Regionální síť mikroregionu Horácko
SO 03 Aktivní technologie

A.1 Technická zpráva

Stavební objekt SO 03 řeší aktivní technologii stavby „Regionální síť mikroregionu Horácko“. Jde regionální síť spojující 13 specifikovaných obcí, tj. **Budišov, Číměř, Hodov, Kamenná, Kojatín, Koněšín, Nárameč, Pozďatín, Přeckov, Rohy, Studnice, Trnava a Vladislav,** stavební objekt SO 03 řeší aktivní část propojovací sítě, tj. návrh aktivních síťových prvkův rozsahu koncových zařízení, serverové platformy, FO transceiverů, pasivního zakončení a propojovacích kabelů i souvisejících non-IT komponent (UPS, monitorovací systém), včetně rozpočtu stavby. Součástí je i návrh aktivních prvků pro hlavní vstupní uzly sítě „Main POP“, situované v Třebíči (Objekt Nemocnice Třebíč, Purkyňovo náměstí 133/2) a Velkém Meziříčí (objekt MěÚ Velké Meziříčí, Radnická 29/1).

SO 03 navazuje na SO 02 Regionální síť mikroregionu Horácko, přístupová síť, ve kterém je navržena pasivní optická infrastruktura. Při zpracování projektu SO 03 byl využit zejména dokument „Technická studie řešení projektu „Regionální sítě mikroregionu Horácko““, z nějž byla převzata topologie sítě a požadované specifikace aktivních prvků.

1. Aktivní část propojovací sítě

1.1. Technologie pro aktivní část sítě

Aktivní část sítě bude realizována síťovými prvky splňující standard Ethernet, určenými pro výstavbu transportních sítí.

Komplexní řešení je tvořeno transportní vrstvou a technologiemi zajišťujícími samotný provoz celku. Základní stavebním kamenem transportní části je logický kruh s propustností 10GBps. Vlastnosti aktivních prvků v distribučním kruhu jsou koncipovány pro provoz charakteristický v sítích poskytovatelů služeb (TELCO operátorů). To kromě běžných funkcí přepínače a směrovače vyžaduje vlastnosti k efektivnějšímu řešení řízení provozu v síti (MPLS/VPLS), k prokazování kvality poskytovaných služeb (IP SLA agenti, a atd.) a k jejich vysoké dostupnosti. Díky tomuto návrhu splňuje infrastruktura podmínky pro nasazení základních datových služeb, ale i služeb multimediálního charakteru, jako je VoIP nebo IP TV.

Technologie zajišťující dohled a správu, dále analýzu chování sítě a monitoringu SLA budou umístěny v technologickém centru rozprostřeném do dvou lokalit. Mezi těmito celky bude vytvořena bezpečnostní hranice v podobě clusteru dvou firewallů. Vlastnosti této vrstvy zajišťují především vzdálený přístup pro smluvní partnery (poskytovatele služeb) k reportingu a službám prokazujícím SLA (funkce remote VPN, autorizace, atd.), administraci, dále pak zajišťují bezpečné oddělení systémových zdrojů umístěných v technologickém centru (využití NAT, PAT, atd.)

Ve všech lokalitách jsou navrženy součinné systémy (non-IT systémy) pro zajištění fyzické bezpečnosti a ochrany investic do pořizovaného majetku. Sledování environmentálních veličin, jako je vlhkost, teplota apod. napomáhá také k celkovému zvýšení dostupnosti všech zařízení.

Oblasti řešení z hlediska prvků a zařízení:

1. **Pasivní ukončení tras**
   (datové rozvaděče, DWDM pasivní rozbočovače a multiplexery)

2. **Aktivní prvky**
   (koncová zařízení - páteřní přepínače, páteřní směrovače, monitorovací sondy). Pro zajištění homogenního komunikačního prostředí je požadováno, aby nabízené přepínače a směrovače (popř. L3 přepínače) v rámci transportní sítě byly od jednoho výrobce.

3. **Serverová platforma**
   (HW, SW, OS/DB, Virtualizační SW, kolektor s mechanismy analýzy chování sítě, monitorovací SW)

4. **FO Trancievery**
   (optické, metalické trancievery)

5. **Propojovací kabely**

6. **Součinné systémy non-IT systémy**
   (, jednotky distribuovaného napájení, UPS agregát, Rackmontoring systém (RMS) – čidla výpadku napájení, dveřní a teplotní čidla, kouřový detektor)

Požadované parametry a funkcionality na vybavení PoP, MainPoP, TC u výše uvedených prvků řešení jsou následně podrobně specifikovány v následující kapitole 1.2

1.2. Vybavení aktivními prvky a součinnými NON-IT subsystémy

Tato kapitola popisuje vybavení aktivními prvky a součinnými NON-IT subsystémy v rámci aktivní části propojovací sítě v jednotlivých bodech a lokalitách:

- MainPoP
  - Velké Meziříčí
  - Třebíč

- PoP
  - Budišov
  - Číměř
  - Hodov
  - Kamenná
  - Kojatín
  - Koněšín
  - Nárameč
  - Pozďatín
  - Přeckov
  - Rohy
  - Studnice
  - Trnava
  - Vladislav

- Technologické centrum
    - Velké Meziříčí
    - Třebíč

- Zemní spojka + DWDM add/drop moduly
    - Rudíkov
    - Vlčatín
    - Trnava

1.2.1. Instalace bodu typu MainPOP

V lokalitě tohoto typu je očekáváno již alespoň minimální zázemí technologické místnosti, minimálně v podobě řízeného přístupu osob, zajištění dodávky el. energie do místa umístění technologie mikroregionu a také klimatizace.
Všechny aktivní technologie budou instalovány do nového, samostatně zamykatelného datového rozvaděče v provedení 19“, 42U , min 800x1000mm s perforovanými dveřmi.
V datovém rozvaděči budou umístěny tyto technologie a vybavení:

- Komunikační infrastruktura:
    - Páteřní Router (popř. přepínač s funkcí směrování)
    - DWDM MUX/DEMUX 8kanál 1 vláknový

- NON-IT:
    - UPS
    - RMS RackMonitoring Systém - včetně čidel
    - PDU (PowerDistributionUnit)
    - Podružný elektrický rozvaděč s centrálním vypínačem (jističem)

Páteřní PE směrovač (popř. L3 přepínač) MainPOP bodu KI

Požadované vlastnosti:
- zajištění plné kompatibility s obecnými link-state a distance-vector protokoly (pathvectorprotocol), včetně rozšíření BGP – MP BGP, a kompatibility s rfc4364, rfc2547, rfc4577, rfc4684, rfc5462 (MPLS),
- minimálně 24x 10/100/1000Base-T, 8 porty 10GbE v provedení SFP+ a 16x 100/1000Base-X (SFP),
- redundandní zdroje napájení,
- maximální velikost 2U,
- možnost rozšířitelnosti o minimálně 4 40gbE porty
- podpora minimálně 256 000 MAC adres
- možnost dynamicky (LACP - 802.3ad) vytvářet agregované kanály z několika paralelně vedených segmentů,
- přepínání v L3 (IPv4 a IPv6),
- bezpečnostní filtrace provozu podle L2/3/4 atributů. Seznamy pravidel musí být aplikovatelné na L2 port, virtuální LAN, fyzický nebo virtuální (VLAN) L3 port
- diferencovaná obsluha (QoS) podle L2/3/4 atributů,
- podpora MPLS a VPLS,
- klasifikace a reklasifikace (EthernetCoS, IP DSCP/ToS),
- omezování provozu (policing) a/nebo „uhlazování“ (shaping) provozu na výstupu,
- per-user policing, 8 front na výstupu každého portu (z toho jedna s absolutní prioritou)

- hardwarová podpora monitorování paketů protokolu IGMP a inteligentního přepínání multicastového provozu podle IGMP ver. 2, resp. 3 požadavků z jednotlivých portů (IGMP snooping),
- zadavatel požaduje, aby již dodaná konfigurace podporovala dynamické směrovací protokoly RIP v1/v2 OSPFv1/v2/v3 BGP-4 a BGP 4+,,PIM, PIMv6,
- zadavatel požaduje, aby již dodaná konfigurace podporovala MPLS a to jak MPLS VPN (L3) tak MPLS Traficengineering (MPLS TE),
- zadavatel požaduje, aby již dodaná konfigurace podporovalaVPLS VPN (L2),
- možnost současné konfigurace IPv4 i IPv6 adresy na 1 rozhraní,
- podpora IEEE 802.1w a 802.1s,
- podpora mechanizmu pro detekci jednosměrných tras (UDLD),
- podpora 4096 VLAN dle standardu 802.1Q,
- podpora privátních VLAN (izolace portů nebo skupin portů uvnitř VLAN),
- podpora protocolbased VLAN dle standardu 802.1v, u IP protocolbased VLAN musí být podpora na IP subnet a příslušnou masku,
- podpora Q-in-Q VLAN (VLAN stacking) dle standardu 802.1ad,
- podpora SuperVLAN (RFC3069),
- podpora GARP a GVRP,
- podpora následujících směrovacích protokolů: RIPv1/v2, RIPng OSPF, OSPFv3, BGP-4, BGP-4+, PIM, PIMv6 a MSDP,
- podpora protokolu VRRP a VRRPv3 v režimu virtual MAC,
- podpora DHCP serveru, UDP helperu, DHCP Relay Agent InformationOption (RFC3046),
- prostředky ochrany proti útokům využívajícím protokolu ARP a IP spoofingu: monitorování DHCP provozu (s hardwarovou podporou) a vytváření dynamické tabulky korektního přiřazení portu, MAC adresy a IP adresy (DHCP snooping), na jejímž základě se rozpozná a indikuje a/nebo nepovolí nekorektní pakety protokolu ARP (Dynamic ARP Inspection), popř. datové pakety s nekorektní kombinací zdrojové IP adresy a MAC adresy (IP Source Guard), konfigurovatelné prostředky ochrany CPU proti DoS útokům, IP packetattack, ARP packetattack a 802.1X packetattack na CPU,
- prostředky na řízení maximálního množství broadcast a multicast provozu v každé definované virtuální síti,
- na L2 je požadována podpora protokolů IEEE 802.1w (Rapid SpanningTree),
- prostředky ochrany před rámci BPDU s nižší prioritou, než má předpokládaný kořenový přepínač sítě SpanningTree domény (RootGuard),
- snadná instalace (Auto IP, DHCP klient, BootP klient),
- možnost pro diagnostické účely zrcadlit na zvoleném portu provoz libovolného jiného portu, skupiny portů nebo VLAN. A to s podporou filtrace podle přístupového seznamu. Podpora více monitorujících stanic k jednomu zrcadlenému zdroji a možnost vzdáleného monitorování RSPAN,
- plná podpora Network Login 802.1X (požadováno ověřování pro každý systém registrovaný na portu se zapnutý 802.1X individuálně – registrace svázána s MAC adresou, nikoliv fyzickým portem přepínače),
- řízení přístupu správce zařízení pomocí RADIUS,
- podpora SSHv2, SNMPv3.

Centrální firewally

Pro oddělení datových toků mezi transportní sítí a TC bude použita dvojice firewallových jednotek. Požadované vlastnosti:

- HW appliance.
- Podpora instalace do clusteru.
- Celková propustnost zařízení: alespoň 20 Gbps
- Propustnost IPS alespoň 8Gbps.
- Propustnost IPSec VPN alespoň 15Gbps.
- Počet současně navázaných konexí alespoň 7.000.000.
- Počet portů: min. 2x 10Gb SFP+, 16x10/100/1000 Mbps z toho alespoň 8 SFP portů a 1x10/100/1000 Mbps management port pro OOB.
- Zařízení licencováno neomezeně, ne na počet chráněných uživatelů ani IP adres.
- Maximální velikost 3U
- Možnost rozšíření o antivirovou ochranu stanic a uživatelů.
- Možnost rozšíření o antispamovou ochranu stanic a uživatelů.
- Možnost rozšíření o IPS (IntrusionPreventionSystem) ochranu stanic a uživatelů.
- Možnost rozšíření o WEB filtering ochranu stanic a uživatelů.
- Rozpoznání, detekce a řízení aplikací na 7. vrstvě.
- Podpora IPv6 alespoň v následujících oblastech – na síťové úrovni, firewall, antivir, webfiltering, IPS, dynamický routing (RIP, OSPF, BGP), SIP, DNS, bridge mód, IPv6 tunnelover IPv4, IPv4 tunnelover IPv6.
- Podpora VPN spojení (IPSec, VPN, SSL VPN, L2TP VPN, MPLS VPN a GRE)).
- Podpora SSL VPN v portálovém i tunelovém módu.
- Podpora autorizace uživatelů (LDAP, TACACS+, RADIUS, lokální databáze, X-Auth).
- Podpora Vulnerability Managementu (schopnost zařízení aktivně skenovat síť a vyhledávat její zranitelnosti a problémy).
- Podpora HighAvailability (clusterování v režimech A-P i A-A) na L2 vrstvě s licencí obsaženou v ceně zařízení.
- Možnost provozu zařízení v routovacím režimu (routing, NAT, PAT).
- Možnost provozu zařízení v režimu bridge (při zachování všech relevantních kontrol provozu).
- Podpora VLAN tagging (802.1Q).
- Možnost použít zařízení jako http/https/ftpproxy.
- Možnost definice vlastních IPS a aplikačních signatur.
- Podpora více WAN linek připojení do internetu.
- Podpora PPPoE.
- Schopnost zařízení fungovat jako DHCP klient i DHCP server.
- Podpora dynamického routování pro IPv4 i IPv6 (RIP, OSPF i BGP).
- Podpora routování multicast protokolů.
- Podpora VRRP protokolu.
- Podpora prioritizace provozu až na aplikační úrovni (7. vrstva) – priorita provozu, garantovaná a maximální šířka pásma, atp ...
- Podpora SNMP v1, v2c i v3.
- Možnost využít zařízení jako loadbalancer pro interní servery poskytující shodný obsah.
- Možnost počeštění veškerých dialogů komunikujících s uživatelem.
- Podpora virtualizace firewallu - plná funkcionalita jednotlivých virtuálních firewallů.
- Možnost podrobného reportování událostí na síti, aktivit a tendencí, které se odehrávají na firewallu v reálném čase.
- Grafické rozhraní pro kompletní správu firewallu.

V rámci ochrany investic a instalovaných technologií, budou datové rozvaděče (DR) vybaveny součinnými systémy, které nemají přímý charakter IT. Jedná se o:

Napájecí zdroj UPS

Jeho účelem je pokrýt okamžiky přerušení dodávek napájení el. energie. UPS musí být vybavena síťovým komunikačním modulem s rozhraním RJ-45 a podporou SNMP. UPS v provedení pro montáž do 19“ racku. Minimální doba pro běh instalovaných technologií je 60 minut. POZOR: UPS bude zabezpečovat i provoz instalace Technologického centra dle 1.2.3.

Vyvazovací panely pro kabeláž

Vyvazovací panely datové kabeláže je opět nutno volit v dostatečném počtu, tak aby všechny kabely mohly být bezpečně vyvázány – minimálně 1ks v každém rozvaděči.

RMS – Rack Monitoring System

Systém pro kontrolu environmentálních veličin by měl obsahovat čidla, která budou zajišťovat kontrolu definovaných parametrů. Klíčovou vlastností je také schopnost systému předávat události do centrálního dohledového systému. Součástí řešení každého RMS by měly být také následující čidla:

- dveřní čidla – instalované na dveře DR
- teplotní/vlhkostní čidlo – instalované uvnitř DR
- kouřové čidlo – uvnitř DR
- čidlo výpadku napájení – umístěno uvnitř racku, před UPS

Jednotky distribuovaného napájení, PDU

Distribuce přívodu elektřiny k síťové a serverové technologii musí být systémově řešena. PDU jednotky je nutno volit minimálně pro příkon 16A. Jejich zásuvky musejí být monitorovatelné a kontrolovatelné z hlediska jednotlivého vypnutí nebo zapnutí po IP protokolu. Počet zásuvek v PDU musí pokrýt potřebu navržené technologie. Zpráva PDU musí být podporována minimálně pomocí CLI (Telnet) nebo http protokolu.
Při implementace je nutné nezapomenout na zajištění revizní zprávy.POZOR: PDU bude zabezpečovat i instalaci Technologického centra dle 1.2.3.

1.2.2. Instalace bodu typu POP

Jak již bylo zmíněno, v lokalitě tohoto typu není očekáváno žádné zázemí technologické místnosti, proto je nutné zajistit podmínky pro celoroční chod technologie uvnitř datového rozvaděče (DR). V mnohých případech budou nutné také úpravy přívodní elektrické soustavy do místa umístění DR.
Umístění všech aktivních technologií bude v novém, samostatně zamykatelném rozvaděči v provedení 19“, minimálně 20U, min. 600x900mm s plnými dveřmi. Rack musí být přístupný zepředu i zezadu.
Pro lokality s plánovanou výstavbou lokální přístupové sítě je pak minimální výška skříně 42U.
V datovém rozvaděči by měly být umístěny tyto technologie a vybavení:

- Komunikační infrastruktura:
    - Páteřní L3 přepínač

- NON-IT:
    - UPS
    - RMS RackMonitoring Systém - včetně čidel
    - ventilační jednotka včetně termostatu
    - PDU (PowerDistributionUnit)
    - Podružný elektrický rozvaděč s centrálním vypínačem (jističem)

PE přepínač POP bodu KI

Požadované vlastnosti:
- Minimálně 24 100/1000Base-X (SFP), 4 porty 10GbE v provedení SFP+ a slot pro volitelný modul s podporou dalších minimálně 4 portů 10GbE
- redundandní zdroje napájení,
- možnost dynamicky (LACP - 802.3ad) vytvářet agregované kanály z několika paralelně vedených segmentů,
- přepínání v L3 (IPv4 a IPv6),
- redundantní zdroj napájení,
- maximální velikost 1U,
- bezpečnostní filtrace provozu podle L2/3/4 atributů. Seznamy pravidel musí být aplikovatelné na L2 port, virtuální LAN, fyzický nebo virtuální (VLAN) L3 port,
- diferencovaná obsluha (QoS) podle L2/3/4 atributů,
- podpora MPLS a VPLS,
- klasifikace a reklasifikace (EthernetCoS, IP DSCP/ToS),
- omezování provozu (policing) a/nebo „uhlazování“ (shaping) provozu na výstupu,
- per-user policing, 8 front na výstupu každého portu (z toho jedna s absolutní prioritou)
- hardwarová podpora monitorování paketů protokolu IGMP a inteligentního přepínání multicastového provozu podle IGMP ver. 2, resp. 3 požadavků z jednotlivých portů (IGMP snooping),
- zadavatel požaduje, aby již dodaná konfigurace podporovala dynamické směrovací protokoly RIP v1/v2 OSPFv1/v2/v3 BGP-4 a BGP 4+,,PIM, PIMv6,
- zadavatel požaduje, aby již dodaná konfigurace podporovala MPLS a to jak MPLS VPN (L3) tak MPLS Traficengineering (MPLS TE),
- zadavatel požaduje, aby již dodaná konfigurace podporovala VPLS VPN (L2),
- možnost současné konfigurace IPv4 i IPv6 adresy na 1 rozhraní,
- podpora IEEE 802.1w a 802.1s,
- podpora mechanizmu pro detekci jednosměrných tras (UDLD),
- podpora 4096 VLAN dle standardu 802.1Q,
- podpora minimálně 128 000 MAC adres
- podpora privátních VLAN (izolace portů nebo skupin portů uvnitř VLAN),
- podpora protocolbased VLAN dle standardu 802.1v, u IP protocolbased VLAN musí být podpora na IP subnet a příslušnou masku,
- podpora multicast VLAN,
- podpora Q-in-Q VLAN (VLAN stacking) dle standardu 802.1ad,
- podpora SuperVLAN (RFC3069),
- podpora GARP a GVRP,
- podpora následujících směrovacích protokolů: RIPv1/v2, RIPng OSPF, OSPFv3, BGP-4, BGP-4+, PIM, PIMv6 a MSDP,
- podpora protokolu VRRP a VRRPv3 v režimu virtual MAC,

- podpora DHCP serveru, UDP helperu, DHCP Relay Agent InformationOption (RFC3046),
- prostředky ochrany proti útokům využívajícím protokolu ARP a IP spoofingu: monitorování DHCP provozu (s hardwarovou podporou) a vytváření dynamické tabulky korektního přiřazení portu, MAC adresy a IP adresy (DHCP snooping), na jejímž základě se rozpozná a indikuje a/nebo nepovolí nekorektní pakety protokolu ARP (Dynamic ARP Inspection), popř. datové pakety s nekorektní kombinací zdrojové IP adresy a MAC adresy (IP Source Guard), konfigurovatelné prostředky ochrany CPU proti DoS útokům, IP packetattack, ARP packetattack a 802.1X packetattack na CPU,
- prostředky na řízení maximálního množství broadcast a multicast provozu v každé definované virtuální síti,
- na L2 je požadována podpora protokolů IEEE 802.1w (Rapid SpanningTree)
- prostředky ochrany před rámci BPDU s nižší prioritou, než má předpokládaný kořenový přepínač sítě SpanningTree domény (RootGuard),
- snadná instalace (Auto IP, DHCP klient, BootP klient),
- možnost pro diagnostické účely zrcadlit na zvoleném portu provoz libovolného jiného portu, skupiny portů nebo VLAN. A to s podporou filtrace podle přístupového seznamu. Podpora více monitorujících stanic k jednomu zrcadlenému zdroji a možnost vzdáleného monitorování RSPAN,
- plná podpora Network Login 802.1X (požadováno ověřování pro každý systém registrovaný na portu se zapnutý 802.1X individuálně – registrace svázána s MAC adresou, nikoliv fyzickým portem přepínače),
- řízení přístupu správce zařízení pomocí RADIUS,
- podpora SSHv2, SNMPv3
- možnost rozšíření o licenci pro správu WIFI přístupových bodů, podpora až 100AP

Síťový L3 prvek bude zapojen ze dvou směrů do síťových prvků v sousedních uzlech dle logické topologie pomocí jednoho nebo dvou optických vláknech nebo dvou DWDM lambd. Tomu musí odpovídat zvolené optické moduly.

V rámci ochrany investic a instalovaných technologií, budou DR v Uzlových bodech vybaveny součinnými systémy, které nemají přímý charakter IT. Jedná se o:

Napájecí zdroj UPS

Jeho účelem je pokrýt okamžiky přerušení dodávek napájení el. energie. UPS musí být vybavena síťovým komunikačním modulem s rozhraním RJ-45 a podporou SNMP. UPS pro montáž do 19“ racku. Minimální doba pro běh instalovaných technologií je 60 minut. Umístěn ve spodní části skříně.

Vyvazovací panely pro kabeláž

Vyvazovací panely datové kabeláže je opět nutno volit v dostatečném počtu, tak aby všechny kabely mohly být bezpečně vyvázány – minimálně 1ks v každém rozvaděči.

.

RMS – Rack Monitoring System

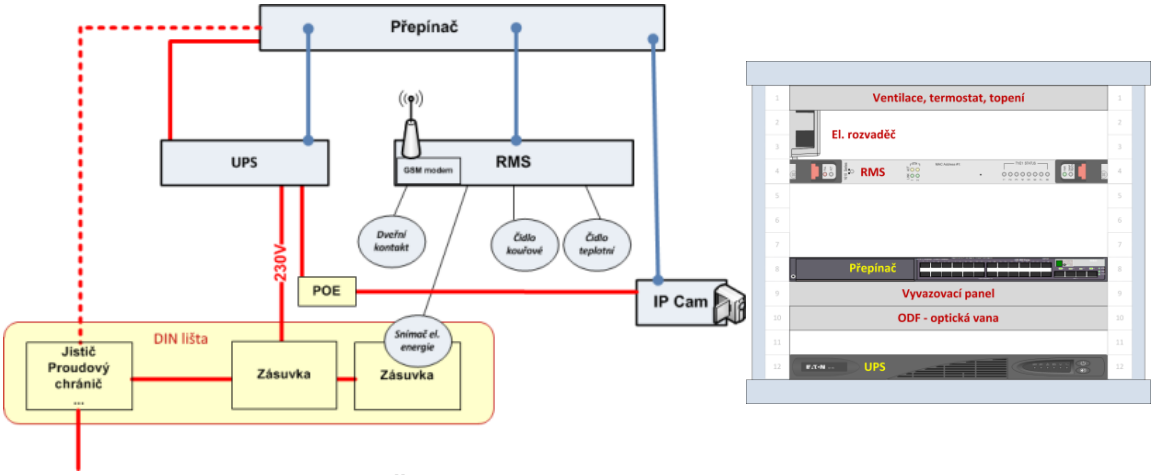
Systém pro kontrolu environmentálních veličin by měl obsahovat čidla, která budou zajišťovat kontrolu definovaných parametrů. Klíčovou vlastností je také schopnost systému předávat události do centrálního dohledového systému. Součástí řešení každého RMS by měly být také následující čidla:
- dveřní čidla – instalované na dveře DR

- teplotní/vlhkostní čidlo – instalované uvnitř DR
- teplotní čidlo – instalované vně
- kouřové čidlo – uvnitř DR
- čidlo výpadku napájení – umístěno uvnitř racku, před UPS

Jednotky distribuovaného napájení, PDU,Podružný elektrický rozvaděč s centrálním vypínačem (jističem)

Distribuce přívodu elektřiny k síťové a serverové technologii musí být systémově řešena. PDU jednotky je nutno volit minimálně pro příkon 16A. Jejich zásuvky musejí být monitorovatelné a kontrolovatelné z hlediska jednotlivého vypnutí nebo zapnutí po IP protokolu. Počet zásuvek v PDU musí pokrýt potřebu navržené technologie. Zpráva PDU musí být podporována minimálně pomocí CLI (Telnet) nebo http protokolu.
Při implementace je nutné nezapomenout na zajištění revizní zprávy.
Umístění ve spodní části skříně.

Doporučené schéma zapojení aktivních technologií



Obrázek č.10: Schéma zapojení aktivních technologií

1.2.3. Instalace Technologického centra

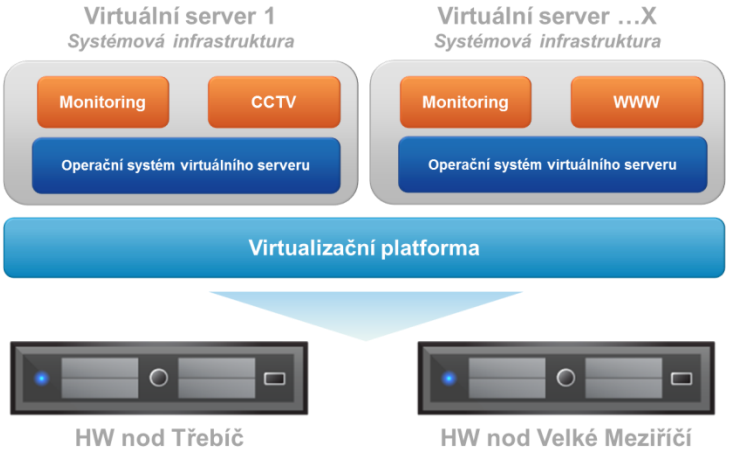
Technologické centrum je v projektu regionální sítě určeno především pro systémovou infrastrukturu zajišťující vlastní chod a životní cyklus infrastruktury a služeb, které nabízí.
Bude instalováno v lokalitách Main POP do datových rozvaděčů osazených v rámci části Instalace bodu typu Main POP – kapitola 1.2.1.

Jedná se především o:
- Řešení serverové platformy pro účely dohledu a správy subsystému
- Performance monitoring a monitoring SLA poskytovaných služeb
- Řešení kamerového dohledu

Řešení serverové platformy pro účely dohledu a správy KI

Technologické centrum se skládá z HW prvků v obou Main POPech. Základem každého HW nodu je klasický server s interními pevnými disky. Nad HW vrstvou nodů bude implementována virtualizační platforma a vlastní aplikace pak budou spouštěny z virtuálních serverů s definovaným operačním systémem.

Obrázek č.11: Schéma doporučeného řešení serverové platformy



Požadované vlastnosti HW nodů:

- provedení do racku, rozměr max. 4RU
- minimálně 2x fyzický procesor
- min. 8 slotů na paměti DDR3 typu ECC Unbuffered
- minimálně 32 GB RAM DDR3 provozována minimálně na 1600 MHz
- 64-bit architektura
- velikost disků 2x 4TB 7.2K RPMNear-Line SAS 6Gbps 3.5in Hot-plug Hard Drive, zapojených v RAID 1
- USB porty (pro možnost připojit USB licenční klíče)
- redundantní napájecí zdroj
- energetická účinnost zdrojů 80 PLUS Silver nebo lepší
- IPMI vč. licence.
- minimálně 8x Hot-swap 3,5" SAS/SATA HDD pozice
- LAN konektivita minimálně 2x 1Gbit rozhraní
- podpora nejrozšířenějších operačních systémů (Windows server, Linux Debian atd.)
- včetně 2x OS Windows Server 2012 a potřebných licencí, které umožní provoz 4 virtuálních serverů s tímto OS v rámci dodané virtualizační platformy

Přepínače pro připojení serverů TC

- minimálně 24 10/100/1000Base-T, 4 porty 10GbE v provedení SFP+ a slot pro volitelný modul s podporou dalších minimálně 4 portů 10GbEmožnost dynamicky (LACP - 802.3ad) vytvářet agregované kanály z několika paralelně vedených segmentů,
- přepínání v L3 (IPv4 a IPv6),
- redundantní zdroj napájení,
- maximální velikost 1U,
- bezpečnostní filtrace provozu podle L2/3/4 atributů. Seznamy pravidel musí být aplikovatelné na L2 port, virtuální LAN, fyzický nebo virtuální (VLAN) L3 port,
- diferencovaná obsluha (QoS) podle L2/3/4 atributů,
- podpora MPLS a VPLS,

- klasifikace a reklasifikace (EthernetCoS, IP DSCP/ToS),
- omezování provozu (policing) a/nebo „uhlazování“ (shaping) provozu na výstupu,
- per-user policing, 8 front na výstupu každého portu (z toho jedna s absolutní prioritou)
- hardwarová podpora monitorování paketů protokolu IGMP a inteligentního přepínání multicastového provozu podle IGMP ver. 2, resp. 3 požadavků z jednotlivých portů (IGMP snooping),
- zadavatel požaduje, aby již dodaná konfigurace podporovala dynamické směrovací protokoly RIP v1/v2 OSPFv1/v2/v3 BGP-4 a BGP 4+,,PIM, PIMv6,
- zadavatel požaduje, aby již dodaná konfigurace podporovala MPLS a to jak MPLS VPN (L3) tak MPLS Traficengineering (MPLS TE),
- zadavatel požaduje, aby již dodaná konfigurace podporovala VPLS VPN (L2),
- možnost současné konfigurace IPv4 i IPv6 adresy na 1 rozhraní,
- podpora IEEE 802.1w a 802.1s,
- podpora mechanizmu pro detekci jednosměrných tras (UDLD),
- podpora 4096 VLAN dle standardu 802.1Q,
- podpora minimálně 128 000 MAC adres
- podpora privátních VLAN (izolace portů nebo skupin portů uvnitř VLAN),
- podpora protocolbased VLAN dle standardu 802.1v, u IP protocolbased VLAN musí být podpora na IP subnet a příslušnou masku,
- podpora multicast VLAN,
- podpora Q-in-Q VLAN (VLAN stacking) dle standardu 802.1ad,
- podpora SuperVLAN (RFC3069),
- podpora GARP a GVRP,
- podpora následujících směrovacích protokolů: RIPv1/v2, RIPng OSPF, OSPFv3, BGP-4, BGP-4+, PIM, PIMv6 a MSDP,
- podpora protokolu VRRP a VRRPv3 v režimu virtual MAC,
- podpora DHCP serveru, UDP helperu, DHCP Relay Agent InformationOption (RFC3046),
- prostředky ochrany proti útokům využívajícím protokolu ARP a IP spoofingu: monitorování DHCP provozu (s hardwarovou podporou) a vytváření dynamické tabulky korektního přiřazení portu, MAC adresy a IP adresy (DHCP snooping), na jejímž základě se rozpozná a indikuje a/nebo nepovolí nekorektní pakety protokolu ARP (Dynamic ARP Inspection), popř. datové pakety s nekorektní kombinací zdrojové IP adresy a MAC adresy (IP Source Guard), konfigurovatelné prostředky ochrany CPU proti DoS útokům, IP packetattack, ARP packetattack a 802.1X packetattack na CPU,
- prostředky na řízení maximálního množství broadcast a multicast provozu v každé definované virtuální síti,
- na L2 je požadována podpora protokolů IEEE 802.1w (Rapid SpanningTree)
- prostředky ochrany před rámci BPDU s nižší prioritou, než má předpokládaný kořenový přepínač sítě SpanningTree domény (RootGuard)
- snadná instalace (Auto IP, DHCP klient, BootP klient)
- možnost pro diagnostické účely zrcadlit na zvoleném portu provoz libovolného jiného portu, skupiny portů nebo VLAN. A to s podporou filtrace podle přístupového seznamu. Podpora více monitorujících stanic k jednomu zrcadlenému zdroji a možnost vzdáleného monitorování RSPAN.
- plná podpora Network Login 802.1X (požadováno ověřování pro každý systém registrovaný na portu se zapnutý 802.1X individuálně – registrace svázána s MAC adresou, nikoliv fyzickým portem přepínače),
- řízení přístupu správce zařízení pomocí RADIUS,
- podpora SSHv2, SNMPv3

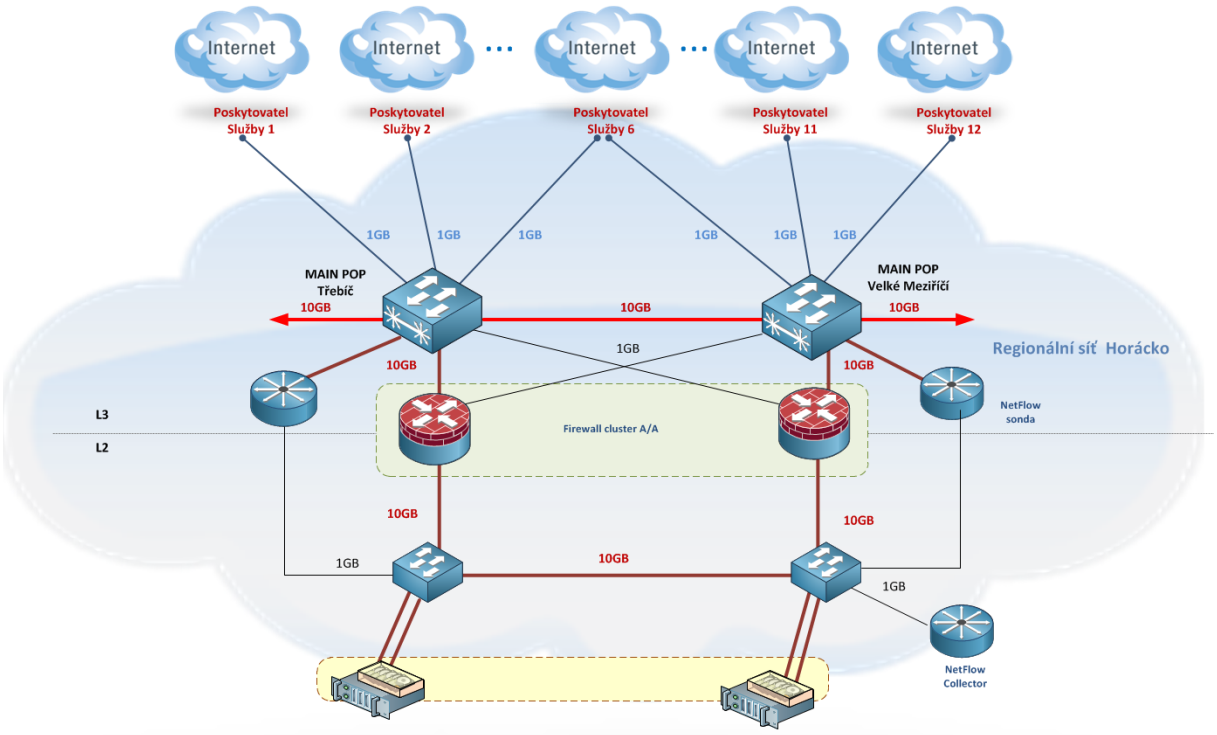
Performance monitoring a monitoring SLA poskytovaných služeb

Požadované funkcionality:

- data ukládaná a zpracovávaná v centrálním miste bez nutné návaznosti na jiné externí SQL systémy
- monitoring 24x7 s procentuálním vyhodnocením dostupnosti každého zařízeni, rovněž i konkrétní měřené hodnoty
- Výstup a konfigurace formou webového interface
- nativní podpora protokolů: SNMP (v1-3), WMI, ICMP, HTTP,
- notifikační kanály: web interface, e-mail, sms a instant messaging (jabber)
- Podpora zpracování Syslog
- Podpora sledování základních hodnot serverů (CPU, paměť, volné místo na disku) na OS Linux a OS Microsoft Windows
- SNMP Trap server vč. filtrování a uchování příchozích zpráv v centrálním místě
- podpora pro vzájemné porovnání (základní matematické operace) různých snímaných hodnot do jednoho výstupu
- zobrazování hodnot do grafů
- systém uživatelských práv administrátorů
- konfigurovatelné závislosti jednotlivých sledovaných hodnot či celých zařízeni napříč monitoring stromem
- podpora pro tvorbu šablon zařízeni
- systém běžící na OS Linux nebo OS Microsoft Windows

Doporučené schéma zapojení aktivních technologií

Obrázek č.12: Schéma doporučeného zapojení aktivních technologií



1.2.4. Instalace v zemních spojkách

V zemních spojkách Rudíkov, Vlčatín, Trnava budou instalovány navařením pásmové DWDM add/drop moduly pro 4 kanály / 1 vlákno.

1.3. Výstavba aktivní části propojovací sítě

Aktivní zařízení (síťové prvky) dodané do každého bodu v konfiguraci dle typu bodu (MainPoP, PoP) bude

- namontováno do datového rozvaděče
- pomocí optického „PATCH CORD“ propojeno s odpovídajícím optickým vláknem
- nakonfigurováno podle přidělené role v síti (dle navrženého logického modelu sítě).

Podmínky pro instalaci sítě
Aktivní síťové zařízení (včetně datových rozvaděčů) musí splňovat ČSN normy pro provoz elektrické zařízení, tzn. že musí být umístěny v dostatečně suchých, bezprašných místnostech Teploty v rozvaděčích je nutné udržovat v rozmezí vhodném pro provoz zde instalovaných zařízení (dle doporučení konkrétních výrobců) a to ventilováním prostoru racku nebo celé místnosti.
Toto je nutné zejména kvůli dodržení podmínek provozu zařízení v záruční době, aby nedošlo k porušení záručních podmínek.

1.4. Požadavky na dodavatele aktivní sítě

Požadavky na dodavatele aktivní části propojovací optické sítě

- Požadované parametry řešení:

    - Požadované parametry a funkcionality na vybavení PoP, MainPoP, TC výše uvedenými prvky jsou velmi podrobně specifikovány v kapitole 5.2. („Požadované funkcionality“ a „Požadované vlastnosti“)
- dohodnuté výstupy dodání (včetně měřících protokolů)
- garantované termíny dodání zařízení a prvků, instalace a implementace služeb (včetně vypracovaného harmonogramu prací)
- zpracování „Katalogu služeb“
- návrh „Architektonického plánu“
- zpracování „Provozní a bezpečnostní dokumentace“:
    - Provozní a bezpečnostní politika
    - Provozní řád a Havarijní plány
- alternativní cenová nabídka na rozšířenou záruku 7 let na veškerá dodaná aktivní zařízení (komunikační infrastrukturu)
- alternativní cenová nabídka na servis, opravy a údržbu aktivní části propojovací optické sítě při zajištění dostupnosti 99,5%, sjednán na základě SLA smluv s parametry 8/5/NBD

-

1.5. Zprovoznění, záruky, servis, oprava a údržba aktivní části sítě

Po úplném dokončení instalací bude na aktivní části propojovací sítě zhotovitelem spuštěn zkušební provoz pro ověření funkčnosti celé sítě s minimální délkou trvání 3 dny. Na provedení zkušebního provozu bude vystaven protokol se specifikací provedených testů a dosažených výsledků, případné závady musí být během zkušebního provozu odstraněny.

Oprava jednotlivých síťových komponent a zařízení bude během životnosti projektu řešena v rámci záručního servisu provozovatelem. Po skončení projektu budou opravy řešeny opět v rámci uzavřených servisních smluv investora s provozovatelem sítě.

Na veškeré dodané technické komponenty a zařízení by měla platit min. 2-letá záruka. Rozšířená 7-letá záruka nad rámec standardní záruky bude zvážena jako alternativa.,

V rámci rozšířené záruky by provozovatel měl zaručit reakci na základě SLA smlouvy v režimu 8/5/NBD. Servisní práce a opravy prováděné po dobu záruky by měly být plně bezplatné.

Během záručního období, nejpozději před jeho ukončením, by měla být s provozovatelem nebo jeho servisní organizací sepsána pozáruční servisní smlouva, upravující servisní práce, opravy, jejich rozsah, způsob provedení po záruce.

Vlastní technickou údržbu a správu sítě (aktivity nad rámec záruky) bude provádět firma vybraná investorem, jejíž náplní bude zajištění provozu sítě jak po stránce obchodní, tak technické. Údržba a správa budou řešeny formou outsourcingu provozovatelem propojovací sítě (tzv. servisním kontraktem zajišťujícím SLA, zásahy, help-desk a správu sítě).

V Brně, listopad 2014

Za itself s.r.o. zpracoval: Mgr. Radek Bednář, Ing. Vladimír Kolodin