Příloha č. 1 – Specifikace předmětu díla

Název zakázky: Implementace MS AD včetně migrace stanic a segmentace sítě
Číslo zakázky: P18V00000055
Zadavatel: Statutární město Frýdek-Místek, se sídlem Frýdek-Místek, Radniční 1148, PSČ 738 01

1. Technická specifikace předmětu plnění veřejné zakázky

Předmět plnění veřejné zakázky je rozdělen do dvou celků.

Jeden celek obsahuje implementaci Microsoft Active Directory, Windows File server, RDS server, nastavení zálohování file serveru a síťových protokolů. Popis stávajícího stavu a podrobnější popis technické specifikace je obsažen v kapitole 2.1 tohoto dokumentu.

Druhý celek je zaměřen na readresaci a segmentaci celé síťové infrastruktury zahrnující také aplikaci bezpečnostních opatření a nastavení. Implementace bude probíhat na stávající síťové infrastruktuře rozmístěné do celkem 5 lokalit Magistrátu města Frýdku-Místku. Popis stávajícího stavu a podrobnější popis technické specifikace je obsažen v kapitole 2.2 tohoto dokumentu.

Veškerá implementace musí splňovat požadavky zadavatele, které vycházejí z analýz domény a sítě, provedených firmou AutoCont CZ a.s., Hornopolní 3322/34, 702 00 Ostrava. Analýzy obsahují cílové návrhy a popisy podrobnějšího nastavení. Základní specifikace níže vychází z provedených analýz. Analýzy domény a sítě budou k dispozici vybranému dodavateli.

Dodavatel před zahájením implementace odevzdá zadavateli harmonogram prací, který musí obě strany schválit a v průběhu implementace se jim řídit. Změny v harmonogramu v průběhu realizace veřejné zakázky jsou možné po odsouhlasení oběma stranami.

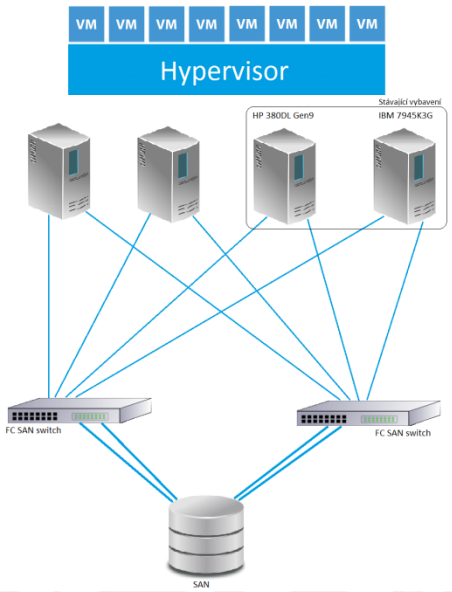
Dodavatel vypracuje písemnou technickou dokumentaci, která bude obsahovat zejména konfigurace a nastavení jednotlivých celků. Tuto dokumentaci předá zadavateli. Technická dokumentace se po předání zadavateli stává jeho majetkem a může s ní nakládat dle svých potřeb.

1.1. Implementace Microsoft Active Directory, Windows File server, RDS server, nastavení zálohování domény a síťových protokolů

1.1.1. Popis stávajícího stavu

Stávající doména MMFM.LOCAL byla vytvořena za účelem budoucího nasazení do ostrého provozu, ale k tomu nedošlo a byla používána pro testování. Doména obsahuje 4 servery (2x doménové řadiče, management server včetně Remote Desktop Services a file server) ani jeden objekt typu počítač. Na management serveru je nainstalována role Remote Desktop Services, která umožňuje externím dodavatelům přístup do prostředí zákazníka. Doména nebude použita (bude smazána) a vedle ní bude vytvořena doména nová.

Implementace nové domény bude probíhat na stávající IT infrastruktuře. Stávající infrastruktura obsahuje dva identické produkční servery Huawei RH2288H V3, na kterých je provozována virtualizace VMware 6.0. Jeden server HPE Proliant DL380 G8 s virtualizační platformou VMware 6.0 dedikovaný jako databázový a jeden server IBM 7945 K3G pro testovací účely s VMware 6.0. Virtualizační platforma je centrálně spravována přes vCenter 6.0. Dále je součásti IT infrastruktury diskové pole Huawei Storage OceanStor 2800 V3 s dostatečnou kapacitou pro nové servery (doménové řadiče, RDS, FS, DHCP). Datová struktura pro komunikaci mezi servery a diskovým polem je vybudovaná na technologii fiber channel s využitím SAN switchů Huawei Brocade SNS2224 a redundantních cest pro případ výpadku. Magistrát města Frýdku-Místku vlastní dvě licence Microsoft Windows Server 2016 Datacenter pro produkční servery. Zálohování probíhá prostřednictvím software VMware vSphere Data Protection. DHCP není ve stávající síti implementováno.



Magistrát města Frýdku-Místku tvoří celkem 17 odborů a městská policie s celkovým počtem přibližně 432 uživatelů, kteří budou pracovat v nové doméně. Uživatelské profily na stanicích jsou lokální s oprávněním USER. Následující tabulka ukazuje přehled využívaných operačních systémů na koncových stanicích:

Seznam koncových stanic (PC)

Operační systém	Celkem
Windows 10 Pro	373
Windows 7 Professional	15

Seznam koncových stanic (NB)

Operační systém	Celkem
Windows 10 Pro	27

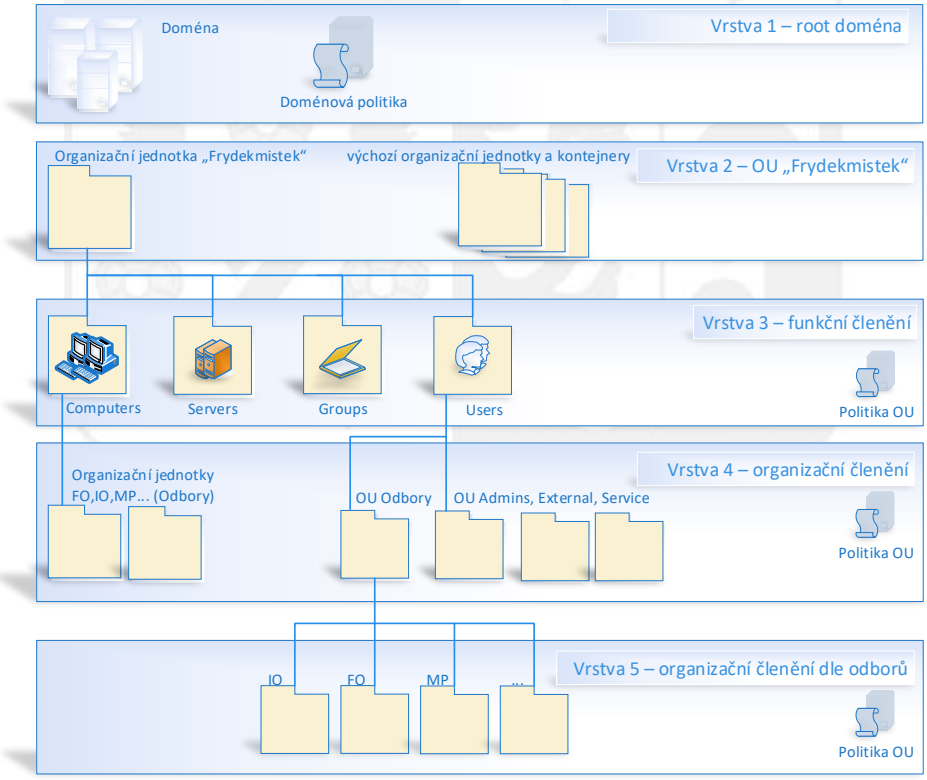
1.1.2. Technická specifikace

Tato kapitola popisuje základní požadavky pro implementaci. Podrobnější požadavky pro nastavení plynoucí z analýzy budou dodány zadavatelem.

Základní požadavky na implementaci domény

- Odebrání některých serverů ze staré domény, smazání staré domény a doménových řadičů
- Příprava dvou virtuálních serverů s Windows Server 2016 v aktuálním buildu + aktualizace v součinnosti se zadavatelem
- Instalace dvou nových doménových řadičů a ověření funkčnosti (replikace atd.), včetně možnosti používání snapshotů ve virtualizačním prostředí
- Instalace DNS rolí na doménových řadičích, konfigurace split DNS v součinnosti s pracovníky IT, nastavení DNS předávání

- Úprava subnetingu a výchozích lokalit v AD
- Zapnutí funkce recycle bin
- Instalace certifikační authority pro doménu
- Nastavení FSMO rolí
  - 1. doménový řadič (DC01) bude mít role global katalog, schema master, domain naming master
  - 2. doménový řadič (DC02) bude mít role global katalog, RID master, PDC emulator, infrastructure master
- Nastavení NTP na DC01, který bude sloužit jako NTP server pro novou doménu
- Vytvoření 5 vrstvého organizačního členění
  - Vrstva 1: Root doména
  - Vrstva 2: OU „Frydekmistek"
  - Vrstva 3: OU funkčního členění – členění dle typů objektů (stanice, servery, uživatelé, skupiny)
  - Vrstva 4: OU organizačního členění – členění dle odboru jako celku, externích, administrátorských a servisních účtů (pouze u OU pro stanice a uživatele)
  - Vrstva 5: OU organizačního členění – členění dle jednotlivých odborů



- Vytvoření uživatelských účtů, administrátorských účtu, účtů pro externí dodavatele, uživatelských skupin

  - Migrační seznam s atributy bude dodán oddělením IT

- Přiřazení uživatelských účtů do skupin
- Delegování oprávnění globálním a lokálním administrátorům
- Vytvoření doménových politik a uložení v group policy central store:
  - Politiky s definicí bezpečnostních pravidel pro hesla
  - Politiky pro koncové stanice – nasměrování aktualizací koncových stanic na místní WSUS server, nasazení aplikace TeamViewer (Light verze s omezením přístupu), nasazení aplikace AuditPro, která je dostupná jako MSI balíček
  - Politiky pro řadiče domény
  - Politiky nahrazující skripty spouštěné při prvotní instalaci počítače – přibližně 60 nastavení (úprava v registrech, nastavení Windows)
- Nastavení politik hesel pro správce pomocí Fine Grained Password Policy
- Připojení serverů do domény
- Nastavení zálohování pomocí nástroje zadavatele a dle požadavku zadavatele

DHCP server

- Příprava dvou virtuálních serverů s Windows Server 2016 v aktuálním buildu + aktualizace v součinnosti se zadavatelem
- Instalace DHCP role na oba servery
- Definice DHCP pool a vytvoření rezervací
  - Seznam IP bude dodán oddělením IT zadavatele
- Autorizace DHCP serverů v AD
- Konfigurace IP helperů/DHCP relay na potřebných zařízeních
- Konfigurace DHCP serverů v módu Active-Standby

Migrace stanic

Migrace stanic bude probíhat po otestování migrace na vybraném vzorku stanic a uživatelů. Zaměstnanci odboru IT musí být podrobně seznámení s postupem migrace a dostat písemný postup migrace, včetně nastavení, které bude migrováno.

- Změna síťového nastavení TCP/IP
- Změna jména stanice
- Přidání stanice do domény
- Migrace lokálních profilů na stanici do doménových profilů na stanici
  - migrace dokumentů, vlastnictví dokumentů, nastavení tiskáren, nastavení registrů, migrace certifikátů (osobní, šifrovací EFS) včetně privátního klíče, nastavení používaných aplikací Magistrátu města Frýdku Místku

Implementace File serveru

- Příprava dvou virtuálních serverů s Windows Server 2016 v aktuálním buildu + aktualizace v součinnosti se zadavatelem
- Implementace MS Failover Clusteru
- Konfigurace file serveru včetně FSRM, DFSN a Data Deduplication
- Vytvoření cluster resources dle zadavatele
- Implementace Access-based Enumeration na všechny sdílené složky
- Definice oprávnění na cluster resources
- Implementace funkce předchozí verze na sdílených souborech a složkách
- Migrace dat ze stávajícího FS (SAMBA)
    - Postupné vypínání původních sdílených složek a přejmenovávání cluster resources.
    - Úprava přístupu ze starého FS na nové sdílení na klientských stanicích
    - Pozn.: Migrace používané samby bude provedena po migraci koncových stanic a uživatelských účtů. Během migrace musí být dostupný přístup na původní FS pomocí stávajících přístupů.
- Definice kvót na sdílených složkách
- Nasazení technologie Dynamic Access Control s klasifikačními pravidly na sdílených složkách dle zadavatele
    - Nastavení schvalovacího procesu pro vedoucí odboru (cca 17 odborů)
- Začištění prostředí, ověření funkčnosti
- Instalace antivirové ochrany, zálohovacího software dle požadavků zadavatele
- Nastavení zálohování dle potřeb zadavatele na stávající NAS uložiště (Synology RS816), včetně konfigurace daného uložiště

Instalace RDS serveru

- Příprava virtuálního serveru s Windows Server 2016 v aktuálním buildu + aktualizace v součinnosti se zadavatelem
- Deaktivace licencí na stávajícím RDS serveru
- Instalace RDS role na novém serveru
- Konfigurace RDS rolí na novém RDS serveru – RD Web Access, RD Gateway, RD licensing, RD conntection broker, RD virtualization host, RD session host
- Vygenerování certifikátu, použití certifikátu pro RDS připojení
- Publikace RemoteApp aplikací

- Přenesení licence a aktivace RDS licenční služby
- Otestování připojení

Zaškolení pracovníku OIT

- první školení po dokončení implementace v rozsahu 8 hodin
- druhé školení po měsíci od dokončení implementace v rozsahu 8 hodin

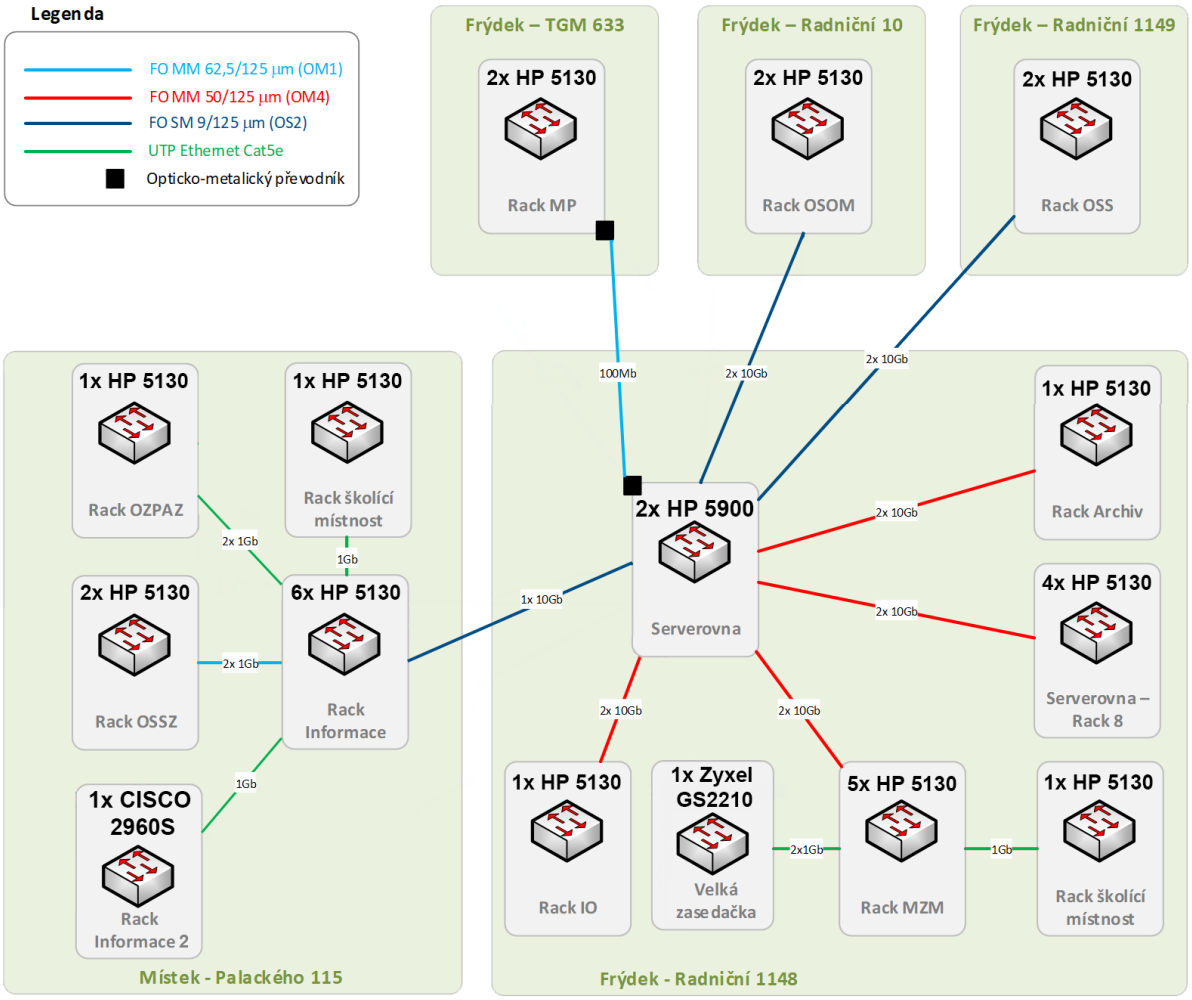
1.2. Readresace a segmentace síťové infrastruktury a aplikace bezpečnostních opatření

1.2.1. Popis stávajícího stavu

Stávající síťová struktura je rozmístěná do 5 lokalit. Jednotlivé lokality jsou mezi sebou propojeny optickou kabeláží. Konkrétní lokality jsou uvedeny v následující tabulce:

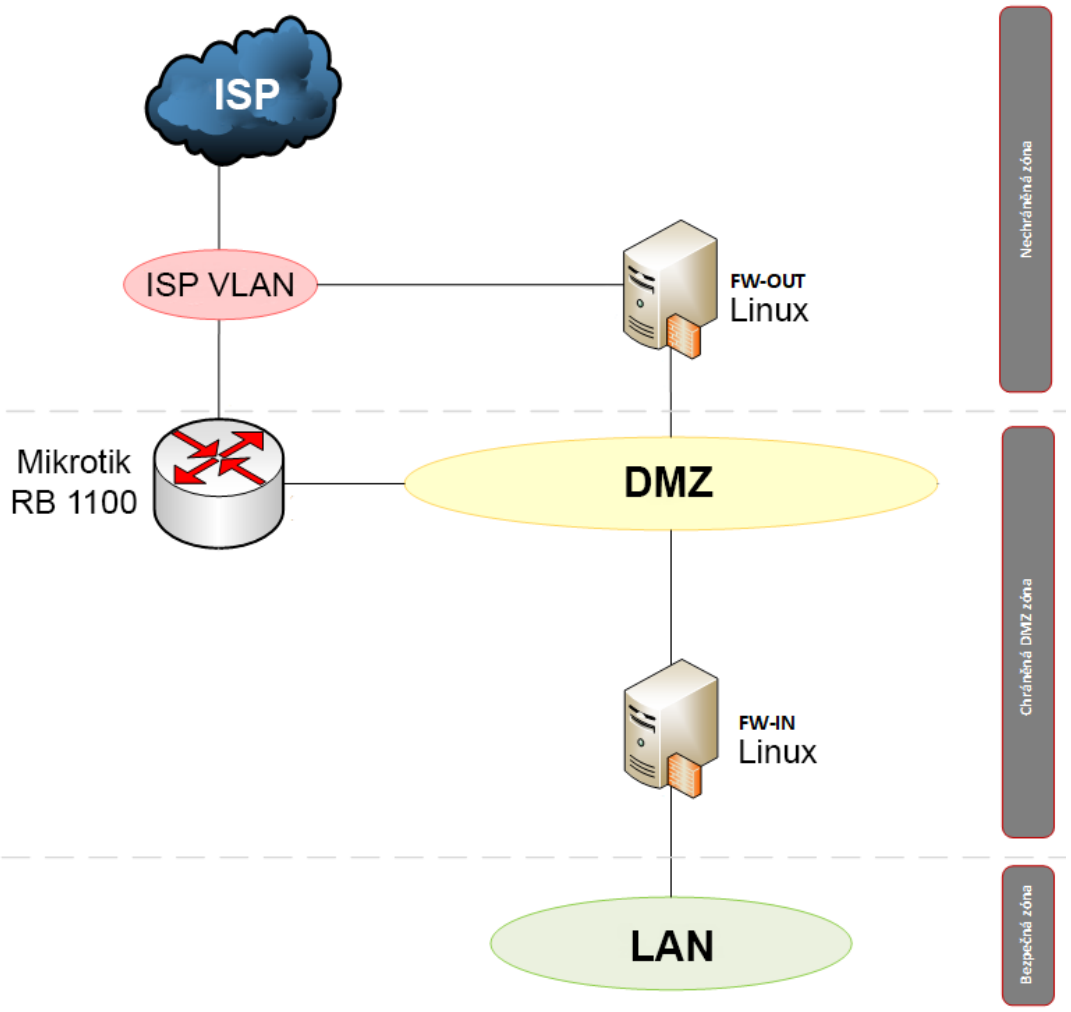
Č.	Lokalita (adresa)	Popis
1	**Radniční 1148, Frýdek**	Hlavní budova (lokace hlavní serverovny)
2	**Radniční 1149, Frýdek**	Vedlejší budova (odbor sociální služeb OSS)
3	**Radniční 10, Frýdek**	Vedlejší budova (odbor správy obecního majetku OSOM)
4	**Tř. TGM 633, Frýdek**	Sídlo Městské policie
5	**Palackého 115, Místek**	Odbor správy sociálního zabezpečení (OSSZ) apod.

Současná síťová infrastruktura je postavená na 2x core switchi HP 5900, 28x switchi HP 5130, 1x switchi Cisco 2960-S a 1x Zyxel GS2210-24HP. V jednotlivých rack rozvaděčích jsou switche zapojeny do jednoho stacku. Rozmístění všech switchů znázorňuje následující obrázek:



Celá LAN síť (zahrnující počítače, servery, tiskárny, aktivní prvky apod.) běží v jedné defaultní VLAN v jednom IP prostoru. Všechny přepínače pracují v režimu L2.

Výchozí bránou pro zařízení v LAN síti je linuxový firewall „FW-IN". Vnější rozhraní firewallu je připojeno do DMZ zóny. Rozhraní mezi DMZ zónou a internetem tvoří další linuxový firewall „FW-OUT". V síťové infrastruktuře figuruje třetí firewall Mikrotik. Toto zařízení slouží jako výchozí brána pro vybrané servery v DMZ zóně. Schéma zapojení je zobrazeno na obrázku níže.



1.2.2. Technická specifikace

Tato kapitola popisuje základní požadavky pro implementaci. Podrobnější požadavky pro nastavení plynoucí z analýzy budou dodány zadavatelem.

Readresace síťové infrastruktury s ohledem na jednotlivé segmenty sítě

- readresace IP adres bude provedená na všech síťových zařízeních a rozhraních připojených do síťové infrastruktury, do které patří:
  - přibližně 50 virtuálních produkčních serverů
  - přibližně 10 systémů napájení a dohledu (PDU, UPS, apod.)
  - přibližně 20 zařízení a rozhraní serverové infrastruktury (SAN, NAS, virtualizační prostředí, management rozhraní, apod.)
  - přibližně 500 koncových stanic uživatelů – desktopy, notebooky
  - přibližně 350 tiskáren a kopírek
  - přibližně 15 terminálů (docházka, závory, čtečky, přístupové systémy, platební terminály)

  - přibližně 30 aktivních prvků
  - přibližně 10 zařízení kamerového systému (kamery, rekordéry, enkodéry)
  - přibližně 20 zařízení velké zasedací místnosti (audiovizuální technika)

- součástí readresace bude vytvoření rezervací adres jednotlivých zařízení na straně DHCP serverů (vazba IP/MAC)
- readresace ze starého rozsahu na nový bude probíhat postupně v určitých úsecích jak za provozu, tak v případných odstávkách, bude-li třeba (možnost odstávek je popsán v kapitole 2.3 tohoto dokumentu)
- během migrace je potřeba zajistit společnou funkčnost obou IP rozsahů, nových a stávajících, až do doby, než bude dokončená readresace celé síťové infrastruktury (zajištění dostupnosti všech serverů a aplikací)
- konkrétní IP rozsahy jednotlivých segmentů bude dodán zadavatelem
- celá readresace bude vycházet z podrobné dokumentace s popisem implementace, která bude předána zadavatelem
- readresace koncových stanic bude prováděná současně během migrace do nové domény
- nastavení potřebných DHCP relay

Segmentace síťové infrastruktury na logické celky pomocí VLAN

- vytvoření příslušných VLAN v rámci celé infrastruktury (přibližně 30 VLAN segmentů)
- oddělení DMZ od vnitřní LAN sítě
- vytvoření L3 rozhraní na páteřním (core) přepínači (směrování pomocí inter-vlan routingu a případně access listů)
- definice IP poolů na DHCP severech pro jednotlivé segmenty VLAN
- celá segmentace pomocí VLAN bude vycházet z podrobné dokumentace s popisem implementace, která bude předána zadavatelem

Zabezpečení síťové infrastruktury

- nastavení přístupu na síťové zařízení s využitím uživatelských účtů administrátorů z domény (autentizace, autorizace a accounting vůči RADIUS/TACACS serveru)
- nastavení a konfigurace multiple spanning-tree protokolu (definice priorit přepínačů)
- nastavení „edge" a „point-to-point" na portech všech přepínačů
- nastavení bezpečnostních mechanismů BPDU Guard, STP Root Guard, Loop Guard
- zabezpeční proti VLAN hoppingu, MAC floogingu (port security, nastavení access portů), DHCP spoofingu (DHCP snooping) a ARP spoofingu (Dynamic ARP Inspection, IP source Guard)

Zaškolení pracovníku OIT

- první školení po dokončení implementace v rozsahu 8 hodin
- druhé školení po měsíci od dokončení implementace v rozsahu 8 hodin

1.3. Plán migrace a odstávek

Migrace stanic a dat bude probíhat postupně za provozu po pracovní době s tím, že první část migrace bude testovací na vybrané množině zařízení a uživatelů, po otestování veškeré funkčnosti bude provedená migrace zbylých zařízení a uživatelů.
Harmonogram migrací bude vycházet z možností odstávek systémů a sítě následovně:

- pondělí a středa od 17:30 do 19:00
- úterý a pátek od 14:00 do 19:00
- čtvrtek od 15:30 do 19:00

Pro migrace stanic budou k dispozici zaměstnanci OIT.