

## Požadované technické parametry dodávky

Předmětem dodávky je 1 ks 48 portového PoE+ přepínače s 1 Gb uplink porty dle technických podmínek uvedených níže.

### Tabulka povinných požadavků pro 48 portový PoE+ přepínač s 1 Gb uplink porty (1 ks)

Požadavek na funkcionalitu	Minimální požadavky
<b>Základní vlastnosti</b>	
Třída zařízení	L2 přepínač
Formát zařízení	fixní konfigurace, rozšiřitelný na stohování, 1RU
Stohovatelný	ano, modulem
Stohování kompatibilní se všemi přepínači požadovanými v této ZD	ano
Interní redundantní ventilátory	ano
Možnost instalovat interní redundantní napájecí zdroj	ano
<b>Vlastnosti stohování</b>	
Vzájemné stohování všech modelů stejné řady s 1GE/10GE uplinky	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	4000
IEEE 802.1X - Port Based Network Access Control	ano
IEEE 802.1s - multiple spanning trees	ano
IEEE 802.1w - Rapid Tree Spanning Protocol	ano
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
Minimální počet HW QoS front	8
QoS classification – ACL, DSCP, CoS based	ano
QoS marking - DSCP, CoS	ano
QoS – Strict Priority Queue	ano
QoS Policing	ano
QoS i na stohovacím spoji	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	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
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ano
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ano
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ano
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>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
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ano
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ano
Streaming telemetrie prostřednictvím NETCONF/XML	ano
Zařízení musí být možno spravovat používaným management nástrojem v celém možném rozsahu jeho funkcí bez omezení	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>Požadavek na funkcionalitu</b>	<b>Minimální požadavky</b>
Počet RJ-45 portů 10/100/1000	48
Podpora PoE (IEEE 802.3af, 15,4 W/port)	ano
Podpora PoE+ (IEEE 802.3at, 30 W/port)	ano
Dostupný výkon pro napájení PoE portů	700 W
Počet uplink portů a jejich typ	4x 1GE SFP
Stohování požadováno	ano
Minimální délka stohovacího kabelu	50 cm
Schopnost poskytovat PoE napájení připojeným zařízením i během restartu přepínače	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.

## 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 síťení 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 totéž fyzickém nebo logickém rozhraní, dualstack).
- 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 Oxidized<sup>1</sup> periodicky alespoň jednou denně. Archivace (změn) historie konfigurací je udržována minimálně po dobu jednoho roku.

Pro hromadné konfigurace skupin zařízení se využívají systémy Netmanager<sup>2</sup>, umožňující paralelní vykonávání příkazů.

#### ***Správa bezdrátové sítě***

Na ZČU je provozována bezdrátová síť eduroam<sup>3</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>4</sup>. Pro správu a konfiguraci bezdrátových přístupových bodů je využíváno centralizované

<sup>1</sup><https://github.com/ytti/oxidized>

<sup>2</sup>Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

<sup>3</sup><http://www.eduroam.cz>

<sup>4</sup><http://freeradius.org>

řešení. Jako centrální prvky jsou použity čtyři bezdrátové řadiče<sup>5</sup> pracující v režimu active/standby, které jsou schopny současně spravovat až 1500 AP. K udržení konzistentní konfigurace obou bezdrátových řadičů je používán specializovaný software<sup>6</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>7</sup> v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet<sup>8</sup> v prostředí kolejni 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<sup>9</sup>, který na základě periodicky získávaných informací z aktivních komunikačních prvků pomocí protokolů SNMP a CDP poskytuje 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>10</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 nonstop dostupnosti na úrovni služeb se používá systém Nagios<sup>11</sup>, který je současně také využíván pro monitorování dostupnosti všech aktivních komunikačních prvků a služebních/management serverů, včetně konfigurace automatického upozorňování/eskalace emailem při detekci problémové/chybové situace.

Pro sledování nonstop 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 emailem při detekci problémové/chybové situace.

Pro nonstop historii sledování základních L2 provozních charakteristik aktivních komunikačních prvků všech prostředí pomocí SNMP<sup>12</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 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<sup>13</sup>.

---

<sup>5</sup>Dva bezdrátové řadiče Cisco Wireless Controller Catalyst 9800-40.

<sup>6</sup>Cisco Catalyst Center pro 4000 uzlů provozovaný ve virtualizovaném prostředí.

<sup>7</sup><http://sauron.jyu.fi/>

<sup>8</sup>Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

<sup>9</sup><https://nav.uninett.no/>

<sup>10</sup>Z bezpečnostních důvodů se však záměrně nevyužívají integrované služby manipulace se stavy portů přepínačů vyžadující SNMP přístup pro zápis.

<sup>11</sup><http://www.nagios.org/>

<sup>12</sup>Konfigurace aktivních prvků pouze v režimu pro čtení s povolenými IP adresami management stanic dle ACL.

<sup>13</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>

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>14</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>15</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 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 nejbližší místu svého vzniku podle typu komunikačního prvku) je řízeno pomocí nástroje NetSpy<sup>16</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>17</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>14</sup><http://www.zenoss.com/solution/network-monitoring>

<sup>15</sup><http://www.ossec.net/>

<sup>16</sup>Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

<sup>17</sup>S výjimkou menšího počtu zastaralých přepínačů, které SSH nepodporují a jsou postupně podle finančních možností nahrazovány.