TECHNICKÁ ZPRÁVA

ZMĚNY			DATUM		PODPIS	
	c					
	b					
	a	Doplnění v rámci výběrového řízení - DI 04		03/2024		Michal ULIČNÝ

INVESTOR:

Západočeská univerzita v Plzni	**Západočeská univerzita v Plzni** Univerzitní 2732/8, 301 00 Plzeň tel.: +420 377 631 111, fax: +420 377 631 112 e-mail: podatelna@zcu.cz

PROJEKTANT:

TECHNICO Opava s.r.o.	TECHNICO architects & engineers TECHNICO Opava s.r.o. Hradecká 1576/51 746 01 Opava tel: 553 760 970 info@technico.cz

PROJEKTANT:

ZODP. PROJEKTANT:	Ing. Matěj KUDLÍK	
VYPRACOVAL:	Michal ULIČNÝ	
KONTROLOVAL:	Ing. Martin ULIČNÝ	

ČÍSLO PARÉ:

ČÁST DOKUMENTACE:

D.1.4.8. ELEKTRONICKÉ KOMUNIKACE

ZU - rekonstrukce objektu Klatovská 51/Chodské náměstí 1 Budova Chodské nám. 1	FORMÁT	A4
	DATUM	09/2023
	STUPEŇ	DPS
	ZAKÁZKOVÉ ČÍSLO	TO-617-DPS
K.ú. Plzeň, parc.č. 6907, 6908/1, 6909, 6910, 6911	MĚŘÍTKO:	ČÍSLO VÝKRESU:
TECHNICKÁ ZPRÁVA		D.1.4.8.a.01_a.

a) výpis použitých norem – normových hodnot a předpisů

Projekt je řešen dle předpisů a norem ČSN, z nichž nejdůležitější uvádíme:

ČSN 33 2000-1 ed.2 Elektrické instalace budov. Rozsah platnosti, účel a základní hlediska, stanovení základních charakteristik, definice.

ČSN 33 2000-4-41 ed.2 Elektrické instalace nízkého napětí Část 4-41: Ochranná opatření pro zajištění bezpečnosti – Ochrana před úrazem elektrickým proudem

ČSN 33 2000-4-43 ed.2 Elektrické instalace budov. Část 4:Bezpečnost - Kapitola 43:Ochrana proti nadproudům.

ČSN 33 2000-5-51 ed.3 Elektrická instalace budov-část-5-51: Výběr a stavba elektrických zařízení - Všeobecné předpisy.

ČSN 33 2000-5-52 ed.2 Elektrotechnické předpisy - Elektrická zařízení - Část 5: Výběr a stavba elektrických zařízení - Kapitola 52: Výběr soustav a stavba vedení

ČSN 33 2000-5-54-ed.3 Elektrické instalace nízkého napětí – Část 5-54: Výběr a stavba el. zařízení – Uzemnění, ochranné vodiče a vodiče ochranného pospojování.

ČSN 33 2000-7-701-ed.2 Elektrické instalace nízkého napětí. Část 7-701: Zařízení jednoúčelová a ve zvláštních objektech. Prostory s vanou nebo sprchou

ČSN 33 0340 Elektrotechnické předpisy. Ochranné kryty elektrických zařízení a předmětů.

ČSN 33 2130 ed.3 Elektrotechnické předpisy. Vnitřní elektrické rozvody

ČSN 33 3060 Elektrotechnické předpisy. Ochrana elektrických zařízení před přepětím

ČSN EN 50173-1 ed.3 Strukturovaná kabeláž všeobecné požadavky

ČSN EN 50173-2 Strukturovaná kabeláž kancelářské prostory

b) výchozí podklady a stavební program

- požadavky investora a architekta
- požadavky projektantů a dodavatelů technologického zařízení
- stavební půdorysy a řezy objektu

c) požadavky na profesi – zadání, klimatické podmínky místa stavby – výpočtové parametry venkovního vzduchu – zima / léto

Projekt je zpracován v rozsahu projektu stavební povolení.

Projekt obsahuje:

- EPS viz. samostatná technická zpráva
- ERO
- Strukturovaná kabeláž
- PZTS
- CCTV
- Přístupový systém

d) požadované mikroklimatické podmínky – zimní / letní, minimální hygienické dávky čerstvého vzduchu, podíl vzduchu oběhového

Neobsazeno.

e) údaje o škodlivinách se stanovením emisí a jejich koncentrace

Neobsazeno.

f) provozní podmínky – počet osob, tepelné ztráty, tepelné zátěže apod.

Pracovní, provozní a bezpečnostní předpisy

Základní podmínkou pro bezpečnost provozu el. zařízení je dodržování zařizovacích předpisů a norem. Zvláštní pozornost je zapotřebí věnovat ochraně před úrazem elektrickým proudem. Před uvedením do provozu musí být provedena výchozí revize a zpracovány místní provozní předpisy.

Pro provoz el. zařízení platí ČSN 343100 a návazné. Všechny příkazy pro obsluhu a práci musí být v souladu s těmito normami. S ohledem na bezpečnost a ochranu zdraví při práci je nutno dodržovat ustanovení vyhlášky 48/1982 Sb.

g) popis navrženého řešení a dimenzování, popis funkce a uspořádání instalace a systému

Strukturovaná kabeláž (SK)

Společná datová síť je navržena jako strukturovaná kabeláž V místnosti KL-330 bude umístěná serverovna ve které se bude nacházet 6 RACK skříní. Serverovna je napojena

stávající optikou od poskytovatele CETIN a.s. kabelem OM4 24 vl. MM zakončen konektorem. Jeden ze šestice RACKů bude sloužit pro rozvody strukturované kabeláže, zbývajících pět slouží pro potřeby pedagogické fakulty. Síť bude provedena kabely UTP a bude kategorie 6A. Podružné datové rozvaděče budou propojeny optickým kabelem OM4 12. vl. MM.

Instalaci smí provádět pouze certifikovaná firma. Po dokončení bude na strukturovanou kabeláž poskytnuta systémová záruka od výrobce přímo koncovému uživateli 25 let.

Evakuační rozhlas (ERO)

V objektu bude instalován evakuační rozhlas. Ústředna ERO je umístěna společně s ústřednou EPS v m.č. CH-002. Mikrofonní stanice bude v m.č. CH-108.

Přístupový systém

Do vybraných místností bude umožněn přístup pouze pomocí čipů/karet. Čtečky karet budou instalovány vedle dveří na straně kliky. Systém bude kompatibilní se stávajícími čipy/kartami. Čtečky budou v systému on-line. Ve vstupech do objektů budou čtečky z obou stran vstupních dveří. V případě neoprávněného použití proti panikové kliky budou opatřeny akustickou signalizací.

Přístupový systém bude propojen se systémem PZTS. Při vstupu do prostoru přes budou prvky PZTS přepnuty do provozního stavu.

Přístupový systém bude kompatibilní se stávajícími JIS kartami.

Poplachový Zabezpečovací a Tísňový systém (PZTS)

V objektu bude instalován PZTS sloužící především k ochraně majetku mimo provozní hodiny. Ústředna bude rozvodně v m.č. CH-102. Z ní povede linka k expandérům kabelem SUPERBUS 2×2×0,5+2×1 Z expandérů pak budou napojeny jednotlivé prvky kabelem SYKFY 2×2×0,5. Rozdělení prvků do skupin umožní zastřežení samostatně jednotlivých prostor. U vchodu budou umístěna ovládací klávesnice. Ústředna bude napojena v rozvaděči na samostatný jistič, bude mít vlastní zálohovaný akumulátor a bude také obsahovat GSM modul. V případě poplachu bude podávat zprávu na pult centrální ochrany.

Ústředna bude propojena s přístupovým systémem, aby bylo umožněno odblokování střežení pomoci přístupového systému.

Kamerový systém (CCTV)

V objektu bude instalovaný kamerový systém u vstupů do objektu na chodbách. Kamery budou IP s napájením přes PoE min. 2MPx s odklopitelným IR filtrem. Záznamové zařízení bude

instalováno v datovém rozvaděči v hlavní serverovně m.č. KL 330. bude umožňovat záznam v plné kvalitě 14 dní přístup z kteréhokoliv počítače, jemuž byla přidělena práva.

Kabelové trasy

Veškeré kabelové trasy budou uloženy v PVC trubkách, lištách, nebo v konstrukcích stěn. Hlavní kabelové trasy budou uloženy v ocelových žlabech instalovaných nad pohledy. Od silových kabelů budou vzdáleny min 20 cm. Pokud budou ve společném ocelovém žlabu, bude použita stíněná uzemněná přepážka. Napájení a uzemnění bude součástí dodávky silnoproudu.

h) bilance energií, médií a potřebných hmot

Elektrická síť

NN - ~ 3+NPE / 50 Hz, 400/230 V, TN-C-S, napájení datových rozvaděčů.

Základní ochrana před NDN: - v soustavě nn – samočinným odpojením od zdroje.

Zvýšená ochrana nn – proudovým chráničem, místně doplňkovým pospojováním.

Bilance spotřeby

Celková spotřeba slaboproudých systému je cca 0,4 kW. V celkovém odběru je tato spotřeba zanedbatelná.

i) ochrana životního prostředí, ochrana proti hluku a vibracím, požární opatření

Pracovní, provozní a bezpečnostní předpisy

Veškerá instalace musí být provedena v souladu s výše uvedenými normami a jejich postup musí být koordinován s ostatními profesemi a stavbou. Pro bezpečné uvedení do provozu musí být provedena výchozí revize a zpracovány místní provozní předpisy.

Revize

Výchozí revizi provede dodavatel montážních prací dle ČSN 33 1500. Další revize (periodické) provede provozovatel v předepsaných lhůtách a po každé opravě vyvolané poruchou či poškozením el. zařízení (dílčí revize).

Výchozí i pravidelné revize budou provedeny i u slaboproudu dle ČSN 33 2000-6. Periodické revize ve lhůtách dle ČSN 33 2000-6 čl. 62.2 a v souladu s ČSN 33 1500

Vypracoval: Adam SKÁCELÍK

Michal ULIČNÝ

Příloha: Technická specifikace Aktivních prvků

Požadované technické parametry dodávky

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

- 6 ks 48 portový PoE+ přepínač s 10 Gb uplink porty s podporou mGig.
- 6 ks 48 portový PoE+ přepínač s 1 Gb uplink porty.
- 3 ks 48 portový přepínač s 1 Gb uplink porty.
- 3 ks 24 portový přepínač s 1 Gb uplink porty.

Tabulka povinných požadavků pro všechny požadované přepínače

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
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
Vlastnosti stohování	
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 řídícím prvkem stohu (1:N redundance)	ano
Protokoly fyzické vrstvy	
IEEE 802.3-2005	ano
IEEE 802.3ad	ano
Podpora "jumbo rámců"	ano
Protokoly spojové vrstvy	
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
Protokol IP	
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
Protokol IPv6	
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
Směrování multicastu	
IGMPv2 snooping	ano
IGMPv3 snooping	ano
IPv6 MLDv1 & v2 snooping	ano
Bezpečnost	
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
Management	
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	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

Tabulka povinných požadavků pro 48 portový PoE+ přepínač s 10 Gb uplink porty s podporou mGig (6 ks)

Požadavek na funkcionalitu	**Minimální požadavky**
Počet RJ-45 portů 10/100/1000	36
Počet RJ-45 portů mGig 10/5/2,5 Gb/s IEEE 802.3bz a 802.3an	12
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	1000 W
Počet uplink portů a jejich typ	4x 10GE SFP+
Požadovaný počet a typ transceiverů	2 ks, 10GBase-LR SFP+
Požadovaný počet a typ optických patch kabelů	4 ks, SM LC-E2000, 3 m
Stohování požadováno	ano
Minimální délka stohovacího kabelu	100 cm
Redundantní AC (230 V) napájení (zařízení musí být schopno plné funkce při poruše jednoho napájecího zdroje)	ano
Schopnost poskytovat PoE napájení připojeným zařízením i během restartu přepínače	ano

Tabulka povinných požadavků pro 48 portový PoE+ přepínač s 1 Gb uplink porty (6 ks)

Požadavek na funkcionalitu	**Minimální požadavky**
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

Tabulka povinných požadavků pro 48 portový přepínač s 1 Gb uplink porty (3 ks)

Požadavek na funkcionalitu	Minimální požadavky
Počet RJ-45 portů 10/100/1000	48
Počet uplink portů a jejich typ	4x 1GE SFP
Stohování požadováno	ano
Minimální délka stohovacího kabelu	50 cm

Tabulka povinných požadavků pro 24 portový přepínač s 1 Gb uplink porty (3 ks)

Požadavek na funkcionalitu	Minimální požadavky
Počet RJ-45 portů 10/100/1000	24
Počet uplink portů a jejich typ	4x 1GE SFP
Stohování požadováno	ano
Minimální délka stohovacího kabelu	50 cm

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 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 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.

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[3] v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet[4] 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[5], 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.[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 Nagios[7], 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[8] (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

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

[3] http://sauron.jyu.fi/

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

[5] https://nav.uninett.no/

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

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

[8] Konfigurace 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 FTAS[9].
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[10] 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[11] 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[12]. 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[13] 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.zenoss.com/solution/network-monitoring
[11] http://www.ossec.net/
[12] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.
[13] S výjimkou menšího počtu zastaralých přepínačů, které SSH nepodporují a jsou postupně podle finančních možností nahrazovány.

Požadované technické parametry dodávky

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

- 58 ks bezdrátových přístupových bodů.

Tabulka povinných požadavků pro bezdrátový přístupový bod (58 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

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 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 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 dva bezdrátové řadiče[5] pracující v režimu active/standby, které jsou schopny současně spravovat až 1000 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

[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 Controller Catalyst 9800-40 pro 1000 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/

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

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.

---

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

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.

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