB cache a dvěma 8Gb FC porty pro připojení diskového pole do SAN. Diskové pole dále umožňuje on-line dynamické zvyšování kapacity logických disků a hot swap výměnu disků, stejně tak jako redundantní zdroje. Součástí nabídky je i požadovaný management.

Podporované serverové operační systémy:

- Apple MAC O/S 10.8 or greater
- Citrix XenServer 6.1
- HP-UX
- IBM AIX
- IBM VIOS 2.2, 2.3
- Microsoft Windows Server 2008, Windows Server 2008 R2+
- Windows Server 2012, Windows Server 2012 R2*
- Microsoft Windows 7, Microsoft Windows 8 and Vista
- Microsoft Hyper-V
- Novell Suse Enterprise Linux
- Oracle Linux
- RedHat Enterprise Linux
- Solaris 10 x86, Solaris 10 Sparc
- Solaris 11 and 11.1 supported, SPARC & x86

VMware® ESXi5.x®

2.6.5 Diskové pole iSCSI/NFS (Uzlový objekt typu 2)

Nabízené diskové pole disponuje dvěma redundantními řidiči a hrubou diskovou kapacitou 24TB. Tato disková kapacita je složena z celkem dvancti SAS disků, každý o kapacitě 4TB. Celkově je diskové pole rozšiřitelné až na celkový počet 150 disků což odpovídá hrubé kapacitě 600TB. Každý řadič je osazen 12GB cache a dvěma 8Gb FC porty pro připojení diskového pole do SAN. Diskové pole dále umožňuje on-line dynamické zvyšování kapacity logických disků a hot swap výměnu disků, stejně tak jako redundantní zdroje. Součástí nabídky je i požadovaný management.

Podporované serverové operační systémy:

- Apple MAC O/S 10.8 or greater
- Citrix XenServer 6.1
- HP-UX
- IBM AIX
- IBM VIOS 2.2, 2.3
- Microsoft Windows Server 2008, Windows Server 2008 R2+
- Windows Server 2012, Windows Server 2012 R2*
- Microsoft Windows 7, Microsoft Windows 8 and Vista
- Microsoft Hyper-V
- Novell Suse Enterprise Linux
- Oracle Linux
- RedHat Enterprise Linux
- Solaris 10 x86, Solaris 10 Sparc
- Solaris 11 and 11.1 supported, SPARC & x86

VMware® ESXi5.x®

2.7. Řešení umístění a zálohování technologie

2.7.1 Datové rozvaděče (RACK)

Navrhované řešení splňuje požadované parametry v plném rozsahu. Podrobnosti jsou uvedeny v technické specifikaci zařízení.

2.7.2 UPS

Navrhované řešení splňuje požadované parametry v plném rozsahu. Podrobnosti jsou uvedeny v technické specifikaci zařízení.

2.8. Řešení IP telefonie

2.8.1 Řídící část

Navržené řešení IP telefonního systému umožňuje nasazení centralizovaného modelu zpracování hovorů formou jediného společného aplikačního clusteru, který bude zajišťovat jednotnou sadu multimediálních služeb (hlas, video, data) dostupnou všem uživatelům regionu:

- přenositelnost čísla a uživatelských služeb v rámci systému IP telefonie,
- centralizovanou správu celého systému,
- zálohu systému na již vybudovanou infrastrukturu IOS,
- funkční kompatibilitu se stávající vybudovanou IP telefoníí

Hlavními komponenty řešení jsou:

- geografický cluster softwarové ústředny Cisco Unified Communications Manager (CUCM)
- hlasové brány pro prostup do veřejné telefonní sítě
- HW a SW zdroje pro transkódování hovorů
- skupina serverů pro zabezpečení tarifkace hovorů
- skupina serverů pro zabezpečení nahrávání hovorů
- směrovače na pobočce pro zabezpečení hlasových funkcí
- skupina serverů pro zabezpečení video konferencí a připojení

Pro x64 HW platformu centralizovaných služeb bylo zvoleno řešení Cisco Unified Computing System (UCS) zajišťující virtualizaci jednotlivých serverů s využitím operačního systému Vmware ESX. Virtuální prostředí VMware ESXi bude instalováno na dedikovaném HW zařízení s vysokou spolehlivostí a dostupností (redundantní napájecí zdroje typu hot swap, redundantní NIC, redundantní disky typu hot swap). Cisco Unified Computing System představuje platformu pro virtualizaci datových center, která sjednocuje servery, síť, storage a virtualizaci do jednotného systému, jehož cílem je zvýšit spolehlivost a flexibilitu řešení. Systém integruje nízkou latenci s bezztrátovým 10GB přenosem s x86-server architekturou, představuje integrovanou, škálovatelnou, multichassis platformu s podporou vysoké dostupnosti. Použitelnost systému zvyšuje přenositelnost fyzických i virtuálních strojů a úzká vazba na LAN a SAN řešení.

Jednotlivé systémy budou umístěné v geograficky distribuovaných lokalitách pro dosažení plné redundance s možností rozkládání zátěže na jednotlivé servery. Jako sekundární řídicí server pro IPT bude použit stávající server umístěný v objektu KŘ PČR Karlovy Vary, primární servery budou umístěny lokálně v objektu KŘ PČR Plzeňského kraje.

Architektura řešení sestává ze skupiny serverů CUCM (Cisco Unified Communications Manager) zabezpečujících funkce hlasové ústředny a dalších serverů zabezpečujících ostatní funkce v rámci IP telefonie. Tyto servery budou umístěné ve dvou lokalitách pro zabezpečení vysoké dostupnosti. Signalizační funkce pro všechny IP telefony a hlasové brány a další zařízení zajišťuje jedna logická skupina CUCM serverů. Servery pracují ve

dvou režimech tzv. Publisher, který slouží k provádění konfiguračních změn a další servery ve funkci tzv. Subscriber - k těmto serverům se registrují jednotlivé zařízení. Změny provedené na serveru Publisher se propagují do databáze Subscriber serverů. Cluster se tak chová jako jedna virtuální ústředna. Telefony mohou být primárně registrovány k jednomu serveru a další použít k registraci v případě výpadku primárního serveru. V případě ztráty spojení s centrem mohou využít možnost registrace k lokálnímu prvku tzv. SRST (Survivable Remote Site Telephony). Část telefonů může používat k registraci jeden server, další část telefonů může být registrována k dalším serverům a ostatní použít jenom v případě výpadku, což umožňuje optimální rozdělování zátěže v případě velkého množství telefonů. Architektura vzdálených poboček zohledňuje použití modelu centralizovaného řízení hovorů s lokálním SRST zálohováním. Funkci SRST bude splňovat Cisco WAN směrovač.

Řešení podporuje všechny požadované kodeky iLBC, G711, G729 a G722 napříč celou navrhovanou infrastrukturou.

Uživatelské služby v tomto návrhu nejsou vázány jenom na dostupnost primárního konfiguračního uzlu, každá služba je současně poskytována dalšími servery v geografickém clusteru. Tato koncepce rovněž umožňuje realizovat rozkládání zátěže služeb mezi jednotlivé uzly clusteru přičemž jednotlivé uzly clusteru sdílejí společnou konfigurační databázi a jsou vzájemně zastupitelné.

Řešení v plné míře splňuje požadovanou vysokou dostupnost pro HW prvky ve formě:

- redundance úložiště typu hot-swap
- redundance procesorů a paměťových prostředků
- redundance síťového připojení
- redundance napájecích zdrojů typu hot swap

Registrace telefonů v případě výpadku IP konektivity z lokality do centra bude přecházet na lokální hlasovou bránu do tzv. záložního SRST režimu. V tomto režimu zůstává zachován očíslovací plán a dostupnost lokálních služeb. Zdroje pro konference a transkódování jsou rovněž realizovány na lokální hlasové bráně čili dostupné i v případě výpadku konektivity lokality do centra. Pro vytvoření konferencí proto není nutné použít zařízení v centru a zbytečně používat pásmo WAN linek.

Redundance serverů je řešena v režimu 1:1. Každý subscriber server bude mít další subscriber server jako zálohu pro svou část registrovaných telefonů. Každý z dvojice subscriber serverů bude umístěn v jiném datovém centru. Takto je možné dosáhnout vysoké dostupnosti služeb pro každou skupinu serverů nezávisle na umístění. Nikdy nedojde k situaci, kdy výpadek jednoho z datových center způsobí hromadný výpadek části telefonů, protože zálohovací server pro konkrétní skupinu se bude nacházet ve druhém datovém centru.

Řešení v plné míře umožňuje realizaci UC infrastruktury pro všechny lokality a daný počet přístrojů. Umístění jednotlivých uzlů clusteru není vázáno na jednu lokalitu, umožňuje flexibilitu v umístění, či v přesunu jednotlivých uzlů clusteru. Kapacitu řešení je možné navyšovat v čase, přičemž navyšování kapacity je řešeno postupným přidáváním jak uživatelských licencí, tak i hardwarových zdrojů pro pokrytí výkonnostních požadavků.

Navržené řešení poskytuje otevřená a dokumentovaná rozhraní následujících služeb:

- Signalizace SIP, H.323, MGCP
- WebServices - HTTP, XML, SOAP, CTI (např. TAPI, JTAPI, CSTA)

IP telefonní systém podporuje jak protokol IPv4, tak i protokol IPv6 (dle Pokynu vlády ČR č.727ze dne 8.6.2009). Řídící část poskytuje službu dostupnosti uživatele přes wifi síť a softwarového klienta v chytrých telefonech a tabletech.

2.8.2 Řešení číslovací plánu

Řešení IP telefonního systému umožňuje tvorbu a správu více číslovacích plánů, jejich vzájemnou izolaci i provázání, je podporováno:

- Zachování stávajících číslovacích plánů v jednotlivých objektech.
- Postupnou implementaci centralizovaného číslovacího plánu s časovým překryvem původních číslovacích plánů podle harmonogramu projektu.
- Podporu číslovacího plánu ve formátu E164 a URI (přiřazení obou identifikací uživateli).
- Pružnou manipulaci s číslem volaného i volajícího v průběhu sestavování hovoru.

Řešení v navržené velikosti s rezervou podporuje všechny lokality s uživateli, navržený model podporuje až 2000 vzdálených lokalit. Navíc řešení umožňuje modulárním způsobem rozšiřovat počet pracovníků, stávajících i nových lokalit.

Rozhodující při návrhu číslovacího plánu je i požadavek na zachování existujícího nastavení. Tento požadavek může znamenat nasazení nástrojů pro úpravu čísla, jako např. prefixové předvolby, odstraňování číslic, přidávání prefixu, změna čísla volajícího/volaného, které jsou součástí řešení.

Při návrhu designu celého systému je bráno v úvahu také směřování hovorů na systémy informačních a záchranných služeb (112, policie, hasiči). Tyto hovory jsou v rámci veřejné telefonní sítě směřovány jiným způsobem, než ostatní hovory. Volání na krizové linky musí být směřovány na dispečink, který je uživateli geograficky nejbližší.

2.8.3 Identifikace hovorů

Řešení standardně podporuje, bez ohledu na signalizační protokol, následující služby identifikace:

- Zobrazení volanému číslo volajícího na displeji IP telefonu.
- Zobrazení volajícímu skutečné číslo linky, na kterou se dovolal.
- Zobrazení informace o jménu volajícího a volaného účastníka.

Pokud je potřeba provádět prakticky libovolné změny čísla (maskování) volajícího či volaného, nebo pokud chceme identifikaci úplně zakázat, můžeme jednak využít prostředků CUCM, jednak překlad provádět na hlasové bráně.

Všechny tyto úpravy se mohou povolit pro určité přístroje nebo skupiny přístrojů, nebo se mohou uplatnit při průchodu hovoru konkrétní hlasovou bránou. Úpravy je možné provádět pro příchozí i odchozí hovory.

Řešení umožňuje zachování i modifikaci čísla volajícího pro příchozí i odchozích hovory. Maskování čísel je podporováno pro jednotlivé telefonní přístroje, linky a pro skupiny linek příslušné objektu nebo organizačnímu celku.

2.8.4 Směrování hovorů

Řešení umožňuje Least Cost Routing (LCR) z pohledu místa vzniku hovoru. Hovor bude směrován na základě volby tarifu a volby přenosové cesty. Směrovací pravidla budou spravována centralizovaně a reflektují ekonomická kritéria pro služby jednotlivých operátorů veřejných sítí. Pro výběr směrovací cesty na základě čísla volaného se používá metoda Leased Cost Routing (LCR), která zvolí optimální cestu jak z hlediska ceny, tak z hlediska vytížení bran. Příklad nastavení LCR:

- Hovory do JTS se směřují na lokální bránu, při obsazení či nedostupnosti na jinou bránu dle specifikovaného seznamu.
- Mezinárodní hovory mohou být směrovány na centrální brány, kde se očekává lepší cena za tyto hovory
- Hovory do sítí GSM použijí speciální bránu připojenou k těmto operátorům, umístěnou většinou v centru.

Možnost směrování hovoru prakticky přes jakoukoli bránu je možné uplatnit při návrhu počtu hlasových kanálů do sítě JTS na jednotlivých lokalitách, brány stačí dimenzovat pouze pro průměrný počet současných hovorů, ostatní hovory budou obslouženy jinými branami. To vede k výrazným úsporám nákladů za telefonní linky.

2.8.5 Call Admission Control

Navržené řešení umožňuje přenos hlasových kanálů jak v tradičním prostředí TDM, tak i v prostředí IP. Administrátor systému je schopen určit, kudy budou jednotlivé hovory realizovány:

- Pro komunikaci v rámci pobočky platí, že komunikace probíhá po LAN síti.
- Pro komunikaci mezi lokalitami mohou být využity jak privátní IP datová síť, tak veřejná telefonní síť.

Řídící servery zajistí, aby hovory mezi pobočkami byly primárně směrovány prostřednictvím IP sítě a v případě její nedostupnosti nebo nedostatečné šířky přenosového pásma byly hovory směrovány prostřednictvím VTS, Cisco CAC obsahuje:

- Centrální správu a řízení.
- Řízení přenosového pásma pro hlasové i video služby společně.
- Specifikaci garantované šířky pásma a použitého kódování hlasových a video toků.
- Zohlednění dynamického chování a vytížení komunikační infrastruktury.
- Využití více komunikačních cest (rozložení zátěže a záložní trasy) s různou přenosovou kapacitou.
- Podporu protokolu RSVP.
- Specifikaci garantované šířky pásma a použitého kódování hlasových a video toků.

Navržené řešení umožňuje efektivní řízení využití přenosové kapacity (Call Admission Control) transportní IP/MPLS infrastruktury propojující jednotlivé objekty MV a PČR. CAC umožňuje centrální správu a řízení včetně real-time komunikace mezi řídicími servery IP telefonního systému a komunikačními prvky IP infrastruktury o dostupnosti přenosového pásma pro hlasové a video hovory. Pro řízení přenosového pásma bude použit protokol RSVP, který je podporován na zařízeních tvořících stávající infrastrukturu sítě ITS MV.

Pokud CAC při pokusu o nový hovor zjistí, že datová linka nebo její vyhrazená část šířky pásma pro hovory je již plně utilizovaná, zabrání uskutečnění nového hovoru. Tím je zajištěna kvalita všech právě probíhajících hovorů.

2.8.6 Konferenční hovory

Navržené řešení podporuje realizaci telefonních konferenčních hovorů s možností připojit do jedné konference min. 10 účastníků z různých objektů, jejichž telefonní přístroje využívají různé typy hlasových kodeků (G.711, iLBC, G.722 apod.). Řešení dále umožňuje realizovat telefonní konferenci alespoň pro 40 účastníků a dále podporuje:

- Konferenci v režimu Ad-hoc i Rendezvous s autentizací PINem.
- Automatické sestavení konference formou obvolání účastníků a jejich připojení do konference.

2.8.7 Záložní systém volání v jednotlivých objektech

Navržené řešení obsahuje na všech Koncových objektech typu 1 a 2 připojených do IP WAN záložní řešení Cisco SRST, které je schopné obsloužit i nadále příchozí i odchozí volání do sítě VTS včetně volání na tísňové linky pro lokálně zapojené IP telefony.

Telefonní systém uživatele o tomto stavu upozorňuje o běhu v záložním režimu zprávou na displeji IP telefonu a při opětovném zprovoznění IP WAN sítě systém sám okamžitě přejde do původního režimu.

2.8.8 Integrace analogových telefonních přístrojů, faxů a modemů

Navržené řešení umožňuje v jednotlivých lokalitách připojení a integraci analogových přístrojů různých typů - telefon, fax a modem za pomoci analogových bran VG a ATA.

2.8.9 Integrace IP telefonů s aplikacemi na PC

Navržené řešení IP telefonního systému podporuje plnou integraci IP telefonních přístrojů s aplikacemi na desktopových počítačích prostřednictvím protokolu CTI (Computer Telephony Integration). IP telefonní systém poskytuje službu CTI pro všechny uživatele centralizovaně, s vysokou dostupností a možností rozkládání zátěže. Integrace dále umožňuje vytáčení hovorů na IP telefonních přístrojích pouhým kliknutím v aplikaci na počítači. Mezi podporované aplikace patří webový prohlížeč, MS Outlook a MS SharePoint.

Řešení podporuje následující služby:

- vytáčení hovorů na IP telefonních přístrojích pouhým kliknutím v aplikaci (např. MS Outlook) na požadovaný kontakt, telefonní číslo,
- „Pop-up“ okno při příchozím hovoru a jeho identifikace textem z adresářových služeb,
- Přístup k adresářovým službám MS Active Directory a Osobní adresář MS Outlook,
- Přístup ke kalendářovým službám MS Exchange,
- Zobrazení dostupnosti uživatelů v MS Outlook.

2.8.10 Bezpečnost IP telefonního systému

Nabízené řešení umožní snadnou implementaci šifrovaného přenosu telefonních hovorů v prostředí transportní IP sítě v následujících scénářích:

- šifrovaný přenos signalizace mezi „IP telefon – IP telefon“ i „IP telefon – hlasová brána“
- šifrovaný přenos telefonního hovoru (RTP stream) mezi „IP telefon – IP telefon“ i „IP telefon – hlasová brána“.

Řídící servery IP telefonie, hlasové brány a koncové telefonní přístroje nebo video konferenční jednotky budou připojeny do stávající dedikované IP VPN sítě „Voice“. SW IP telefony a aplikace provozované na pracovních stanicích, tabletech nebo smartphonech budou připojeny do stávající datové IP VPN „Hermes“. Řešení IP telefonního systému umožňuje bezpečnou a rychlou komunikaci mezi klienty v datové IP VPN síti „Hermes“ a klienty v hlasové IP VPN síti „Voice“ bez nutnosti směrování real-time telefonního provozu (UDP/RTP) přes centrální firewall propojující obě oddělené IP VPN sítě. Toto bude umožněno za pomoci funkcionality Cisco Trusted Relay Point, která je součástí dodávaného řešení.

2.8.11 Integrace IP telefonního systému s tel. sítěmi operačních středisek

Navržené řešení IP telefonního systému bude zajišťovat centralizované a spolehlivé propojení do stávající privátní hlasové sítě Operačních středisek (OS) PČR. Služba OS je realizována na platformě IP telefonie Cisco Communications Manager v9.1 a to prostřednictvím IP trunků se signalizací SIPv2 (RFC 3261 a návazné) a tunelování signalizačních zpráv Q.SIG a Q.931. Pro tyto potřeby řešení podporuje:

- Q.SIG Basic call dle standardu ECMA 143,
- Q.SIG Supplementary Services dle standardu ECMA 165,
- přenos „původně volaného“ čísla pomocí "Diversion" SIP header dle standardu RFC 6044.

- DTMF relay přes IP - in-band podle RFC 2833, KPML – RFC 4730, SIP Notify – RFC 3265 a SIP Info – RFC 2976.
- Sestavení hovoru v režimu „Delay offer“ i „Early Offer“.
- Specifikace komunikačních parametrů v SDP záhlaví SIPové zprávy dle RFC 4566.
- Možnost modifikace algoritmu zpracování signalizace (například pomocí skriptů) pro zajištění interoperability a implementace dodatečných služeb.

2.8.12 Integrace IP telefonního systému s externími telefonními sítěmi

Navržené řešení IP telefonního systému umožňuje realizovat centralizované a spolehlivé propojení do stávající privátní hlasové sítě PČR realizované na platformě pobočkových ústředěn Alcatel 4400 a Alcatel 4300 a to prostřednictvím ISDN/PRI trunků se signalizací Q.SIG s podporou jak Q.SIG Basic call dle standardu ECMA 143, tak Q.SIG Supplementary Services dle standardu ECMA 165. Interoperabilita se stávající PBX infrastrukturou Alcatel v rámci kraje i s jinými kraji bude zajištěna za pomoci příslušných hlasových rozhraní na dodávaných zařízeních.

Řešení dále s pomocí dodávaných hlasových rozhraní zajišťuje centralizované a spolehlivé propojení se stávající radiovou sítí Pegas prostřednictvím E1 ISDN/PRI trunku, dále se stávající sítí VoFR prostřednictvím E1 ISDN/PRI trunku, spojení se sítí mobilních operátorů pomocí E1 ISDN/PRI trunku, resp. IP trunku a spojení s hlasovou sítí HZS pomocí IP trunku. Toto propojení zajistí oddělení externí a interní telefonní komunikace, normalizaci a překlad signalizačního protokolu H.323, resp. SIP a překlad (transkodování) hlasového kanálu.

Navržené řešení podporuje pro příchozí i odchozí směr komunikace možnost specifikace konkrétního hlasového kodeku i seznamu kodeků s jejich prioritním pořadím. Může se jednat o nutnost vynucení specifického kodeku (např. G.711, G.729, G.723) při změně transportní technologie TDM/IP/VoFR.

Nedílnou součástí řešení IP telefonního systému je i jeho propojení s veřejnou telefonní sítí prostřednictvím ISDN/PRI nebo ISDN/BRI trunků realizovaných v objektech jednotlivých typů. Pro tento typ propojení byl navržen dostatečný počet hlasových rozhraní. Řešení umožňuje rovněž propojení IP telefonního systému s veřejnou telefonní sítí na centrální úrovni s pomocí IP trunku.

Pro propojení s externími hlasovými sítěmi jsou podporovány následující funkce a služby:

- Podpora signalizačních protokolů H.323v4, SIPv2 (RFC 3261 a návazné).
- Podpora HW prostředků (DSP procesory) pro kódování přenášeného hlasového signálu s použitím různých kodeků, které zajistí efektivní a vysoce kvalitní transport hlasového signálu jak v prostředí LAN sítí s použitím kodeků G.722, resp. G.711, tak i v prostředí WAN sítí s použitím kodeků iLBC, resp. G.729.
- Podpora rozhraní ISDN BRI/PRI (Euro ISDN, Q.SIG BC a Q.SIG GF/SS).
- Podpora přenosu faxů přes IP (T.38, T.37 store and forward fax, fax detection).
- DTMF relay přes IP - in-band podle RFC 2833 a out-of-band KPML – RFC 4730 a SIP Notify – RFC 3265.
- Převod kódování hlasových kanálů (transcoding).
- Podpora nástrojů pro lokální přehrávání oznamovacích hlášení volajícím.

- Funkce přímé provolby - Direct inward dial, Direct outward dial.
- Šifrovaný přenos VoIP spojení (SRTP)
- Možnost modifikace algoritmu zpracování signalizace (například pomocí skriptů) pro zajištění interoperability se stávajícími systémy hlasové komunikace používaných v rámci PČR.

V případě potřeby řešení umožňuje snadné připojení externích telefonních sítí (hlasových bran/IP PBX) pomocí IP trunků, které zajistí oddělení externí a interní telefonní komunikace, normalizaci a překlad signalizačního protokolu H.323, resp. SIP a překlad (transkodování) hlasového kanálu.

2.8.13 Uživatelské služby IP telefonního systému

Navržené řešení splňuje následující minimální požadavky:

- sestavení a přijetí hovoru
- předání hovoru
- opakované vytáčení posledního čísla
- zkrácené vytáčení
- volání druhého účastníka (zpětný dotaz na dostupnost, střídání mezi hovory);
- variabilní přesměrování volání – každé (off-net a on-net), zaneprázdněn, bez odpovědi
- přidržení hovoru a pokračování
- připojení k hovoru
- parkování a vyzvednutí hovoru
- skupinové převzetí hovoru
- možnost vytváření přímých linek – volba bez vytáčení, pouze zvednutím sluchátka
- zpětné volání
- čekání a vyzvednutí hovoru (s konfigurovatelnou zvukovou výstrahou)
- identifikace volajícího – CLIP (identifikace volající linky CLID - Calling Line Identification, identifikace jména volajícího CNID - Calling Party Name Identification)
- možnosti nastavování oprávnění pro externí hovory
- vytvoření konferenčního hovoru
- odmítnutí hovoru
- adresářové služby – resortní i osobní telefonní seznamy
- přidělení a přenositelnost uživatelského profilu v prostředí podniku
- hudba při čekání - Music on Hold (MoH)

U vybraných uživatelů navíc služby:

- sekretářské soupravy
- spojovatelské pracoviště
- rozšíření hlasových služeb o video složku v kvalitě, dle možností koncových přístrojů
- integrace mobilních služeb – dostupnost na jediném čísle, předávání hovoru mezi pevnou linkou a mobilním přístrojem

- možnost specifikace času pro dostupnost na jednom čísle (např. pouze v pracovní době v pracovní dny) individuálně pro každého uživatele

Pro vybranou skupinu uživatelů umožňuje navržený telefonní systém navíc integraci s prostředím MS Windows (XP – 8.1) a MS Office:

- Vytočení telefonního čísla z MS aplikace (Word, Excel, Outlook, SharePoint) na lokálním IP telefonu (CTI integrace se stolním telefonem),
- indikaci stavu dostupnosti volaného účastníka (volno, obsazeno, nerušit),
- přístup k adresářovým službám Active Directory a osobní adresář MS Outlook, přístup ke kalendářovým službám MS Exchange,
- možnost zaslání krátkého vzkazu (chat) na displej IP telefonu nebo softwarového klienta na PC.

2.8.14 Telefonní přístroje a videokonferenční jednotky pro objekty

Navržené koncové stanice včetně licencí uvedené v technické specifikaci bez výjimky splňují požadavky zadání.

2.8.15 Integrace IP telefonní infrastruktury a LAN

Z důvodu minimalizace nákladů na provoz a správu datové a hlasové infrastruktury PČR Plzeňského kraje umožňuje navržené řešení:

- automatickou detekci IP telefonu připojeného k portu LAN přepínače a jeho automatické přiřazení do dedikované hlasové VLAN,
- automatickou detekci IP telefonu připojeného k portu LAN přepínače a automatické nastavení vhodných QoS parametrů daného portu,
- automatickou detekci IP telefonu připojeného k portu LAN přepínače a inteligentní PoE management - zajištění napájení IP telefonu podle konkrétních požadavků daného typu IP telefonu,
- možnost připojení pracovní stanice uživatele ke komunikační infrastruktuře prostřednictvím IP telefonu.

2.8.16 Integrace videoklientů s videokonferenčními systémy

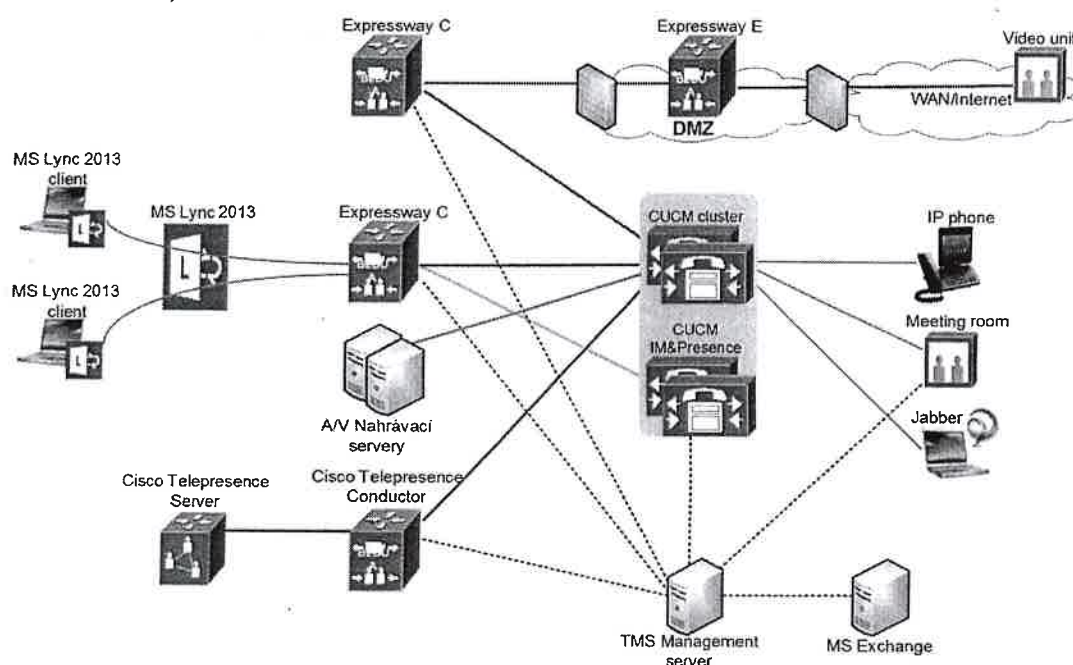
Navržené řešení umožňuje pro videokonferenční systémy:

- Integraci videokonferenčních terminálů do společného číslovacího plánu (E164/URI) a pod jedno centrální řízení tak, že je možné spojit konferenci i s účastníky, kteří nemají klienta s podporou videa.
- Registraci k centrálnímu řídícímu uzlu s autentizací (například SIP/TLS) a šifrování media kanálu (sRTP – AES).
- Podporu kvalitu obrazového rozlišení v různých formátech od CIF až po HD/FullHD a kodeků H.261/263/264. Terminály podporují hlasové kodeky jak v širokopásmové oblasti (například AAC-LD, G.722, G.711) tak i kodeky s nižšími nároky či opravnými mechanismy (například G.729, iLBC).
- Podpora režimu druhé obrazovky (Dual Display) a možnost paralelního prezentačního kanálu nebo dokument kameru u vybraných modelů.

- Přístup k adresářovým službám, telefonním seznamům v rámci organizace (centrální řídicí uzel, AD, apod.)
- Propojení s videokonferenčními jednotkami, které jsou umístěné v jiných organizacích státní správy (např. HZS, ZZS apod.), tj. dostupné přes firewall a překlad adres.

2.8.17 Videokonferenční hovory

Navržený systém podporuje realizaci video konferenčních hovorů s možností připojit do jedné konference min. 14HD účastníků z různých objektů, jejichž terminály podporují různé typy kodeků a rozlišení. IP telefonní systém rovněž umožňuje účast uživatelů v konferenci i v případě, že jejich přístroj podporuje pouze audio služby (telefonní přístroj, mobilní telefon, hovor z VTS).



Obr. Architektura navrhovaného řešení

Videokonferenční server pro spojení více účastnické konference podporuje:

- formu zobrazení účastníků schůzky v různých scénářích (Continuous Presence) s možností definování vlastního rozložení obrazu.
- „Ad-hoc“ konference – eskalace dvoubodového spojení do konference více účastníků. Výběr konferenčních zdrojů v rámci sítě podle umístění účastníků – optimalizace datových toků v síti.
- Více účastnická „Rendezvous“ konference s možností ověření přístupu PINem.
- Automatické obvolání účastníků konference.
- Integraci s plánovacím systémem, vytváření schůzek v MS Outlook, a připojení na kalendářový systém MS Exchange.
- Sdílení doprovodného prezentačního kanálů v rámci konference.
- Podpora rozlišení jednotlivých účastníků v rozsahu CIF – FullHD. Přidělování kapacity konferenčních zdrojů odpovídající požadavkům rozlišení jednotlivých účastníků.
- Registrace k centrálnímu řídicímu uzlu s autentizací (SIP/TLS) a šifrování media kanálu (sRTP – AES).
- Podporu video kodeků H.264/H.263

2.8.18 Integrace s prostředím MS Lync

Pro zajištění užité hodnoty IP telefonního řešení je zajištěno centrální propojení na infrastrukturu MS Lync 2013. Propojení je obousměrné a přenáší následující služby:

- Presence (dostupnost) uživatelů a telefonních linek - na straně Lync je vidět informace "dostupný / mimo kancelář / obsazeno" z nabízeného systému. Tutéž informaci odeslanou z MS Lync je nabízený systém schopen zpracovat a prezentovat.
- Instant Messaging (textové zprávy) - přenos textových zpráv protokolem SIP/SIMPLE mezi oběma systémy.
- Hlasové volání - sestavení hlasového hovoru v kodeku G.711 u-law mezi oběma systémy. Signalizace probíhá vytvořením URI, tj. ve formátu "sip:uzivatel@pcr.cz", kde "uzivatel@pcr.cz" je e-mailová adresa uživatele tak, jak je vedena v Active Directory PČR.
- Video volání - sestavení video hovoru v kodeku H.264 SVC mezi oběma systémy. Stejně jako u hlasového hovoru je k sestavení hovoru použit formát URI. Kvalita video hovoru je v úrovni HD spojení (720p/30).

Primárním zdrojem informací o uživateli je Active Directory (dále AD), doména "pcr.cz". Systém synchronizuje uživatelské účty z AD v read-only módu. Z AD získává minimálně tyto informace:

- uživatelské jméno
- URI pro komunikaci s MS Lync

2.8.19 Systém nahrávání hovorů

Systém nahrávání hovorů splňuje následující minimální požadavky:

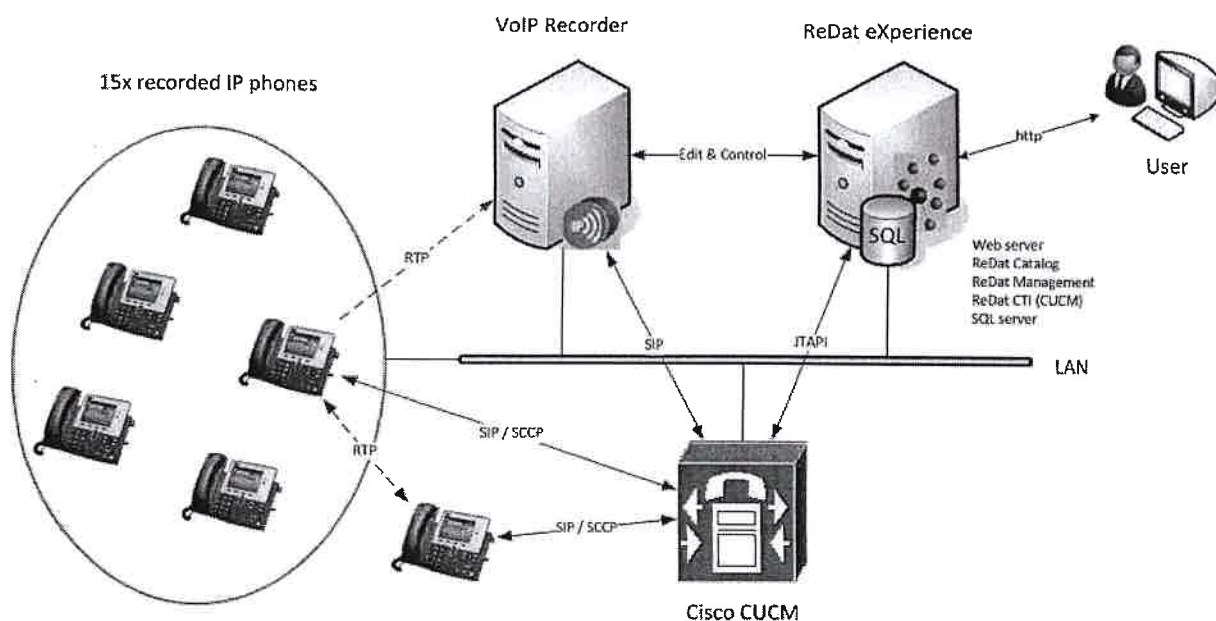
- Selektivní/volitelné nahrávání až 15 telefonů, jež bude moci vždy specifikovat administrátor dle aktuálních potřeb bez zásahu do konfigurace síťové infrastruktury
- Selektivní/volitelné nahrávání až 5 videokonferenčních spojení (dvou i více účastníků), jež bude moci vždy specifikovat administrátor dle aktuálních potřeb bez zásahu do konfigurace síťové infrastruktury. Je požadován záznam i případného doprovodného prezentačního kanálu
- Server pro správu nahraných hovorů musí umožnit hierarchické řízení oprávnění přístupu k nahrávkám
- Ukládání audio nahrávek ve formátu MP3 nebo WAV
- Ukládání video nahrávek ve formátu MPEG4 nebo Windows Media
- Nahrávání videa v rozlišení HD 720p a nižší s podporou standardu H264 a starší
- Možnost archivace záznamů lokálně v systému a možnost jejich odsunu na jiná datová úložiště dle specifikace „starší než“ nebo při překročení datového úložného objemu
- Server s lokální diskovou kapacitou pro provoz systému a nahrávané hovory s celkovou diskovou kapacitou 1TB pro záznam.
- Kompatibilita s dodávaným telefonním systémem.

- Integrace s adresářovými službami, které využívá telefonní komunikační systém pro jednotnou správu uživatelů
- Jednotné grafické uživatelské rozhraní pro uživatele i administrátory dostupné přes tenkého klienta ve webovém prohlížeči

Pro záznam hovorů je navržen systém firmy Retia. Tento systém se skládá ze dvou základních částí

- Záznamového zařízení ReDat® VoIP Recorder – zde probíhá vlastní záznam RTP streamů a CTI
- Aplikační nadstavby ReDat® eXperience – obsahující MS SQL databázi, CTI rozhraní, Apache Web server, moduly pro konfiguraci a správu uživatelů, nastavení způsobu záznamu, archivace, výběr/přehrávání záznamů atd.

Záznamové zařízení ReDat® VoIP Recorder, může být administrátorem systému nastaveno na libovolnou sadu zaznamenávaných telefonů do výše počtu licencí (celkem 15). Při změně nahrávaných telefonů dojde pouze ke změně konfigurace nastavených kanálů na záznamovém zařízení dle předem definovaných pravidel.



Pro samotný záznam hovorů bude použit tzv. aktivní způsob záznamu hovorů (neboli SPANless recording). Při použití aktivního způsobu nahrávání hovorů, není nutné konfigurovat zrcadlení VoIP provozu na LAN přepínačích. Místo toho je třeba odpovídajícím způsobem konfigurovat CUCM

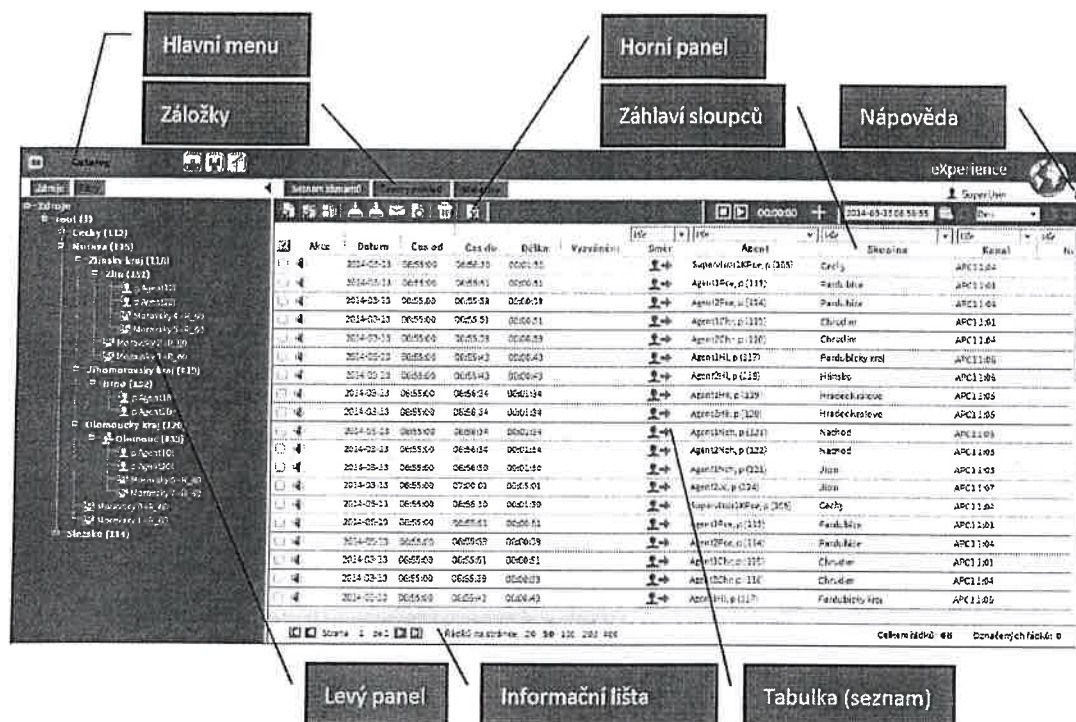
a zajistit dostatečnou IP konektivitu mezi nahrávanými IP telefony, záznamovým systémem a CUCM. To především v případě topologie zahrnující komunikaci přes WAN nebo MAN síť. Další nezbytnou podmínkou je použití IP telefonů, které aktivní způsob nahrávání podporují – jsou to modely IP telefonů Cisco tzv. 3. generace, které mají zabudovaný „built-in-bridge“ (BIB), např. telefony řady 79xx. Pro aktivní záznam se využívá funkce Cisco Call Recording. Cisco Call Recording je funkce, která je konfigurovatelná jako volitelná vlastnost konkrétní pobočky (linky), definované na CUCM (podporovaná verze 6.0 a vyšší). V případě aktivace

této funkce je při aktivním volán na nahrávané lince iniciováno ze strany CUCM spojení na přiřazeném SIP trunku, jehož druhý konec obsluhuje rekordér (ReDat® VoIP Recorder). Po úspěšném sestavení „záznamové“ relace je posílána kopie RTP streamu přímo z daného IP telefonu na IP adresu rekordéru. Funkce Cisco Call Recording nezávisí na použitém signalizačním protokolu, používaném nahrávaným telefonem (SKINNY nebo SIP).

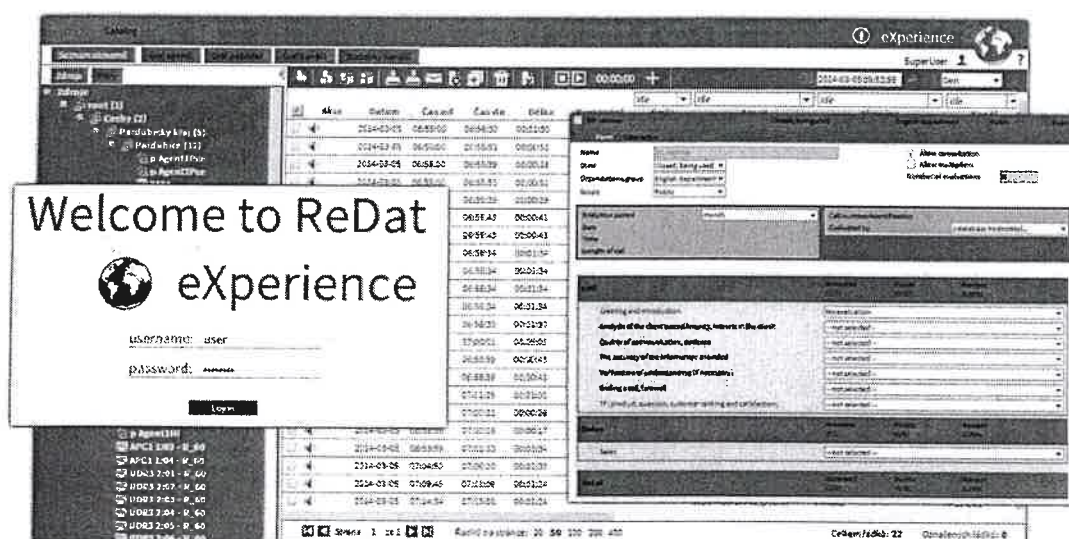
Součástí návrhu řešení je CTI integraci s platformou Cisco CUCM. CTI integrace se využívá k řízení záznamu a k zajištění informací (metadat) o jednotlivých hovorech mezi které patří: Agent (AgentID), ID nahrávky, číslo volajícího a volaného (ANI, DNIS), číslo nahrávané linky, skupina do které nahrávka spadá, datum a čas uskutečnění hovoru, délka hovoru, telefonní číslo volajícího a volaného (ANI, DNIS), a popřípadě dalších informací, které jsou dostupné ve CTI.

Všechny zaznamenané hovory (audio soubory + údaje o hovoru) jsou nejprve uloženy do dočasného úložiště na záznamová zařízení ReDat® VoIP Recorder. Následně jsou záznamy automaticky replikovány do SQL databáze a audio soubory uloženy do archivu v rámci aplikační nadstavby ReDat® eXperience na požadovanou dobu (pozn.: aplikační nadstavba ReDat® eXperience zajistí přístup k hovorům po celou dobu jejich archivace). V rámci archivace je možné nastavit úroveň komprese *.wav nebo určitou úroveň kompilace ve formátu *.mp3 (8, 12, 16, 24 a 32 kbps). Jedná se o automatický proces tvorby a ukládání *.mp3 nebo *.wav souborů na disk či externí úložiště do jednotné archivní adresářové struktury (file systém). Na tyto audio soubory je z databáze nastaven odkaz a mohou být přehrávány, stahovány na disk agentských desktopů připojených přes webový prohlížeč (např. IE, Mozilla, Google Chrome) nebo odesílány e-mailem. Archivace hovorů probíhá průběžně nebo v nastaveném časovém intervalu (konfigurovatelná vlastnost systému). Vyřazení záznamů z on-line archivu lze po uplynutí stanovené doby archivace, které lze nastavit v pravidlech retence záznamu (nastavení podmínek dle příznaků dostupných v listu záznamů) nebo naplněním kapacity úložiště. Ve výchozím nastavení systému se standardně záznamy (hovory) archivují až do naplnění datové kapacity archivu, poté jsou nejstarší hovory nahrazovány novějšími.

Součástí dodávky je aplikační nadstavba ReDat® eXperience včetně všech potřebných licencí. Jedná se o jednoduché grafické uživatelské rozhraní, které zajišťuje přístup k záznamům přes webové rozhraní (tenký (http) klient).



Aplikační nadstavba je přístupná přes internetové prohlížeče (IE v.11, Mozilla Firefox verze ESR nebo Google Chrome) a dále prostřednictvím hierarchických přístupových práv a uživatelských profilů.



Záznamový systém ReDat® podporuje integraci se systémy pro jednotnou správu uživatelů LDAP a AD. Tímto se snižuje náročnost na správu uživatelských účtů a jejich synchronizaci s ostatními systémy. Systém podporuje nahrávání šifrovaných hovorů.

Pro záznam videokonferenčních hovorů je navržen systém firmy Cisco. Navrhovaný systém splňuje požadavky.

2.8.20 Tarifikační systém

Součástí dodávky telefonního systému je systém pro tarifikaci a hovorů pro všechny telefony nového telefonního systému PČR Plzeň. Systém plně splňuje zadání a bude dodán

včetně serverové kapacity s lokální diskovou kapacitou pro provoz systému a ukládání tarifikačních dat.

Tarifikační systém splňuje následující požadavky:

- Tarifikaci na úrovni koncového uživatele IP telefonu s danou linkou
- Souhrnnou tarifikaci na úrovni oddělení, do kterého patří daná linka
- Souhrnnou tarifikaci na úrovni pobočky/lokality
- Možnost rozlišení hovorů na pracovní a soukromé
- Import dat a účetních sestav od operátorů mobilních sítí a přiřazení hovorů k lokálním uživatelům telefonního systému
- Tarifikační software musí umožnit hierarchické řízení přístupu k datům
- Integrace s adresářovými službami, které využívá telefonní komunikační systém pro jednotnou správu uživatelů
- Jednotné grafické uživatelské rozhraní pro uživatele i administrátory dostupné přes tenkého klienta ve webovém prohlížeči
- Export dat pro centrální tarifikační systém Ministerstva Vnitra ve formátu CSV