



SPRÁVA KOLEJÍ
A MENZ

Identifikace veřejné zakázky

Název:	Dodávka prvků pro realizaci pokrytí vybraných objektů Správy kolejí a menz MU Wi-Fi signálem
Druh veřejné zakázky:	Dodávky
Druh zadávacího řízení:	Otevřené řízení
Adresa veřejné zakázky:	https://zakazky.muni.cz/vz00005090

Identifikační údaje zadavatele

Název:	Masarykova univerzita- Správa kolejí a menz
Sídlo:	Vinařská 472/5b, 603 00 Brno
IČ:	00216224
Zastoupen:	Ing. Zdeňkem Čížkem, ředitelem

Vysvětlení a změna Zadávací dokumentace II.

Zadavatel na základě doručené žádosti dodavatele poskytuje v souladu s ust. § 99 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, (dále jen „ZZVZ“), následující vysvětlení a změnu Zadávací dokumentace:

Dotaz č. 1:

„Dotaz switch 1:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH“ parametr: **“Možnost připojit externí redundantní zdroj”** S ohledem na skutečnost, že zadavatel nedefinuje podrobnější požadavky na vlastnosti externího redundantního zdroje, zvažuje dotazovatel nabídnout ekonomičtější variantu přepínače, který nepodporuje možnost připojení externího redundantního zdroje. Připouští zadavatel přepínače bez možnosti připojení externího redundantního zdroje?“

Odpověď:

Ne, Zadavatel navrhouvanou variantu nepřipouští. Cílem požadavku je možnost využít dvě napájení pro případ výpadku jednoho napájecího okruhu. Bližší podrobnosti na vlastnosti externího redundantního zdroje nebyly specifikovány, protože Zadavateli na konkrétní implementaci tohoto požadavku nezáleží. Jedinou přípustnou alternativou tohoto požadavku je nabídka přepínačů s integrovanými redundantními zdroji, vyměnitelnými za běhu (tzv. hot-swap).



Dotaz č. 2:

„Dotaz switch 2:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr: “Minimální rychlost stohovacího propojení 80Gb/s”. S ohledem na počet koncových portů přepínače a obvyklé doporučené agregační poměry v přístupové vrstvě se dotazovatel domnívá, že pro stohovací propoj, postačuje nižší rychlost. Připouští zadavatel přepínače, které podporují minimální rychlost stohovacího propojení 20Gb/s?”

Odpověď:

Ne, nepřipouští. Vzhledem k předpokládanému budoucího připojení přepínačů do univerzitní infrastruktury rychlostí 2x 10 Gbps do každého ze dvou centrálních prvků a počtu připojených přístupových bodů lze akceptovat nejnižší rychlost stohovacího propojení alespoň 40 Gbps.

Dotaz č. 3:

„Dotaz switch 3:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr: “Automatická kontrola a sjednocení verze software přepínačů ve stohu”. Aktuálně na trhu existují stohovací technologie, která s ohledem na vyšší bezpečnost provozu stohu nepodporují automatickou kontrolu a sjednocení verze software přepínačů ve stohu, ale podporuje sjednocení firmware přepínače např. při upgrade stohu. Připouští zadavatel přepínače, které nepodporují automatickou kontrolu a sjednocení verze firmware přepínačů ve stohu?”

Odpověď:

Ne, nepřipouští. Cílem požadavku je možnost rychlého zapojení (resp. náhrady vadného) přepínače do stohu bez toho, aby byla nezbytná jeho konfigurace kvalifikovanou osobou.

Dotaz č. 4:

„Dotaz switch 4:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr: “RADIUS, TACACS+ over IPv6”. Dotazovatel hodlá nabídnout přepínače s podporu pouze TACACS+ over IPV4. Připouští zadavatel přepínače, které nepodporují TACACS+ over IPv6 ale podporují TACACS+ over IPv4?”

Odpověď:

Ne, nepřipouští. Vzhledem k výraznému deficitu IPv4 adres je další rozšíření již nasazené IPv6 technologie v univerzitní síťové infrastruktuře nezbytným budoucím krokem jejího rozvoje, včetně přechodu zmíněných obslužných služeb aktuálně funkčních na IPv4. Předpokládaná doba života nakupovaných prvků by bez této podpory znamenala výrazná omezení v tomto rozšiřování IPv6.



Dotaz č. 5:

„Dotaz switch 5:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr: *“IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači, sdílení ověření koncových stanic”*. Připouští zadavatel přepínače, které místo role 802.1X supplicant podporují roli 802.1X authenticator?“

Odpověď:

Ne, nepřipouští. Role supplicant je nutná pro ověření identity a autentizaci přepínače vůči nadřazenému přepínači (s podporou role authenticator) a není možné ji nahradit rolí authenticator.

Dotaz č. 6:

„Dotaz switch 6:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr: *“Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)”*. Připouští zadavatel přepínače, které místo konfigurovatelné kombinace pořadí podporují mechanismus kdy MAC autentizace je spuštěna současně s 802.1X autentizací a pokud není 802.1X autentizace úspěšná platí výsledek MAC autentizace?“

Odpověď:

Přepínače podporující MAC autentizaci spuštěnou současně s mechanismem IEEE 802.1x Zadavatel připouští. Nezbytnou součástí této konfigurace ověřování zařízení na portu však musí být i možnost webové autentizace.

Dotaz č. 7:

„Dotaz switch 7:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr *“Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů”*. Připouští zadavatel přepínače, které výše uvedenou funkcionalitu podporují srovnatelnou formou digitálně podepsaného firmware, který je před zavedením do přepínače kontrolován, zda nedošlo k jeho modifikaci?“

Odpověď:

Ne, nepřipouští – zmíněnou možnost nepovažuje Zadavatel za dostatečně bezpečnou. Firmware je do přepínače obvykle možné dostat i jinými způsoby než standardní nahrávací procedurou (přes sériovou linku po bootování rescue systému a podobně). Proto požadujeme variantu tzv. SecureBoot, kdy má přepínač integrován nějakou variantu TPM modulu, ve kterém uchovává patřičné šifrovací/podepisovací klíče, a podle nich kontroluje zaváděný OS.



Dotaz č. 8:

„Dotaz switch 8:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr **“Měření a ovládání spotřeby energie připojených koncových zařízení”**. Připouští zadavatel přepínače, které podporují standardní funkcionalitu PoE nebo PoE+ podle IEEE 802.3af a IEEE802.3at bez měření a ovládání spotřeby energie připojených koncových zařízení?“

Odpověď:

Ne, nepřipouští. Cílem tohoto požadavku je mít přehled o dostupném PoE „budgetu“ na zařízení.

Dotaz č. 9:

„Dotaz switch 9:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr **“10/100 management out-of-band port”**. S ohledem na vícenásobný a funkčně shodný požadavek na management rozhraní chce uchazeč nabídnout zařízení s podporu CLI a SSH rozhraním. Připouští zadavatel přepínače bez podpory 10/100 management out-of-band port avšak s podporu CLI a SSH rozhraní?“

Odpověď:

Ne, nepřipouští – vyžadováno je „out-of-band“ ethernetové rozhraní. Cílem zadavatele je zachovat možnost přístupu k přepínačům i v případě, kdy bude datová síť vyřazena z provozu (přístupem k prvku skrze separátní „out-of-band“ síť, včetně jejich vzájemné izolace).

Dotaz č. 10:

„Dotaz switch 10:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr **“NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955)”**. Uchazeč chce nabídnout srovnatelnou technologii sFlow pro monitoring aplikačních toků. Připouští zadavatel přepínače, které podporují srovnatelnou technologii sFlow?“

Odpověď:

Ne, nepřipouští – sFlow Zadavatel nepovažuje za srovnatelnou technologii s NetFlow/IPFIX (náhodné „samplerování“ datových paketů vs. informace o všech datových tocích). Masarykova univerzita dlouhodobě disponuje centrální infrastrukturou pro analýzu bezpečnostních hrozeb a kyberútoků v síti MU, která je založena na analýze informací o zachycených datových tocích vyjádřených dle specifikace NetFlow/IPFIX – absence podpory této technologie by tak znemožnila bezpečnostní analýzu zranitelnosti a kyberútoků na síťová zařízení budované infrastruktury.



Dotaz č. 11:

„Dotaz switch 11:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr **“Sběr dat pro NetFlow nebo IPFIX export z každého portu přepínače”**. Uchazeč chce nabídnout srovnatelnou technologii sFlow pro monitoring aplikačních toků. Připouští zadavatel přepínače, které podporují srovnatelnou technologii sFlow?“

Odpověď:

Ne, nepřipouští – viz reakce na dotaz č. 10.

Dotaz č. 12:

„Dotaz switch 12:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr **“Detailní flexibilní definice “flow” dle L2, L3 i L4 parametrů”**. Uchazeč chce nabídnout srovnatelnou technologii sFlow pro monitoring aplikačních toků, která používá jinou funkcionalitu. Připouští zadavatel přepínače, které podporují srovnatelnou technologii sFlow?“

Odpověď:

Ne, nepřipouští – viz reakce na dotaz č. 10.

Dotaz č. 13:

„Dotaz switch 13:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr **“Statistiky určovány z každého paketu daného “flow”**. Uchazeč chce nabídnout srovnatelnou technologii sFlow, která pracuje s jinou technologií statistik určování vzorků. Připouští zadavatel přepínače, které podporují srovnatelnou technologii sFlow?“

Odpověď:

Ne, nepřipouští – viz reakce na dotaz č. 10.

Dotaz č. 14:

„Dotaz switch 14:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr **“Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb”**.

Pro monitoring aplikačních toků lze využít alternativní technologii sFlow která monitoring bezpečnostních hrozeb řeší jiným způsobem. Připouští zadavatel páteřní zařízení, které nepodporuje technologii NetFlow a místo ní podporuje technologii sFlow?“



Odpověď:

Ne, nepřipouští – viz reakce na dotaz č. 10.

Dotaz č. 15:

„Dotaz switch 15:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr *“Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů)”*. Za automatizovanou reakci obsluhy lze považovat např. pravidelné zálohování konfigurace na externí systém pomocí funkce job scheduler. Lze nabídnout zařízení, které místo funkce uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů) podporuje srovnatelnou funkci job scheduler?“

Odpověď:

Ne, nelze. Zadavatel požaduje uživatelsky modifikovatelnou automatickou reakci či obsluhu událostí, kdy systém – například při pádu linky, změně topologie STP, apod. – provede nějakou správce definovanou aktivitu. Varianta job scheduleru již ze své podstaty podobnou obsluhu náhodně nastalých událostí neumožňuje.

Dotaz č. 16:

„Dotaz switch 16:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr *“Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute)”*. Technologie L2 traceroute využívá pro svojí činnost protokol CDP (Cisco Discovery Protocol). Identické funkce lze získat postupným procházením ARP a MAC adres tabulek jednotlivých přepínačů. Připouští zadavatel přepínače, které nepodporuje L2 traceroute a místo toho umožňuje procházení záznamů v ARP a MAC adres tabulce?“

Odpověď:

Ne, nepřipouští. L2 traceroute nabízí několik výrobců síťových prvků, většinou s použitím standardního protokolu LLDP, případně s možností do přepínače takový program nahrát (pokud není v základní příkazové sadě). Požadavek podpory L2 traceroute považuje Zadavatel za důležitý, protože tento nástroj může být použit pro ladění např. problémů IP konektivity (kdy ARP tabulka není k dispozici a přepínače nejsou po IP dosažitelné).

Dotaz č. 17:

„Dotaz switch 17:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část SWITCH” parametr *“Přepínač si může automaticky zazálohovat a obnovit firmware včetně konfigurace z nadřazeného*



směrovače". Připouští zadavatel přepínače, který podporuje funkci zálohy a obnovy firmware včetně konfigurace ze secure FTP serveru?"

Odpověď:

Tazatelem navrhovaná či jiná alternativní varianta jsou přípustné pouze v okamžiku, kdy lze vhodnou konfigurací dalších prvků infrastruktury (např. DHCP serveru, nadřazeného směrovače či přepínače, atp.) docílit stavu, ve kterém nově instalovaný a z výroby konfigurovaný přepínač (nahrazující nefunkční kus) nevyžaduje po svém zapojení do infrastruktury žádný zásah odborné obsluhy pro aktualizaci svého firmware a získání aktuální konfigurace, kdy obojí získá – plně automatizovaně – z ostatních prvků infrastruktury.

Dotaz č. 18:

„Dotaz AP 18:

Zadavatel v rámci technických požadavků VR požaduje v "Příloha č. 1, část AP" parametr: "Podpora 3x3 MIMO nebo vyšší pro obě rádiová pásma" S ohledem na skutečnost, že site survey probíhala za pomoci klienta s podporou 2x2 MIMO, jeví se zadavateli technicky vhodnější a pro finální řešení bezpečnější nabídnout přístupové body s podporou 2x2 MIMO. Připouští zadavatel přístupové body s podporou 2x2 MIMO."

Odpověď:

Ne, nepřipouští. Zadavatel v budované infrastruktuře předpokládá využívání klientských zařízení schopných využít 3x3 MIMO (v obou rádiových pásmech), jejichž schopnosti by byly v infrastruktuře poskytující pouze 2x2 MIMO degradovány. I v tazatelem zmiňované site-survey bylo uvažováno s pokrytím lokalit přístupovými body s podporou 3x3 MIMO v obou rádiových pásmech.

Dotaz č. 19:

„Dotaz AP 19:

Zadavatel v rámci technických požadavků VR požaduje v "Příloha č. 1, část AP" parametr: "Maximální vysílací výkon v pásmu 5 GHz pro oblast použití (tzv. regulatory domain) v ČR, bez započteného zisku antény 22dBm". S ohledem různou přípustnou hodnotu maximálního dBm, která závisí na počtu aktuálně využitých MIMO, spatial stream je vhodnější maximální hodnotu vysílacího výkonu definovat pomocí hodnoty "dBm per chain", která je typicky nižší. Připouští zadavatel přístupové body s minimálním vysílacím výkonem v pásmu 5GHz 18dBm per chain?"

Odpověď:

Zadavatel akceptuje návrh tazatele a upřesňuje technickou specifikaci AP následovně:

V "Příloze č. 1, části AP" je požadováno splnění již uvedených parametrů „Maximální vysílací výkon v pásmu 2.4 GHz pro oblast použití (tzv. regulatory domain) v ČR, bez započteného zisku antény“ (min. 18 dBm) a „Maximální vysílací výkon v pásmu 5 GHz pro oblast použití (tzv. regulatory domain) v ČR, bez započteného zisku antény“ (min. 22 dBm) **NEBO** splnění parametru "Maximální vysílací výkon per



chain (v obou rádiových pásmech 2.4 GHz i 5 GHz) pro oblast použití (tzv. regulatory domain) v ČR, bez započteného zisku antény“ (min. 17 dBm).

Dotaz č. 20:

„Dotaz kontroler 20:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část CTRL“ parametr: *“Možnost autentizace nových klientů k AP pomocí 802.1x/EAP i v případě výpadku centrálního kontroleru”* S ohledem na jeden z dalších požadavků tunelovat provoz do kontroleru se jeví tento požadavek jako velmi složitě splnitelný, neboť při výpadku kontroleru nelze nikam transportovat následný provoz bezdrátových klientů. Připouští zadavatel kontroler, který nepodporuje autentizaci nových klientů při výpadku centrálního kontroleru?“

Odpověď:

Ne, nepřipouští. Cílem požadavku je zajistit možnost elementární autentizace nových bezdrátových klientů (např. správců, operátorů, lokálních zaměstnanců, atp.) při výpadku centrálního kontroleru, kdy lze provoz těchto klientů transportovat do lokální sítě, a tím zajistit síťovou konektivitu pro elementární práci (např. přístup na síťové tiskárny) či usnadňující analýzu daného problému.

Dotaz č. 21:

„Dotaz kontroler 21:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část CTRL“ parametr: *“Podpora IPv6 – bezpečnost (RAGuard, IPv6 Source Guard, DHCPv6 Server Guard, ACL)”* S ohledem na skutečnost že velká část IPv6 wireless klientů nepodporuje nativní přidělování IP adres pomocí DHCPv6, jeví se tento požadavek v praxi velmi složitě využitelný. Připouští zadavatel kontroler, který podporuje RA Guard a IPv6 firewall?“

Odpověď:

Ne, nepřipouští. IPv6 SourceGuard a DHCPv6 Server Guard chrání infrastrukturu a její klienty proti podvržení zdrojové adresy a podvrženým DHCP serverům. S ohledem na účel použití poptávané infrastruktury jsou tyto požadavky zcela nezbytné pro její dostatečné zabezpečení.

Dotaz č. 22:

„Dotaz mgmt 22:

Zadavatel v rámci technických požadavků VR požaduje v “Příloha č. 1, část MGMT“ parametr: *“Zobrazování současných i historických hodnot a trendu kvality signálu bezdrátové sítě”*. Připouští zadavatel nástroj pro management, který zobrazuje historická data pouze aktuálně připojených bezdrátových klientů?“



SPRÁVA KOLEJÍ
A MENZ

Odpověď:

Ne, nepřipouští. Pro realizaci Zadavatelem uvažovaných analýz jsou vyžadována historická data všech klientů připojených v požadovaném (analyzovaném) období.

S ohledem na to, že Zadavatel změnil některé z technických parametrů uvedených v Zadávacích podmínkách a tyto změny mohou dle názoru zadavatele vést k rozšíření okruhu možných účastníků zadávacího řízení, rozhodl se Zadavatel prodloužit lhůtu pro podání nabídek.

Čl. 6 odst. 6.1. Zadávací dokumentace tedy v souladu s ust. § 99 odst. 2 ZZVZ zní:

„Nabídky je nutné podat nejpozději do 11. 10. 2018, 10:00 hod.“

V dalším zůstávají Zadávací podmínky beze změn. Opravená příloha č. 1 – Technické podmínky návrhu Kupní smlouvy je přílohou této odpovědi a dodavatelé jsou povinni ji použít pro zpracování své nabídky.

Ing. Zdeněk Čížek
ředitel Správy kolejí a menz

Přílohy:

- Příloha č. 1 – Technické podmínky – změna