

Požadované technické parametry dodávky

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

- 1 ks 48portový DC přepínač s 8 ks 10GBASE-T SFP+ transceiverů a 2 ks 100GBASE-CWDM4 QSFP28 transceiverů.

Tabulka povinných požadavků pro 48portový DC přepínač s transceivery

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Třída zařízení	L2/L3 přepínač
Formát zařízení	fixní konfigurace, 1RU
Redundantní AC zdroj	ano
Výdech teplého vzduchu na straně portů	ano
Napájecí kabely s koncovkou IEC 60320 C14	ano, délka minimálně 2 m
Redundantní vyměnitelné ventilátory s výdechem na straně portů	ano, redundance N+1
Celková propustnost přepínače	Neblokující architektura s maximální rychlostí všech použitelných rozhraní
Minimální velikost operační paměti	16 GB
Minimální počet neblokovaných portů typu 1/10/25GE s volitelným fyzickým rozhraním SFP+	48
Minimální počet aktivních neblokovaných portů typu 1/10/25GE s volitelným fyzickým rozhraním SFP+/SFP28	24
Minimální počet aktivních neblokovaných uplink portů 40/100GE s volitelným fyzickým rozhraním typu QSFP+/QSFP28	6
Podpora dual-rate 40/100GE QSFP+/QSFP28 rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4	ano
Možnost rozšířit funkcionalitu přepínače o VXLAN routing	ano
Možnost rozšířit funkcionalitu přepínače o VXLAN with MP-BGP EVPN control plane, podporu EVPN Route Type 2 (MAC/IP Advertisement Route), Route Type 3 (Inclusive Multicast Ethernet Tag Route), Route Type 4 (Ethernet Segment Route) a Route Type 5 (IP Prefix Route)	ano
Protokoly fyzické vrstvy	
IEEE 802.3-2005	ano
IEEE 802.3ad	ano
IEEE 802.3ad přes více šasi (Multichassis Link Aggregation)	ano
Podpora "jumbo rámců"	ano
Protokoly spojové vrstvy	
IEEE 802.1Q	ano
Počet aktivních VLAN	3900
Podpora instance spanning-tree protokolu per VLAN	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
Minimální počet MAC záznamů	200000
Detekce jednosměrnosti optické linky	ano
Protokol IP	

QoS classification – ACL, DSCP, CoS based	ano
QoS marking - DSCP, CoS	8
QoS - Priority Based Flow Control (IEEE 802.1Qbb)	ano
QoS - Flow aware congestion management	ano
QoS - Flow aware packet prioritization	ano
Možnost rozšířit funkcionalitu přepínače o podporu technologie IEEE 802.1AE (AES-GCM-XPB-256) na všech SFP a QSFP portech	ano
IGMP snooping	ano
Port ACL, VLAN ACL	ano
IPv6 First Hop Security (Binding guard, RA guard, DHCPv6 snooping)	ano
Bezpečnost	
Control Plane Policing	ano
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu a to prostřednictvím nemodifikovatelných interních HW prostředků	ano
Podpora funkce umožňující administrátorovi ověřit, že zařízení skutečně nabootovalo důvěryhodný operační systém	ano
Ochrana proti modifikaci HW prostředků zařízení využívající X.509 PKI pro ověření autentičnosti HW prostředků zařízení	ano
Management	
CLI rozhraní	ano
SSHv2	ano
SSHv2 over IPv6	ano
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	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
Syslog	ano
Model-driven programovatelnost prostřednictvím NETCONF/YANG a RESTConf	ano
Python scripting	ano
Ansible programming	ano

Další technické požadavky

- Nedílnou součástí dodávky jsou následující transceivery, plně kompatibilní s nabízeným DC přepínačem v aktuálních i budoucích SW verzích:
 - 8 ks 10GBASE-T SFP+**,
 - 2 ks 100GBASE-CWDM4 QSFP28.**
- 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 multicasu 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 Oxidized¹ periodicky alespoň jednou denně. Archivace (změn) historie konfigurací je udržována minimálně po dobu jednoho roku.

Pro hromadné konfigurace skupin zařízení se využívají systémy Netmanager², umožňující paralelní vykonávání příkazů.

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 Sauron³ v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet⁴ 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 NAV⁵, 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.⁶) 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 Nagios⁷, 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 SNMP⁸ (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.

¹<https://github.com/ytti/oxidized>

²Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

³<http://sauron.jyu.fi/>

⁴Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

⁵<https://nav.uninett.no/>

⁶Z bezpečnostních důvodů se však záměrně nevyužívají integrované služby manipulace se stavy portů přepínačů vyžadující SNMP přístup pro zápis.

⁷<http://www.nagios.org/>

⁸Konfigurace aktivních prvků pouze v režimu pro čtení s povolenými IP adresami management stanic dle ACL.

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 FTAS⁹.

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 OSSEC¹⁰ 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 NetSpy¹¹. 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 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.

⁹<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>

¹⁰<http://www.ossec.net/>

¹¹Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.