

## POŽADAVKY NA AKTIVNÍ PRVKY A FUNKCIONALITY GDS TYPOVÉ LOKALITY

### 1 IP/MPLS páteřní infrastruktura GDS

Základem jsou IP/MPLS servisní směrovače, které umožní zpřístupnění technologické výhody servisního směrování napříč celou komunikační sítí. Zároveň umožní realizaci poskytovaných služeb využívající IP technologií pro různé typy koncových uživatelů a to od neutajených multimediálních dat až po data utajovaná hardwarovými šifratory.

Navrhované IP/MPLS servisní směrovače musí primárně vyhovovat potřebám pro realizaci služeb určených pro kritické komunikační aplikace.

Servisní směrovače musí vytvářet plně konvergentní, škálovatelnou, IP víceúčelovou infrastrukturu, která umožní poskytovat síťový provoz spolehlivěji, efektivněji, s výrazně nižšími náklady.

Servisní směrovače musí poskytovat datovou propustnost minimálně 80 Gbit/s (half duplex) prostřednictvím různých typů Ethernet, E1/E3 rozhraní až do rychlostí 10Gbit s podporou důkladně propracovaného řízení Quality of Service (QoS), s vysoce škálovatelným ovládáním a nativní hardwarovou podporou IPv6. Současně musí nabízet funkce pro vysokou dostupnost zahrnující bez výpadkové směrování (NSR), bez výpadkové poskytování služeb (NSS), Multi-link PPP, zálohování pseudo-linek, podporu široké škály IP funkcí (blíže upřesněno ve specifikačních listech jednotlivých zařízení), TDM, L2 protokolů a různých typů Ethernet rozhraní.

IP/MPLS servisní směrovače musí být plně říditelné prostřednictvím dohledového systému, který musí poskytovat integrovanou správu sítě a služeb s cílem zajistit hladký provoz, administraci, zjednodušené řízení a sjednocení poskytovaných služeb.

IP/MPLS servisní směrovače jsou požadovány dodat ve dvou variantách:

- Páteřní IP/MPLS servisní směrovač – P1-MPLS a P2-MPLS.
- Koncový IP/MPLS servisní směrovač – P3-MPLS.

#### 1.1 Páteřní IP/MPLS P servisní směrovač – P1-MPLS a P2-MPLS

Jedná se o směrovač plnící funkci MPLS P směrovače v páteřní síti GDS. Požadavky na základní funkce a vlastnosti P směrovače v infrastruktuře GDS:

- podpora rozhraní 100 / 1 000 Mbps,
- podpora rozhraní 10 Gigabit Ethernet (10 GE),
- podpora WAN rozhraní STM1, E1, E3,
- Hot-swap redundantní zdroj n+1,

- Hot-swap ventilátory,
- redundantní procesorová jednotka,
- základní směrování v připojených LAN sítích,
- podpora technologie MPLS, VPLS, Q-in-Q
- ověření identity dle standardu 802.1X,
- ve spolupráci s IDS/IPS systémem omezit provoz na portech generujících nežádoucí provoz,
- označit (otagovat) provoz dle MPLS standardu.

IP/MPLS servisní router musí pracovat v režimu „Non-Stop routing“ a „Non-Stop Services“. To znamená, že duplikovaný systém musí být plně redundantní a při výpadku jednoho nesmí dojít k rekalkulaci směrovacích tabulek ani služeb konfigurovaných na zařízení (VPLS, VPRN,...).

Routování v IP-MPLS síti bude pro jednotlivé VPN zabezpečovat BGP/MPLS dle doporučení RFC 2547.

Případný update softwaru musí být aplikovatelný bez restartu zařízení.

IP/MPLS servisní přepínač musí umožňovat souběžně pracovat jako service router (PE-router) a zároveň jako MPLS router (P-router).

## **1 Přístupová IP/MPLS infrastruktura**

### **2.1 Koncový IP/MPLS servisní směrovač – P3-MPLS**

Jedná se o směrovač plnící funkci MPLS P směrovače v páteřní síti GDS. Požadavky na základní funkce a vlastnosti MPLS P směrovače v infrastruktuře GDS:

- podpora rozhraní 100 / 1 000 Mbps,
- podpora rozhraní 10 Gigabit Ethernet (10 GE),
- podpora WAN rozhraní STM1, E1, E3,
- Hot-swap redundantní zdroj n+1,
- Hot-swap ventilátory,
- základní směrování v připojené LAN síti,
- podpora technologie MPLS, VPLS, Q-in-Q,
- ověření identity dle standardu 802.1X,
- přidělení práv uživateli dle informací z AAA serveru,
- ve spolupráci s IDS/IPS systémem omezit provoz na portech generujících nežádoucí provoz,
- označit (otagovat) provoz dle MPLS standardu.

Případný update softwaru musí být aplikovatelný bez restartu zařízení.

IP/MPLS servisní přepínač musí umožňovat souběžně pracovat jako service router (PE-router) a zároveň jako MPLS router (P-router).

## **2 LAN a MAN infrastruktura GDS**

### **2.1 LAN infrastruktura**

Přístupové L2 přepínače LAN jsou základním přístupovým prostředkem pro vstup do sítě GDS. Musí proto zabezpečit pro koncové uživatele následující portfolio služeb:

- přenosovou rychlost 10/100/1000 Mbps po standardním metalickém UTP/FTP kabelu do vzdálenosti minimálně 90m od aktivního prvku nebo univerzální konektivitu pro připojení optických vláken,
- napájení dle standardu 802.3af/802.3at,
- ověření identity dle standardu 802.1X,
- přidělení práv uživateli dle informací z AAA serveru,
- ve spolupráci s IDS/IPS systémem omezit provoz na portech generujících nežádoucí provoz,
- označit (otagovat) provoz dle standardů 802.1Q, 802.1p/TOS/DSCP,
- umožnit oddělení specifického provozu pomocí Q-in-Q protokolu.

Požadujeme plně propustné přístupové LAN přepínače ve stohovatelném provedení (stack) ve třech provedeních – malý, velký a optický. Malý přepínač musí podporovat minimálně 20 metalický portů RJ45, velký přepínač minimálně 40 metalických portů RJ45. Optický přepínač musí podporovat minimálně 20 univerzálních portů pro připojení optických kabelů.

### 2.1.1 Interkonektivita uvnitř LAN sítě

V rámci LAN infrastruktury musí být možné navrhnout následující varianty topologií:

- Varianta č. 1 – Hvězdicová topologie.  
Přepínače propojeny optickými kabely o minimální rychlosti 2x1 Gbps. Obě linky budou v agregaci. Ochrana proti smyčkám dle normy 802.1w (RSTP).
- Varianta č. 2 – Kombinovaná topologie.  
Přepínače propojeny optickými kabely o minimální rychlosti 1 Gbps. Pokud se použije konektivita 2x 1Gbps obě linky budou agregovány. Ochrana proti smyčkám dle normy 802.1Q (MSTP).
- Varianta č. 3 – Kombinace výše uvedených.  
Jedná se především o kombinaci varianty č. 1 s výše uvedenými. Ochrana proti smyčkám dle normy 802.1Q (MSTP).

Ve výše uvedených topologiích využít v maximální míře a tam, kde je to účelné, funkci stohování aktivních prvků.

### 2.1.2 Konektivita do GDS

LAN infrastruktura může být připojena do GDS dvěma způsoby:

- Připojení k IP-MPLS servisnímu směrovači (router).  
Konektivita je realizována přes hraniční L2 přepínač metalickým/optickým propojem o rychlosti 1x10Gbps.
- Připojení do MAN sítě.  
Pro připojení do MAN sítě se používá hvězdicová topologie, kdy ve středu je umístěn L3 přepínač. Přepínače propojeny optickými kabely o minimální rychlosti 2x10 Gbps. Obě linky budou agregovány. Ochrana proti smyčkám dle normy 802.1w (RSTP).

### 2.1.3 Základní parametry zařízení LAN-ACC

- minimální počet přepínačů ve stohu je 5, konfigurací lze určit, kdo bude hlavním přepínačem,
- minimální fyzická přenosová rychlost v rámci stohu (stacku) je 2x 10 Gbps,

- v rámci stohu jednotný management, jedna IP a MAC adresa, která je zachována i v případě změny hlavního přepínače,
- vytváření stohu lokálně, ale i pomocí optických kabelů s možností použít MM nebo SM vláken,
- všechny provedení (optický, malý, velký) lze ve stohu kombinovat,
- napájecí napětí 230V/50Hz,
- redundantní napájení řešit samostatným zdroji pro každý přepínač nebo pomocí centrálního napájecí vany. Vana musí umožňovat zálohování N+1 a N+N (dvě oddělené sítě),
- napájení PoE/PoE+ pro jednotlivé porty,
- dynamické přidělování VLAN dle definovaných pravidel a přidělení z AAA serveru,
- možnost volby přenosové rychlosti uplinku - 1Gbps a 10 Gbps,
- minimální počet linek pro uplink je 2,
- pro zabránění smyček na druhé vrstvě bude použit MSTP dle standardu 802.1s,
- pro připojení kritické infrastruktury (např. servery) bude použit protokol VRRP dle RFC 2338 (VRRP) a RFC 2787 (Definitions of Managed Objects for the Virtual),
- vytváření agregovaných linek dle 802.3ad,
- podpora multicast,
- zrcadlení provozu z předem definovaných portů na interní paměť nebo po síti,
- certifikace dle standardu MEF 9 a MEF 14.

#### 2.1.4 Záložní napájení

Přístupové LAN přepínače jsou děleny do dvou kategorií:

- Krizové přepínače.
- Standardní přepínače.

U krizových LAN přepínačů požadujeme zabezpečit nepřetržité napájení po dobu 6 hodin. Standardní přepínače jsou vybaveny zálohou 20 minut.

Rozdělení přepínačů/lokalit je uvedeno v příloze čj. D31/2013-1341.

## 2.2 MAN infrastruktura

Pro zabezpečení komunikačních služeb v rozsáhlých lokalitách, je nutné vybudovat MAN infrastrukturu. Pro vytvoření MAN infrastruktury požadujeme plně propustné L3-METRO přepínače ve stohovatelném provedení (stack) ve dvou provedeních – malý, velký. Malý přepínač musí podporovat minimálně 20 univerzálních portů 10 Gbps a velký přepínač minimálně 40 univerzálních portů 10 Gbps.

MAN infrastruktura zabezpečuje následující portfolio služeb:

- směrování provozu dle směrovacího protokolu OSPF v2,
- univerzální rozhraní pro připojení zařízení o přenosové rychlosti 1/10 Gbps,
- ověření identity dle standardu 802.1X,
- přidělení práv uživateli dle informací z AAA serveru,
- ve spolupráci s IDS/IPS systémem omezit provoz na portech generujících nežádoucí provoz,
- označit (otagovat) provoz dle standardů 802.1Q, 802.1p/TOS/DSCP,
- oddělit specifický provoz pomocí Q-in-Q protokolu.

MAN infrastruktura bude založena na optickém propojení přes SM optické kabely o minimální rychlosti 2x10 Gbps. Předpokládáme, že maximální délka optických spojů nepřesáhne 40km.

MAN infrastruktura bude připojena přímo do IP/MPLS sítě pomocí páteřních IP/MPLS P směrovačů. Minimální rychlost připojení do IP-MPLS sítě je 1x10Gbps.

MAN infrastruktura je tvořena dvěma druhy zařízení:

- koncový MAN směrovač zabezpečující připojení LAN sítí,
- centrální MAN směrovač zabezpečující propojení jednotlivých LAN sítí a připojení do IP/MPLS sítě.

Pro zvýšení bezpečnosti celého řešení, bude centrální přepínač standardně zdvojen a propojen do stohu (stack). Předpokládáme, že každý z dvojice může být umístěn v rozdílných lokalitách. Pro propojení obou centrálních přepínačů požadujeme minimální rychlost 10Gbps pro malé lokality a 40Gbps pro velké lokality.

Na koncovém MAN směrovači budou ukončeny i zařízení zabezpečující IP ekosystém, případně IP hlasová brána.

### **2.2.1 Inter konektivita uvnitř MAN sítě**

V rámci MAN infrastruktury musí být možné navrhnout následující varianty topologií:

- Varianta č. 1 – kruhová topologie.  
Přepínače propojeny do kruhu o minimální rychlosti 1x 10Gbps. Pokud se použije konektivita 2x 10 Gbps obě linky budou agregovány. Ochrana proti smyčkám bude zabezpečena pomocí Ethernet Ring Protection Switching popsané v doporučení G.8032v1 nebo G.8032v2.
- Varianta č. 2 – Hvězdicová topologie.  
Přepínače propojeny optickými kabely o minimální rychlosti 2x10 Gbps. Obě linky budou v agregaci.
- Varianta č. 3 – kombinace výše uvedených. Ochrana proti smyčkám dle normy 802.1w (RSTP).

### **2.2.2 Konektivita do IP-MPLS**

MAN infrastruktura je připojena do páteřního IP-MPLS přepínače metalickým/optickým propojem o rychlosti nejméně 1x10Gbps.

### **2.2.3 Základní parametry zařízení MAN-ACC a MAN-CORE**

- minimální počet přepínačů ve stohu je 2, konfigurací lze určit, kdo bude hlavním přepínačem,
- minimální fyzická přenosová rychlost v rámci stohu (stacku) je 2x 10 Gbps MAN ACC a 2x 40 Gbps pro MAN-CORE,
- v rámci stohu jednotný management, jedna IP a MAC adresa, která je zachována i v případě změny hlavního přepínače,
- vytváření stohu lokálně, ale i pomocí optických kabelů s možností použít MM nebo SM vláken s maximální vzdáleností do 40km,
- všechny provedení (optický, malý, velký) lze ve stohu kombinovat,
- napájecí napětí 230V/50Hz,
- redundantní napájení řešit samostatným zdroji pro každý přepínač nebo pomocí centrálního napájecí vany. Vana musí umožňovat zálohování N+1 a N+N (dvě oddělené sítě),
- dynamické přidělování VLAN dle definovaných pravidel a přidělení z AAA serveru,
- možnost volby přenosové rychlosti uplinku – 1Gbps, 10 Gbps, 40Gbps ,
- minimální počet linek pro uplink je 2,
- pro připojení kritické infrastruktury (např. servery) bude použit protokol VRRP dle RFC 2338 (VRRP) a RFC 2787 (Definitions of Managed Objects for the Virtual),
- vytváření agregovaných linek dle 802.3ad,
- podpora multicast,

- zrcadlení provozu z předem definovaných portů na interní paměť nebo po síti,
- certifikace dle standardu MEF 9 a MEF 14.

#### **2.2.4 Záložní napájení**

MAN infrastruktura je vždy brána jako infrastruktura krizová. Proto musí být u MAN infrastruktury zabezpečeno nepřetržité napájení po dobu 6 hodin.

## **3 Hlasový systém GDS**

### **3.1 Cíl obměny hlasových služeb**

Vybudovat komunikační infrastrukturu s využitím společných služeb. Pro realizaci projektu je kladen důraz na:

- vysokou dostupnost služeb celého řešení,
- komplexnost a škálovatelnost služeb,
- vysoký stupeň zabezpečení budované infrastruktury a služeb,
- zabezpečit hlasové služby pro vojenské mise AČR,
- propojení na rezortní a mezirezortní sítě a do sítí veřejných poskytovatelů hlasových služeb.

Řešení musí obsahovat vyjmenovaný seznam uživatelských a infrastrukturních služeb v oblasti společných služeb. Zejména se jedná o kategorie:

- služby hlasu a videa,
- služby mobility uživatelů,
- nástroje pro spolupráci uživatelů a sdílení dokumentů a informací v rámci týmů.

### **3.2 Způsob řešení**

#### **3.2.1 Architektura**

Požaduje se nasazení řešení komunikační infrastruktury s centrální správou ale s decentralizovaným zpracováním hovorů ve více lokalitách, propojených IP WAN sítí (MPLS) s využitím přístupů do veřejné telefonní sítě. Řešení musí zajišťovat pro rezort následující základní služby:

- vysoce dostupnou unifikovanou hlasovou komunikaci,
- jednotnou sadu služeb dostupnou uživatelům v rámci celého resortu,
- přenositelnost čísla a uživatelských služeb v rámci resortu,
- centralizovanou správu systému,
- centralizovanou hlasovou poštu,
- centralizovanou faxovou službu,
- centrální audio a video konferenční systém.

Lokality instalace budou rozčleněny do čtyř typů:

- Lokalita A – součást krizové infrastruktury.
- Lokalita B – zabezpečující útvary.
- Lokalita C – výcvikové základny.
- Lokalita D – ostatní.

### **3.2.1.1 Lokalita A – nejvyšší důležitost.**

Požadujeme nezávislý prvek pro spojování hovorů (Řídící Server Hlasových Služeb – RSHS), který zajistí plné služby pro místní účastníky i při výpadku konektivity směrem do WAN sítě. V takovém případě nesmí dojít k přerušení již navázané místní komunikace. Výpadkem mohou být dotčeny pouze některé centralizované služby (hlasová pošta...). Veškeré informace o voláních musí zůstat zachovány a po obnovení přenosového prostředí přeneseny do centrálního tarifikačního systému.

Řešení musí také zajistit plné služby v případě poruchy tohoto nezávislého prvku. V síti WAN nebo LAN musí existovat nejméně jeden dostupný prvek o stejné funkcionalitě, který je schopen bez přerušení již navázané komunikace plně převzít roli porouchaného prvku.

Lokalita musí být připojena nejméně dvěma nezávislými technologiemi s dalšími prvky sítě.

Hlavním přenosovým prostředím pro přenos je IP prostředí (protokol H323, SIP). Záložním prostředím je TDM prostředí (E1 rozhraní využívající TDM), které je zabezpečenou rozhraními nainstalovanými na hlasové bráně. Kapacita záložního spoje je rovná ½ kapacity hlavního přenosového toku. Pro záložní spojení se používá rozhraní PRI se signalizací QSIG-GF/SS.

Pro připojení do veřejné telefonní sítě nebo pro připojení do jiných privátních sítí se používá rozhraní PRI se signalizací EuroISDN, respektive QSIG-GF/SS.

### **3.2.1.2 Lokalita B – vysoká důležitost.**

Požadujeme instalaci pomocného serveru pro spojování hovorů (Pomocný Řídící Server Hlasových Služeb – RSHS), který zajistí plné služby pro místní účastníky i při výpadku konektivity směrem do WAN sítě. V takovém případě může dojít k přerušení již navázané místní komunikace. Výpadek lokálních služeb nesmí přesáhnout 1 minutu. Dále mohou být výpadkem dotčeny pouze centralizované služby (hlasová pošta...). Veškeré informace o voláních musí zůstat zachovány a po obnovení přenosového prostředí přeneseny do centrálního tarifikačního systému.

Lokalita musí být připojena nejméně dvěma nezávislými technologiemi s dalšími prvky sítě.

Hlavním přenosovým prostředím pro přenos je IP prostředí (protokol H323, SIP). Záložním prostředím je TDM prostředí (E1 rozhraní využívající TDM), které je zabezpečenou rozhraními nainstalovanými na hlasové bráně. Kapacita záložního spoje je rovná ½ kapacity hlavního přenosového toku. Pro záložní spojení se používá rozhraní PRI se signalizací QSIG-GF/SS.

Pro připojení do veřejné telefonní sítě nebo pro připojení do jiných privátních sítí se používá rozhraní PRI popřípadě BRI se signalizací EuroISDN, respektive QSIG-GF/SS.

### **3.2.1.3 Lokalita C – nižší důležitost.**

Požadujeme instalaci pomocného serveru pro spojování hovorů (Pomocný Řídící Server Hlasových Služeb – RSHS), který zajistí plné služby pro místní účastníky i při výpadku konektivity směrem do WAN sítě. V takovém případě může dojít k přerušení již navázané komunikace.

Jediným přenosovým prostředím pro přenos je IP prostředí (protokol H323, SIP). Pro připojení do veřejné telefonní sítě nebo pro připojení do jiných privátních sítí se používá rozhraní PRI popřípadě BRI se signalizací EuroISDN, respektive QSIG-GF/SS.

#### 3.2.1.4 Lokalita D – ostatní.

Pro lokalitu je řešeno v rámci GDS pouze rozhraní, kterým bude zabezpečena konektivita. Typ a počet rozhraní je uveden v samostatné tabulce.

### 3.2.2 Kapacitní plánování

V rámci budování komunikační infrastruktury bude vybudovaná hlasová síť o maximálním počtu 30 000 účastníků. Z tohoto počtu bude 58% analogových portů tj. 17 000. Zbývajících počet tj. 13 000 poboček jsou IP nebo SIP telefony.

Při kalkulaci zatížení je nutné vycházet z následujících zatížení:

- Dělení koncových zařízení dle hlasového provozu:

- Nízký 0,1 E (Erlang)
- Standard 0,16 E
- Vysoký 0,25 E

- Ostatní:

- Standardní příčka 0,7 E
- Pracoviště spojovatelky 1 E

- Hlasová brána (Media Gateway):

- Interní provoz 34%
- Vnější provoz 66%

Pro monitoring hovorů je nutné garantovat zdroje tak, aby bylo možné současně monitorovat minimálně 50 hovorů. Při výpočtu zatížení je nutné kalkulovat, že každá hlasová brána musí umožnit záznam pěti koncových zařízení současně.

Centralizovaná hlasová pošta – centralizovaný model bude dostupný pro 50% z celkového počtu účastníků. Každý účastník hlasové schránky má k dispozici 1 hodinu záznamového prostoru. Celkový počet současných přístupů do hlasové pošty je nejméně 32.

Centrální správa hlasového systému – bude dostupná v rámci celé hlasové sítě. Software musí umožnit správu všech koncových zařízení v síti. Diskové pole pro tarifikační údaje musí mít kapacitu pro uložení informací o hovorném zpětně za 1 rok. Do systému lze současně přistupovat minimálně pěti správci současně. Centrální telefonní seznam mohou využívat současně všichni uživatelé hlasové sítě GDS.

Centralizovaná faxová služba – bude dostupná v rámci celé hlasové sítě. Ve faxovém serveru v režimu HA bude možné zřídit minimálně 1 000 faxových čísel. Celkový počet současně přijímaných faxů je nejméně 20. Každý uživatel má k dispozici k archivaci minimálně 1 000 faxových stránek.

Centralizovaný audiokonferenční systém – řešení poskytuje současně vytvoření pěti střetávacích a dvou dispečerských konferencí na každém uzlu A. V každé audiokonferenci může být minimálně 20 uživatelů.

Centralizovaný videokonferenční systém – řešení poskytuje současně vytvoření pěti videokonferencí. V každé videokonferenci může být maximálně 20 uživatelů v HD kvalitě.



U všech systémů a služeb se požaduje garance možnosti navyšování kapacity postupným přidáváním jak uživatelských licencí, tak i HW zdrojů pro pokrytí výkonnostních požadavků. Toto navyšování však není součástí této veřejné zakázky.

### **3.2.3 Dostupnost**

Požaduje se řešení, které poskytuje službu s vysokou úrovní dostupností služeb:

- Rozdělit řízení hlasových služeb dle geografických pravidel. Eliminovat zátěž způsobenou centralizací na minimum.
- Centrální systémy a služby realizovat ve virtualizovaném prostředí s vysokou dostupností. (předpokládá se využití dvou datových center).
- Při výpadku jednoho datového centra přechází služba automaticky na datové centrum záložní.
- HW platformy virtualizačních serverů musí obsahovat prvky vysoké dostupnosti (zdvojení napájecích zdrojů, pevných disků, procesorů a síťových karet).
- V případě výpadku IP konektivity z lokality do centra, musí Analogové i IP telefony přejít na záložní systém, a to tak, že zůstane zachován číslovací plán s možností využití záložních linek a dostupností lokálních služeb.

### **3.2.4 Řízení využití přenosové kapacity (Call Admission Control – CAC)**

- Pobočková komunikace v koncové lokalitě prochází v prostředí IP/LAN a musí umožnit kódování protokolem G. 711 nebo G. 722.
- Komunikace mezi lokalitami využívá privátní IP/WAN propojení, s možností použití privátní nebo veřejné telefonní sítě. Komunikace musí umožňovat kódování protokolů G. 711, G. 722, G. 723, G. 729.
- Využívání obou přenosových technologií (IP a TDM) je dáno okamžitým vytížením/využitím přenosových kapacit. Požaduje se řízená optimalizace hlasových toků s centrální správou.
- Využití více komunikačních cest (rozložení zátěže a záložní trasy) s různou přenosovou kapacitou.

## **3.3 Vlastnosti hlasového systému GDS**

### **3.3.1 Základní vlastnosti hlasového systému**

Hlasový systém musí splňovat následující základní vlastnosti:

- musí se chovat jako homogenní celek, musí mít možnost jednoduché centrální správy a dohledu na jedné platformě,
- musí umožňovat centralizované, a jednoduše zpracovatelné vyhodnocení nákladů na hovorné za volání do veřejných telefonních sítí.

#### **3.3.1.1 Základní systémové služby**

- centralizovaná správa hlasového systému,
- zasílání SNMP trapů (min verze 2) v reálném čase,
- terminálová správa nezávislá na IP infrastruktuře,
- přenos incidentů při výpadku běžné konektivity tam, kde je záložní přenosové prostředí,
- záznam všech hovorů do centrálního tarifikačního systému (příchozí, odchozí, vnitřní, vnější),
- možnost trasování hovorů a signalizace,
- kategorie účastníka pro omezení přístupu do VTS, na příčkové spoje nebo mezi koncovými účastníky,
- možnost ochrany před přesměrováním trunk-trunk,
- použití direct RTP/SRTP,

- potlačení echa a detekce hlasu (VAD),
- identifikace zlomyslného volání a jeho trasování.
- vyhodnocování kvality IP hovorů na základě IP tiketů RTCP protokolu.

### **3.3.1.2 Základní uživatelské služby**

- Integrace – předávání hovorů mezi pevnou linkou a mobilním přístrojem v rámci mobilních čísel VPN AČR.
- Integrace pracovních stanic a telefonního přístroje pomocí klientské SW aplikace zajišťující přístup ke službám hlas, video, IM, konference, sdílení dokumentů.
- Služba jedno telefonní číslo – dosažitelnost účastníka jedním číslem (jménem) v rámci resortní sítě a sítě mobilních telefonů VPN AČR.

## **3.3.2 Bezpečnost**

Řešení bezpečnosti hlasové infrastruktury dělíme do následujících částí.

### **3.3.2.1 Management a údržba hlasové infrastruktury**

Přístup do centrální databáze je ověřován přes centrální AAA server. Uživatelé jsou rozděleni do skupin, kdy každá skupina má přístup do předem definovaných částí hlasového systému. Připojení k systému je realizováno pomocí zabezpečeného připojení. Pro CLI se požaduje využívat SSHv2 pro web připojení SSLv2/v3.

Veškeré činnosti provedené v centrální databázi nebo přes CLI jsou logovány a přehledně zobrazeny v jednotném grafickém rozhraní. V logu musí být uvedeno, kdo (jméno z Rádus serveru), kdy a co prováděl při práci se systémem.

### **3.3.2.2 Ověřování přístupu IP koncových zařízení**

Přístup koncových IP zařízení je řešen pomocí 802.1X MD5/TLS. Jednotlivá koncová zařízení jsou vybavena certifikátem, který je následně ověřen na AAA serveru. Zároveň AAA server předá koncovému aktivnímu prvku informaci, do které skupiny uživatelů zařízení patří.

### **3.3.2.3 Šifrování signalizace a hovoru IP koncových zařízení**

IP komunikace (signalizace, hlas) z IP koncového zařízení nebo IP hlasové brány musí být zabezpečena minimálně pomocí symetrické blokové šifry AES 128.

### **3.3.2.4 Monitoring hovorů**

Pro potřeby speciálních složek musí být systém připraven k monitoringu hlasové komunikace libovolných koncových zařízení instalovaných v rámci hlasového systému. Monitorovací rozhraní musí být kompatibilní dle ETSI ES 201671 a musí umožňovat zadávání nahrávání dle HI1 a nahrávání hovorů na úrovni HI2 a HI3.

## **3.3.3 Číslovací plán**

### **3.3.3.1 Interní číslovací plán**

Řešení musí umožňovat tvorbu homogenního číslovacího plánu, který musí být spravovaný z jednoho místa a dostupný v rámci interního telefonního seznamu.

U hlasového systému požadujeme implementaci nového číslovacího plánu, který odpovídá normě STANAG 4705 (International Network Numbering for Communications Systems in use in NATO) při zachování stávajících číslovacích plánů v jednotlivých lokalitách.

### **3.3.3.2 Dostupnost krizových linek**

Dostupnost krizových linek (112, 150, atd.) musí být zajištěna nejbližší hlasovou branou v lokalitě uživatele. V případně nedostupnosti, pak nejbližší možnou nebo centrální hlasovou bránou. Identifikace volajícího musí být zachována a předána operátorovi veřejné telefonní sítě.

### **3.3.3.3 Identifikace hovorů**

Řešení musí umožnit zachování i modifikaci čísla volajícího pro příchozí i odchozí hovory. Maskování musí být podporováno pro jednotlivé telefonní přístroje, linky a pro skupiny linek příslušné lokalitě nebo organizačnímu celku.

### **3.3.4 Uživatelské služby hlasového systému**

Požaduje se implementace následujícího minima služeb pro všechny uživatele:

- sestavení a přijetí hovoru,
- zobrazení jména a čísla volajícího (CLIP),
- přepojení hovoru,
- dotazovací volání (střídání hovorů),
- opakovaná volba posledního čísla (redial),
- napojení do hovoru,
- automatické zpětné volání na obsazeného účastníka, příčku,
- čekání na obsazené stanici,
- přesměrování hovorů,
- parkování hovorů,
- skupinové převzetí hovoru,
- personální konferenční hovory (3 cestné),
- zachycení zlomyslného volání,
- systémové uzamčení stanice pro zabránění volání na zpoplatněné příčky,
- prioritní volání,
- osobní adresář,
- rozdílné vyzvánění pro identifikaci vnějšího, vnitřního volání,
- hlasoví průvodci pro použití systémových služeb a hudba v přídrží,
- dvoujazyčná jazyková podpora pro informace na displejích a hlasové průvodce (angličtina čeština).

Pro vyčleněné přístroje další funkce a služby:

- více linek na jednom koncovém přístroji (vícelinková stanice),
- dohled koncových přístrojů a příček,
- ředitelsko-sekretářské soupravy v provedení 1+1, 1+5, 5+5
- historie volání,
- centrální spojovatelské pracoviště,
- hotelové a nemocniční služby,

- využívání centrálního telefonního seznamu z integrované klávesnice přístroje,
- integrace telefonních služeb do systému sjednocené komunikace Microsoft Lync a Microsoft Outlook.

## 4 Centrální služby

Kromě služeb poskytovaných na koncových přístrojích bude hlasový systém poskytovat následující centrální služby.

### 4.1 Centralizovaná správa hlasového systému

Centralizovaná správa systému musí obsahovat:

- grafický management účastníků,
- ověřování přístupu k managementu dle RADIUS serveru,
- sběr chybových hlášení,
- grafická prezentace stavu hlasové sítě,
- zpracování a prezentace provozu na zpoplatněných linkách,
- vyhodnocování zatížení celého systému (Past Time Performance):
  - o zpracování informací o zatížení hlasové sítě,
  - o vyhodnocování kvality IP hovorů na základě IP tiketů RTCP protokolu,
- centrální telefonní seznam,
- přehledný systém o managementu,
- zálohování databází ze všech součástí hlasového systému,
- SNMP rozhraní pro připojení k nadřazenému dohledovému systému.

Každý správce systému má přístup jen k části, která je v jeho působnosti.

Veškerý management je zaznamenáván a lze jej zobrazit na jednom zobrazovacím zařízení.

Jsou sbírány informace o standardním hlasovém provozu a o kvalitě hovoru přes IP síť. Na serveru jsou zpracovány a zobrazeny v přehledných reportech, které zobrazují reálný stav hlasové i datové sítě. Dle požadavků lze reporty modifikovat popřípadě vytvářet zcela nové.

### 4.2 Faxový server

Požadujeme aby použitá technologie umožňovala nasazení čistě softwarového řešení fax serveru v HA provedení integrujícího technologie VoIP a T.38. Řešení musí být integrováno do nové hlasové sítě pomocí IP protokolu s možností dalšího rozšiřování. Faxové servery budou nainstalovány na virtualizovaných serverech umístěných ve dvou oddělených datových centrech.

Faxy lze zasílat z různých uživatelských rozhraní. Příchozí faxy lze směřovat podle různých pravidel na dané uživatele, kteří mohou být dále vyrozuměny různými způsoby.

Základní vlastnosti:

- podporuje protokol SIP/T.38 bez požadavku na speciální hardware (karty),
- podporuje faxy G3 a přenosovou rychlost až 14.4kbps,
- umožňuje zasílání faxů (uživatelská rozhraní):
  - o odkudkoliv přes zabezpečený webový přístup (HTTPS) – uživatelské webové rozhraní,
  - o z klienta Microsoft Outlook (SMTP),
  - o z jakékoliv aplikace přes vlastní virtuální faxovou tiskárnu (Print to Fax),

- umožňuje příjem faxů (notifikace):
  - o do webového rozhraní uživatele,
  - o do emailové schránky uživatele,
  - o tisk na síťovou tiskárnu,
- zajišťuje správu serveru odkudkoliv přes zabezpečený webový přístup (HTTPS),
- konfigurace serveru pro vysokou dostupnost (High Availability) N+1.

### 4.3 Hlasová pošta

Požadujeme nasazení čistě softwarového řešení hlasové pošty integrujícího technologii VoIP. Řešení musí být integrováno do nové hlasové sítě pomocí IP protokolu s možností dalšího rozšiřování.

Server hlasové pošty bude instalován na virtualizovaném serveru v centrálním hlasovém serveru.

Základní vlastnosti:

- standardní záznamník se záznamem časového razítka a identifikace volajícího,
- záznam probíhající konverzace – dostupné z IP telefonů,
- komprese záznamu,
- přeposlání záznamu emailem,
- personifikace záznamníku.

### 4.4 Audiokonferenční systém

Audiokonferenční systém je plně integrován do hlasového systému. Systém musí umožňovat následující konference:

- střetávací konference pro minimálně 20 současných účastníků,
- dispečerské konference pro minimálně 20 současných účastníků.

Střetávací konference musí být možné aktivovat z libovolného koncového přístroje nebo mobilního telefonu.

Dispečerskou konferenci je možné aktivovat z IP telefonů. Jednotlivé uživatele lze přidávat, ubírat popřípadě volat z předdefinovaných seznamů.

### 4.5 Videokonferenční systém

Řešení musí poskytovat video služby v rámci jediného, společného číslovacího plánu. Řešení musí umožnit nasazení video konferenčních prostředků (MCU) pro více bodové video spojení. Koncové terminály pro videokonferenční služby bude možno zaregistrovat do systému jako běžného účastníka s telefonním číslem.

Centralizovaný videokonferenční systém musí umožnit poskytovat videokomunikaci s minimálním reálným obrazovým rozlišením 1280 x 720 při rychlosti 30 snímků za sekundu prostřednictvím IP sítě. U systému požadujeme optimalizovaný přenos videa pro všechny druhy provozu včetně přenosu obrazu přes satelit a do mobilního telefonu.

Videokonferenci bude možno sestavit přímo z koncového zařízení, nebo z PC přes webové rozhraní (HTTP, HTTPS). Bude možno využívat videokonference s přednastavenými účastníky s manuálním, nebo časovým spouštěním. Přístup do nastavení a videokonference bude chráněn heslem. Musí být umožněno zašifrování komunikace a také možnost nahrání. Bude možno současně s obrazem hovořícího přenášet prezentaci nebo snímání dokumentů.

Pro přenos videa systém musí podporovat video normy H.261, H.264, H.263 a H.239 a datový tok pro rozlišení od FCIF až do FullHD od 128 Kb/s do 4Mb/s dle doporučení SIP nebo H.323 (IP LAN/WAN). Integrované šifrování AES.

V případě audio norem systém musí podporovat normy G. 711, G. 722, G. 729, MPEG-4 AAC.

Videokonferenční systém musí pomocí NAT/firewall traversal umožnit připojení mobilních telefonů.

## **5 Fyzická infrastruktura**

Řešení musí respektovat novou datovou infrastrukturu resortu v prostředí LAN, WAN, která zajišťuje provoz aplikací a služeb resortu. Navržené řešení musí být v souladu s doporučeními výrobce již provozovaných dotčených zařízení na způsob implementace:

- integrovaných datových a hlasových služeb,
- zajištění QoS v prostředí LAN/WAN,
- bezpečnostních opatření v prostředí LAN/WAN,
- zajištění vysoké dostupnosti služeb,
- zajištění propojení do rezortních a mezirezortních sítí,
- zajištění propojení do sítí veřejných telefonních služeb,
- zajištění spojení pro vojenské mise AČR.

### **5.1 Řídící server hlasových služeb (RSHS)**

RSHS je základním prvek pro zabezpečení hlasových a video služeb. RSHS pracuje v režimu HA (High availability). To znamená, že v případě výpadku hlavního systému je záložní systém schopen převzít veškerou funkcionalitu bez ztráty spojení.

RSHS zabezpečuje uvedené služby samostatně pro zařízení k němu zaregistrovaná.

Zaregistrovaným zařízením se rozumí:

- IP telefon,
- SIP zařízení (telefon, videoterminál,...),
- Hlasová brána.

RSHS je nainstalován jen v nejdůležitějších lokalitách (Lokalita typu A – viz výše). Pro zabezpečení ostatních lokalit proti výpadku je v místě provozován tzv. pomocný RSHS, který převeze po dobu výpadku roli hlavního RSHS.

Propojení všech serverů RSHS vytváří homogenní síť s přenosem služeb. Některé služby mohou být zabezpečeny centrálně. Jedná se např. o hlasovou poštu (voice mail), videokonferenční zařízení, faxový server apod.

Hlavní a záložní servery musí být implementovány formou dedikovaných HW zařízení vybavených redundantním napájecím zdrojem a redundantní NIC. Pomocné RSHS je možné řešit jako virtualizované stroje, které sdílí HW s dalšími virtualizovanými servery.

## 5.2 Hlasová brána (Media gateway)

Hlasové brány slouží pro:

- zabezpečení konektivity pro Analogové telefonní rozhraní,
- jako přípojný bod pro zabezpečení analogové konektivity do veřejných nebo privátních telefonních sítí,
- záložní TDM (E1 rozhraní) připojení v případě výpadku hlavní IP konektivity,
- zdroj DSP procesorů, které zabezpečují především kódování hlasu, hlasové průvodce a hudbu v přídrži, detektory tónů a jiné systémové příslušenství,
- označkování datového provozu dle 802.1q s prioritizací dle 802.1p.

Analogové telefonní rozhraní se dělí do dvou skupin:

- Analog 1 - standardní analogové telefonní rozhraní pro připojení koncových zařízení s dosahem maximálně 1 km.
- Analog 2 - telefonní rozhraní s nutnou garancí funkcionality i ve výbušném prostředí s vyzváněcím napětím minimálně 80 VAC a dosahem ne menším než 5 km.

Prostupy do veřejných a privátních telefonních sítí budou realizovány především digitálním rozhraním ISDN BRI/PRI se signalizací EuroISDN respektive QSIG-GF/SS. Ostatní typy rozhraní budou specifikovány u příslušných hlasových bran.

Hlasová brána bude umístěna v blízkosti stávajícího slaboproudého rozvodu tak, aby bylo možné využít v co nejvyšší míře existující slaboproudý rozvod.

Hlasové brány musí poskytovat následující funkcionalitu:

- Podpora protokolů H.323v4, SIPv2 (RFC3261 a návazné).
- Integrované DSP procesory pro kódování a kompresi hlasu (preferované kodeky G.722, G.711, G.729).
- Podpora rozhraní FXS, FXO, E&M, ISDN BRI/PRI (Euro ISDN a Q.sig), E1 R2.
- Podpora přenosu faxového a modemového provozu přes IP.
- Všechna analogová telefonní rozhraní umožňují funkcionalitu zobrazení čísla volajícího – CLIP.
- Necertifikovaný šifrovaný přenos hlasu a signalizace.
- Převod kódování hlasových kanálů (transcoding).
- DSP procesory budou navrženy v režimu HA (záloha n+1).
- Dálkový dohled, zasílání SNMP trapů.

## 5.3 Koncová zařízení

| Uživatelské služby hlasového systému |   |
|--------------------------------------|---|
| 1.1                                  | sestavení a přijetí hovoru                        |
| 1.2                                  | zobrazení jména a čísla volajícího (CLIP)         |
| 1.3                                  | opakovaná volba posledního čísla (redial)         |
| 1.4                                  | napojení do hovoru                                |
| 1.5                                  | automatické zpětné volání na obsazeného účastníka |
| 1.6                                  | zpětné volání posledního volajícího               |
| 1.7                                  | čekání na obsazené stanici                        |
| 1.8                                  | přepojení hovoru                                  |
| 1.9                                  | přesměrování hovorů                               |
| 1.10                                 | parkování hovorů                                  |

|      |   |
|------|---|
| 1.11 | skupinové převzetí hovoru   |
| 1.12 | dotazovací volání (střídání hovorů)   |
| 1.13 | personální konferenční hovory (ad-hoc a meet-me)  |
| 1.14 | zachycení zlomyslného volání  |
| 1.15 | skrytí identity účastníka   |
| 1.16 | funkce nerušit  |
| 1.17 | prioritní volání  |
| 1.18 | systémové uzamčení stanice pro zabránění volání na zpoplatněné příčky                             |
| 1.19 | osobní adresář  |
| 1.20 | rozdílné vyzvánění pro identifikaci vnějšího, vnitřního volání                                    |
| 1.21 | hlasová schránka - centralizovaný model   |
| 1.22 | hlasoví průvodci pro použití systémových služeb a hudba v přídrži                                 |
| 1.23 | dvoujazyčná jazyková podpora pro informace na displejích a hlasové průvodce (angličtina, čeština) |
| 1.24 | přepnutí na tónovou volbu po sestavení spojení (In-band dual tone multifrequency - DTMF)          |

| Další funkce a služby pro odpovídající přístroje |   |
|--|---|
| 2.1  | více linek na jednom koncovém přístroji (vícelinková stanice)                     |
| 2.2  | dohled koncových přístrojů a příček   |
| 2.3  | ředitelsko-sekretářské soupravy v provedení 1+1, 1+5, 5+5                         |
| 2.4  | historie volání   |
| 2.5  | centrální spojovatelské pracoviště  |
| 2.6  | hotelové služby   |
| 2.7  | využívání centrálního telefonního seznamu z integrované klávesnice přístroje      |
| 2.8  | integrace telefonního přístroje s počítačem (CTI)                                 |
| 2.9  | integrace telefonních služeb do systému sjednocené komunikace a Microsoft Outlook |

## 5.4 Napájení

Napájecí systém je nedílnou součástí návrhu hlasové infrastruktury. Napájecí systém musí být navržen ve třech variantách:

- Varianta č. 1 – kritická napájecí soustava.
- Varianta č. 2 – standardní napájecí soustava.

Použitá varianta je vyspecifikovaná v seznamu všech lokalit.

### 5.4.1 Kritická napájecí soustava

Kritická napájecí soustava musí minimálně splňovat následující požadavky:

- Napájecí zdroj s dvojitou konverzí a účinností vyšší než 91%.
- Paralelní řazení UPS – sdílení zátěže bez jakéhokoliv dalšího komunikačního propojení.
- Samostatná věžová konstrukce nebo instalace do datového stojanu.
- Vstupní napájení 1x230V nebo 3x400V dle zatížení a místních podmínek. Výstupní napájení 230V.



- Předpokládaná zátěž počítána na 130% skutečné zátěže.
- Automatický a manuální bypass.
- Minimální doba zálohy:
  - o lokalita s dieselagregátem – 2 hodiny po celou dobu životnosti baterií,
  - o lokalita bez dieselagregátu – 8 hodin po celou dobu životnosti baterií.
- Připojení do dohledového systému přes IP adaptér – podpora SNMP.
- Řešení n+1.

#### **5.4.2 Standardní napájecí soustava**

Standardní napájecí soustava musí minimálně splňovat následující požadavky:

- Napájecí zdroj s dvojitou konverzí a účinností vyšší než 91%.
- Paralelní řazení UPS – sdílení zátěže bez jakéhokoliv dalšího komunikačního propojení.
- Samostatná věžová konstrukce nebo instalace do datového stojanu.
- Vstupní napájení 1x230V nebo 3x400V dle zatížení a místních podmínek.
- Výstupní napájení 230V.
- Předpokládaná zátěž počítána na 130% skutečné zátěže.
- Automatický a manuální bypass.
- Minimální doba zálohy – 20 minut po celou dobu životnosti baterií.
- Připojení do dohledového systému přes IP adaptér – podpora SNMP.
- Řešení n+1.

## **6 Bezdrátová infrastruktura GDS**

### **6.1 Cíl nasazení bezdrátové technologie WiFi**

Vybudovat základ bezpečné bezdrátové komunikační infrastruktury pro zabezpečení pokrytí Internetem všech nezbytných lokalit. Při realizaci projektu je kladen důraz na:

- vysokou dostupnost služeb celého řešení,
- komplexnost a škálovatelnost služeb,
- vysoký stupeň zabezpečení budované infrastruktury a služeb.

Vybudování základní WiFi komunikační infrastruktury s centrální administrací a dohledem, s možností snadného rozšíření hardwarových i softwarových prostředků pro pokrytí výkonnostních požadavků.

Bezdrátová infrastruktura může být nasazena ve dvou variantách:

- zabezpečení bezdrátové konektivity do Internetu,
- zabezpečení bezdrátových WiFi telefonů a konektivity do Internetu.

### **6.2 Způsob řešení**

#### **6.2.1 Architektura**

Základním prvkem WLAN bude distribuovaný systém s centrálním prvkem, který pracuje v režimu HA.

Kontroléry budou rozděleny do dvou typů:

- centrální kontrolér,

- koncový kontrolér.

Komunikace mezi centrálním kontrolérem a koncovými kontroléry bude pomocí GRE tunelu.

#### **6.2.1.1 Centrální kontrolér**

Centrální kontrolér je základním prvkem, který pracuje v režimu HA. Centrální kontroléry jsou umístěny v datových centrech, ve kterých je provozován IP ekosystém GDS. Centrální kontrolér zabezpečuje následující funkcionalitu:

- správa koncových kontrolérů,
- unifikovaný management z jednoho místa,
- zabezpečení IP mobility mezi koncovými kontroléry,
- řízení záložního provozu v případě výpadku koncového kontroléru.

Je požadována možnost navyšování kapacity v čase podle potřeb objednatele. Navyšování kapacity bude řešeno postupným přidáváním HW zdrojů a uživatelských licencí (není součástí této veřejné zakázky) bez negativních dopadů na provoz již instalovaných AP.

Konstrukce pro umístění zařízení do 19“ skříně datového rozvaděče:

- napájení 230V AC,
- hot-swap redundantní zdroj,
- hot-swap ventilátory,
- podpora 500 AP s možností rozšiřování až na 2000 AP,
- konektivita do páteřní sítě přes optické rozhraní o kapacitě 2 x 10 GB/s.,
- podpora AP standardu 802.11n a 802.11ac.

#### **6.2.1.2 Koncový kontrolér**

Koncový kontrolér je nainstalován v každé lokalitě, ve které je požadavek na zabezpečení bezdrátovou konektivitou. Je řízen centrálním kontrolérem. Koncový kontrolér zabezpečuje následující funkcionalitu:

- správu přístupových bodů,
- rychlý roaming mezi přístupovými body dle standardu 802.11r,
- IP mobility na druhé a třetí vrstvě,
- analýzu provozu v rámci kontrolovaných přístupových bodů,
- spektrální analýzu pokrývaného prostředí,
- ochranu proti útokům na bezdrátové prostředí,
- firewall omezující provoz pro WiFi uživatele.

Je požadována možnost navyšování kapacity v čase podle potřeb objednatele. Navyšování kapacity bude řešeno postupným přidáváním HW zdrojů a uživatelských licencí (není součástí této veřejné zakázky) bez negativních dopadů na provoz již instalovaných AP.

- konstrukce pro umístění zařízení do 19“ skříně datového rozvaděče,
- napájení 230V AC,
- konektivita do páteřní sítě přes optické rozhraní o kapacitě 2 x 1 GB/s.,
- podpora AP standardu 802.11n a 802.11ac.

### 6.2.1.3 Přístupový bod (AP)

AP, jejichž pořízení není součástí této zakázky, budou rozmisťovány uživatelem podle projektu dodavatele. Projekt bude vyspecifikován na základě požadavků objednatele. Projekt musí být zpracován tak, aby splňoval v celé definované oblasti dostupnou minimální rychlost 100 Mb/s s garantovanou úrovní služeb.

Jednotlivé AP budou rozmisťovány i v místech bez datové infrastruktury. WLAN systém musí umožňovat bezdrátové propojení AP a koncového kontroléru, vytvořením bezdrátové sítě typu Mesh. Pro tento způsob nasazení budou z důvodu zajištění dostatečné přenosové kapacity použity minimálně dvou-rádiové AP (802.11ac).

Základní požadavky:

- Podpora standardu 802.11a/b/g/n/ac.
- Dodavatel musí dodat Wi-Fi AP a antény (zejména jejich výkonnostní parametry – EIRP) v souladu generální licenci ČTÚ.
- Integrovaný standard Power-over-Ethernet (PoE) 802.3af nebo 802.3at.
- Možnost napájení prostřednictvím Power injektoru 802.3af. V případě vyšších nároků na příkon AP budou napájeny nestandardními injektory s požadovaným výkonem. Všechny napájecí injektory budou součástí nabídky.
- Dvě formy provedení AP pro vnitřní a vnější instalaci.
- V provedení pro vnější instalaci musí být provedení pláště a vysokou odolnost proti vlhkosti – krytí IP66.
- Provedení AP pro vnitřní instalaci do prostor bez potřeby korekce zisku a směrovosti antén. – integrované antény.
- Provedení AP do rozlehlých prostor s možností volby externích antén s požadovaným výkonem, směrovostí nebo mechanickým upevněním.
- Podpora minimálně MIMO 2x2 802.11n do 300 Mbps pro jedno rádio.
- Podpora SIP volání, Admission Control pro optimální výkon VoWLAN, stejně jako video streaming a propustnost dat pro 802.11 a / b / g / n klienty.
- Podpora rychlého a bezpečného roamingu.
- Podpora 8 SSID vytvořených na jednom AP.

### 6.2.2 Kapacitní plánování

V rámci budování bezdrátové komunikační infrastruktury bude vybudovaná bezdrátová síť o maximálním počtu 30 000 účastníků.

V rámci projektu GDS bude dodána HW a SW platforma, která pokryje dvě koncové lokality, každá s 250 AP a 2000 uživateli s centrálním řízením a jednotnou správou.

Síť musí být navržena tak, aby na jeden přístupový bod bylo připojeno maximálně 10 uživatelů.

### 6.2.3 Kvalita služeb

WLAN bude využívána i pro přenos hlasu pomocí bezdrátových SIP telefonů. Pro zajištění priority hlasového provozu před ostatním datovým tokem musí být odpovídajícím způsobem zajištěna kvalita služeb QoS. Pro řízení kvality multimediálních služeb musí WLAN systém podporovat standard IEEE 802.11e.

#### 6.2.4 Zabezpečení

- Všechny aktivní prvky WLAN (centrální řídicí prvky a AP) musí plně podporovat standard IEEE 802.11i.
- Přístup všech koncových zařízení do všech WLAN/SSID bude řízen na základě ověření na RADIUS serveru pomocí standardu IEEE 802.1x.
- Pro ověření uživatelů a jejich správného hesla bude sloužit uživatelská databáze RADIUS serveru.
- Uživatelská oprávnění budou uživatelům přidělována automaticky AAA serverem na základě přihlášení (loginu) do WLAN/SSID.
- WLAN/ SSID budou umožňovat připojení pouze registrovaným a úspěšně ověřeným uživatelům a koncovým zařízením.
- Neověření uživatelé nebo koncová zařízení nebudou do WLAN sítí vůbec připojeni. Systém musí umožnit zablokování uživatele v případě 5 neúspěšných pokusů o přístup do WLAN/SSID.
- Koncová zařízení budou ověřována pomocí digitálních certifikátů. Zařízení nepodporující použití digitálních certifikátů, budou ověřována pomocí MAC adresy.
- AP budou připojeny k WLAN řídicímu prvku pomocí šifrovaného tunelu (např. IPsec, GRE). AP musí podporovat možnost směřovat veškerý datový tok od Wi-Fi klientů do šifrovaného tunelu i směřovat datové toky lokálně na AP.
- WLAN musí zabezpečit ochranu proti útokům Denial-Of-Service (DoS).

#### 6.2.5 Roaming

WLAN systém musí zajistit bezešvý přechod uživatelských zařízení mezi jednotlivými AP. Z důvodu možného budoucího rozšíření o další řídicí prvky WLAN, musí systém umožnit přechod klientských Wi-Fi zařízení mezi těmito prvky bez ztráty IP adresy (RFC 3344).

#### 6.2.6 Ostatní služby

Systém musí podporovat rozšíření o sledování bezdrátového prostředí v okolí všech AP a v případě zjištění rušení automaticky informovat administrátora nebo dohled WLAN sítě. Celý systém bezdrátové sítě musí podporovat možné rozšíření o centrální dohledový systém WLAN (vytváření reportů o využití sítě, statistiky, tracking, monitoring, apod.).

### 7 Centralizovaná správa bezdrátové infrastruktury

Centralizovaná správa systému musí obsahovat:

- grafický management účastníků,
- ověřování přístupu k managementu dle RADIUS serveru,
- sběr chybových hlášení,
- grafická prezentace stavu bezdrátové sítě,
- přehledný systém o managementu,
- SNMP rozhraní pro připojení k nadřazenému dohledovému systému.

Přístup do centralizované správy bezdrátového systému musí být ověřovaný pomocí RADIUS serveru. Veškerý management je zaznamenáván a lze jej zobrazit v jednom okně.

## 8 Požadavky na zařízení s označením DWDM – DWDM multiplexor

Jednotlivé páteřní routery GDS budou propojeny pomocí 10GbE rozhraní. Jednotlivé spoje 10GbE z routerů budou zakončeny v DWDM multiplexerech, které budou umístěny ve stejném místě, jak páteřní routery. Jednotlivé DWDM multiplexery budou propojeny mezi sebou pronajatým optickým vláknem do kruhové topologie (viz obrázek páteře GDS).

Do DWDM multiplexerů budou připojeny i další přenosové systémy AČR na rozhraní STM-16 a STM-1 (TS STM), a tím bude vytvořena nová optická zálohovaná přenosová vrstva, jak pro využití propojení dalších zařízení v GDS, tak dalších systémech AČR.

Pro některé IP systémy, které z různých příčin nemohou být provozovány přímo v rámci GDS, bude na každém DWDM multiplexeru připraveno další nezávislé rozhraní o rychlosti 10/100/1000Eth.

V konečném součtu tedy bude jedno pronajaté optické vlákno přenášet 4 nezávislé datové toky (10GbE pro GDS, STM-16 spoj pro propojení páteřních STM multiplexerů, STM-1 spoj pro zálohu systému, a 10/100/1000Eth pro datové spoje mimo systém GDS).

Tím dojde k mnohem lepšímu využití pronajatého optického vlákna, a vytvoření kruhové zálohy na optické úrovni, nezávislé na stávajících přenosových systémech TS AČR, pro kritické systémy (řízení letového provozu, speciální jednotky, zahraniční mise a účastníci atd.) Vzhledem k téměř neomezené přenosové kapacitě optického vlákna lze DWDM multiplexer v případě nenadálé potřeby velmi rychle doplnit o další potřebná rozhraní (patřičný laser a lokální modul) a umožnit tak přenos velkého množství informací dle potřeby resortu bez navýšení ceny pronájmu.

Každý DWDM ROADM multiplexer bude osazen lasery pro provoz minimálně 4 nezávislých optických kanálů (různých barev) v pásmu C - 1550nm dle ITU-T G.694 pro každý optický směr. Jednotlivé lasery musí být dálkově plně přeladitelné v celém pásmu. Multiplexer bude dále vybaven potřebnými klientskými rozhraními dle popisu (1 x 10GbE, 1 x STM-16, 1 x STM-1, 1 x 10/100/1000Eth) pro každý optický směr. Celý multiplexer bude tedy dodán s vybavením pro dva optické směry, a doplněn potřebnými jednotkami pro řízení, napájení, chlazení atd. dle výrobce.

Chassis multiplexeru musí být v dodané sestavě jednoduše rozšiřitelné minimálně o další dva přenosové optické kanály (barvy) formou např. zásuvných jednotek nebo modulů, a k nim příslušných lokálních rozhraní (10GbE, STM-16, STM-1, E1, 10/100/1000Eth) bez potřeby rozšiřování vlastního chassis nebo napájení.

Napájení zařízení (požadujeme napájení 48V DC) a jeho řízení musí být plně redundantní, s možností dálkového dohledu zařízení minimálně na úrovni SNMP. K zařízení musí být výrobcem dodána potřebná MIB pro integraci zařízení do centrálního dohledu AČR.

Na základě dodaných parametrů optických vláken vypracuje dodavatel potřebná nastavení jednotlivých DWDM multiplexerů, nastaví DWDM multiplexery a provede jejich oživení a nastavení, včetně instalace a nastavení případných potřebných mezilehlých zesilovačů.

Multiplexer musí na optické úrovni používat automatické řízení vysílací úrovně.

Multiplexer musí být umísťitelný do racku 19“.