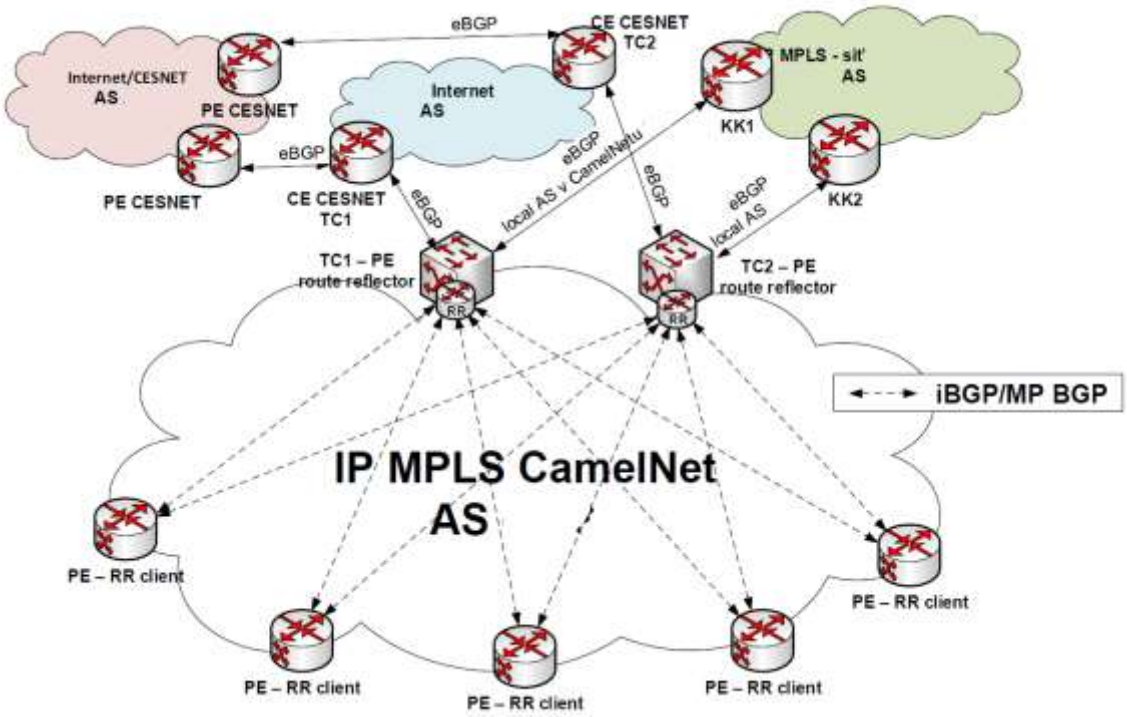
1 OBSAH

1.1 SEZNAM OBRÁZKŮ

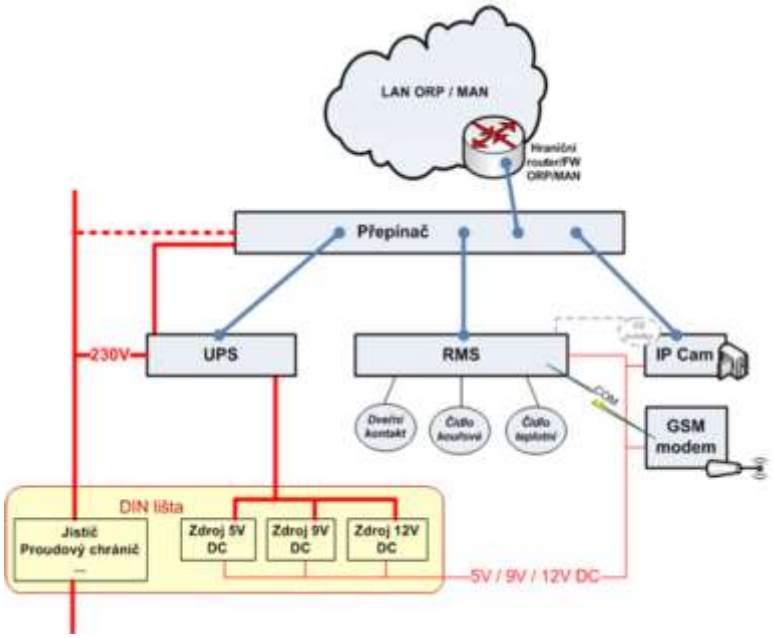
2 OBECNÝ POPIS

2.1 SCHÉMATA

Mapa sítě CamelNET: http://mapy.plzensky-kraj.cz/gis/camelnet_km/



Obrázek 1 – Zobecněné orientační schéma sítě Technologických center DC1,2 a uzlových bodů sítě CamelNET



Obrázek 2 – orientační schéma zapojení uzlového bodu

2.2 POPIS

- PI routery ve vysoké dostupnosti: GW-BGP1, GW-BGP2 - s možností rozšíření na 3ks,
- VPN uzly ve vysoké dostupnosti: VPN-1, VPN-2 - s možností rozšíření na 3ks
- firewally ve vysoké dostupnosti: FW-1, FW-2 - s možností rozšíření na 3ks,
- MPLS ve vysoké dostupnosti: GW-MPLS-1, GW-MPLS-2 - s možností rozšíření na 5ks
- přepínače datového centra ve vysoké dostupnosti: TC1-SW-1,TC2-SW-1 s možností rozšíření na 5ks pro každé datové centrum
- uzlové PE MPLS routery v kruhové topologii a částečně hvězdicové: 25x L3-SW-MPLS s možností rozšíření na 40ks
- podpůrné prvky/HW (ups, rms, čidla, převodníky, pdu, 2xDNS, 1xMGMT-SRV, 1xLOG-SRV

2 datová centra s možností rozšíření na 3

Až 40 uzlových bodů

Až 300 koncových bodů

Až 500 zařízení s požadavkem na pasivní dohled (aktivní prvky a podpůrné technické prostředky)

Aktivní prvky určené k svěřené správě budou Cisco. V případě nasazení prvků jiného výrobce budou zařazeny do svěřené správy po oboustranné dohodě.

3 POPIS ČINNOSTI

3.1 OBECNÉ

Primárním cílem svěřené správy komunikační infrastruktury (SSKI) je dohled a správa sítě CamelNET v režimu 24x7x365:

proaktivně - dohled a správa aktivních prvků v technologických centrech a v uzlových bodech vzdáleně i na místě.

reaktivně - informativní dohled koncových přípojek a ostatních podpůrných prvků - problém se začíná řešit až na požadavek objednatele.

Dostupnost proaktivně spravované sítě bude zajištěna minimálně 99,5% v režimu 24x7x365. tato dostupnost může být nedodržena v případech popsaných v kapitole 3.7 SLA VÝJIMKY nebo zásahu vyšší moci.
Kvartálně proběhne 4h schůzka se síťovým architektem dodavatele, na které dodavatel projde s objednavatelem provozní dokumentaci.

Objednateli bude poskytnut seznam týmu včetně kontaktů obsahující minimálně

1) Helpdesk, emailový a telefonický kontakt v režimu 24/7, v případě telefonního automatu bude poskytnut návod na rychlé projití nabídkou
2) Technický dozor schopný interpretovat data monitoringu sítě, telefonický kontakt v režimu 24/7
3) Výjezdový tým techniků, telefonický kontakt v režimu pracovní doby
4) Síťového architekta, telefonický kontakt v režimu pracovní doby

Zadavatel požaduje v pracovním týmu z důvodu zastupitelnosti alespoň 4 osoby s certifikací CISCO, kde mají alespoň 2 osoby CCIE Routing&Switching, alespoň 2 osoby CCNP Routing&Switching, alespoň jedna osoba CCNP Security, alespoň jedna osoba CCNP SP.

3.2 ZPŮSOB ZAHÁJENÍ PROVOZU

Do tří měsíců od podepsání smlouvy, převzetí předchozí dokumentace a přístupů k systémům sítě CamelNET bude nastaven zejména dohled, zálohování, aktualizována a doplněna dokumentace. Dodavatel se seznámí fyzicky se zařízenými v datových centrech a v uzlových lokalitách.

3.3 VÝJEZDOVÝ TECHNIK

K výjezdu technika do lokality dojde:

a) v režimu 24x7 do jedné hodiny od poruchy v lokalitě nezávisle na potvrzení závady ze strany objednatele

b) v ostatních režimech do jedné hodiny od její fyzické přístupnosti

režimy lokalit jsou uvedeny v Operativní Evidenci CamelNET, podrobnosti dle kapitoly výjimky SLA

v případě, příjezdu technika do lokality dojde k zjištění, že porucha nesouvisí s předmětem svěřené správy nebo se nepodaří vstup do lokality do 2 hodin od příjezdu je tento výjezd evidován jako preventivní. Počet preventivních výjezdů za rok je limitován na 12.

3.4 SVĚŘENÁ SPRÁVA A KONFIGURAČNÍ POŽADAVKY ZAHRNUTÉ V SSKI.

V ceně je 20 nových konfiguračních požadavků na měsíc. Požadavky se na sčítávají v průběhu trvání smlouvy, jejich využití určuje objednatel.

Požadavkem se rozumí:

1) Příprava konfigurace přípojek standardních koncových bodů na straně CamelNETu
2) konfigurace standardních VPN přípojek pro koncové uživatele dle již existujícího nastavení
3) konfigurace site-to-site VPN dle již existujícího vzoru
4) základní konfigurační zásahy (úprava pravidel, přidání VLAN, apod.)
5) přidání DNS záznamů
6) standartní konfigurace nového aktivní prvku v síti
7) standardní virtuální serverovna – do 3x VLAN v datovém centru (DC), prostupy do existujících vrf, do DC VLAN a Internetu

Nadstandardní složitější požadavky lze po oboustranné dohodě směnit za několik konfiguračních požadavků.

3.5 MONITORING SÍTĚ – ZÁKLADNÍ INFORMACE

Monitoring bude centrální, nad celou sítí, z virtuální serverovny v technologickém centru KÚPK.

Veškerá data ohledně chodu sítě budou konsolidována v systému pro monitoring provozu sítě, minimálně s historií za jeden rok

Nové zařízení zadané k monitorování objednatelem bude do monitoringu zařazeno do 5 pracovních dnů

Monitoring bude aktivně sledovat a reagovat na:

1) Výpadek konektivity nebo selhání infrastrukturních prvků
2) události bezprostředně ohrožující provozuschopnost infrastrukturních prvků, jako například: výpadek el. energie, kritická teplota, aktivace čidla vodní hladiny, …

Monitoring bude pasivně sledovat a umožňovat zobrazit historii stavu:

1) Konektivitu všech klientských zařízení na základě stavu portu (up/down)

2) U objednatelem zadaných zařízení ping echo a/nebo SNMP v1,v2,v3 po dohodě všech zúčastněných stran.

Systém pro monitoring: Nagios, Zabbix, PRTG – systém podporuje SNMP a reporting dostupnosti 24x7 za období den, měsíc, rok. S podporou API (json, XML, případně jiné strojově zpracovatelné formáty) Jiné dohledové systémy budou implementovány jen po oboustranné dohodě.

3.6 HELPDESK A GARANCE DOHLEDU AKTIVNÍ ČÁSTI

3.6.1 Helpdesk

Dodavatel zajistí možnost hlášení a ověřování poruch a jejich stavů v režimu 24x7x365 na telefonu i emailu.

Objednatel po dohodě s dodavatelem zajistí způsob identifikace osob oprávněných zadávat incidenty. Těmito osobami můžou být externí kontakty (správci připojených organizací a podobně)

3.6.2 Garance dohledu aktivní části

V rámci struktury je nutné vzniklé servisní incidenty členit do skupin, viz dále a dle těchto skupin přistupovat k jejich řešení:

- Incident/vada kategorie A
  Služba není použitelná ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující používání služby. Tento stav může ohrozit běžný provoz, případně může způsobit větší finanční nebo jiné škody.
- Incident/vada kategorie B
  Služba je ve svých funkcích degradována tak, že tento stav omezuje běžný provoz.
- Incident/vada kategorie C
  Ostatní - drobné incidenty/vady, které nespadají do kategorií A a/nebo B.

	Garantovaná doba přijetí a akceptace hlášeného incidentu	Garantovaná doba zahájení prací na řešení incidentu	Garantovaná doba ukončení incidentu
A	10 min	1 hod	Do 24 hod***
B	10 min	8 hod	NBD*
C	10 min	NBD*	5BD**

* NBD – next business day, následující pracovní den
** BD – business day, počet pracovních dnů.
***Do24 = čas opravy do 24h od nahlášení závady, doba poskytování služby je 7 dnů v týdnu 24h denně

Oprava je definována jako povinnost dodavatele opravit nahlášenou závadu, případně realizovat požadovaný zásah do konfigurace zařízení, ve stanoveném čase. Dodavatel informuje objednatele o postupu prací směřujících k odstranění hlášené závady, nebo k realizaci požadavku.

3.7 SLA VÝJIMKY

Dodavatel bude vybaven od objednatele sadou náhradních dílů pro uzlové lokality. Při zahájení a za provozu budou průběžně udržovány náhradní díly. V případě nedostupnosti náhradního dílu, kterou způsobí objednatel, se SLA počítá od dodání náhradního dílu.

Dodavatel bude vykonávat správu pouze nad aktivními prvky bez ohledu na pasivní část. V případě závady na pasivní infrastruktuře se SLA počítá od okamžiku vyřešení závady na pasivní infrastruktuře, pokud neexistuje náhradní řešení situace, na kterém se obě strany dohodly.

4 PROVOZNÍ DOKUMENTACE

Dokumentace aktivní části musí obsahovat **detailní nákres síťové topologie tak, jak je konfigurována na aktivních prvcích**. Dále musí obsahovat **kompletní soupis instalované techniky**.

Dokumentace musí **přesně popsat zvolené způsoby IP adresace**. Z provozní dokumentace musí být zřejmé, kdo je odpovědný za přidělování a správu IP rozsahů použitých v rámci sítě. Nedílnou součástí dokumentace proto bude **IP adresní plán sítě** vč. zvolených rozsahů a jejich rozložení. V dokumentaci nesmí chybět samostatná tabulka použitých adres pro management aktivních prvků a monitorovacích zařízení, jako například IP kamer a RMS.

Dokumentace musí přesně popsat **způsoby zajištění vysoké dostupností**. Kromě samotného funkčního principu musí být detailně popsány jednotlivé mechanismy vysoké dostupnosti s uvedením jejich nastavené konfigurace, a to jednotlivě pro každou část sítě, kde je vysoká dostupnost požadována. Tam kde bude konfigurace vysoké dostupnosti proměnlivá v závislosti na okolnostech, musí být uvedeno na jakých okolnostech a jaký bude jejich dopad.

Dokumentace musí přesně popsat privátní sítě jednotlivých přípojných a uzlových bodů.

Dokumentace musí obsahovat **seznam bezpečnostních opatření**, nutných k zajištění provozu aktivní části sítě CamelNET. Zabezpečení musí být rozpracováno pro jednotlivé síťové vrstvy ISO/OSI modelu, pro které je zabezpečení požadováno a na kterých je aplikováno. Předávací dokumentace musí být doplněna o tabulku/seznam/princip konfigurovaných ACCESS listů (tzv. ACL) včetně jejich řádků. K těmto musí být popsán způsob vedení provozní dokumentace v případě jejich úprav. Musí být zároveň vypracován **schvalovací diagram pro proces změny bezpečnostních pravidel** jako součást dokumentace aktivní části.

V případě více monitorovacích nástrojů musí být popsána **vzájemná spolupráce monitorovacích systémů, stejně jako způsoby jejich napojení na centrální monitorovací systémy sítě**.

Provozní dokumentace musí popsat řešení přístupových práv. Musí být vydefinovány **jednotlivé přístupové úrovně ke správě prvků v aktivní části**. Musí být popsán způsob evidence účtů a konfigurace za tímto účelem instalovaných přístupových systémů a jejich ověřovacích protokolů použitých pro správu oprávnění, nebo identifikaci uživatele.

Samostatnou součástí provozní dokumentace aktivní části musí být **detailní popis napojení sítě CamelNET na mezirezortní a akademické sítě a sítě jiných providerů** a způsoby komunikace do těchto sítí.

Hlavní body technické dokumentace jsou zahrnuty v této zadávací dokumentaci, kompletní, stávající technická dokumentace bude v plném rozsahu poskytnuta až vítěznému dodavateli.

5 MINIMÁLNÍ ZÁSADY PRO SPRÁVU CAMEINET

1. Údržba programového vybavení

- Udržování aktuálních verzí systémových programů, bezpečná aplikace oprav do operačních systémů podle pokynů výrobce u všech komponent sítě CamelNET. Dále udržování aktuálních verzí systému jmenných služeb 2x DNS(IPv4 a 6, dnssec) pro potřeby sítě CamelNET a připojených organizací.

2. Systémový a bezpečnostní dohled

- Přístupy a zásahy dodavatele budou logovány a archivovány (více viz bod 8).
- Správa a konfigurace zařízení bude prováděna vzdáleně bezpečným způsobem odpovídající aktuálnímu bezpečnému protokolu (v čase se může změnit) prostřednictvím sítě Internet nebo jinou sítí. V případě nedostupnosti tohoto spojení navštíví pracovník dodavatele bez zbytečného odkladu lokalitu objednatele, kde pracovník dodavatele pokračuje v práci až do úplného vyřešení problému.
- Při výskytu bezpečnostní chyby produktu, který je předmětem svěřené správy, bude tato v nejkratším možném čase odstraněna. Není-li řešení chyby známé, bude Objednatel na tuto skutečnost upozorněn, budou mu navrženy jednoduché metody obrany i za cenu dočasné ztráty funkčnosti s ohledem na dopad zranitelnosti.
- Po zveřejnění opravy bezpečnostní chyby produktu, budou neprodleně po zveřejnění opravy bezpečnostní chyby, programy upraveny či vyměněny za jinou verzi v závislosti na licenčních podmínkách produktu a zaplacení licenčních poplatků.
- Objednatel bude upozorněn na případné útoky.
- Opravu závad programového vybavení způsobených jinými vlivy (např. chybou HW).
- Pomoc při odstraňování následků útoků na aktivní prvek.
- Sledování a vyhodnocování provozu dle požadavků objednatele v rozsahu definovaném při zahájení služby. Dodavatelem bude veden deník incidentů.

3. Podpora administrace

- Udržování provozní konfigurace prvků včetně provádění takových změn, které nesnižují funkčnost systému.
- Návrhy opatření proti obtížným nebo nebezpečným systémům na síti (zamezení přístupu ze sítí, ze kterých jsou podnikány útoky atp.).
- Doporučení opatření, zabraňujících zneužití sítě k provádění útoků.
- uživatelský účet pro správce Objednatele, který umožňuje správu DNS záznamů (v případě úprav Objednatel oznámí Dodavateli zásah do DNS konfigurace), čtení logů a konfigurací aktivních prvků, další možná oprávnění budou přidána po oboustranné dohodě (např. přidávání VLAN jednotlivým portům na aktivních prvcích).

4. Zálohování

- definice a konfigurace zálohovacích mechanizmů – ve spolupráci se správcem sítě Objednatele, odpovědným za centrální zálohování TC, minimální rozsah jsou logy a konfigurace aktivních prvků
- Aktivní prvky budou mít dedikovaný přístupový účet k účelům zálohování konfigurace a stahování logů, pokud to bude technicky možné.

5. Základní požadavky na sledování provozních informací

- U aktivních prvků bude monitorováno zatížení na všech síťových rozhraních, výkon procesoru, velikost volného místa. Pro přístup na grafický výstup těchto informací bude zřízen pro správce Objednatele účet. Dále je monitorována IP komunikace (src, dst, ports, time...). Bude veden deník incidentů (datum; čas problému - např. zaplněn flash disk nad 95%; opatření, apod.)

6. Údržba technického vybavení

- Návrhy opatření pro zvýšení funkčnosti systému a po dohodě jejich implementace (vhodné nové prvky, rozšíření kapacity virtuální serverovny, a podobně).
- Dodržení všech výše uvedených parametrů služby je zaručeno po celou dobu, kdy je předmět podpory zařízení podporován výrobcem resp. Dodavatelem. O ztrátě takové podpory z důvodu morální zastaralosti, tzn. přechodu do stavu „End Of Service“ nebo „End Of Life“, bude Objednatel e-mailem, s požadavkem na potvrzené formou odpovědi, informován dodavatelem minimálně 3 měsíce předem.

7. Podmínky provádění služby

- Dodavatel si ponechá přístupová hesla systémů, Objednateli budou hesla poskytnuta v zalepené obálce. Objednatel smí otevřít obálku buď na výslovnou žádost Dodavatele, či při nepředvídaných okolnostech. V tomto případě musí o použití hesla neprodleně vyrozumět Dodavatele. Dodavatel nebude hesla používat pro jiný subjekt, tedy hesla budou unikátní.
- Bude-li třeba osobní návštěva technika Dodavatele, Objednatel zajistí pracovníkům Dodavatele přístup k systému na základě předchozí dohody smluvních stran.

8. Dokumentace

- Dodavatel povede k systémům dokumentaci, která se bude skládat z aktuální konfigurace (konfigurační soubory, popis řešení, sítí, apod.) a provozního deníku (kdy, kde, kým, jak, schválil, důvod, popis, apod.).

9. Správa záložního spojení

- Dodavatel nastavuje záložní spojení dle požadavků Objednatele, který v případě potřeby změní poskytovatele záložního spojení.