

## Požadované technické parametry dodávky

Předmětem dodávky je 8 ks bezdrátových přístupových bodů dle technických podmínek níže.

### Tabulka povinných požadavků pro bezdrátový přístupový bod (8 ks)

Požadavek na funkcionalitu	Minimální požadavky
<b>Základní vlastnosti</b>	
Typ zařízení	bezdrátový přístupový bod
Montáž	na strop
Rádiové rozhraní pro pásmo 2,4 GHz	ano
Rádiové rozhraní pro pásmo 5 GHz	ano
Dvě rádia pracující v režimu 2,4 a 5 GHz pro standardní prostředí nebo duální 5 GHz pro HD nasazení, možnost statické i dynamické volby režimu	ano
Samostatné rádio pro monitorování 2,4 a 5 GHz RF spektra – detailní spektrální analýza, detekce útoků na bezdrátovou síť, lokalizace klientů	ano
Rozhraní 100/1000/2500 Mb/s kompatibilní s 802.3bz	ano
Podpora IEEE 802.3af/at napájení z přepínače nebo injektoru	ano
Typ antén	integrované pro obě pásma
Podpora stávajících centralizovaných řadičů bezdrátové sítě	ano
Podpora systému centralizované správy bezdrátových řadičů	ano
Fyzická přenosová rychlost celé bezdrátové části	5 Gb/s
<b>Protokoly fyzické vrstvy</b>	
IEEE 802.11a/b/g/n/ac a Wi-Fi6 (IEEE 802.3ax)	ano
MIMO (Multiple Input Multiple Output)	4x4:4
MU-MIMO	ano
IEEE 802.11n Maximal ratio combining (MRC)	ano
Agregace rámců A-MPDU a A-MSDU	ano
Dynamický výběr volné frekvence DFS	ano
Podpora 20 MHz a 40 MHz kanálů pro IEEE 802.11n	ano
Podpora 80 MHz a 160 MHz kanálů pro IEEE 802.11ac a 802.11ax	ano
Podpora BSS Coloring	ano
Optimalizace fáze vysílaného bezdrátového signálu směrem k 802.11a/g/n/ac 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 otisku	ano
Výpočet závažnosti dopadu interference na kvalitu rádiového signálu	ano
Minimální počet inzerovaných SSID (BSSID)	8/rádiové rozhraní
Rádio podporující BLE 5.0, ZigBee a Target Wake Time (TWT)	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 odchyťáváním provozu a jeho zasíláním do analyzátoru (například Wireshark)	ano

## Další technické požadavky

- Všechny poptávané aktivní síťové prvky musí být z důvodů ochrany stávajících investic a minimalizace celkových nákladů na vlastnictví a provoz počítačové sítě zadavatele kompatibilní se všemi již používanými zařízeními, komunikačními protokoly a systémy správy sítě specifikovanými níže.

## Struktura technické části nabídky

Technická část nabídky musí obsahovat:

- **Podrobný popis technických a funkčních parametrů** nabízeného řešení, z něhož bude jasné patrné splnění jednotlivých položek technických a funkčních požadavků technického zadání.
- **Podrobný popis servisních a záručních podmínek**, z něhož bude jasné 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 Cisco je prováděno centrálně automaticky pomocí systému RANCID<sup>1</sup> s webovou nadstavbou Subversion (pro přehledné zobrazování změn) periodicky alespoň jednou denně. Archivace (změn) historie konfigurací je udržována minimálně po dobu jednoho roku. Navíc jsou paralelně zálohovány konfigurace (a jejich přehledných sumárních změny) všech aktivních komunikačních prvků Cisco pomocí systému NeDi<sup>2</sup> periodicky alespoň jednou denně. Archivace (změn) historie konfigurací je opět v systému NeDi udržována minimálně po dobu jednoho roku.

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

#### ***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 čtyři bezdrátové radiče<sup>6</sup> pracující v režimu active/standby, které jsou schopny současně spravovat až 1100 AP. K udržení konzistentní konfigurace obou bezdrátových radičů 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

<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.

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

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

<sup>6</sup>Dva bezdrátové radiče Cisco Wireless LAN Controller (WLC) 5520 pro 600 AP a dva bezdrátové radiče Cisco Wireless LAN Controller (WLC) 5508 pro 400 AP.

<sup>7</sup>Cisco Prime Infrastructure verze 3.5 pro 1000 uzlů provozovaný ve virtualizovaném prostředí.

<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/>

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 upozorňování/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 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.

---

<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/>

<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/>

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

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

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