

## **Požadované technické parametry dodávky**

Předmětem dodávky jsou aktivní síťové prvky a záložní zdroj napájení UPS dle technických podmínek uvedených níže:

- Modulární přístupový/agregační přepínač (2 ks),
- Nemodulární přístupový stohovatelný gigabitový přepínač s možností napájení po Ethernetu (3 ks),
- Agregační přepínač/směrovač (1 ks),
- Bezdrátový přístupový bod (70 ks),
- Záložní zdroj napájení UPS (3ks),
- Stojanový rozvaděč (1ks).

Všechny poptávané síťové prvky musí být z důvodů ochrany stávajících investic a minimalizace celkových nákladů na vlastnictví a provoz počítačové sítě ZČU kompatibilní se všemi již používanými zařízeními, komunikačními protokoly a systémy správy sítě. Ze stejného důvodu musí být poptávané stohovatelné prvky stohovatelné i s prvky již používanými v síti ZČU.

**Tabulka mandatorních požadavků pro modulární přístupový/agregační přepínač (požadovány 2 ks)**

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
<b>Základní vlastnosti</b>		
Typ zařízení	L3 přepínač	
Formát zařízení	modulární	
Počet slotů pro moduly rozhraní	5	
Počet 10GE portů na řídicím modulu	2	
Požadovaný počet a typ 10GE transceiverů	2x 10GBase-LR, SFP+	
Typ 10GE portu na bezprostředně připojeném zařízení	X2	
Redundantní zdroje, dosažitelný výkon každého	2500W	
Podpora modulů 48x 10/100/1000 Ethernet, neblokující, 802.3at (PoE+) na všech portech současně, L2 šifrování dle 802.1AE, IEEE 802.3az	ano	
Požadovaný počet modulů 48x 10/100/1000Base-T, neblokující, 802.3at (PoE+) na všech portech současně, L2 šifrování dle 802.1AE, IEEE 802.3az	5	
Podpora modulů 48x 10/100/1000Base-T, neblokující, L2 šifrování dle 802.1AE, IEEE 802.3az	ano	
Požadovaný počet modulů 48x 10/100/1000Base-T, neblokující, L2 šifrování dle 802.1AE, IEEE 802.3az	0	
Podpora modulů 48x 10/100/1000Base-T, agregace 2:1, 802.3af (PoE+) na 24 portech současně	ano	
Podpora modulů 48x 10/100/1000Base-T, agregace 2:1	ano	
Podpora modulů s minimálně 12 porty GE/6x10GE, Jumbo rámce	ano	
Podpora modulů s 24xSFP sloty, neblokující	ano	
Podpora Non-Stop Forwarding	ano	
Podpora upgrade software za provozu	ano	
Podpora virtualizace – možnost sloučit alespoň dvě fyzická šasi do jednoho logického celku – virtuálního šasi	ano nebo povýšením software	
Statické směrování IPv4, IPv6	ano	
Dynamické směrování IPv4, IPv6	ano	
Podpora IPv4, IPV6 v hardware	ano	
<b>Výkonnostní parametry</b>		
Celková propustnost centrálních řídicích modulů (IPv4/IPv6)	200/100 milionů paketů/vteřinu	
Celková potenciální propustnost přepínacího subsystému	500 Gbit/s	
Dostupná kapacita na slot	48 Gbit/s	
Počet záznamů ve směrovací tabulce - IPv4 unicast	64000	
Počet záznamů ve směrovací tabulce – IPv6 unicast	32000	
Počet MAC adres	50000	
<b>Protokoly fyzické vrstvy</b>		
IEEE 802.3-2005	ano	

IEEE 802.3ad	ano	
IEEE 802.3ad přes více karet	ano	
Podpora "jumbo rámců"	ano	
<b>Protokoly spojové vrstvy</b>		
IEEE 802.1D	ano	
IEEE 802.1Q	ano	
Počet aktivních VLAN	4000	
Tunelování 802.1Q v 802.1Q	ano	
IEEE 802.1X - Port Based Network Access Control	ano	
IEEE 802.1s - multiple spanning trees	ano	
IEEE 802.1w - Rapid Tree Spanning Protocol	ano	
IEEE 802.1p	ano	
Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní	ano	
Detekce protilehlého zařízení	ano	
Protokol pro definici šířených VLAN	ano	
Detekce jednosměrnosti optické linky	ano	
STP root guard nebo ekvivalentní	ano	
STP loop guard nebo ekvivalentní	ano	
Možnost autorecovery po chybovém stavu	ano	
Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ano	
<b>Protokol IP</b>		
IP alias (více IP sítí na jednom rozhraní)	ano	
QoS (DiffServ)	ano	
DHCP relay	ano	
Router redundancy protokol (např. VRRP, HSRP)	ano	
<b>Protokol IPv6</b>		
Certifikace IPv6 ready logo – Phase II	ano	
Router redundancy protokol pro IPv6	ano	
Podpora IPv6 ACL	ano	
Podpora IPv6 QoS (DiffServ)	ano	
Podpora IPv6 services (DNS, Telnet, SSH, Syslog, ICMP, DHCP)	ano	
Podpora IPv6 Multicast (MLDv1 & v2)	ano	
Podpora IPv6 Multicast (PIM SSM)	ano	
Podpora IPv6 Multicast (PIM SM)	ano	
Podpora IPv6 MLDv2 snooping	ano	
Podpora IPv6 First Hop Security (IPv6 Port ACL, RA guard, DHCPv6 guard, Destination guard)	ano	
Podpora IPv6 Tunneling: ISATAP Tunnel	ano	
<b>Směrovací protokoly</b>		
OSPF	ano	
OSPF s MD5 a NSSA	ano	
RIPv2	ano	
Statické směrování	ano	

<b>Směrování multicastu</b>		
PIM (dense i sparse mód)	ano	
Source-Specific Multicast (SSM)	ano	
IGMPv2	ano	
IGMPv3	ano	
IGMPv3 snooping	ano	
IPv6 MLDv1 & v2 snooping	ano	
<b>Bezpečnost</b>		
Podpora reverse path check (uRPF)	ano	
ACL pro IP	ano	
IPv6 ACL	ano	
Možnost definovat povolené MAC adresy na portu	ano	
Možnost definovat maximální počet MAC adres na portu	ano	
Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	ano	
Podpora zabezpečení a analýzy DHCP protokolu	ano	
Podpora ochrany ARP protokolu	ano	
Podpora ochrany podvrženého mapování IP/MAC adresy	ano	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ano	
Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)	ano	
Vynucení IEEE 802.1x ověřování i na externím připojeném přepínači	ano	
Ochrana centrálního procesoru (control plane) před útoky typu DoS	ano	
Podpora klasifikace bezpečnostní role přístupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Security Group Exchange Protocol nebo funkčně ekvivalentní).	ano	
<b>Podpora koncových zařízení</b>		
Podpora PoE (IEEE 802.3af)	ano	
Podpora PoE+ (IEEE 802.3at, 30W/port)	ano	
Podpora PoE (60W/port)	ano	
Automatické i manuální ovládání PoE výkonu portu	ano	
Měření a ovládání spotřeby energie připojených koncových zařízení	ano	
Integrovaný nástroj na profilování připojovaných koncových zařízení	ano	
<b>Management</b>		
CLI rozhraní	ano	
SSHv2	ano	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	

SNMPv2	ano	
SNMPv3	ano	
Konzolová linka	ano	
Interpretace uživatelských CLI a Tcl skriptů a jejich aktivace asynchronní události v systému zařízení	ano	
DNS klient	ano	
NTP klient s MD5 autentizací	ano	
IPFIX RFC 3917, RFC 3955	ano	
Detailní flexibilní definice "flow" dle L2/L3/L4 parametrů	ano	
Export statistik "flow" selektivně na více kolektorů	ano	
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano	
TACACS+ klient	ano	
Port mirroring	ano	
Vzdálený port mirroring	ano	
Syslog	ano	
Nástroje pro měření odezev v síti (například IP SLA nebo ekvivalentní)	ano	
Nástroje pro pasivní monitorování i aktivní testování odezev provozovaných aplikací (např. IP SLA Video Operation, performance monitor nebo ekvivalentní)	ano	
Možnost v software přepínače integrovat další aplikace (například WireShark, profilování koncových zařízení,...)	ano	
Automatická konfigurace portu dle připojeného zařízení	ano	
Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)	ano	
<b>Služby</b>		
Podpora NTP	ano	
DHCP server	ano	

**Tabulka mandatorních požadavků pro nemodulární přístupový stohovatelný gigabitový přepínač s možností napájení po Ethernetu (požadovány 3 ks)**

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
<b>Základní vlastnosti</b>		
Třída zařízení	L2 přepínač	
Formát zařízení	fixní konfigurace, rozšiřitelný na stohování, 1RU	
Stohovatelný	ano, volitelným modulem	
Stohování požadováno	ne	
Počet portů 10/100/1000	48	
Podpora PoE (IEEE 802.3af)	ano	
Podpora PoE+ (IEEE 802.3at, 30W/port)	ano	
Dostupný výkon pro napájení PoE portů	350W	
Počet uplink portů 1GE a jejich typ	4x SFP	
Možnost připojit externí redundantní zdroj	ano	
<b>Výkonnostní parametry</b>		
Propustnost přepínacího subsystému	170 Gbit/s	
Paketový výkon přepínače	75 milionů paketů/vteřinu	
Rychlost stohovacího propojení	80 Gbit/s	
<b>Vlastnosti stohování</b>		
Vzájemné stohování všech modelů stejné řady s 1GE/10GE uplinky	ano	
Stohování kompatibilní se stávajícími stohovatelnými přepínači	ano	
Počet přepínačů ve stohu	8	
Automatická kontrola a sjednocení verze software přepínačů ve stohu	ano	
Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením	ano	
Seskupování portů (IEEE 802.3ad) mezi různými prvky stohu	ano	
Kterýkoli prvek ve stohu může být řídicím prvkem stohu (1:N redundance)	ano	
<b>Protokoly fyzické vrstvy</b>		
IEEE 802.3-2005	ano	
IEEE 802.3ad	ano	
Podpora "jumbo rámců"	ano	
<b>Protokoly spojové vrstvy</b>		
IEEE 802.1D	ano	
IEEE 802.1Q	ano	
Počet aktivních VLAN	1000	
IEEE 802.1X - Port Based Network Access Control	ano	

IEEE 802.1s - multiple spanning trees	ano	
IEEE 802.1w - Rapid Tree Spanning Protocol	ano	
IEEE 802.1p - počet vnitřních front	4	
Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní	ano	
Detekce protilehlého zařízení	ano	
Detekce parametrů protilehlého zařízení	ano	
Protokol pro definici šířených VLAN	ano	
Detekce jednosměrnosti optické linky	ano	
STP root guard	ano	
STP loop guard	ano	
Možnost autorecovery po chybovém stavu	ano	
Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ano	
<b>Protokol IP</b>		
IP alias (více IP sítí na jednom rozhraní)	ano	
QoS	ano	
QoS i na stohovacím propoju	ano	
DHCP relay	ano	
<b>Protokol IPv6</b>		
Podpora IPv6 ACL	ano	
Podpora IPv6 services ( DNS, Telnet, SSH, Syslog, ICMP)	ano	
Podpora IPv6 MLDv2 snooping	ano	
Podpora IPv6 Port ACL	ano	
Podpora IPv6 First Hop Security RA guard	ano	
Podpora IPv6 First Hop Security DHCPv6 guard	ano	
Podpora IPv6 First Hop Security IPv6 Binding Integrity Guard	ano	
<b>Směrování multicastu</b>		
IGMPv2 snooping	ano	
IGMPv3 snooping	ano	
IPv6 MLDv1 & v2 snooping	ano	
<b>Bezpečnost</b>		
ACL na rozhraní IN/OUT (včetně virtuálních - VLAN, loopback, 802.1ad)	ano	
ACL pro IP	ano	
ACL pro ethernetové rámce	ano	
IPv6 ACL	ano	
Možnost definovat povolené MAC adresy na portu	ano	
Možnost definovat maximální počet MAC adres na portu	ano	
Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	ano	
Podpora zabezpečení a analýzy DHCP protokolu	ano	
Podpora ochrany ARP protokolu	ano	
Podpora ochrany podvrženého mapování IP/MAC	ano	

adresy		
IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu	ano	
IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači, sdílení ověření koncových stanic	ano	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ano	
Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)	ano	
<b>Podpora koncových zařízení</b>		
Podpora PoE (IEEE 802.3af)	ano	
Podpora PoE+ (IEEE 802.3at, 30W/port)	ano	
Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury	ano	
Podpora IEEE (IEEE 802.3az)	ano	
<b>Management</b>		
CLI rozhraní	ano	
SSHv2	ano	
SSHv2 over IPv6	ano	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	
SNMPv2	ano	
SNMPv3	ano	
Konzolová linka	ano	
DNS klient	ano	
NTP klient s MD5 autentizací	ano	
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano	
TACACS+ klient	ano	
Port mirroring	ano	
Vzdálený port mirroring	ano	
Syslog	ano	
Měření zakončení a délky metalického kabelu (TDR)	ano	
Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute)	ano	
Přepínač si může automaticky zazálohovat a obnovit firmware včetně konfigurace z nadřazeného směrovače	ano	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ano	
<b>Služby</b>		
DHCP server	ano	



**Tabulka mandatorních požadavků pro agregační přepínač/směrovač  
(požadován 1 ks)**

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
<b>Základní vlastnosti</b>		
Typ zařízení	L3 přepínač	
Formát zařízení	1RU, fixní konfigurací, s rozšiřujícím slotem uplink modulu	
Počet portů	16x SFP+, podporujících i SFP moduly	
Počet rozšiřujících slotů	1	
Uplink moduly vyměnitelné za chodu (hot swap)	ano	
Typ uplink modulu	8x SFP+, podporujících i SFP moduly	
Redundantní AC zdroje	ano	
Požadovaný počet a typ 10GE (SFP+) a GE (SFP) transceiverů a konvertorů	1 pár 10GBase-BX (20 km), 1 pár 1000Base-BX10 (10 km), 4x 10GBase-LR, 1x 10GBase-SR, 3x 1000Base-LH, 2x 1000Base-SX, 8x 1000Base-T, 4x 10GBase-CU (1 m), 2x konvertor rozhraní XENPAK na SFP+ transceiver	
Napájecí zdroje vyměnitelné za chodu	ano	
Proudění chladícího vzduchu zepředu dozadu (front-to-back)	ano	
Změna směru proudění chladícího vzduchu pouhou výměnou ventilátorů a zdrojů	ano	
Redundantní ventilátory (výpadek jednoho nemá vliv na funkci přepínače), vyměnitelné za chodu	ano	
Podpora Non-Stop Forwarding NSF se zachováním stavových informací	ano, ve dvojici	
Podpora upgrade software za provozu (ISSU)	ano, ve dvojici	
Statické směrování IPv4	ano	
Dynamické směrování IPv4	ano	
Podpora IPv4, IPV6 v hardware	ano	
<b>Výkonnostní parametry</b>		
Celková propustnost řídicích modulů (IPv4/IPV6)	240/120 Mp/s	
Celková potenciální propustnost přepínacího subsystému	480 Gbit/s	

Minimální počet záznamů ve směrovací tabulce - IPv4 unicast	32000	
Minimální počet záznamů ve směrovací tabulce - IPv6 unicast	24000	
Minimální počet záznamů ve směrovací tabulce - IPv4 multicast	12000	
Minimální počet záznamů ve směrovací tabulce - IPv6 multicast	6000	
Počet MAC adres	32000	
<b>Protokoly fyzické vrstvy</b>		
IEEE 802.3-2005	ano	
IEEE 802.3ad	ano	
IEEE 802.3ad přes více přepínačů	ano	
Podpora "jumbo rámců"	ano	
<b>Protokoly linkové vrstvy</b>		
IEEE 802.1D	ano	
IEEE 802.1Q	ano	
Minimální počet aktivních VLAN	4000	
Tunelování 802.1Q v 802.1Q	ano	
IEEE 802.1X - Port Based Network Access Control	ano	
IEEE 802.1s - multiple spanning trees	ano	
IEEE 802.1w - Rapid Tree Spanning Protocol	ano	
IEEE 802.1p	ano	
Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní	ano	
Detekce protilehlého zařízení (např. CDP)	ano	
Protokol pro definici šířených VLAN (např. VTP)	ano	
Detekce jednosměrnosti optické linky (např. UDLD)	ano	
STP root guard nebo ekvivalentní	ano	
STP loop guard nebo ekvivalentní	ano	
Možnost automatického zotavení po chybovém stavu (UDLD, root guard, loop guard)	ano	
Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ano	
<b>Protokol IP</b>		
IP alias (více IP sítí na jednom rozhraní)	ano	
QoS dle DiffServ	ano	
DHCP relay	ano	
Router redundancy protokol (např. VRRP, HSRP)	ano	
<b>Protokol IPv6</b>		
Certifikace IPv6 ready logo – Phase II	ano	
Podpora HSRP nebo VRRP pro IPv6	ano	
Podpora IPv6 ACL	ano	
Podpora IPv6 QoS dle DiffServ	ano	
Podpora IPv6 services ( DNS, Telnet, SSH, Syslog, ICMP, DHCP)	ano	
Podpora IPv6 Multicast (MLDv1 & v2)	ano	

Podpora IPv6 Multicast (PIM SSM)	ano	
Podpora IPv6 Multicast (PIM SM)	ano	
Podpora OSPFv3	ano	
Podpora MP BGP	ano	
Podpora IS-IS pro IPv4 a IPv6	ano	
Podpora IPv6 MLDv2 snooping	ano	
Podpora IPv6 First Hop Security (IPv6 Port ACL, RA guard)	ano	
Podpora IPv6 SLA	ano	
Podpora IPv6 Tunneling: ISATAP Tunnel	ano	
Podpora DHCPv6 Relay	ano	
<b>Směrovací protokoly</b>		
BGPv4	ano	
OSPF	ano	
OSPF s MD5 a NSSA	ano	
RIPv2	ano	
Policy-based routing podle ACL	ano	
Statické směrování	ano	
<b>Směrování multicastu</b>		
PIM (dense i sparse mód)	ano	
Source-Specific Multicast (SSM)	ano	
IGMPv2	ano	
IGMPv3	ano	
IGMPv3 snooping	ano	
IPv6 MLDv1 & v2 snooping	ano	
<b>Bezpečnost</b>		
Podpora reverse path check (uRPF)	ano	
ACL pro IP	ano	
IPv6 ACL	ano	
Možnost definovat povolené MAC adresy na portu	ano	
Možnost definovat maximální počet MAC adres na portu	ano	
Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	ano	
Podpora zabezpečení a analýzy DHCP protokolu (např. DHCP snooping)	ano	
Podpora ochrany ARP protokolu (např. Dynamic ARP inspection)	ano	
Podpora ochrany podvrženého mapování IP/MAC adresy (např. IP source guard)	ano	
Podpora šifrování na L2 dle IEEE 802.1AE	ano	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ano	
Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)	ano	
Vynucení IEEE 802.1x ověřování i na externím	ano	

připojeném přepínači		
HW ochrana centrálního procesoru (control plane) před útoky typu DoS	ano	
<b>Virtualizace</b>		
Virtualizace směrovače (například Multi-VRF)	ano	
Zjednodušená, zautomatizovaná konfigurace virtualizace směrovačů a jejich propojů	ano	
Virtualizace dvou fyzických přepínačů do jednoho virtuálního, jedné síťové entity z pohledu L2 i L3	ano	
<b>Podpora koncových zařízení</b>		
Měření a ovládání spotřeby energie do LAN připojených koncových zařízení	ano	
<b>Management</b>		
CLI rozhraní (příkazová řádka)	ano	
Konfigurace zařízení v člověku čitelné textové formě	ano	
Možnost povýšení operačního software zařízení po síti pomocí protokolů TFTP, FTP a HTTP	ano	
Možnost nahrání/zálohování textové konfigurace zařízení po síti pomocí protokolů TFTP, FTP a HTTP	ano	
Podpora vzdáleného přístupu pomocí SSHv2	ano	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	
SNMPv2	ano	
SNMPv3	ano	
Interpretace uživatelských CLI a Tcl skriptů a jejich aktivace asynchronní událostí v systému zařízení	ano	
USB port pro datové úložiště a zavádění operačního systému	ano	
Sériová konzolová linka	ano	
10/100/1000 out-of-band management port	ano	
DNS klient	ano	
NTP klient s MD5 autentizací	ano	
NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955)	ano	
Detailní flexibilní definice "flow" dle L2/L3/L4 parametrů	ano	
Export statistik "flow" selektivně na více kolektorů	ano	
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano	
TACACS+ klient	ano	
Zrcadlení portů, alespoň 4 paralelní obousměrné relace	ano	
Vzdálené zrcadlení portů, alespoň 4 paralelní obousměrné relace	ano	
Syslog	ano	
Možnost rozšiřování o další funkce licenčními klíči bez nutnosti výměny firmware	ano	
Nástroje pro měření odezev v síti (například IP SLA nebo ekvivalentní)	ano	
Nástroje pro pasivní monitorování i aktivní testování odezev provozovaných aplikací (např. IP SLA Video	ano	

Operation, performance monitor nebo ekvivalentní)		
Možnost v software přepínače integrovat další aplikace (například WireShark, profilování koncových zařízení, ...)	ano	
Automatická konfigurace portu dle připojeného zařízení	ano	
Proaktivní autodiagnostika HW zařízení při startu i běhu zařízení, konfigurovatelná.	ano	
<b>Služby</b>		
Podpora NTP	ano	
DHCP server	ano	

**Tabulka mandatorních požadavků pro bezdrátový přístupový bod  
(požadováno 70 ks)**

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
<b>Základní vlastnosti</b>		
Typ zařízení	bezdrátový přístupový bod	
Rádiové rozhraní pro pásmo 2,4 GHz	ano	
Rádiové rozhraní pro pásmo 5 GHz	ano	
Počet portů 10/100/1000	1	
Možnost IEEE 802.3af napájení z přepínače nebo injektoru	ano	
Typ antén	integrované pro obě pásma	
Montáž	na betonový strop	
Podpora stávajících centralizovaných radičů bezdrátové sítě	ano	
Podpora centralizovaného radiče poptávaného v této ZD	ano	
<b>Výkonnostní parametry</b>		
Fyzická přenosová rychlost bezdrátové části	450 Mb/s	
<b>Protokoly fyzické vrstvy</b>		
IEEE 802.11a/b/g/n	ano	
Podpora MIMO (Multiple Input Multiple Output)	3x4:3	
IEEE 802.11n Maximal ratio combining (MRC)	ano	
Podpora agregace rámců A-MPDU a A-MSDU	ano	
Dynamický výběr volné frekvence DFS	ano	
Podpora 20 MHz a 40 MHz kanálů	ano	
Optimalizace fáze vysílaného bezdrátového signálu směrem k 802.11a/g/n klientům (Beam Forming)	ano	
Podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma	ano	
Hardwarová podpora spektrální analýzy (detekce zdroje rušivého signálu – interferencí)	ano	
Hardwarová podpora rozpoznání zdroje rušivého signálu podle signatur	ano	
Podpora výpočtu závažnosti dopadu interference na kvalitu radiového signálu bezdrátové sítě	ano	
Minimální počet inzerovaných SSID (BSSID)	8/rádiové rozhraní	
Nastavitelný DTIM interval pro jednotlivé bezdrátové sítě	ano	
<b>Bezpečnost</b>		
Certifikát s lokální platností pro nasazení PKI	ano	
Fyzické zabezpečení/zamknutí k okolním pevným částem	ano	
<b>Management</b>		
CLI rozhraní	ano	
SSHv2	ano	
Konzolová linka	ano	

Detekce a monitorování problémů bezdrátové sítě odchytáváním provozu a jeho zasíláním do analyzátoru (například Wireshark)	ano	
--	-----	--

**Tabulka mandatorních požadavků pro záložní zdroj napájení UPS  
(požadovány 3 ks)**

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
<b>Základní vlastnosti</b>		
Typ zařízení	záložní zdroj napájení UPS	
Použitá technologie Line-Interactive	ano	
Výstupní napětí 230V	ano	
Minimální počet IEC 320 C13 portů	8	
Minimální počet IEC 320 C19 portů	1	
Maximální výška 2U	ano	
Přídavný externí teplotní senzor	ano	
<b>Výkonnostní parametry</b>		
Minimální výstupní kapacita	3000 VA	
Minimální délka zálohování při plné zátěži	3 min	
<b>Management</b>		
Podpora protokolu HTTP/HTTPs	ano	
Podpora protokolu IPv4/IPv6	ano	
Podpora protokolu SSHv2	ano	
Podpora protokolu SNMPv1/SNMPv2c/SNMPv3	ano	



**Tabulka mandatorních požadavků pro stojanový rozvaděč (požadován 1 ks)**

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
<b>Základní vlastnosti</b>		
Rozměr 800 x 800 (h x š), 42U	ano	
Perforace dveří	85%	
Čtyřbodové zamykání dveří	ano	
Vertikálně dělené zadní dveře rozváděče	ano	
Zatížitelnost rozváděče	1500 kg	
Stropní kabelové průchodky v rozváděči podélné po celé délce rozváděče s možností prostupu po obou stranách	ano	
Jednoduchá manipulace s 19" rovinou	ano	
Popis rastru pro snadnou orientaci na 19" rovině	ano	
Jednoduchá montáž příslušenství - bez nutnosti nářadí	ano	

## **Požadavky na záruku a servis dodávky:**

Všechny dodané síťové prvky (Zařízení) musí být z důvodů ochrany stávajících investic a minimalizace celkových nákladů na vlastnictví a provoz počítačové sítě ZČU kompatibilní se všemi již používanými komunikačními protokoly a systémy správy sítě.

Požadovaná záruční doba na dodaná Zařízení činí 60 měsíců.

Další požadované související plnění:

- dodávka Zboží do místa plnění
- technická dokumentace (v elektronické podobě, čeština, angličtina);
- Uchazeč poskytne Zadavateli po dobu trvání záruky všechny relevantní verze operačního software nabízené výrobcem tak, aby dodané řešení fungovalo bez závad. Dodavatel se současně zavazuje informovat Zadavatele o nových softwarových verzích a funkcích, které mohou rozšiřovat dodané řešení. Dodavatel se zavazuje získat potřebné softwarové produkty legálním způsobem za podmínek stanovených výrobcem zařízení.
- Uchazeč zajistí Zadavateli přístup k dokumentaci výrobce zařízení a znalostní bázi, pokud ji výrobce v rámci své podpory koncovým uživatelům poskytuje.
- veškeré zákonem vyžadované dokumenty potřebné pro provoz nabízených zařízení na území České republiky (prohlášení o shodě apod.);
- Uchazeč je povinen zajistit dostupnost nových originálních náhradních dílů od výrobce pro dodané řešení za podmínek specifikovaných Zadavatelem v režimu 8h x 5d x NBD (počet hodin dostupnosti servisu uchazeče x počet dní v týdnu dostupnosti servisu dodavatele x doba pro doručení náhradního dílu Zadavateli do místa plnění).
- Výše specifikovanou záruční lhůtu, servis a dostupnost náhradních dílů Zadavatel požaduje po dobu 60 měsíců.

## **Struktura technické části nabídky**

Technická část nabídky musí obsahovat:

- Podrobný popis technických a funkčních parametrů nabízeného řešení, z něhož bude jasně patrné splnění jednotlivých položek technických a funkčních požadavků technického zadání.
- Podrobný popis servisních a záručních podmínek, z něhož bude jasně patrné splnění jednotlivých položek servisních a záručních požadavků zadání.
- Podrobnou položkovou specifikaci nabízených zařízení (např. typů šasi, jednotlivých modulů, operačního software, napájecích zdrojů apod.).

## **Popis prostředí počítačové sítě ZČU**

### **Používané komunikační protokoly a podpůrné vlastnosti aktivních prvků sítě ZČU**

V akademické síti ZČU WEBnet jsou v současné době používány následující komunikační protokoly a další podpůrné vlastnosti aktivních prvků, s nimiž musí být poptávaná zařízení kompatibilní:

- Podpora IEEE 802.1Q/p (minimálně 1000 VLAN, konfigurační možnosti statického omezování šíření VLAN), IEEE 802.1s/w (RSTP/MSTP), IEEE 802.3ad, IGMPv2/v3, MLDv1/v2 a vlastnické L2 protokoly VTPv3, PVRSTP+, CDPv2, UDLD.
- Možnosti ochrany spanning tree protokolu vůči zneužití (filtrace BPDU rámců na jednotlivých rozhraních, kontrola přípustnosti BPDU apod.).

- Podpora agregace linek (LACP nebo PAgP).
- Podpora privátních VLAN (logická izolace jednotlivých rozhraní nebo skupin rozhraní v rámci téže VLAN).
- Podpora omezení (procentuálního poměru) broadcastového a multicastového provozu na rozhraní.
- Duální podpora IPv4 a IPv6 unicast i multicast (možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, dual-stack).
- Podpora směrovacích protokolů BGPv4, OSPFv2, OSPFv3, PIM-SMv2, RIP, statického směrování a možnosti redistribuce směrovacích informací mezi jednotlivými protokoly, rozkládání zatížení na L3 paralelních cestách, možnosti vytváření logicky oddělených instancí virtuálních směrovacích tabulek v rámci téhož L3 přepínače (podpora virtuálních směrovacích instancí).
- Podpora HSRP nebo VRRP pro zajištění redundance výchozí brány koncovým stanicím/serverům.
- Podpora GRE tunelů.
- Podpora IGMPv2, IGMPv3 a hardwarová podpora omezování zbytečného šíření multicastových rámců/paketů na rozhraní bez explicitních příjemců (IGMPv2/v3 a MLDv1/v2 snooping).
- Možnost definovat povolené MAC adresy na portu, jejich maximální počet na portu a definování různého chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy).
- Hardwarová podpora bezstavové bezpečnostní filtrace provozu podle L2/L3/L4 atributů na úrovni linkové/síťové/transportní vrstvy aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní (VLAN).
- Vzdálený management aktivních prvků (typicky pomocí protokolů Telnet, SSH, HTTP/HTTPS nebo SNMPv2/v3).
- Implementace čítačů přenesených bytů/paketů pro jednotlivé relevantní entity síťových informací (typicky rozhraní, filtry apod.) přístupné přes příkazovou řádku a SNMP.
- Možnost nastavení omezení distribuce IP multicastu ve VLAN.
- Možnost ochrany proti útokům na úrovni síťové a linkové vrstvy (IP DHCP Snooping, Dynamic ARP Inspection, IP Source Guard).
- Hardwarová podpora zajištění kvality služby (QoS) podle L2/L3/L4 atributů umožňující implementaci QoS podle modelu rozlišovaných služeb (DiffServ).

### **Nástroje používané pro správu sítě ZČU**

Pro správu sítě ZČU jsou používány následující nástroje síťového managementu, s nimiž musí být poptávaná zařízení kompatibilní.

#### ***Správa konfigurací***

Zálohování konfigurací všech aktivních komunikačních prvků je prováděno centrálně automaticky pomocí systému RANCID<sup>1</sup> s webovou nadstavbou Subversion (pro přehledné zobrazování změn). Archivace (změn) historie konfigurací je udržována minimálně po dobu jednoho roku. Navíc jsou paralelně zálohovány konfigurace (a jejich přehled sumárních změn) všech aktivních komunikačních prvků pomocí systému NeDi<sup>2</sup>.

Pro hromadné konfigurace skupin zařízení se využívají systémy Netmanager<sup>3</sup>, umožňující paralelní vykonávání příkazů, a NeDi.

<sup>1</sup> <http://www.shrubbery.net/rancid/>

<sup>2</sup> <http://nedi.ch/>

<sup>3</sup> Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

## ***Správa bezdrátové sítě***

Na ZČU je provozována bezdrátová síť eduroam<sup>4</sup>, která podporuje IP mobilitu a roaming uživatelů v rámci české sítě národního výzkumu a vzdělávání. Kromě toho je provozována síť zcu-mobile, která mobilitu a roaming nepodporuje. Pro její provoz byl vyvinut vlastní systém založený na open-source řešení. Obě řešení jsou navázána na AAA infrastrukturu založenou na ověřovacím serveru freeRADIUS<sup>5</sup>. Pro správu a konfiguraci bezdrátových přístupových bodů je využíváno centralizované řešení. Jako centrální prvky jsou použity dva bezdrátové řadiče<sup>6</sup> pracující v režimu active/active, které jsou schopny současně spravovat až 200 AP. K udržení konzistentní konfigurace obou bezdrátových řadičů je používán specializovaný software<sup>7</sup>.

## ***Inventarizace síťových zařízení***

Pro inventarizaci veškerých síťových zařízení (typicky aktivních komunikačních prvků a koncových zařízení jako jsou uživatelská PC, notebooky, servery a síťové tiskárny) se využívají dva druhy nástrojů:

- registrační systém Sauron<sup>8</sup> v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet<sup>9</sup> v prostředí kolejní sítě (včetně funkce řízení přístupu oprávněných uživatelů do sítě na základě konfigurace kolejních DHCP/DNS serverů a pravidel na centrálním kolejním firewallu)
- on-line systémy Netdisco<sup>10</sup> a NeDi, které na základě periodicky získávaných informací z aktivních komunikačních prvků pomocí protokolů SNMP a CDP poskytují informace o zařízeních připojených do sítě (např. počty, typy a verze OS aktivních prvků, informace o topologii sítě, VLAN, IP podsítích, bezdrátových SSID, mapování MAC adres na IP adresy, připojení MAC/IP adres za konkrétními fyzickými porty jednotlivých přepínačů, informace o SMB atd.<sup>11</sup>) s možností pokročilého vyhledávání (např. nalezení fyzického připojení zařízení s danou IP/MAC adresou, nalezení duplicitních MAC/IP adres apod.), včetně uchovávání stavové historie.

## ***Monitorování provozu***

### **Provozní trendy**

Pro sledování non-stop dostupnosti na úrovni služeb se používá systém Nagios<sup>12</sup>, který je současně také využíván pro monitorování dostupnosti všech aktivních komunikačních prvků a služebních/management serverů, včetně konfigurace automatického upozornění/eskalace e-mailem při detekci problémové/chybové situace.

Pro sledování non-stop dostupnosti na úrovni služeb pro systém VoIP ZČU se používá systém Nagios<sup>13</sup>, který je využíván pro monitorování dostupnosti všech aktivních komunikačních

---

<sup>4</sup> <http://www.eduroam.cz>

<sup>5</sup> <http://freeradius.org>

<sup>6</sup> Bezdrátový řadič Cisco Wireless LAN Controller (WLC) 5508 pro 100 AP a Cisco WLC 4404 pro 100 AP.

<sup>7</sup> Cisco Prime Infrastructure verze 1.3 pro 200 AP.

<sup>8</sup> <http://sauron.jyu.fi/>

<sup>9</sup> Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

<sup>10</sup> <http://www.netdisco.org/>

<sup>11</sup> Z bezpečnostních důvodů se však záměrně nevyužívají integrované služby manipulace se stavy portů přepínačů vyžadující SNMP přístup pro zápis.

<sup>12</sup> <http://www.nagios.org/>

<sup>13</sup> <http://www.nagios.org/>

prvků a služebních/management serverů systému VoIP ZČU, včetně konfigurace automatického upozorňování/eskalace e-mailem při detekci problémové/chybové situace.

Pro sledování non-stop dostupnosti všech aktivních komunikačních prvků včetně IP telefonů se používá systém Mikrotik The Dude<sup>14</sup>.

Pro non-stop historii sledování základních L2 provozních charakteristik aktivních komunikačních prvků všech prostředí pomocí SNMP<sup>15</sup> (typicky zatížení CPU, obsazení operační paměti, stav napájecích zdrojů, teplota, počet BGP prefixů a stavové informace jednotlivých portů/rozhraní jako počet přenesených bytů/rámců/paketů, chybovost portů/rozhraní atd.) se používá optimální konfigurace dvojice nástrojů Cricket<sup>16</sup> a Torrus<sup>17</sup> pracujících nad RRD databázemi.

Pro sledování provozu na úrovni L3/L4 datových toků se využívá technologie NetFlow v9. NetFlow informace exportované ze směrovačů, linuxových firewallů (kolejní extranet) a specializované FlowMon<sup>18</sup> sondy (kolejní intranet) se zpracovávají jednak nevzorkované pomocí produkčního IPv4 software Caligare Flow Inspector/CFI<sup>19</sup> a jednak vzorkované 1:10 pomocí testovacího IPv4/IPv6 software FTAS<sup>20</sup>.

Pro monitorování historie latence/jitteru/ztrátovosti paketů (typicky VoIP subsystému) se používá aktivní nástroj Smokeping<sup>21</sup>.

Pro monitorování problémových provozních stavů se používá standardní mechanismus zpracování nevyžádaných deníkových zpráv generovaných aktivními prvky na bázi protokolu Syslog a SNMP trap, přičemž se navíc využívá i nadstavba Zenoss Core<sup>22</sup> pro inteligentní korelaci trapů.

### Bezpečnostní monitorování

Pro monitorování síťové bezpečnosti se jednak využívají standardní nástroje Syslog a SNMP trapy, které mohou být ještě dále inteligentně předzpracovány/filtrovány, korelovány a reportovány SIEM systémem zpracování Syslog hlášení z aktivních prvků OSSEC<sup>23</sup> a pro SNMP trapy systémem Zenoss Core.

Přehled o anomáliích na úrovni automatické detekce podezřelých IPv4 datových toků podle analýzy NetFlow dat poskytuje software Caligare Flow Inspector/CFI.

Automatický přehled o (změnách) mapování aktivních MAC adres na IP adresy pro všechna zařízení připojená do vybraných/důležitých podsítí zajišťuje software ARPwatch<sup>24</sup>.

Vynucování bezpečnostní síťové přístupové politiky umožňující centralizované systémové zablokování přístupu problémových uživatelů do sítě či síťových služeb (blacklist) zejména na úrovni L2 VACL nebo L3 ACL případně ještě s kombinací vypnutí daného portu na přístupovém prvku (typicky nejbližší místu svého vzniku podle typu komunikačního prvku) je řízeno pomocí nástroje NetSpy<sup>25</sup>. Tento vlastní nástroj také poskytuje další potřebné podpůrné

---

<sup>14</sup> <http://www.mikrotik.com/thedude.php>

<sup>15</sup> Konfigurace aktivních prvků pouze v režimu pro čtení s povolenými IP adresami management stanic dle

ACL.

<sup>16</sup> <http://cricket.sourceforge.net/>

<sup>17</sup> <http://torrus.org/>

<sup>18</sup> <http://www.invea.cz/produkty-sluzby/flowmon/flowmon-sondy>

<sup>19</sup> <http://www.caligare.com/>

<sup>20</sup> <http://www.cesnet.cz/doc/techzpravy/2004/ftas-arch/>,

<http://www.cesnet.cz/doc/techzpravy/2006/ftas-interface/>,

<http://www.cesnet.cz/akce/2009/zazemi-pro-cert-csirt/p/sledovani-provozu.pdf>

<sup>21</sup> <http://oss.oetiker.ch/smokeping/>

<sup>22</sup> <http://www.zenoss.com/solution/network-monitoring>

<sup>23</sup> <http://www.ossec.net/>

<sup>24</sup> <http://www.securityfocus.com/tools/142>

<sup>25</sup> Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

administrátorské funkce jako např. automatickou detekci neregistrovaných zařízení, vyhledání různých konfliktních síťových stavů, management VLAN/IP podsítí atd.

Vzdálený administrátorský přístup ke všem aktivním síťovým prvkům je zajištěn pouze<sup>26</sup> pomocí SSH protokolu s autentizací/autorizací protokolem TACACS+ z předdefinovaných povolených bezpečných podsítí/IP adres. Management rozhraní L2 přepínačů je umístěno ve vyhrazené IP podsíti chráněné firewallem. Pro L3 přepínače/směrovače je konfigurována ochrana Control Plane Policing/CoPP, pokud tuto vlastnost podporují. AAA auditní informace o administrátorských přístupech ke konfigurovaným zařízením je k dispozici na TACACS+ serverech CIV ZČU.

---

<sup>26</sup> S výjimkou menšího počtu zastaralých přepínačů, které SSH nepodporují a jsou postupně podle finančních možností nahrazovány.