Příloha č. 1

Specifikace předmětu veřejné zakázky

1. 110 ks WAN směrovačů - typ A

Směrovač musí mít modulární architekturu s možností přidávat moduly rozhraní dle budoucí potřeby.

Směrovač musí podporovat šifrování aplikačního provozu s využitím technologie IPSec a s podporou Suite-B šifrovacích algoritmů definovaných v RFC 6379. Je požadována hardwarová podpora šifrování ve směrovači.

Směrovače musí zajistit plnou podporu IP adresace a směrovacích protokolů pro IPv4 a IPv6 s minimálními požadavky na směrovací protokoly OSPFv2/v3, BGPv4 a Multiprotocol BGP.

Směrovač musí plně podporovat pokročilé mechanismy pro řízení kvality služeb (QoS) včetně Hierarchical QoS, klasifikace provozu, markování provozu (DSCP, COS) a vyčlenění šířky pásma provozu v jednotlivých aplikačních kategoriích a definici prioritní fronty pro provoz IP telefonie.

Směrovač musí mít plnou podporu IPv6 služeb jako jsou DNS, Telnet/SSH, DHCP, Multicast a QoS. Směrovače musí podporovat technologii DualStack (IPv4 a IPv6).

Směrovač musí plně podporovat monitorování aplikačních toků (všech paketů) s využitím technologie NetFlow nebo ekvivalentní technologie a musí obsahovat nástroje pro on-line měření kvality přenosové infrastruktury.

Přesná požadovaná funkční specifikace WAN směrovače typu A je uvedena v následující tabulce.

Tabulka 1 Funkční specifikace WAN směrovače- typ A

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
110 ks WAN směrovačů typ A		
Výrobce zařízení	Uvedení výrobce	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	
Typ zařízení	Směrovač	
Formát zařízení	Modulární	
Požadovaný počet portů GigabitEthernet	2x10/100/1000Base-TX, 1x1000BASE-X s volitelným fyzickým rozhraním	
Interní AC napájecí zdroj	ANO	
Min. 3 volné sloty pro rozšiřující moduly	ANO	
Možnost instalovat LAN modul s min. 24x 10/100/1000Base-TX porty s podporou PoE+ napájení	ANO	
Směrování IPv4	ANO	
Směrování IPv6	ANO	
OSPFv2	ANO	

Příloha č. 1

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
BGPv4	ANO	
Podpora 4 byte AS numbers in BGP	ANO	
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	
GRE (Generic Routing Encapsulation)	ANO	
Policy-based routing podle ACL	ANO	
IP Multicast (PIM SSM, PIM SM)	ANO	
IGMPv2, IGMPv3	ANO	
uRPF	ANO	
First Hop Redundancy Protokol pro IPv6	ANO	
OSPFv3	ANO	
MP BGP	ANO	
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO	
Minimální počet oddělených (nezávislých) směrovacích tabulek	30	
IPv6 Multicast (MLDv1 & v2)	ANO	
IPv6 Multicast (PIM SM, PIM SSM)	ANO	
QoS classification – ACL, DSCP, CoS based	ANO	
QoS marking - DSCP, CoS	ANO	
QoS Shaping and Policing	ANO	
Class Based and Priority queuing	ANO	
Rate Limiting	ANO	
Hierarchical QoS	ANO, min. 3 úrovně	
RSVP	ANO	
Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)	ANO	
ACL na rozhraní IN/OUT	ANO	
Zone-based firewall	ANO	
IPSec AES-GCM-256	ANO	
Hardwarová akcelerace šifrování pro IPSec AES-GCM-256	ANO	
Minimální propustnost směrovače (IMIX provoz) při aktivovaných službách IPSec šifrování a QoS	90Mb/s	
Možnost zvýšit propustnost směrovače (IMIX provoz) při aktivovaných službách IPSec šifrování a QoS, např. formou licence	ANO, min. na 270Mb/s	
IKEv2	ANO	
SHA-2 (SHA-256, SHA-512)	ANO	
Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami	ANO	
Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů	ANO	
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	ANO	
Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
Interní nástroje pro debugging procházejícího provozu	ANO	
SSHv2	ANO	
CLI rozhraní	ANO	
SNMPv2/v3	ANO	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	
NTPv3 server	ANO	

2. 185 ks přístupový LAN přepínač 48 portů a 108 ks přístupový LAN přepínač 24 portů

Přístupový LAN přepínač musí mít stohovatelnou nebo modulární architekturu.

Přístupový LAN přepínač musí podporovat standardy pro napájení po Ethernetu (PoE) dle norem 802.3af a 802.3at.

Přístupový LAN přepínač musí podporovat zabezpečení portů dle standardu 802.1x.

Přístupový LAN přepínač musí podporovat optimalizaci IP multicast provozu (IGMP a MLD snooping).

Přístupový LAN přepínač musí umožnit zabezpečení na L2 portech proti podvržení zdrojové MAC a IP adresy a ochranu proti neautorizovaným službám DHCP.

Přístupový LAN přepínač musí plně podporovat řízení kvality služeb (QoS) s možností definice frontování, klasifikace provozu, markování provozu (DSCP, COS) s možností omezení a vyčlenění šířky pásma provozu v jednotlivých kategoriích a definici prioritní fronty.

Přístupový LAN přepínač musí plně podporovat IPv6 protokoly a služby jako jsou DNS, Telnet/SSH, DHCP, ACL a QoS. Přepínač musí podporovat funkcionalitu IPv6 First Hop Security (minimálně IPv6 RA guard a DHCPv6 snooping).

Přístupový LAN přepínač musí plně podporovat monitorování aplikačních toků (všech paketů) s využitím technologie NetFlow nebo ekvivalentní technologie pro účely detekce anomálních datových toků a bezpečnostních útoků.

Přesná požadovaná funkční specifikace přístupového LAN přepínače je uvedena v následujících tabulkách.

Tabulka 2 Funkční specifikace přístupového LAN přepínače – 48 portů

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
185 ks LAN přepínačů - 48 portů		
Výrobce zařízení	Uvedení výrobce	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	
Typ přepínače	L3 přepínač	
Formát přepínače	Stohovatelný nebo modulární	
V případě stohovatelného přepínače možnost rozšířit přepínač o dedikovaný stohovací modul	ANO	
Minimální počet zařízení ve stohu/min. počet slotů v šasi	8	
Minimální kapacita sběrnice stohu/min. kapacita per slot modulárního šasi	160Gb/s	
Stateful Switch Over v rámci stohu nebo šasi	ANO	
Počet portů 10/100/1000 Base-TX s PoE napájením	48	
Minimální počet 1GE uplink portů s volitelným fyzickým rozhraním	4	
Velikost MAC address tabulky	30000	
IEEE 802.3ad (Link Aggregation)	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	
Minimální počet konfigurovatelných Link Aggregation Group trunků	64	
IEEE 802.1Q	ANO	
Minimální počet aktivních VLAN	1000	
IEEE 802.1x	ANO	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	
RADIUS CoA	ANO	
Podpora instance spanning-tree protokolu per VLAN	ANO	
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	
Podpora jumbo rámců (min. 9198 bytes)	ANO	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	
Směrování protokolů IPv4 a IPv6 v hardware	ANO	
OSPFv2	ANO	
OSPFv3	ANO	
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	
Reverse path check (uRPF)	ANO	
IGMPv2, IGMPv3	ANO	
DHCP relay	ANO	
Minimální počet HW QoS front	8	
QoS classification – ACL, DSCP, CoS based	ANO	
QoS marking - DSCP, CoS	ANO	
QoS - Strict Priority Queue	ANO	
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	
QoS Policing	ANO	
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO	
IPv6 services (Telnet, SSH, Syslog, DHCP)	ANO	
IPv6 QoS	ANO	
IPv6 First Hop Security (RA guard, DHCPv6 snooping)	ANO	
IPv6 ACL	ANO	
Možnost definovat povolené MAC adresy na portu	ANO	
PACL, VACL	ANO	
IEEE 802.1ae na 1GE uplink portech	ANO	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	
IEEE 802.3af	ANO	
IEEE 802.3at	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
Minimální PoE budget	390W	
IEEE 802.3az	ANO	
Možnost automatické aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	
Integrovaný WLAN kontrolér	ANO	
Vyhodnocování kvality signálu bezdrátové sítě v reálném čase, zpracování a reakce na informace o rušivých signálech (interference) z AP	ANO	
Podpora 802.11i, respektive jeho implementací WPA a WPA2 včetně enterprise variant autentizace/šifrování	ANO	
Aplikace QoS per WLAN AP, WLAN SSID, WLAN klient	ANO	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	ANO	
Zrcadlení provozu na úrovni jednotlivých fyzických rozhraní i virtuálních sítí (VLAN) do monitorovacího rozhraní (ekvivalent funkce SPAN)	ANO	
Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	
DHCP server	ANO	
SSHv2	ANO	
CLI rozhraní	ANO	
SNMPv2/v3	ANO	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	
NTPv3 server	ANO	

Tabulka 3 Funkční specifikace přístupového LAN přepínače – 24 portů

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
108 ks LAN přepínačů - 24 portů		
Výrobce zařízení	Uvedení výrobce	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	
Typ přepínače	L3 přepínač	
Formát přepínače	Stohovatelný nebo modulární	
V případě stohovatelného přepínače možnost rozšířit přepínač o dedikovaný stohovací modul	ANO	
Minimální počet zařízení ve stohu/min. počet slotů v šasi	8	
Minimální kapacita sběrnice stohu/min. kapacita per slot modulárního šasi	160Gb/s	
Stateful Switch Over v rámci stohu nebo šasi	ANO	
Počet portů 10/100/1000 Base-TX s PoE napájením	24	

Příloha č. 1

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
Minimální počet 1GE uplink portů s volitelným fyzickým rozhraním	4	
Velikost MAC address tabulky	30000	
IEEE 802.3ad (Link Aggregation)	ANO	
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	
Minimální počet konfigurovatelných Link Aggregation Group trunků	64	
IEEE 802.1Q	ANO	
Minimální počet aktivních VLAN	1000	
IEEE 802.1x	ANO	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	
RADIUS CoA	ANO	
Podpora instance spanning-tree protokolu per VLAN	ANO	
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	
Podpora jumbo rámců (min. 9198 bytes)	ANO	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	
Směrování protokolů IPv4 a IPv6 v hardware	ANO	
OSPFv2	ANO	
OSPFv3	ANO	
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	
Reverse path check (uRPF)	ANO	
IGMPv2, IGMPv3	ANO	
DHCP relay	ANO	
Minimální počet HW QoS front	8	
QoS classification – ACL, DSCP, CoS based	ANO	
QoS marking - DSCP, CoS	ANO	
QoS - Strict Priority Queue	ANO	
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	
QoS Policing	ANO	
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO	
IPv6 services (Telnet, SSH, Syslog, DHCP)	ANO	
IPv6 QoS	ANO	
IPv6 First Hop Security (RA guard, DHCPv6 snooping)	ANO	
IPv6 ACL	ANO	
Možnost definovat povolené MAC adresy na portu	ANO	
PACL, VACL	ANO	
IEEE 802.1ae na 1GE uplink portech	ANO	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	
IEEE 802.3af	ANO	
IEEE 802.3at	ANO	
Minimální PoE budget	390W	
IEEE 802.3az	ANO	
Možnost automatické aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	
Integrovaný WLAN kontrolér	ANO	
Vyhodnocování kvality signálu bezdrátové sítě v reálném čase, zpracování a reakce na informace o rušivých signálech (interference) z AP	ANO	
Podpora 802.11i, respektive jeho implementací WPA a WPA2 včetně enterprise variant autentizace/šifrování	ANO	
Aplikace QoS per WLAN AP, WLAN SSID, WLAN klient	ANO	
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	ANO	
Zrcadlení provozu na úrovni jednotlivých fyzických rozhraní i virtuálních sítí (VLAN) do monitorovacího rozhraní (ekvivalent funkce SPAN)	ANO	
Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	
DHCP server	ANO	
SSHv2	ANO	
CLI rozhraní	ANO	
SNMPv2/v3	ANO	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	
NTPv3 server	ANO	

3. Komunikační moduly

K implementaci síťových prvků je počítáno s 325 transceiver moduly.

V současné době je v rámci LAN provozováno 285ks optických 1000Base-SX transceiver modulů od společnosti Cisco Systems – typové označení GLC-SX-MM a GLC-SX-MMD na duplexních multimodových trasách.

Dále pak 40ks optických transceiver modulů 1000Base-LX/LH od společnosti Cisco Systems – typové označení GLC-LH-SM a GLC-LH-SMD na duplexních singlemodových trasách.

Zadavatel v rámci ochrany investic doporučuje, aby tyto transceivery byly nadále použitelné i v novém řešení. Pokud uchazeč nabídne řešení, které tyto transceivery nebude podporovat, musí jeho řešení obsahovat i definovaný počet transceiver modulů potřebných pro propojení LAN. Tyto transceivery musí být plně podporované výrobcem aktivních prvků a toto musí být potvrzeno prohlášením výrobce dodávaných aktivních prvků.

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
40 ks Singlemode SFP (LC) transceivery		
Výrobce zařízení	Uvedení výrobce	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	
285 ks Multimode SFP (LC) transceivery		
Výrobce zařízení	Uvedení výrobce	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	

4. Nástroj pro řízení přístupu do sítě a podpůrné aplikace

Nabídka musí obsahovat nástroj pro řízení přístupu a kontrolu politik pro drátové, bezdrátové a VPN platformy a podpůrné aplikace umožňující jednoduchou správu MAC address a lokalizaci zařízení.

A) 2 ks zařízení pro řízení přístupu včetně podpory pro 10.000 současných koncových zařízení

Zadavatel v rámci obměny plánuje zlepšení úrovně síťového zabezpečení infrastruktury proti neoprávněnému přístupu.

Zadavatel se rozhodl k nasazení řešení, které umožní:

- Identifikaci koncového zařízení
- Autentizaci koncových zařízení (uživatelů)
- Autorizaci koncových zařízení (uživatelů)
- Logování přístupů připojovaných zařízení (uživatelů)

Řešení musí být schopné splnit výše zmíněné body v síti LAN/ Wi-Fi/ VPN, zároveň ověřit identitu uživatele koncového zařízení s cílem zajistit, že jen oprávněným zařízením a uživatelům bude umožněno přistoupit na do LAN/Wi-Fi/VPN infrastruktury Zadavatele.

Mezi další vlastnosti, které řešení musí poskytovat, patří:

- Schopnost registrovat zařízení interních/externích zaměstnanců
- Automatický proces vydávání certifikátů na registrované zařízení
- Nastavení síťových profilů na zařízeních a vydávání certifikátů
- Možnost kontroly, zda zařízení splňuje definované bezpečnostní parametry (kontrola může být provedena dotazem na externí aplikaci, poskytující tyto údaje)

Tyto dodatečné vlastnosti jsou nazývány společným názvem BYOD (Bring Your Own Device) a MDM (Mobile Device Management).

Řešení musí umět zpracovávat požadavky zasílané protokoly RADIUS (NAC) a TACACS+ (síťová administrace).

Řešení musí zajistit ověření pro 10.000 současných zařízení, a pokud je tato funkcionalita samostatně licencována, musí cena zahrnovat i příslušné poplatky včetně podpory.

Zadavatel požaduje řešení postavené na technologii, která bude spravována centrálně. V případě výpadku centrálního serveru nebude ohrožen chod sítě. MDM řešení může být provozován na dedikovaném HW. Zadavatel v rámci zakázky požaduje od dodavatele pomoc při návrhu změn provozních procesů a postupů.

Tabulka 4 Funkční specifikace nástroje pro řízení a kontrolu přístupu

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
2 ks zařízení pro řízení přístupu včetně funkcionality a podpory pro 10.000 současných koncových zařízení		
Výrobce zařízení	Uvedení výrobce	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	
Obecná charakteristika ověřovacího řešení		
Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení apod.)	ANO	
Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo řídícími moduly, VPN branami) poskytuje ochranu před neoprávněným přístupem k pevné LAN síti, bezdrátové wifi síti (metodou 802.1x) a pro VPN přístup	ANO	
Poskytuje AAA funkce (viz níže)	ANO	
Podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control)	ANO	
Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování kapacity	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace	ANO	
Je dostupné ve formě Appliance (hardware i software podporovaný jedním výrobcem)	ANO	
Je dostupné ve formě Virtuálního stroje na platformách ESX nebo ESXi	ANO	
AAA funkce (ověřování, autorizace a záznamy o průběhu připojování uživatelů a zařízení k síti)		
Podporované protokoly		
RADIUS pro autentizaci, autorizaci, logování	ANO	
proxy funkce pro externí RADIUS	ANO	
TACACS+ pro autentizaci, autorizaci a logování	ANO	
TACACS+ pro funkci TACACS+ proxy	ANO	
PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST,EAP-TTLS	ANO	
Podporované databáze uživatelů (s možností definovat pořadí průchodu		
Interní (pro uživatele i koncová zařízení)	ANO	
Active Directory	ANO	
Active Directory – více nezávislých domén	ANO	
LDAP (RFC 2251)	ANO	
RADIUS Token indentity source (RFC 2865)	ANO	
RSA RADIUS token server	ANO	
Ověřování certifikátu koncových stanic/uživatelů na základě definovaného pole z certifikátu.	ANO	
Ověřování uživatelů a zařízení		
Ověření uživatelů heslem nebo certifikátem	ANO	
Ověření MAC adresou připojovaného zařízení	ANO	
Rozpoznávání typu koncových zařízení a jejich stavu		
Automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se síťovou infrastrukturou	ANO	
Předdefinované profily pro běžná mobilní zařízení (zařízení s OS Android, SymbianOS, Apple, Blackberry, HTC)	ANO	
Autorizace: pružný systém pro definici pravidel pro přístup k síti		
Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle • uživatele (role, skupiny), • stavu a typu koncového zařízení (viz výše), • místa připojení, • historie připojení	ANO	
Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě	ANO	
Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě	ANO	
Podpora Change of Authorization (CoA, RFC 3576)	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
Možnost jednoduše identifikovat/označit přenášená data uživatele (rámce) v chráněné oblasti	ANO	
Accounting		
Zaznamenávání aktivity uživatelů a zařízení připojených k síti	ANO	
Dotazovací systém, korelace záznamů, centralizované výkazy	ANO	
Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů)	ANO	
Funkce GUEST serveru		
Vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i WiFi	ANO	
Oprávnění přidělovaná správcem přístupu přes portál pro snadné vytváření dočasných účtů	ANO	
Samoobslužný portál pro uživatele	ANO	
Další vlastnosti		
Aktivace šifrování MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují)	ANO	
Integrace s MDM systémy	ANO	
Funkce pro správu ověřovacího systému		
Centralizovaná správa	ANO	
Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému	ANO	
Zjednodušení správy vytvářeními skupin uživatelů, koncových a síťových zařízení	ANO	
Grafické rozhraní pro definici pravidel přístupu k síti	ANO	
Grafické rozhraní pro monitorování, definici výkazů, řešení problémů	ANO	
Diagnostika problémů (systémová, údaje o chybách přihlašování, TCP dump, packet capture)	ANO	
Zaznamenávání událostí na externí syslog server	ANO	
Podpora SNMPv3	ANO	
NTP pro synchronizaci času	ANO	
SMTP pro zasílání zpráv a výstrah přes e-mail	ANO	
Centrální server musí umět autorizovat mobilních zařízení do wifi sítě na základě kontroly jejich „zdraví“ (kontrola, zda zařízení není rootnuto, má antivir, …) pomocí napojeného MDM systému Zákazníka (Mobile Iron)	ANO	

B) Podpůrná aplikace pro správu MAC adres

Nabídka musí obsahovat aplikaci, která dokáže spravovat databázi velkého množství MAC adres. Aplikace musí umožňovat přidávání a odebíraní MAC adress kontraktorů, interních zaměstnanců, počítačů určených k nové instalaci nebo k reinstalaci a speciálních zařízení. Musí mít uživatelsky přívětivé rozhraní, aby s ní mohli operátoři helpdesk podpory Zadavatele co nejefektivněji pracovat. Tato aplikace bude sloužit k ovládání nástroje pro řízení, kontrolu a monitoring přístupu do sítě. Dále musí umět řídit přístup do jednotlivých částí aplikace na základě ověření uživatele z AD a jeho členství ve skupinách. Práce s MAC adresami musí být umožněna manuálně (administrátor na základě oprávnění v Active Directory dokáže změnit záznamy v databázi) a automaticky, kdy MAC adresy budou odbírány ze systému na základě časového faktoru. Aplikace musí být schopná pracovat v HA režimu.

Aplikace musí umožnit auditování akcí prováděných administrátory při práci s jednotlivými MAC adresami. Aplikace musí umožňovat přístup pouze v režimu ReadOnly.

Zadavatel požaduje řešení, které bude postaveno na technologii, která bude spravována centrálně. V případě výpadku centrálního serveru nebude ohrožen chod sítě. MDM řešení může být provozováno na dedikovaném HW.

C) Podpůrná aplikace pro lokalizaci zařízení

Nabídka musí také obsahovat aplikaci, která poskytne komplexní informace o stavu a umístění zařízení na portu přepínače. Musí umět resolvovat MAC adresu vůči síťovému jménu (jméno uživatele nebo počítače) a na základě těchto informací poskytnout informace o přepínači, do kterého je zařízení připojeno včetně historie událostí na daném portu.

Tabulka 5 Funkční specifikace podpůrných aplikací

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
Podpůrná aplikace pro správu MAC adres		
Výrobce aplikace	Uvedení výrobce	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	
Podpora funkcionality hromadného přidávání a mazání MAC adres v autentizačním systému	ANO	
Podpora funkcionality manuálního přidávání a mazání MAC adres v autentizačním systému	ANO	
Podpora funkcionality Wake On LAN pro zařízení v prostředí 802.1x	ANO	
Umožnit řízení přístupu různých uživatelů v rámci aplikace	ANO	
Umožnit rozlišení read-only / read-write přístupu v rámci aplikace	ANO	
Umožnit uživatelsky přívětivou správu aplikace prostřednictvím webového rozhraní	ANO	
Umožnit jednoduchou blokaci přístupu vybraným zařízením	ANO	
Umožnit funkcionalitu aplikace v rámci HA clusteru	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní Uchazeč dle nabízeného zařízení
Podpora auditovacích akcí	ANO	
Podpůrná aplikace pro lokalizaci zařízení		
Výrobce aplikace	Uvedení výrobce	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	
Umožnit funkcionalitu vyhledání portu, na kterém je uživatel připojen	ANO	
Umožnit zjištění stavu autentizace příslušného portu	ANO	
Umožnit zjištění stavu autentizace vybraného uživatele	ANO	
Umožnit správu síťových přepínačů v rámci aplikace	ANO	
Umožnit funkcionalitu aplikace v rámci HA clusteru	ANO	

Komentář k technické specifikaci:

Zadavatel ve sloupci "Požadovaná funkcionalita/vlastnost" zadal ***minimální*** požadované parametry poptávaných zařízení. **Pokud nebudou tyto minimální požadavky splněny, bude taková nabídka vyřazena v rámci posouzení nabídek.**

Uchazeč v poli „*Doplní Uchazeč dle nabízeného zařízení*" vyplní konkrétní parametry nabízeného zařízení.

Poznámka: ***Specifikace jsou minimální. Uchazeč může nabídnout vyšší úroveň konfigurace, toto zvýšení parametrů však nemá vliv na hodnocení nabídky.***

Požadavky na předvedení funkcionalit

Zadavatel požaduje po dodavateli před uzavřením kupní smlouvy prokázání funkcionality implementovaného systému v prostředí zadavatele dle jednotlivých bodů požadavků se zaměřením na funkce:

Tabulka 6 Popis funkčních testů

Testovaná funkcionalita		*Možný výsledek*	*Výsledek*
WAN směrovač - typ A			
Detekce přímo připojených zařízení			
1	Detekce přímo připojeného zařízení pomocí LLDP	**ANO/NE**	
2	Detekce přímo připojeného zařízení pomocí CDP	**ANO/NE**	
Routing			
3	OSPF pro IPv4	**ANO/NE**	
4	OSPF pro IPv6	**ANO/NE**	
5	OSPF pro IPv4 a IPv6 běžící současně	**ANO/NE**	
6	OSPF autentizace MD5	**ANO/NE**	
7	BGPv4	**ANO/NE**	
8	Podpora 4 byte AS number v BGP	**ANO/NE**	
9	BGP Multiprotocol Support	**ANO/NE**	
10	Generic Routing Encapsulation (GRE)	**ANO/NE**	
11	Multipoint Generic Routing Encapsulation (mGRE)	**ANO/NE**	
12	Unicast Reverse path check (uRPF)	**ANO/NE**	
13	Virtualizace směrovacích tabulek – VRF nebo kompatibilní	**ANO/NE**	
14	Alespoň 30 oddělených a nezávislých routovacích tabulek	**ANO/NE**	
15	Protokoly a služby per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)	**ANO/NE**	
16	Policy based routing na základě ACL	**ANO/NE**	
17	First Hop Redundancy protokol pro IPv4	**ANO/NE**	
18	First Hop Redundancy protokol pro IPv6	**ANO/NE**	
Multicast			
19	IGMP v3	**ANO/NE**	
20	MLD v2	**ANO/NE**	
21	PIM Sparse Mode	**ANO/NE**	
22	PIM Dense Mode	**ANO/NE**	
23	PIM Sparse-Dense Mode	**ANO/NE**	
24	PIM Source Specific Multicast	**ANO/NE**	
Bezpečnost			
25	ACL na rozhraní IN/OUT	**ANO/NE**	
26	Zone-based firewall	**ANO/NE**	
27	Šifrování GRE tunelů	**ANO/NE**	
28	IPSec AES-GCM-256	**ANO/NE**	

29	Propustnost minimálně 90 Mbit (IMIX provoz) při aktivovaných službách IPSec šifrování a QoS	**ANO/NE**	
30	Zvýšení propustnosti směrovače na alespoň 270 Mbit (IMIX provoz) při aktivovaných službách IPSec šifrování a QoS, např. formou licence	**ANO/NE**	
31	IKEv2	**ANO/NE**	
32	SHA-2 (SHA-256, SHA-512)	**ANO/NE**	
33	Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami	**ANO/NE**	
34	Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů	**ANO/NE**	
35	Ochrana Control Plane směrovače před DoS útoky	**ANO/NE**	
Monitorování Aplikačních toků			
36	Monitorování vstupních a výstupních toků na interface současně	**ANO/NE**	
37	Monitoring bez vlivu na výkonnost zařízení	**ANO/NE**	
38	Monitoring bez vlivu na propustnost zařízení	**ANO/NE**	
39	Monitoring IPv4 a IPv6	**ANO/NE**	
40	Lokální zobrazení shromážděných dat na směrovači	**ANO/NE**	
41	Export dat ve formátu Netflow v9	**ANO/NE**	
42	Export dat ve formátu IPFIX	**ANO/NE**	
43	Monitoring všech procházejících paketů (nesamplovaný)	**ANO/NE**	
44	Detekce a klasifikace aplikačních dat procházejících směrovačem až do 7. vrstvy OSI modelu (Deep Packet Inspection)	**ANO/NE**	
45	Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	**ANO/NE**	
Quality of Service			
46	Klasifikace procházející dopravy na základě CoS	**ANO/NE**	
47	Klasifikace procházející dopravy na základě DSCP	**ANO/NE**	
48	Klasifikace procházející dopravy na základě ACL	**ANO/NE**	
49	Klasifikace procházející dopravy na základě analýzy až 7. vrstvy OSI modelu	**ANO/NE**	
50	Značení procházející dopravy pomocí CoS	**ANO/NE**	
51	Značení procházející dopravy pomocí DSCP	**ANO/NE**	
52	Zařazování procházejícího provozu do front na základě dříve rozlišených tříd dopravy	**ANO/NE**	
53	Prioritní fronta pro citlivé aplikace jako je voice a video	**ANO/NE**	
54	Definice šířky pásma pro jednotlivé fronty	**ANO/NE**	
55	Definice délky jednotlivých front	**ANO/NE**	
56	Shaping odcházejícího provozu	**ANO/NE**	
57	Policing odcházejícího a přicházejícího provozu	**ANO/NE**	
58	Rate-limiting odcházejícího a přicházejícího provozu	**ANO/NE**	

59	RSVP	**ANO/NE**	
60	Hierarchický QoS, minimálně 3 úrovně	**ANO/NE**	
Přístupový LAN přepínač 48 portů			
Napájecí zdroje a ventilátory			
1	Redundantní napájecí zdroje	**ANO/NE**	
2	Redundantní ventilátory	**ANO/NE**	
3	Plnohodnotná funkce přepínače v případě výpadku kteréhokoliv redundantního prvku	**ANO/NE**	
4	Výpadek redundantního prvku nezpůsobí ztrátu konektivity připojeného zařízení	**ANO/NE**	
5	U PoE zařízení nesmí dojít v případě výpadku zdroje k výpadku napájení	**ANO/NE**	
6	Všechny redundantní prvky jsou vyměnitelné za chodu a to bez dopadu na provoz procházející přepínačem	**ANO/NE**	
Napájení po datovém kabelu			
7	Napájení koncového zařízení 15W (802.2af)	**ANO/NE**	
8	Napájení koncového zařízení 30W (802.3at)	**ANO/NE**	
9	Napájení až 13x 30W současně	**ANO/NE**	
10	Napájení až 13x 30W současně při jediném funkčním napájecím zdroji	**ANO/NE**	
Detekce přímo připojených zařízení			
11	Detekce přímo připojeného zařízení pomocí LLDP	**ANO/NE**	
12	Detekce přímo připojeného zařízení pomocí CDP	**ANO/NE**	
VLAN			
13	Vytvoření VLAN v rozsahu 1 - 4094	**ANO/NE**	
14	1000 aktivních a funkčních VLAN zároveň	**ANO/NE**	
15	Tagování 802.1Q	**ANO/NE**	
16	Tagování 802.1Q v 802.1Q	**ANO/NE**	
17	Centralizovaná zpráva VLAN databáze	**ANO/NE**	
18	Zařízení slouží jako řídící prvek pro zprávu VLAN databáze	**ANO/NE**	
19	VLAN databáze je chráněna proti nežádoucím změnám	**ANO/NE**	
20	VLAN databáze může být změněna pouze na centrálním prvku	**ANO/NE**	
21	VLAN databáze je chráněna heslem	**ANO/NE**	
Spanning Tree Protocol			
22	802.1w – RSTP	**ANO/NE**	
23	Zpětná kompatibilita s 802.1D – STP	**ANO/NE**	
24	Samostatná STP instance pro alespoň 128 VLAN	**ANO/NE**	
25	Zařízení připraveno na nasazení 802.1s – MSTP	**ANO/NE**	
26	Šíření MSTP konfigurace mezi přepínači z centrálního přepínače	**ANO/NE**	

27	Možnost měnit konfiguraci MSTP regionu pouze na centrálním přepínači	**ANO/NE**	
28	Konfigurace MSTP chráněna heslem	**ANO/NE**	
29	Porty ke koncovým zařízením přecházejí okamžitě do stavu forwarding	**ANO/NE**	
30	Ochrana koncových portů proti připojení nežádoucího přepínače na základě kontroly přijímaných BPDU	**ANO/NE**	
31	Ochrana proti změně STP centrálního switche	**ANO/NE**	
32	Zabránění vzniku smyčky v případě, že port přestane dostávat BPDU (jednosměrná smyčka)	**ANO/NE**	
33	Detekce jednosměrné linky (optické i metalické) mechanismem nezávislým na STP (UDLD nebo kompatibilní)	**ANO/NE**	
Routing			
34	OSPF pro IPv4	**ANO/NE**	
35	OSPF pro IPv6	**ANO/NE**	
36	OSPF pro IPv4 a IPv6 běžící současně	**ANO/NE**	
37	OSPF autentizace MD5	**ANO/NE**	
38	First Hop Redundancy protokol pro IPv4	**ANO/NE**	
39	First Hop Redundancy protokol pro IPv6	**ANO/NE**	
40	Unicast Reverse path check (uRPF)	**ANO/NE**	
Multicast			
41	IGMP snooping v3	**ANO/NE**	
42	MLD snooping v2	**ANO/NE**	
43	PIM Sparse Mode	**ANO/NE**	
44	PIM Dense Mode	**ANO/NE**	
45	PIM Sparse-Dense Mode	**ANO/NE**	
46	PIM Source Specific Multicast	**ANO/NE**	
Bezpečnost			
47	Limitování počtu povolených MAC adres na port	**ANO/NE**	
48	802.1x ověřování koncových zařízení	**ANO/NE**	
49	Ochrana proti podvržení DHCP serveru	**ANO/NE**	
50	Ochrana proti podvržení DHCP release a decline zpráv	**ANO/NE**	
51	Kontrola MAC adresy v DHCP request zprávě vůči MAC adrese v ethernetovém rámci (Ochrana proti DoS)	**ANO/NE**	
52	DHCP messages rate-limiting (Ochrana proti DoS)	**ANO/NE**	
53	Ochrana proti podvržení IP adresy	**ANO/NE**	
54	Ochrana proti podvržení MAC adresy	**ANO/NE**	
55	Ochrana proti podvržení ARP zprávy – kontrola a ověření jednotlivých polí v ARP zprávě	**ANO/NE**	
56	ARP messages rate-limiting (Ochrana proti DoS)	**ANO/NE**	
57	Ochrana proti podvržení DHCPv6 serveru	**ANO/NE**	
58	Ochrana proti podvržení IPv6 Router Advertisement	**ANO/NE**	

59	Ochrana proti podvržení IPv6 Neighbor Discovery	**ANO/NE**	
60	Ochrana proti podvržení IPv6 adresy	**ANO/NE**	
61	802.1ae – MACsec, line-rate šifrování na L2	**ANO/NE**	
62	802.1ae mezi přepínači	**ANO/NE**	
63	802.1ae ke koncovým stanicím	**ANO/NE**	
64	Ochrana Control Plane přepínače před DoS útoky	**ANO/NE**	
Monitorování Aplikačních toků			
65	Monitorování vstupních a výstupních toků na interface současně	**ANO/NE**	
66	Monitoring bez vlivu na výkonnost zařízení	**ANO/NE**	
67	Monitoring bez vlivu na propustnost zařízení	**ANO/NE**	
68	Monitoring IPv4 a IPv6	**ANO/NE**	
69	Lokální zobrazení shromážděných dat na přepínači	**ANO/NE**	
70	Export dat ve formátu Netflow v9	**ANO/NE**	
71	Export dat ve formátu IPFIX	**ANO/NE**	
72	Monitoring všech procházejících paketů (nesamplovaný)	**ANO/NE**	
Quality of Service			
73	Klasifikace procházející dopravy na základě CoS	**ANO/NE**	
74	Klasifikace procházející dopravy na základě DSCP	**ANO/NE**	
75	Klasifikace procházející dopravy na základě ACL	**ANO/NE**	
76	Značení procházející dopravy pomocí CoS	**ANO/NE**	
77	Značení procházející dopravy pomocí DSCP	**ANO/NE**	
78	Zařazování procházejícího provozu do front na základě dříve rozlišených tříd dopravy	**ANO/NE**	
79	Prioritní fronta pro citlivé aplikace jako je voice a video	**ANO/NE**	
80	Definice šířky pásma pro jednotlivé fronty	**ANO/NE**	
81	Definice délky jednotlivých front	**ANO/NE**	
82	Shaping odcházejícího provozu	**ANO/NE**	
83	Policing odcházejícího a přicházejícího provozu	**ANO/NE**	
84	Hierarchický QoS, minimálně 2 úrovně	**ANO/NE**	
Řízení přístupu do sítě			
85	Aplikovat critical VLAN v případě nedostupnosti AAA	**ANO/NE**	
86	VLAN loadbalancing	**ANO/NE**	
87	Umožnit Radius CoA	**ANO/NE**	
Přístupový LAN přepínač 24 portů			
Napájecí zdroje a ventilátory			
1	Redundantní napájecí zdroje	**ANO/NE**	
2	Redundantní ventilátory	**ANO/NE**	
3	Plnohodnotná funkce přepínače v případě výpadku kteréhokoliv redundantního prvku	**ANO/NE**	

4	Výpadek redundantního prvku nezpůsobí ztrátu konektivity připojeného zařízení	**ANO/NE**	
5	U PoE zařízení nesmí dojít v případě výpadku zdroje k výpadku napájení	**ANO/NE**	
6	Všechny redundantní prvky jsou vyměnitelné za chodu a to bez dopadu na provoz procházející přepínačem	**ANO/NE**	
Napájení po datovém kabelu			
7	Napájení koncového zařízení 15W (802.2af)	**ANO/NE**	
8	Napájení koncového zařízení 30W (802.3at)	**ANO/NE**	
9	Napájení až 13x 30W současně	**ANO/NE**	
10	Napájení až 13x 30W současně při jediném funkčním napájecím zdroji	**ANO/NE**	
Detekce přímo připojených zařízení			
11	Detekce přímo připojeného zařízení pomocí LLDP	**ANO/NE**	
12	Detekce přímo připojeného zařízení pomocí CDP	**ANO/NE**	
VLAN			
13	Vytvoření VLAN v rozsahu 1 - 4094	**ANO/NE**	
14	1000 aktivních a funkčních VLAN zároveň	**ANO/NE**	
15	Tagování 802.1Q	**ANO/NE**	
16	Tagování 802.1Q v 802.1Q	**ANO/NE**	
17	Centralizovaná zpráva VLAN databáze	**ANO/NE**	
18	Zařízení slouží jako řídící prvek pro zprávu VLAN databáze	**ANO/NE**	
19	VLAN databáze je chráněna proti nežádoucím změnám	**ANO/NE**	
20	VLAN databáze může být změněna pouze na centrálním prvku	**ANO/NE**	
21	VLAN databáze je chráněna heslem	**ANO/NE**	
Spanning Tree Protocol			
22	802.1w – RSTP	**ANO/NE**	
23	Zpětná kompatibilita s 802.1D – STP	**ANO/NE**	
24	Samostatná STP instance pro alespoň 128 VLAN	**ANO/NE**	
25	Zařízení připraveno na nasazení 802.1s – MSTP	**ANO/NE**	
26	Šíření MSTP konfigurace mezi přepínači z centrálního přepínače	**ANO/NE**	
27	Možnost měnit konfiguraci MSTP regionu pouze na centrálním přepínači	**ANO/NE**	
28	Konfigurace MSTP chráněna heslem	**ANO/NE**	
29	Porty ke koncovým zařízením přecházejí okamžitě do stavu forwarding	**ANO/NE**	
30	Ochrana koncových portů proti připojení nežádoucího přepínače na základě kontroly přijímaných BPDU	**ANO/NE**	
31	Ochrana proti změně STP centrálního switche	**ANO/NE**	
32	Zabránění vzniku smyčky v případě, že port přestane dostávat BPDU (jednosměrná smyčka)	**ANO/NE**	

33	Detekce jednosměrné linky (optické i metalické) mechanismem nezávislým na STP (UDLD nebo kompatibilní)	**ANO/NE**	
Routing			
34	OSPF pro IPv4	**ANO/NE**	
35	OSPF pro IPv6	**ANO/NE**	
36	OSPF pro IPv4 a IPv6 běžící současně	**ANO/NE**	
37	OSPF autentizace MD5	**ANO/NE**	
38	First Hop Redundancy protokol pro IPv4	**ANO/NE**	
39	First Hop Redundancy protokol pro IPv6	**ANO/NE**	
40	Unicast Reverse path check (uRPF)	**ANO/NE**	
Multicast			
41	IGMP snooping v3	**ANO/NE**	
42	MLD snooping v2	**ANO/NE**	
43	PIM Sparse Mode	**ANO/NE**	
44	PIM Dense Mode	**ANO/NE**	
45	PIM Sparse-Dense Mode	**ANO/NE**	
46	PIM Source Specific Multicast	**ANO/NE**	
Bezpečnost			
47	Limitování počtu povolených MAC adres na port	**ANO/NE**	
48	802.1x ověřování koncových zařízení	**ANO/NE**	
49	Ochrana proti podvržení DHCP serveru	**ANO/NE**	
50	Ochrana proti podvržení DHCP release a decline zpráv	**ANO/NE**	
51	Kontrola MAC adresy v DHCP request zprávě vůči MAC adrese v ethernetovém rámci (Ochrana proti DoS)	**ANO/NE**	
52	DHCP messages rate-limiting (Ochrana proti DoS)	**ANO/NE**	
53	Ochrana proti podvržení IP adresy	**ANO/NE**	
54	Ochrana proti podvržení MAC adresy	**ANO/NE**	
55	Ochrana proti podvržení ARP zprávy – kontrola a ověření jednotlivých polí v ARP zprávě	**ANO/NE**	
56	ARP messages rate-limiting (Ochrana proti DoS)	**ANO/NE**	
57	Ochrana proti podvržení DHCPv6 serveru	**ANO/NE**	
58	Ochrana proti podvržení IPv6 Router Advertisement	**ANO/NE**	
59	Ochrana proti podvržení IPv6 Neighbor Discovery	**ANO/NE**	
60	Ochrana proti podvržení IPv6 adresy	**ANO/NE**	
61	802.1ae – MACsec, line-rate šifrování na L2	**ANO/NE**	
62	802.1ae mezi přepínači	**ANO/NE**	
63	802.1ae ke koncovým stanicím	**ANO/NE**	
64	Ochrana Control Plane přepínače před DoS útoky	**ANO/NE**	
Monitorování Aplikačních toků			
65	Monitorování vstupních a výstupních toků na interface současně	**ANO/NE**	

66	Monitoring bez vlivu na výkonnost zařízení	**ANO/NE**	
67	Monitoring bez vlivu na propustnost zařízení	**ANO/NE**	
68	Monitoring IPv4 a IPv6	**ANO/NE**	
69	Lokální zobrazení shromážděných dat na přepínači	**ANO/NE**	
70	Export dat ve formátu Netflow v9	**ANO/NE**	
71	Export dat ve formátu IPFIX	**ANO/NE**	
72	Monitoring všech procházejících paketů (nesamplovaný)	**ANO/NE**	
Quality of Service			
73	Klasifikace procházející dopravy na základě CoS	**ANO/NE**	
74	Klasifikace procházející dopravy na základě DSCP	**ANO/NE**	
75	Klasifikace procházející dopravy na základě ACL	**ANO/NE**	
76	Značení procházející dopravy pomocí CoS	**ANO/NE**	
77	Značení procházející dopravy pomocí DSCP	**ANO/NE**	
78	Zařazování procházejícího provozu do front na základě dříve rozlišených tříd dopravy	**ANO/NE**	
79	Prioritní fronta pro citlivé aplikace jako je voice a video	**ANO/NE**	
80	Definice šířky pásma pro jednotlivé fronty	**ANO/NE**	
81	Definice délky jednotlivých front	**ANO/NE**	
82	Shaping odcházejícího provozu	**ANO/NE**	
83	Policing odcházejícího a přicházejícího provozu	**ANO/NE**	
84	Hierarchický QoS, minimálně 2 úrovně	**ANO/NE**	
Řízení přístupu do sítě			
85	Aplikovat critical VLAN v případě nedostupnosti AAA	**ANO/NE**	
86	VLAN loadbalancing	**ANO/NE**	
87	Umožnit Radius CoA	**ANO/NE**	
Nástroje pro řízení, kontrolu a monitoring přístupu do sítě			
Systém pro řízení přístupu do sítě			
1	Ověřit možnost redundance/loadbalancingu RADIUS komunikace	**ANO/NE**	
2	Ověřit, že autentizační systém umožňuje autorizaci pomocí Jména, nebo čísla VLAN	**ANO/NE**	
3	Ověřit možnost zasílat autorizaci pomocí downloable access listu	**ANO/NE**	
4	Ověřit autentizaci koncového zařízení na základě MAC adresy	**ANO/NE**	
5	Ověřit možnost monitorování aktuálních přístupů do sítě včetně historie	**ANO/NE**	
6	Ověřit možnost zasílání autentizačních informací pomocí syslog protokolu (UDP, TCP, Secure TCP)	**ANO/NE**	
7	Autentizační server umožňuje ověřování certifikátů koncových stanic / uživatelů	**ANO/NE**	

8	Ověřit funkcionalitu stavu certifikátu metodou CRL	**ANO/NE**	
9	Ověřit funkcionalitu stavu certifikátu metodou OCSP	**ANO/NE**	
10	Ověřit funkcionalitu autentizace IP telefonu do VOICE domény	**ANO/NE**	
11	Ověřit, že autentizační server je schopen být integrován do více MS AD, které nejsou ve vzájemném „trustu“.	**ANO/NE**	
12	Ověřit, že integrace s doménou může být provedena pomocí MS KERBEROS protokolu	**ANO/NE**	
13	Ověřit, že autentizační server umožňuje načítání uživatelských skupin z AD	**ANO/NE**	
14	Ověřit, že autentizační server umožňuje načítání vlastností objektu typu uživatel	**ANO/NE**	
15	Ověřit, že autentizační server umožňuje načítání atributů objektu typu machine	**ANO/NE**	
16	Ověřit podporu Radius CoA	**ANO/NE**	
17	Ověřit, že autentizační server je schopen shromažďovat informace o typu koncových zařízení	**ANO/NE**	
18	Ověřit, že autentizační server umožňuje odmítnout vpustit do sítě nedoménového uživatele přihlašujícího se na doménovém zařízení	**ANO/NE**	
19	Zakomponovat ověřování mobilní laboratoře	**ANO/NE**	
Podpůrná aplikace pro správu MAC adres			
20	Ověřit možnost hromadného přidávání MAC adres do autentizačního systému	**ANO/NE**	
21	Ověřit možnost hromadného mazání MAC adres z autentizačního systému	**ANO/NE**	
22	Ověřit možnost manuálního přidávání MAC adres do autentizačního systému	**ANO/NE**	
23	Ověřit možnost manuálního mazání MAC adres z autentizačního systému	**ANO/NE**	
24	Ověřit funkcionalitu Wake On LAN	**ANO/NE**	
25	Předvést možnost řízení přístupu různých uživatelů a uživatelských skupin v rámci aplikace	**ANO/NE**	
26	Předvést možnost rozlišení read-only / read-write přístupu v rámci aplikace	**ANO/NE**	
27	Předvést funkcionalitu umožnění přístupu na základě Sponzorského účtu	**ANO/NE**	
28	Předvést možnost hlídání času validity MAC adres a jejich automatické mazání z databáze autentizačního systému	**ANO/NE**	
29	Předvést postup blokace přístupu vybraným zařízením	**ANO/NE**	
30	Předvést možnost samostatné správy konfigurace aplikace prostřednictvím webového rozhraní	**ANO/NE**	
Podpůrná aplikace pro lokalizaci zařízení			

31	Předvést funkcionalitu vyhledání portu, na kterém je uživatel připojen	**ANO/NE**	
32	Zjištění stavu autentizace příslušného portu	**ANO/NE**	
33	Zjištění stavu autentizace vybraného uživatele	**ANO/NE**	
34	Předvést správu síťových přepínačů v rámci aplikace	**ANO/NE**	

Povinností dodavatele je zajistit pro předvedení v rámci prokázání funkcionalit veškeré nabízené produkty včetně nezbytných licencí a všechny potřebné nástroje pro simulaci provozu a měření požadovaných hodnot.