# Regionální síť Kraje Vysočina - ROWANet

# Zadání projektu Zvýšení dostupnosti služeb a navýšení kapacity přenosových linek sítě

## Obecné požadavky

Cílem projektu je vybudování nové datové sítě, která bude vystavěna na moderních technologiích a budou zavedeny moderní principy řízení. Stávající síť je postavena na optických vláknech s xWDM technologií a na virtualizaci MPLS VPN. Je v ní provozováno 70 L3VPN a jednotky L2VPN. Nová síť bude postavena paralelně ke stávající a musí být kapacitně nastavena na 250 L3 VPN a 50 L2 VPN.

Realizace se skládá z následujících kroků:

1. Vytvoření prováděcího projektu včetně měření optických tras
2. Dodávka HW a SW
3. Instalace přenosového systému
4. Instalace aktivních prvků
5. Vytvoření migračních můstků pro přesun služeb ze staré sítě (konkrétní služba musí být provozována ve staré i nové síti zároveň)
6. Splnění akceptačních testů a ukázka typových úloh
7. Dokumentace a zaškolení
8. Servis a údržba po dobu trvání servisní smlouvy

Požadavky na bezpečnost a dostupnost služeb:

1. Infrastruktura bude zajišťovat plnohodnotnou dostupnost, řiditelnost a možnost sběru informací o stavu bez dostupnosti sítě internet
2. Zajištění plné funkčnosti sítě i v případě neprodloužení maintenance na aktivní nebo pasivní část. Neprodloužení maintenance nesmí mít vliv na chod a řízení stávajícího systému.
3. Nabízená technologie bude splňovat všechny podmínky pro bezpečný provoz včetně doporučení NUKIB.
4. Na základě analýzy rizik je použití technických nebo programových prostředků následujících výrobců, včetně jejich dceřiných společností, v tomto řešení vyloučeno:
   1. Huawei Technologies Co., Ltd.,Šen-čen, Čínská lidová republika
   2. ZTE Corporation, Šen-čen, Čínská lidová republika
5. Licence perpetual (časově neomezená) umožňující využití požadovaných portů a funkcí na zařízeních
6. Přístup k administrativním rozhraním musí být zabezpečen pomocí autentizace (viz požadavky níže) a komunikace s administrativním rozhraním nesmí probíhat v nezabezpečené a nešifrované formě. Tato komunikace musí splňovat požadavky na kryptografii

## Požadavky na datovou síť

Datová síť je rozdělena na tyto části:

1. Přenosová část – řešení pro propojení aktivních částí sítě přes nenasvícená optická vlákna zadavatele
2. Aktivní část – vytvoření konfigurovatelné sítě splňující akceptační kritéria zadavatele
3. Řídící část – dodávka potřebného SW pro řízení a správu sítě

### Přenosová část sítě

Zadavatel vlastní optická vlákna mezi jednotlivými uzly sítě s následujícími parametry:

Vysvětlení zkratek:

HB - Havlíčkův Brod, CHO - Chotěboř, SnS - Světlá nad Sázavou, HU – Humpolec, PE - Pelhřimov, PA – Pacov, JI – Jihlava, NMNM - Nové Město na Moravě, BnP - Bystřice nad Pernštejnem, ZnS - Žďár nad Sázavou, MB - Moravské Budějovice, VM - Velké Meziříčí, VB - Velká Bíteš, NnO - Náměšť nad Oslavou

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Číslo trasy** | **Označení trasy** | **Délka [L] m** | **Typ kabelu** | **Útlum 1310 nm [dB]** | **Útlum 1550 nm [dB]** | **Chromatická disperze 1550 nm [CD]** |
| 1 | HB – CHO | 18 888 | 652 | 9,5 | 7,7 | 16.55 |
| 2 | HB – SnS | 19 890 | 652 | 8,72 | 5,72 | 16,6 |
| 3 | HB – HU | 29 030 | 652 | 10,7 | 6,6 | 15.1-16.2 |
| 4 | PE – PA | 28 101 | 652 | 15,9 | 7,2 | < 17 |
| 5 | JI – PE | 59 370 | 652 | 25 | 18,79 | < 17 |
| 6 | NMNM – BnP | 23 570 | 652 | 8,7 | 5,3 | 15.1-16.2 |
| 7 | ZnS – NMNM | 14 717 | 652 | 5,6 | 3,5 | 15.1-16.2 |
| 8 | JI – NMNM | 63 228 | 655 i 652 | 26 | 17,5 | 8,7-16,2 |
| 9 | JI – TŘEŠŤ | 23 675 | 652 | 8,6 | 6,2 | 15.1-16.2 |
| 10 | TŘEŠŤ – TELČ | 37 532 | 652 | 13,1 | 7,8 | 15.1-16.2 |
| 11 | TELČ – MB | 46 714 | 652 | 16,4 | 9,2 | 15.1-16.2 |
| 12 | PE – HU | 23 640 | 652 | 8,9 | 5,1 | < 17 |
| 13 | MB - TŘEBÍČ | 25 480 | 652 | 11 | 7 | < 17 |
| 14 | VM - TŘEBÍČ | 25 069 | 652 | 10,1 | 6,2 | 15.1-16.2 |
| 15 | JI - VM | 71 122 | 655 i 652 | 30,7 | 18,6 | 8,7-16,2 |
| 16 | VM-VB | 23 592 | 652 | 8,6 | 5 | 15.1-16.2 |
| 17 | VB - NnO | 37 197 | 652 | 13,2 | 7,7 | 15.1-16.2 |
| 18 | JI - HB | 43 877 | 655 i 652 | 21 | 13 | 7,9-8,7 |
|  |  |  |  |  |  |  |
| Společné parametry pro všechna vlákna: | | Polarizační vidová disperze [PMD] : | | | | < 0,2 |
|  |  | Celkový útlum odrazu [ORL] : | | |  | 40 |
|  |  | Nejhorší bodová reflektance [RMAX] : | | | | < -60 |

POZNÁMKA:

Trasa č. 4(PE-PA) a trasa č. 5 (JI-PE) je nyní osazena systémem CWDM 16ch a zadavatel požaduje pouze spojení na aktivní části zářičem o rychlosti 10Gb/s. Číslo kanálu bude upřesněno v rámci prováděcího projektu.

V ostatních páteřních trasách bude osazen přenosový systém s těmito požadovanými vlastnostmi:

1. Použití zářičů o rychlosti 100G a vyšší u aktivní části sítě
2. Využití pouze **jednoho** vlákna v trasách pro spojení aktivních uzlů.
3. Po zapojení dané trasy ještě musí zbývat minimálně 8 vlnových délek v pásmu DWDM pro pozdější osazení zářiči s překlenutelným útlumem max. 20dB na zbývajících vlnových délkách
4. Monitorovací port optického signálu (min. 1% výkonu z celkového přenášeného spektra pro příchozí i odchozí směr) nebo součástí přenosového systému pro každou trasu monitoring optického signálu (optical channel monitoring)
5. Port pro monitoring pomocí OTDR na vlnové délce 1650 (tolerance +-15) nm
6. Kompletní dodávka včetně lokální kabeláže atd.
7. Montáž do RACK 19”

V případě zesílení signálu systémem xWDM/OTN musí řešení dále splňovat následující technické minimální požadavky na jeden uzel:

1. Rackmount, výška max. 2U
2. Licence perpetual (časově neomezená) umožňující využití požadovaných portů a funkcí na zařízeních
3. Redundantní napájecí zdroje a ventilátory, hotswap
4. Přenos 1x100G full duplex
5. Automatická optimalizace signálu na obou stranách xWDM systému na základě parametrů přenosového vlákna včetně kompenzace disperze
6. Konfigurace a dohledování stavu systému přes IP, RESTCONF popř. NETCONF, SNMP, CLI
7. Vybavení pro troubleshooting – zasílání logů, signalizace mezních stavů na přenosových linkách
8. Kompletní dodávka včetně lokální kabeláže, zařičů atd.
9. LED indikace základních provozních stavů (napájecí zdroje, chybový stav, …)
10. Musí být zajištěno logování a sběr auditní stopy

Před vlastní realizací projektu budou parametry optických vláken v trasách zkontrolovány novým měřením, které budou prováděna z obou konců vláken a budou obsahovat následující změřené veličiny:

Délka trasy [m]

Celkový útlum trasy při 1310 nm [dB]

Celkový útlum trasy 1550 nm [dB]

Chromatická disperze 1550 nm [CD]

Polarizační vidová disperze [PMD]

Celkový útlum odrazu [ORL]

Nejhorší bodová reflektance [RMAX]

Pokud navrhovaný přenosový systém vyžaduje pro ověření předpokladu funkčnosti další veličiny, budou tyto veličiny zahrnuty do prováděného měření.

V propojení uzlů sítě jsou zavedeny i další linky (viz obrázek č.1):

1. **Místní optická trasa** – 1ks optického SM vlákna, pro každou trasu dodávka pasivního xWDM MUX/DEMUX, po propojení dodaných aktivních prvků v trase ještě musí zbývat minimálně 8 vlnových délek v pásmu DWDM pro pozdější využití, Port pro monitoring pomocí OTDR na vlnové délce 1650 (tolerance +-15) nm, Monitorovací port optického signálu (min. 1% výkonu z celkového přenášeného spektra pro příchozí i odchozí směr) nebo součástí přenosového systému pro každou trasu monitoring optického signálu (optical channel monitoring)
2. **xWDM kanály pro provoz 100G linek** – mezi lokalitami Jihlava Krajský úřad a Jihlava Nemocnice budou 100G linky zapojeny dle nákresu (**2ks MUX/DEMUX pro dvouvláknový přenos součástí dodávky**) s využitím optických tras (k dispozici 4ks šedých vláken ve 2 nezávislých trasách). Na každém MUX/DEMUX po propojení prvků v trase ještě musí zbývat minimálně 8 vlnových délek v pásmu DWDM pro pozdější využití, port pro monitoring pomocí OTDR na vlnové délce 1650 (tolerance +-15) nm, Monitorovací port optického signálu (min. 1% výkonu z celkového přenášeného spektra pro příchozí i odchozí směr) nebo součástí přenosového systému pro každou trasu monitoring optického signálu (optical channel monitoring)
3. **Spojení uvnitř serverových místností** – dodávka zářičů využívajících max.2.vlákna do prvků včetně propojovacích kabelů o délce cca 7m (typ a délka bude upřesněna při prováděcím projektu)

## Aktivní část sítě

aktivní uzly sítě jsou rozděleny následovně:

**CORE** – 2ks zařízení umístěny v Jihlavě v oddělených datacentrech (Krajský úřad, Nemocnice Jihlava) propojených 2ks SM optickými vlákny ve vzdálenosti do 5km

**PE1** – velmi důležitá lokalita - redundantní uzel skládající se ze 2 boxů (propojení přes 1ks SM vlákna do vzdálenosti 5km) - umístěno Jihlava, Havlíčkův Brod, Nové Město na Moravě, Třebíč, Pelhřimov

**PE2** – Světlá nad Sázavou, Humpolec, Žďár nad Sázavou, Bystřice nad Pernštejnem, Velká Bíteš, Velké Meziříčí, Náměšť nad Oslavou, Moravské Budějovice, Telč, Třešť, Pacov, Jihlava (2ks)

**PE3** – zařízení umístěny v Jihlavě, lokality Nemocnice a Krajský úřad

Topologie sítě je zobrazena na obrázku č. 1.

Obsah obrázku text, diagram, snímek obrazovky, Plán

Popis byl vytvořen automaticky

*Obrázek 1 : Topologie sítě*

*POZN.: v topologii jsou zohledněny pouze páteřní trasy sítě*

### Požadavky na aktivní část:

1. Kruhová topologie se 2 centrálními body v Jihlavě se zohledněním redundance na přenosové i aktivní části datové sítě:
   1. Jihlava – Havlíčkův Brod – Humpolec – Pelhřimov – Jihlava
   2. Jihlava – Velké Meziříčí – Třebíč – Moravské Budějovice – Telč - Třešť – Jihlava
2. Datový provoz na bázi protokolu ethernet
3. Rychlost páteřních linek:
   1. CORE – CORE – rychlost min. 200Gb/s (předpokládá se LACP) s  propojením ve 2 nezávislých trasách, viz. xWDM kanály pro provoz 100G linek
   2. Mezi PE a CORE min. 100Gb/s
   3. Mezi PE a PE min. 100Gb/s
   4. Výjimka u linky č. 4(PE-PA) a linky č. 5 (JI-PE) – 10Gb/s přes přenosové CWDM kanály
4. Síť bude virtualizována, komponenty nutné pro virtualizaci sítě v redundantním provedení - návrh bude součástí prováděcího projektu
5. Uzly typu CORE, PE1, PE2 budou součástí virtualizační vrstvy
6. Softwarová část nabízených aktivních prvků CORE, PE1, PE2 je požadována od jednoho výrobce z důvodu jednotnosti řízení sítě
7. Uzly typu PE3 jsou určeny pro připojení internetové konektivity od poskytovatelů (full BGP peering)
8. Minimální technické parametry pro páteřní uzly sítě jsou uvedeny v Příloze 1
9. Musí být zajištěno logování a sběr auditní stopy z prvků aktivní části sítě.

## Řídící část sítě

Software pro řízení a monitoring sítě bude instalován do technologického centra zadavatele ve formě virtuálních strojů. Celková souhrnná využitelná kapacita zdrojů je následující – 8 VM, 96GB RAM, 32 vCPU, 800GB HDD.

Požadavky jsou následující:

1. Zavedení do monitoringu ZABBIX (nyní využívaný zadavatelem) všech použitých aktivních komponent sítě (v rozsahu požadované instalace) včetně vytvoření map, sběru provozních údajů a nastavení alarmů pro chybové stavy sítě (přenosová, aktivní i řídící část)
2. Celá síť řiditelná z jednoho místa formou centrálního MGMT - umožní hromadnou změnu konfigurace zařízení a hromadné získání stavových výpisů (jako jeden celek (fabric) nebo zavedení nástroje na řízení sítě jako celku – např. ANSIBLE, apod.)
3. Nástroj pro zálohování konfigurací s verzováním (uchování min. 40 záloh pro každé zařízení)
   1. Automatická záloha v cyklu nastavené administrátorem s rozdílným nastavením pro přenosovou a aktivní část
   2. Ruční vytvoření zálohy administrátorem včetně zobrazení změn na prvcích v aktivní části
   3. Řízení nástroje a stahování konfiguračních souborů administrátorem přes grafické rozhraní
4. Ověřování a řízení úrovně přístupu napojením na externí identity (SAML2.0 případně LDAP/Kerberos/AD)
5. Nástroj pro sběr a uchování provozních událostí (logů) včetně vyhledávání dle určených kritérií s grafickým rozhraním (uchování logů po dobu 18 měsíců), nastavení přeposílání určených událostí, ověřování a řízení úrovně přístupu napojením na externí identity (SAML2.0 případně LDAP/Kerberos/AD)
6. Nástroj pro řízení úrovně přístupů a ověřování přístupu na MGMT zařízení (přenosová i aktivní část) s  napojením na externí identity (LDAP/AD )
7. UI pro vytváření L3VPN a L2VPN služby v síti
8. Nástroje (požadavky 3 až 6) budou licencovány pro 15 uživatelů a 50 zařízení, je možné dodat i v modulárním provedení

## Požadavky na bezpečnost pro logování, řízení přístupů a GUI rozhraní

1. Logování událostí
   1. Auditní záznamy a logy musí obsahovat minimálně tyto informace:
      1. Přidělení/odebrání oprávnění
      2. Založení/smazání uživatele
      3. Změna konfigurace logování událostí (pokud danou funkcionalitu bude systém obsahovat)
      4. Případně další aktivity uživatele
   2. Auditní záznamy a logy musí obsahovat minimálně tyto parametry a metadata:
      1. identifikace uživatele
      2. identifikátor události
      3. přesné datum vzniku události
      4. přesný čas vzniku události včetně specifikace časového pásma,
      5. typ/název události,
      6. jednoznačnou síťovou identifikaci zařízení původce a úspěšnost nebo neúspěšnost (včetně neprovedení činnosti v důsledku nedostatečných oprávnění) události.
   3. Události musí být možné exportovat do centrálního úložiště logů pomocí syslog protokolu
2. Úrovně všech přístupových oprávnění/jednotlivých rolí musí být detailně popsány
   1. V případě autentizace vůči internímu zdroji identit musí existovat možnost nadefinování vlastní heslové politiky a to minimálně v tomto rozsahu:
   2. stáří hesla,
   3. granulární komplexita hesla (určení kategorií znaků),
   4. délka hesla,
   5. historie hesla (počet opakování).
   6. Uložení hesel v interní DB musí být v souladu s požadavky na kryptografii, tzn., že nesmí být uložena v plaintext podobě ani pomocí nevhodných hash funkcí
   7. zrušení uživatele musí vždy probíhat formou jeho zneplatnění/zneaktivnění, nikoliv jeho vymazáním z důvodu zachování auditní stopy,
3. Každý uživatelský účet musí být unikátní a personifikovaný, nesmí existovat sdílený uživatel či sdílené heslo pro více uživatelů s výjimkou technických/systémových účtů.
4. Pokud bude součástí dodávky webový server/grafické webové rozhraní, musí řídící část sítě podporovat nastavení bezpečnostních HTTP hlaviček webového serveru dle těchto parametrů:
   1. X-Frame-Options
      1. Záhlaví může nabývat pouze hodnot DENY nebo SAMEORIGIN dle potřeby
   2. Strict-Transport-Security
      1. Direktiva max-age musí nabývat hodnoty minimálně 31536000
      2. Ostatní direktivy jsou volitelné
   3. Content-Security-Policy
      1. Nesmí obsahovat direktivy unsafe-inline, unsafe-eval
      2. Aktiva mohou být načítána pouze prostřednictvím zabezpečeného protokolu (direktiva https:)
      3. Aktiva mohou být načítána pouze z konkrétních a bezpečných zdrojů
      4. Pokud by bylo nutné načítat aktiva z jiných zdrojů, které nejsou umístěny na infrastruktuře, která je v držení Kraje Vysočina nebo dodavatele, podléhají tyto zdroje nejprve schválení Krajem Vysočina. Pokud ke schválení Krajem Vysočina nedojde, tyto zdroje nemohou být použity k načítání aktiv spolu se zbytkem webové stránky
   4. X-Content-Type-Options
   5. Referrer-Policy
      1. Nesmí obsahovat direktivy: prázdný string, unsafe-url
   6. Permissions-Policy
      1. Mohou být povolena pouze ta oprávnění, která jsou skutečně potřeba, všechna ostatní musí být explicitně zakázána
   7. X-XSS-Protection
      1. Directiva politiky musí nabývat hodnoty 1; mode=block
   8. Server
      1. Pokud je hlavička implementována, musí být změněna tak, aby neodhalovala citlivé informace odhalující verzi webového serveru
   9. Set-Cookie
      1. Pokud se jedná o session cookies, musí obsahovat direktivu nastavující secure a httponly flagy.
   10. Cross-Origin-Embedder-Policy

Kryptografie obecně

Pro kryptografické funkce nesmí být použity proprietární/uzavřené algoritmy, ale ty, které jsou považovány za standardy, jejichž funkcionalita je všeobecně známá a popsaná.

Požadavky na kryptografii v přenosové a aktivní části datové sítě

Níže jsou uvedeny požadavky na kryptografické funkce a algoritmy, které se vztahují na administrativní funkce přenosové a aktivní části datové sítě. Pokud budou v prvcích a komponentách datové sítě použity kryptografické funkce a algoritmy, musí splňovat tyto níže uvedené požadavky.

Tyto požadavky se neaplikují na kryptografické zabezpečení dat transportovaných prostřednictvím datové sítě, ale pouze na služby, funkce a komponenty zajišťující administraci či správu prvků a komponent datové sítě.

**Hashovací funkce**

Ukládání otisků hesel

* pro ukládání hesel uživatelů mohou být použity pouze tyto tzv. pomalé hashovací funkce:
  + Argon2
  + scrypt
  + PBKDF2 se schválenou hašovací funkcí SHA-2 (viz níže)
* pro ukládání hesel nesmí být použity tzv. rychlé hashovací funkce typu MD-X, SHA-X, apod.

Ostatní použití hash funkcí:

* pokud budou použity hashovací funkce pro jiné účely než pro uložení hesel, musí být použity pouze tyto funkce:
  + SHA-2 (SHA-256, SHA-384, SHA-512, SHA-512/256) a SHA-3 (SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256)

**Asymetrická kryptografie**

Požadavky na SSL/TLS (na nastavení funkcí protokolů sloužících k zapouzdřování protokolů sedmé vrstvy)

* verze protokolu minimálně TLSv1.2 a vyšší
* konfigurace
  + všechny EXPORT cipher suites musí být zakázány
  + algoritmy a funkce pro výměnu klíčů
    - algoritmus pro výměnu klíčů musí podporovat Perfect forward secrecy
      * tzn., že šifrovací klíč je vyměněn mezi klientem a serverem tak, aby jej nebylo možné získat se znalostí privátního klíče serveru, např. musí být použit Diffie-Hellman (DH nebo ECDH) algoritmus
      * a navíc se musí jednat o tzv. ephemeral Diffie-Hellman (DHE, ECDHE), tzn. že pro každou session je generován nový set Diffie-Hellman klíčů
    - délky klíčů:
      * pro Diffie-Hellman (DH) - 3072 bitů a více
      * pro Elliptic Curve Diffie-Hellman (ECDH) – 256 bitů a více
    - nesmí být použita anonymní výměna klíčů
  + algoritmy a funkce pro autentizaci
    - minimální délky klíčů:
      * RSA - 3072 bitů
      * DSA – 3072 bitů
      * ECDSA - 256 bitů
  + algoritmy a funkce pro symetrické šifrování
    - nesmí být použita hodnota NULL v cipher suites
    - nesmí být použity tyto šifry:
      * DES, 3DES, RC4
    - minimální délka šifrovacího klíče - 128 bitů
  + MAC (Message Authentication Code)
    - použití SHA funkce s minimální délkou hashe 256 bitů

Požadavky na asymetrickou kryptografii použitou mimo SSL/TLS protokoly (jiné případy šifrování, podepisování a autentizace):

* minimální délka klíče
  + algoritmus DSA – 3072 bitů a vyšší
  + algoritmus RSA - 3072 bitů a vyšší
  + algoritmus ECDSA - 256 bitů
* Ověřování (např. SSH klíče)
  + délka klíče 3072 bitů u RSA a DSA
  + délka klíče minimálně 256 bitů u algoritmů používajících eliptické křivky

**Symetrická kryptografie**

* mohou být použity tyto šifry:
  + AES, Twofish, Camellia, Serpent, SNOW2.0, SNOW3.0
* nesmí být použity tyto šifry:
  + DES, 3DES, RC4, RC5 Blowfish, Kasumi
* minimální délka šifrovacího klíče u povolených symetrických šifer - 256 bitů
* nesmí být použity tyto módy pro ochranu integrity:
  + HMAC-SHA1, CBC-MAC-X9.19.

Požadavky na kryptografii v řídicí části datové sítě

Níže jsou uvedeny požadavky na kryptografické funkce a algoritmy, které se vztahují na řídicí části datové sítě a tudíž na SW části určené pro administraci a řízení. Tyto požadavky se vztahují na všechny použité funkce a algoritmy.

**Hashovací funkce**

Ukládání otisků hesel

* pro ukládání hesel uživatelů mohou být použity pouze tyto tzv. pomalé hashovací funkce:
  + Argon2 s parametry alespoň t=1, m=221, p=4 a funkcí Argon2id
  + scrypt s parametry alespoň N=32768 (215), r=8, a p=1
  + PBKDF2 s počtem iterací alespoň 100 000 a schválenou hašovací funkcí SHA-2 (viz níže)
* při hashování hesla musí být použit pseudonáhodně vygenerovaný kryptografický salt
* pro ukládání hesel nesmí být použity tzv. rychlé hashovací funkce typu MD-X, SHA-X, apod.

Ostatní použití hash funkcí:

* pokud budou použity hashovací funkce pro jiné účely než pro uložení hesel, musí být použity pouze tyto funkce:
  + SHA-2 (SHA-256, SHA-384, SHA-512, SHA-512/256) a SHA-3 (SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256)

**Asymetrická kryptografie**

SSL/TLS (nastavení funkcí protokolů sloužících k zapouzdřování protokolů sedmé vrstry)

* verze protokolu minimálně TLSv1.2 a vyšší
* konfigurace
  + cipher suite musí být vybrána na základě serverem preferovaného pořadí
  + vyšší priority musí mít cipher suites, které obsahují varianty asymetrických algoritmů s eliptickými křivkami, např.:
    - ECDHE musí mít vyšší prioritu než DHE
    - ECDSA musí mít vyšší prioritu než DSA
  + všechny EXPORT cipher suites musí být zakázány
  + algoritmy a funkce pro výměnu klíčů
    - algoritmus pro výměnu klíčů musí podporovat Perfect forward secrecy
      * tzn., že šifrovací klíč je vyměněn mezi klientem a serverem tak, aby jej nebylo možné získat se znalostí privátního klíče serveru, např. musí být použit Diffie-Hellman (DH nebo ECDH) algoritmus
      * a navíc se musí jednat o tzv. ephemeral Diffie-Hellman (DHE, ECDHE), tzn. že pro každou session je generován nový set Diffie-Hellman klíčů
    - délky klíčů:
      * pro Diffie-Hellman (DH) - 3072 bitů
      * pro Elliptic Curve Diffie-Hellman (ECDH) – 256 bitů a více
    - nesmí být použita anonymní výměna klíčů
  + algoritmy a funkce pro autentizaci
    - minimální délky klíčů:
      * RSA - 3072 bitů
      * DSA – 3072 bitů
      * ECDSA - 256 bitů
  + algoritmy a funkce pro symetrické šifrování
    - nesmí být použita hodnota NULL v cipher suites
    - nesmí být použity tyto šifry:
      * DES, 3DES, RC4
    - minimální délka šifrovacího klíče - 128 bitů
    - cipher suites s šiframi s větší délkou klíče musí mít větší prioritu v seznamu ciphersuites než s menší délkou klíče
  + MAC (Message Authentication Code)
    - použití SHA funkce s minimální délkou hashe 256 bitů
    - vyšší délky otisků musí mít vyšší prioritu v cipher suites

TLS cipher suites

* Doporučené cipher suites (v doporučeném pořadí), které naplňují výše zmíněné požadavky
  + TLS1.3:
    - TLS\_AES\_256\_GCM\_SHA384
    - TLS\_CHACHA20\_POLY1305\_SHA256
    - TLS\_AES\_128\_GCM\_SHA256
    - TLS\_AES\_128\_CCM\_SHA256
  + TLS1.2:
    - TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
    - TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256
    - TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
    - TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
    - TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256
    - TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
    - TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
    - TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
    - TLS\_DHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256

Požadavky na asymetrickou kryptografii použitou mimo SSL/TLS protokoly (jiné případy šifrování, podepisování a autentizace):

* týká se různých technologií PKI, PGP, S/MIME, SSH, apod.
* minimální délka klíče
  + algoritmus DSA – 3072 bitů a vyšší
  + algoritmus RSA - 3072 bitů a vyšší
  + algoritmus ECDSA - 256 bitů
* Ověřování (např. SSH klíče)
  + délka klíče 3072 bitů u RSA a DSA
  + délka klíče minimálně 256 bitů u algoritmů používajících eliptické křivky

**Symetrická kryptografie**

* mohou být použity tyto šifry:
  + AES, Twofish, Camellia, Serpent, SNOW2.0, SNOW3.0
* nesmí být použity tyto šifry:
  + DES, 3DES, RC4, RC5 Blowfish, Kasumi
* minimální délka šifrovacího klíče u povolených symetrických šifer - 256 bitů
  + pro šifru Chacha20 minimálně 256 bitů a se zatížením klíče menším než 256 GB
* nesmí být použity tyto módy pro ochranu integrity:
  + HMAC-SHA1, CBC-MAC-X9.19.

## Akceptační testy a typové úlohy

Instalace a konfigurace dodávané technologie bude provedena do úrovně naplnění požadavků v akceptačních testech a ukázek konfigurace typových úloh.

### Akceptační testy:

1. Instalace a konfigurace prvků přenosové vrstvy (aktivní i pasivní část) včetně vytvoření měřících protokolů použitých vláken
2. Instalace a konfigurace všech aktivních uzlů sítě
3. Vytvoření virtualizační vrstvy sítě aktivních prvků a konfigurace dle bezpečnostních doporučení (hardening)
4. Konfigurace 2xL3VPN a 1xL2VPN, konfigurační práce pouze na koncových boxech (v místě vyvedení VPN- PE1,PE2), nikoliv na boxech po trase v kruhové topologii
5. Zavedení všech instalovaných aktivních prvků (přenosová i aktivní část) do provozního monitoringu (ZABBIX), sledování provozních hodnot (bude upřesněno v rámci prováděcího projektu dle použité technologie)
6. Test redundance služeb L2VPN, L3VPN v konfiguraci kruhové topologie sítě včetně kontroly hlášení v ZABBIX o snížení redundance
7. Test multihomingu v lokalitě PE1 (konfigurace připojení organizace k oběma node PE1) včetně doporučení konfigurace protistrany na zařízení CE, kontrola hlášení v ZABBIX v případě snížení redundance (přerušení připojení k jednomu node PE1)
8. Instalace boxů PE3 včetně vytvoření a konfigurace scénáře migrace připojení do sítě internet ze stávající sítě, zavedení mechanismu lokální validace route RPKI včetně instalace všech potřebných komponent v režimu vysoké dostupnosti
9. Test propustnosti páteřních tras dle Y.1564 včetně dodání měřícího protokolu na úrovni aktivní vrstvy sítě
10. Ukázka centrálního řízení
    1. Nastavení zálohy konfigurace na každém prvku u aktivní části s frekvencí 1x denně, ukázka verzovacího systému
    2. Kontrola nastavení zařízení dle bezpečnostní šablony
    3. Provedení update firmware na určených boxech
    4. Nastavení zasílání logů protokolem syslog na server určený zadavatelem pro PE1 boxy u aktivní části
    5. Zavedení a odstranění uživatele s oprávněním na definovanou sadu příkazů u aktivní části na určené boxy
    6. Ukázka UI pro vytváření L3VPN a L2VPN služby v síti
11. Ukázka konfigurace zařízení přes REST API u aktivní části sítě
12. Konfigurace zrcadlení provozu pro připojení externí FLOW sondy
13. Kontrola úrovní optického signálu mezi jednotlivými PE a CORE na páteřních linkách, zapsání aktuálního stavu do protokolu (přenosová i aktivní část)
14. Vytvoření migračních můstků pro přesun služeb do nové sítě, nutný souběžný provoz služeb v obou sítích současně
15. Na trase č.5 je snížená rychlost na 10G, provedení vhodné konfigurace s rezervací kapacity 80% pro určené subjekty v L3VPN/L2VPN pro případ výpadku primární trasy přes linky 12, 3, 18
16. Ukázka a návod na odstraňování provozních závad
    1. Nefunkční L2VPN
    2. Nefunkční L3VPN
    3. Nízký signál na L1 lince v případě použití aktivní přenosové technologie
17. Provedení testu obnovy dle disaster recovery plánu pro tři určené prvky infrastruktury (přenosová část, aktivní část, řídící část)
18. Otestování přechodu ověření přístupu na MGMT prvků na lokální účty v případě nedostupnosti centrálního ověření
19. Ukázka aplikovaných požadavků zadavatele na kryptografii

### Typové úlohy

1. Začlenění nového PE prvku do sítě na úrovni L1 až L3 - vytvoření konfiguračního předpisu
2. Konfigurace L2VPN (varianta vícebodová i jednobodová) do úrovně vyvedení VLAN pro připojení CE přepínačů, konfigurace pouze na koncových PE boxech
3. Konfigurace L3VPN (varianta vícebodová i jednobodová) do úrovně vyvedení VLAN pro připojení CE přepínačů, konfigurace pouze na koncových PE boxech
4. Konfigurace 2ks vícebodových L3VPN s dynamickým routovacím protokolem včetně konfigurace funkce „VRF route leaking (sloučení routovacích tabulek)“
5. Konfigurace ACL do úrovně L4 pro IPv4 i IPv6
6. Konfigurace L2VPN vícebodobého propojení pro přenos QinQ včetně předání ve formě QinQ na CE
7. Nastavení bezpečnostních funkcí na obranu proti útokům na PE3 – traffic policy, BGP FlowSpec, ACL, Source RTBH, BCP-38
8. Konfigurace přístupu přes SSH na aktivní prvek s ověřením přes RADIUS

Popis konfigurace typových úloh včetně šablony pro zabezpečení aktivních prvků bude součástí dokumentace díla.

## Předání Věcí dle kupní smlouvy

Součástí předání budou následující dokumenty:

1. Měření optických tras
2. Měření propustnosti páteřních tras
3. Seznam předaného vybavení a zařízení
4. Dokument s výsledky akceptačních testů
5. Návody na konfiguraci typových úloh
6. Dokumentace skutečného provedení
7. Bezpečnostní dokumentace
   1. Analýza rizik – dodavatel zpracuje komplexní analýzu rizik informační bezpečnosti v souvislosti s provozem všech částí dodávané datové sítě. Analýza rizik informační bezpečnosti musí být zpracována před nasazením do provozního režimu. Zhotovitel vypracuje a předá zadavateli:
      1. zdokumentovaný postup provedení analýzy rizik (metodiku, jak postupoval),
      2. zprávu z analýzy rizik obsahující vydefinovaná a klasifikovaná rizika, která jsou určena na základě míry dopadu, pravděpodobnosti výskytu zranitelnosti a pravděpodobnosti naplnění hrozby, a popis těchto rizik,
      3. plán zvládání rizik s návrhy opatření na snížení míry případných rizik včetně popisu způsobu jejich nasazení.
   2. Bezpečnostní specifikace datové sítě
      1. Cíl dokumentu: popsat a zdokumentovat veškeré bezpečnostní mechanizmy a opatření za účelem identifikace toho, jaká data jsou jakým způsobem chráněna.
      2. Soupis a popis všech funkcí prosazujících bezpečnost pro:
         1. zajištění integrity dat při jejich přenosu a uložení,
         2. zajištění důvěrnosti dat při jejich přenosu a uložení,
         3. zajištění autentizace a session managementu,
         4. zajištění ošetření, filtrování a prověřování veškerých vstupních dat,
         5. zajištění auditní stopy a logování,
   3. Záloha, obnova, restart
      1. Vytvoření disaster recovery plánu včetně postupů pro obnovení po havárii
      2. Doporučené způsoby zálohování všech částí sítě
      3. Doporučené postupy pro bezpečný restart řídící části
   4. Monitoring
      1. Cíl dokumentu: popsat a zdokumentovat mechanizmus monitorování a zaznamenávání bezpečnostních a provozních logů a auditních událostí.