Požadované technické parametry dodávky

Předmětem dodávky jsou aktivní síťové prvky dle technických podmínek uvedených níže.

- 2 ks centrálních řadičů bezdrátové sítě.
- 110 ks bezdrátových přístupových bodů typu A.
- 340 ks bezdrátových přístupových bodů typu B.

Tabulka povinných požadavků pro centrální řadič bezdrátové sítě (požadovány 2 ks)

Požadavek na funkcionalitu	**Minimální požadavky**
Základní vlastnosti	
Třída zařízení	centrální řadič bezdrátové sítě
Formát zařízení	samostatné zařízení
Počet a typ portů s rychlostí 10Gb/s	4, SFP+
Požadovaný počet a typ transceiverů	4 ks, 10GBase AOC, 3 m
Redundantní napájecí zdroj	ano
Podpora stávající báze instalovaných AP	ano
Podpora AP požadovaných v této ZD	ano
Výkonnostní parametry	
Počet současně připojitelných klientů	30000
Propustnost datového systému	40 Gb/s
Počet současně obsluhovaných AP	2000
Počet bezdrátových sítí WLAN	4000
Počet sítí VLAN	4000
Vysoká dostupnost řadiče	
Možnost redundance na úrovni řadičů a jejich portů	ano
Redundantní provoz v režimu active/standby	ano
Upgrade operačního systému bezvýpadkově za provozu	ano
Schopnost samostatného provozu (dočasné zrušení redundantního provozu)	ano
Vlastnosti správy bezdrátové sítě	
Integrovaný radio-resource management, spolupráce RRM mezi řadiči v clusteru	ano
Mobility management, L2/L3	ano
Automatizované řešení roamingu uživatelů v rámci AP na jednom řadiči i mezi 2 a více řadiči, L2/L3	ano
Optimalizace multicast provozu v bezdrátové síti (IGMP snooping)	ano
Podpora auto-provisioningu AP	ano
Automatizovaná správa frekvenčního pásma AP	ano
Integrované řešení návštěvnického přístupu	ano
Bezpečné oddělení návštěvnického provozu od zaměstnaneckého provozu	ano
Integrovaná správa návštěvnických účtů s možností definice jejich platnosti	ano
Webová autentizace návštěvníků	ano
Podpora možnosti tunelování uživatelských dat z AP až na řadič, možnost šifrování těchto uživatelských dat	ano
Podpora možnosti lokálního bridgování uživatelských dat přímo na příslušném AP	ano
Podpora 802.11e/WMM	ano
Diferenciace úrovní QoS	ano

Mechanismy řízení přístupu (Call Admission Control) pro hlasový a video provoz	ano
Podpora Video-streamingu se spolehlivým multicastem	ano
Podpora indoor a outdoor mesh sítí, současné připojení normálních a mesh AP k jednomu řadiči	ano
Podpora designu s centrálními řadiči a vzdálenými AP na pobočkách připojených přes WAN	ano
Existence programu/mechanismu výrobce pro validaci interoperability bezdrátových klientů třetích stran s infrastrukturou. Zahrnující inovativní funkce bezpečnosti, mobility, QoS, management. Alespoň pro klienty DELL, HP, Lenovo, Fujitsu, Nokia, BlackBerry apod.	ano
Bezpečnost	
Podpora 802.11i, respektive jeho implementací WPA2 včetně enterprise variant autentizace/šifrování	ano
Podpora Wi-Fi Protected Access 3 (WPA3)	ano
802.1X/EAP autentizace: PEAP, EAP-FAST, EAP-TLS, …	ano
Šifrování AES	ano
Integrovaný IDS systém pro detekci útoků na bezdrátovou síť (wireless IDS)	ano
Detekce cizích AP (Rogue AP) a klientů v AdHoc režimu	ano
Možnost vynuceného odpojení klientů od cizích AP	ano
Ochrana řídících rámců na AP a klientovi podle standardu IEEE 802.11w	ano
Centrální administrace správců s granularitou přístupových práv	ano
Spolupráce s cizími sítěmi podle standardu IEEE 802.11u	ano
Rychlý roaming klientů mezi AP podle standardu IEEE 802.11r	ano
Vysoká dostupnost AP	
Automatické zvýšení vysílacího výkonu okolních AP při výpadku AP	ano
Automatické přizpůsobení se bezdrátové sítě na základě indexu kvality radiového signálu	ano
Rychlá detekce selhání komunikace AP-řadič (pod 4 sekundy)	ano
Monitoring a měření kvality radiového signálu	
Vyhodnocování kvality signálu bezdrátové sítě v reálném čase a grafické vyobrazení	ano
Možnost detekce rušivých signálů (interference) a identifikace zdrojů interference na základě signatur	ano
Současná funkčnost AP pro přenos dat, detekci bezpečnostních incidentů a analýzu radiového spektra	ano
Troubleshooting radiového signálu a automatické řešení problému rušivého signálu	ano
Možnost nastavovat prahové hodnoty pro úroveň kvality signálu bezdrátové sítě	ano
Automatické spouštění alarmů na základě překročení prahových hodnot kvality signálu	ano
Management	
CLI rozhraní	ano
Web rozhraní	ano
Přístup přes SSHv2	ano
Omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
SNMPv2 a SNMPv3	ano
Podpora NETCONF/YANG	
Export datových toků pomocí Netflow nebo Sflow	ano
Sériová konzolová linka	ano
RADIUS klient pro AAA (autentizace, autorizace, accounting) bezdrátových klientů	ano
TACACS+ klient pro přístup	ano
Syslog	ano

Tabulka povinných požadavků pro bezdrátový přístupový bod typu A (požadováno 110 ks)

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Typ zařízení	bezdrátový přístupový bod
Montáž	na strop
Montážní konzole součástí dodávky	ne
Rádiové rozhraní pro pásmo 2,4 GHz	ano
Rádiové rozhraní pro pásmo 5 GHz	ano
Rádiové rozhraní pro pásmo 6 GHz	ano
Samostatné rádio pro monitorování 2,4, 5 a 6 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 802.3bt/at napájení z přepínače nebo injektoru	ano
Typ antén	integrované pro všechna pásma
Podpora centralizovaných řadičů bezdrátové sítě poptávaných v této ZD	ano
Podpora systému centralizované správy bezdrátových řadičů	ano
Výkonnostní parametry	
Fyzická přenosová rychlost celé bezdrátové části	7 Gb/s
Protokoly fyzické vrstvy	
IEEE 802.11a/b/g/n/ac/ax a Wi-Fi 6E	ano
MIMO (Multiple Input Multiple Output) v pásmu 2,4/5/6 GHz	2x2:2/4x4:4/4x4:4
Podpora Multiuser Multiple-Input Multiple-Output (MU MIMO)	ano
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 kanálův pásmu 2,4 GHz	ano
Podpora 80 MHz kanálů v pásmu 5 GHz	ano
Podpora 160 MHz kanálů v pásmu 6 GHz	ano
Podpora BSS Coloring	ano
Optimalizace fáze vysílaného bezdrátového signálu směrem ke klientům	ano
Podpora mechanismu pro nucené přepojení klientů mezi pásmy	ano
Podpora současného vysílání a příjmu více klientů najednou (OFDMA)	ano
Hardwarová podpora spektrální analýzy (detekce zdroje rušivého signálu)	ano
Hardwarová podpora rozpoznání zdroje rušivého signálu podle otisku	ano
Výpočet závažnosti dopadu interference na kvalitu radiového signálu	ano
Minimální počet inzerovaných SSID (BSSID)	8/rádiové rozhraní
Rádio podporující BLE 5.1 a Target Wake Time (TWT)	ano
Bezpečnost	
Podpora WPA3	ano
Certifikát s lokální platností pro nasazení PKI	ano
Fyzické zabezpečení/zamknutí k okolním pevným částem	ano
Management	
CLI rozhraní	ano
SSHv2	ano
Konzolová linka	ano
Detekce a monitorování problémů bezdrátové sítě odchytáváním provozu	ano

Tabulka povinných požadavků pro bezdrátový přístupový bod typu B (požadováno 340 ks)

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Typ zařízení	bezdrátový přístupový bod
Montáž	na strop
Montážní konzole součástí dodávky	ne
Rádiové rozhraní pro pásmo 2,4 GHz	ano
Rádiové rozhraní pro pásmo 5 GHz	ano
Rozhraní 100/1000/2500 Mb/s kompatibilní s 802.3bz	ano
Podpora IEEE 802.3bt/at napájení z přepínače nebo injektoru	ano
Typ antén	integrované pro všechna pásma
Podpora stávajících centralizovaných řadičů bezdrátové sítě	ano
Podpora centralizovaných řadičů bezdrátové sítě poptávaných v této ZD	ano
Podpora systému centralizované správy bezdrátových řadičů	ano
Výkonnostní parametry	
Fyzická přenosová rychlost celé bezdrátové části	5 Gb/s
Protokoly fyzické vrstvy	
IEEE 802.11a/b/g/n/ac/ax	ano
MIMO (Multiple Input Multiple Output)	4x4:4
Podpora Multiuser Multiple-Input Multiple-Output (MU-MIMO)	ano
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 kanálův pásmu 2,4 GHz	ano
Podpora 80 MHz a 160 MHz kanálů v pásmu 5 GHz	ano
Optimalizace fáze vysílaného bezdrátového signálu směrem ke klientům (Beam Forming)	ano
Podpora mechanismu pro nucené přepojení klientů mezi pásmy	ano
Podpora současného vysílání a příjmu více klientů najednou (OFDMA)	ano
Minimální počet inzerovaných SSID (BSSID)	8/rádiové rozhraní
Rádio podporující BLE 5.0 a Target Wake Time (TWT)	ano
Bezpečnost	
Podpora WPA3	ano
Certifikát s lokální platností pro nasazení PKI	ano
Fyzické zabezpečení/zamknutí k okolním pevným částem	ano
Management	
CLI rozhraní	ano
SSHv2	ano
Konzolová linka	ano
Detekce a monitorování problémů bezdrátové sítě odchytáváním provozu a jeho zasíláním do analyzátoru (například Wireshark)	ano

Další technické požadavky

- Součástí nabídky musí být samostatná položka **povýšení základních funkčních vlastností centrálního řadiče bezdrátové sítě**, které bude zahrnovat plnou podporu provozu v režimu vysoké dostupnosti (HA režim active/standby včetně statefull switchover) a podporu šifrování uživatelských dat z AP až na řadič.

- 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.

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 síření 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/HTPS 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 Oxidized[1] periodicky alespoň jednou denně. Archivace (změn) historie konfigurací je udržována minimálně po dobu jednoho roku.

Pro hromadné konfigurace skupin zařízení se využívají systémy Netmanager[2], umožňující paralelní vykonávání příkazů.

Správa bezdrátové sítě

Na ZČU je provozována bezdrátová síť eduroam[3], 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[4]. Pro správu a konfiguraci bezdrátových přístupových bodů je využíváno centralizované řešení. Jako centrální prvky jsou použity čtyři bezdrátové řadiče[5] pracující v režimu active/standby, které jsou schopny současně spravovat až 1500 AP. K udržení konzistentní konfigurace obou bezdrátových řadičů je používán specializovaný software[6].

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[7] v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet[8] 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 NAV[9], který 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.[10]) 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

[1] https://github.com/ytti/oxidized
[2] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.
[3] http://www.eduroam.cz
[4] http://freeradius.org
[5] Dva bezdrátové řadiče Cisco Wireless LAN Controller (WLC) 5520 pro 1500 AP.
[6] Cisco Prime Infrastructure verze 3.10 pro 4000 uzlů provozovaný ve virtualizovaném prostředí.
[7] http://sauron.jyu.fi/
[8] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.
[9] https://nav.uninett.no/
[10] Z bezpečnostních důvodů se však záměrně nevyužívají integrované služby manipulace se stavy portů přepínačů vyžadující SNMP přístup pro zápis.

Pro sledování non-stop dostupnosti na úrovni služeb se používá systém Nagios[11], 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, 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 non-stop historii sledování základních L2 provozních charakteristik aktivních komunikačních prvků všech prostředí pomocí SNMP[12] (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 systém NAV.

Pro sledování provozu na úrovni L3/L4 datových toků se využívá technologie NetFlow v9. NetFlow informace exportované ze směrovačů, linuxových firewallů (kolejní extranet) se zpracovávají pomocí software FTAS[13].

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[14] 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[15] a pro SNMP trapy systémem Zenoss Core.

Přehled o anomáliích na úrovni automatické detekce podezřelých IPv4 datových toků podle analýzy NetFlow dat poskytuje software FTAS.

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 nejblíže místu svého vzniku podle typu komunikačního prvku) je řízeno pomocí nástroje NetSpy[16]. 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[17] 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.

---

[11] http://www.nagios.org/

[12] Konfigurace aktivních prvků pouze v režimu pro čtení s povolenými IP adresami management stanic dle ACL. [13] 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 [14] http://www.zenoss.com/solution/network-monitoring

[15] http://www.ossec.net/

[16] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

[17] S výjimkou menšího počtu zastaralých přepínačů, které SSH nepodporují a jsou postupně podle finančních možností nahrazovány.