Kupní smlouva č. P20V00000382/...[DOPLNÍ DODAVATEL[1]]…

(dále jen „Smlouva“)

uzavřená podle ust. § 2079 a násl. zákona č. 89/2012 Sb., Občanský zákoník, ve znění pozdějších předpisů (dále jen „zákon“).

I. Smluvní strany

Kupující:	**Západočeská univerzita v Plzni**
sídlo:	Univerzitní 2732/8, 301 00 Plzeň
zastoupená:	doc. Dr. RNDr. Miroslavem Holečkem, rektorem
IČO:	49777513
DIČ:	CZ49777513
č. účtu:	4811530257/0100

(dále jen „Kupující“ nebo „ZČU“ nebo „Zadavatel“) na straně jedné

a

Prodávající:	Networksys a.s.
sídlo:	Plzeňská 1567/182, 150 00 Praha 5
zastoupená:	xxx
IČO:	26178109
DIČ:	CZ26178109
bankovní spojení:	ČSOB Praha5, Lidická 43
č. účtu:	836617/0300

zapsaný v obchodním rejstříku vedeném MS v Praze, oddíl B, vložka 6563
(dále jen „Prodávající“) na straně druhé; společně dále také jako „smluvní strany“.
(pozn. dodavatel doplní nezbytné údaje)

2. Základní ustanovení

2.1 Tato Smlouva je uzavřena na základě nabídky Prodávajícího předložené na veřejnou zakázku „Výpočetní technika (III.) 093-2020“ v rámci zavedeného dynamického nákupního systému „Dynamický nákupní systém na výpočetní techniku (III.)“ podle zákona č. 134/2016 Sb., o zadávání veřejných zakázkách, ve znění pozdějších předpisů.

2.2 V rámci předmětné veřejné zakázky byla jako nejvhodnější nabídka vyhodnocena nabídka Prodávajícího.

2.3 Prodávající potvrzuje, že se v plném rozsahu seznámil s rozsahem a povahou dodávky týkající se předmětu výše uvedené veřejné zakázky, že jsou mu známy veškeré technické, kvalitativní a jiné podmínky a že disponuje takovými kapacitami a odbornými znalostmi, které jsou k plnění nezbytné.

2.4 Prodávající výslovně potvrzuje, že prověřil veškeré podklady a pokyny Kupujícího, které obdržel do dne uzavření této Smlouvy i pokyny obsažené v zadávacích podmínkách, které Kupující

[1] Dodavatel **může** doplnit svoje evidenční číslo smlouvy.

stanovil pro zadání Smlouvy, že je shledal vhodnými, a že sjednaná cena a způsob plnění Smlouvy obsahuje a zohledňuje všechny výše uvedené podmínky a okolnosti.

2.5 Smluvní strany prohlašují, že údaje v článku 1. této Smlouvy a taktéž oprávnění k podnikání jsou v době uzavření Smlouvy v souladu s faktickým stavem. Smluvní strany se zavazují, že změny dotčených údajů bez prodlení oznámí druhé smluvní straně. Smluvní strany prohlašují, že osoby podepisující tuto Smlouvu jsou k tomuto jednání oprávněny.

2.6 Prodávající bere na vědomí, že Kupující je subjektem povinným zveřejňovat smlouvy dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále jen zák. 340/2015 Sb.), a pokud tato smlouva splňuje podmínky pro uveřejnění, Kupující tuto smlouvu uveřejní v registru smluv. Rozhodnou skutečností pro uveřejnění smlouvy v registru je zejména výše hodnoty za předmět plnění převyšující 50.000,- Kč bez DPH.

3. Předmět smlouvy

3.1 Prodávající se v rozsahu a za podmínek stanovených touto Smlouvou zavazuje dodat Kupujícímu výpočetní techniku (dále jen **„Zboží“).** Požadavky Kupujícího na předmět koupě jsou obsaženy v Přílohách této Smlouvy.

Předmět koupě musí být nový, plně funkční a kompletní, tj. bude připraven k okamžitému plnohodnotnému použití bez nutnosti pořizovat další komponenty a bude dodán se všemi nezbytnými součástmi, a to i v případě, že tyto komponenty nejsou výslovně popsány v Přílohách této Smlouvy.

3.2 Prodávající se zavazuje dodat Kupujícímu veškeré Zboží specifikované v Přílohách této Smlouvy a převést na něj vlastnické právo k předmětu Smlouvy. Kupující se zavazuje předmět Smlouvy převzít a uhradit sjednanou kupní cenu. Kupující je oprávněn odepřít převzetí Zboží pouze v případě uvedeném v článku 4.1 této Smlouvy. Předmět koupě musí být dodán ve sjednaném množství, jakosti, provedení, místě a čase.

4. Lhůta, místo a způsob plnění

4.1 Prodávající je povinen Kupujícímu řádně dodat Zboží do místa plnění a splnit povinnosti uvedené v článku 3. této Smlouvy do **90** kalendářních dnů od dojití výzvy k plnění Smlouvy.

O předání a převzetí Zboží bude smluvními stranami sepsán předávací protokol, jehož obsahem bude potvrzení o předání a převzetí Zboží s uvedením data, kdy se uskutečnilo. Předávací protokol bude podepsán oběma smluvními stranami.

Okamžikem podpisu předávacího protokolu smluvními stranami přechází z Prodávajícího na Kupujícího vlastnické právo ke Zboží. Nebezpečí škody na Zboží nese až do přechodu vlastnického práva na Kupujícího Prodávající. K podpisu Předávacího protokolu je pověřena osoba uvedená v článku 4.4 této Smlouvy.

Kupující je oprávněn odepřít převzetí Zboží v případě, že Zboží nevykazuje vlastnosti požadované Kupujícím v článku 3. této Smlouvy (resp. v Přílohách této Smlouvy). Kupující není povinen převzít předmět koupě vykazující jakoukoliv vadu či nedodělek. Prodávající je povinen

při předání předmětu koupě předat Kupujícímu rovněž doklady potřebné k řádnému předání a následnému užívání předmětu koupě a jejich předání je podmínkou převzetí předmětu koupě Kupujícím.

Prodávající není oprávněn dodat Zboží do místa plnění po částech, ale zásadně dodává kompletní Zboží. Ve výjimečných případech s ohledem na charakter dodávaného Zboží lze dodat Zboží po částech. O této skutečnosti musí Prodávající Kupujícího neprodleně písemně informovat a Kupující musí s touto skutečností souhlasit před dodáním Zboží.

4.2 Místem plnění jsou objekty ZČU, kdy přesná specifikace místa plnění konkrétní položky je uvedena v Příloze č. 1 této Smlouvy.

4.3 Osobou oprávněnou jednat za Prodávajícího je xxx
Změna této osoby musí být Kupujícímu neprodleně písemně oznámena, přičemž je účinná okamžikem doručení tohoto písemného oznámení Kupujícímu.

4.4 Osobami oprávněnými za Kupujícího k převzetí konkrétních položek Zboží jsou osoby uvedené v Příloze č. 1 této Smlouvy

Jakákoli jednání učiněná prostřednictvím výše uvedených e-mailových adres a telefonních kontaktů nezakládají změnu této Smlouvy a nepůjde tak o dodatky dle bodu 10.3 této Smlouvy.

4.5 Spolu se Zbožím dodá Prodávající Kupujícímu příslušné návody k použití v českém nebo anglickém jazyce, jsou-li nezbytné pro používání Zboží.

5. Kupní cena a platební podmínky

5.1 Kupní cena za zboží dle čl. 3 této Smlouvy vychází z cenové nabídky Prodávajícího.

5.2 Kupující se zavazuje uhradit prodávajícímu za dodání Zboží **sjednanou kupní cenu ve výši**:
2 507 513,- Kč bez DPH (slovy: dvamilionypětsetsedmtisícpětsettřinárct korun českých);

Prodávající je oprávněn ke kupní ceně připočíst DPH ve výši stanovené v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a to ke dni uskutečnění zdanitelného plnění, kterým je den převzetí Zboží.

5.3 Kupní cena je sjednána jako nejvýše přípustná, včetně všech poplatků a veškerých dalších nákladů spojených s dodáním Zboží a souvisejícího plnění dle Smlouvy.

5.4 Kupní cena bude Kupujícím uhrazena jako jednorázová platba v české měně na základě daňového dokladu – faktury. Kupní cena bude Prodávajícím fakturována do 30 dnů ode dne dodání a převzetí Zboží, tj. ode dne podpisu předávacího protokolu oběma smluvními stranami a splnění všech povinností dle článku 3. této Smlouvy.

Prodávající se zavazuje vystavit daňový doklad (fakturu), jejíž přílohou bude kopie předávacího protokolu (viz. bod 4.1 této Smlouvy).

Fakturační adresou je sídlo Kupujícího Univerzitní 2732/8, 301 00 Plzeň.

Daňový doklad (faktura) musí obsahovat všechny náležitosti řádného daňového a účetního dokladu ve smyslu příslušných právních předpisů, zejména zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

Je-li předmět smlouvy financován z projektových prostředků (tj. v příloze č. 1 této smlouvy je tato informace uvedena) musí daňový doklad (faktura) obsahovat identifikační údaje projektu v takovém rozsahu, v jakém jsou identifikační údaje projektu uvedeny v příloze č. 1 této smlouvy (tj. zpravidla název a číslo projektu).

Daňový doklad nesplňující předepsané náležitosti bude Kupujícím vrácen do dne splatnosti daňového dokladu k doplnění (opravě), aniž se tak dostane do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněné či opravené faktury Kupujícímu.

5.5 Splatnost faktury se sjednává na 30 kalendářních dnů ode dne jejího prokazatelného doručení Kupujícímu. Kupující si jednostranně vyhrazuje právo prodloužit lhůtu splatnosti faktury až o 30 kalendářních dní. Tato skutečnost nezakládá prodlení Kupujícího s hrazením kupní ceny dle této Smlouvy.

5.6 Kupní cena bude Kupujícím uhrazena na bankovní účet Prodávajícího uvedený v záhlaví této Smlouvy. Povinnost uhradit kupní cenu bude Kupujícím splněna v okamžiku připsání celé výše kupní ceny na bankovní účet Prodávajícího.

5.7 Kupující neposkytuje zálohy na úhradu ceny plnění.

5.8 Kupující je oprávněn započíst jakoukoli smluvní pokutu, kterou je povinen uhradit Prodávající, proti fakturované kupní ceně. Prodávající pro případné započtení musí vystavit zvláštní fakturu a nemůže toto započtení provést např. jednostranným navýšením kupní ceny.

5.9 Povinnost Kupujícího uhradit fakturu uvedenou v čl. 5.8 této Smlouvy je splněna dnem připsání příslušné částky na účet Prodávajícího.

6. Práva a povinnosti smluvních stran

6.1 Prodávající bude poskytovat Kupujícímu technickou podporu (v českém, slovenském nebo anglickém jazyce) v pracovní dny v době od 08:00 do 14:00. Smluvní strany spolu budou komunikovat všemi oběma smluvním stranám dostupnými způsoby komunikace. Sjednávají si, že v případě podnětu (telefonického či e-mailového) bude dotčená strana reagovat do 24 hodin od obdržení tohoto podnětu.

6.2 Prodávající je povinen dodat předmět plnění za podmínek dle této Smlouvy a předmět plnění musí odpovídat technickým požadavkům specifikovaným v Přílohách této Smlouvy a musí být bez jakýchkoliv vad, které by bránily plnohodnotnému užívání Zboží. Případné drobné vady budou uvedeny v předávacím protokolu a bude v něm uvedena i lhůta pro jejich odstranění.

6.3 Prodávající není oprávněn postoupit jakákoliv práva nebo povinnosti z této Smlouvy na třetí osoby bez předchozího písemného souhlasu Kupujícího.

6.4 Prodávající souhlasí s tím, že jakékoliv jeho pohledávky vůči Kupujícímu, které vzniknou na základě této Smlouvy, nebude moci postoupit ani započítat jednostranným právním jednáním.

6.5 Prodávající odpovídá Kupujícímu za újmu (majetkovou i nemajetkovou) způsobenou porušením povinností podle této Smlouvy nebo povinnosti stanovené obecně závazným právním předpisem.

6.6 Prodávající bere na vědomí, že jako osoba povinná dle ust. § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, je povinen spolupůsobit při výkonu finanční kontroly.

6.7 Prodávající je povinen dodržet veškeré závazky obsažené v jeho nabídce do veřejné zakázky, která předcházela uzavření této Smlouvy.

6.8 Prodávající bere na vědomí a souhlasí s tím, že tato smlouva bude uveřejněna na profilu Kupujícího ve smyslu ust. § 219 odst. 1 ZZVZ nebo v souladu se zák. č. 340/2015 Sb. v registru smluv, pakliže podléhá zveřejnění, stejně tak jako bude uveřejněna výše skutečně uhrazené ceny za plnění předmětu z této smlouvy, a to ve lhůtách a způsobem uvedeným v ust. § 219 odst. 3 ZZVZ a jinými příslušnými předpisy.

7. Smluvní pokuty

7.1 V případě prodlení Prodávajícího s dodáním Zboží a splněním veškerých povinností uvedených v článku 3. a 4. této Smlouvy oproti termínu stanovenému v článku 4.1 je Prodávající povinen zaplatit smluvní pokutu ve výši 0,5 % z celkové kupní ceny všech položek bez DPH za každý, byť i jen započatý den prodlení, čímž není dotčen nárok Kupujícího na náhradu újmy (majetkové i nemajetkové).

7.2 V případě nedodržení uvedené (či jinak dohodnuté) lhůty pro provedení záruční opravy ve lhůtě podle článku 8. 3 této Smlouvy je Kupující oprávněn uplatnit na Prodávajícím smluvní pokutu ve výši 0,5% z kupní ceny každé dotčené položky Zboží bez DPH za každý, byť i jen započatý den prodlení. Zaplacením smluvní pokuty není dotčeno právo Kupujícího na náhradu újmy (majetkové i nemajetkové).

7.3 V případě prodlení Kupujícího s úhradou faktury je Prodávající oprávněn uplatnit vůči Kupujícímu úrok z prodlení ve výši 0,05 % z dlužné částky za každý, byť i jen započatý den prodlení s úhradou faktury.

7.4 V případě prodlení Prodávajícího s nástupem k odstranění vad nahlášených Kupujícím dle článku 8.3 této Smlouvy, se Prodávající zavazuje uhradit Kupujícímu smluvní pokutu ve výši 0,5 % z kupní ceny každé dotčené položky Zboží bez DPH za každý, byť i jen započatý den prodlení, čímž není dotčeno právo Kupujícího na náhradu újmy (majetkové i nemajetkové).

8. Záruka za jakost

8.1 Prodávající se zavazuje poskytnout na zboží záruku v délce 24 měsíců, není-li v jednotlivých položkách obsažených v Přílohách této Smlouvy stanovena záruční doba jinak. Záruční doba běží od předání věci Kupujícímu, resp. od podpisu protokolu o předání a převzetí Zboží oběma smluvními stranami (blíže článek 4. této Smlouvy).

Prodávající se zavazuje, že zboží bude po celou záruční dobu způsobilé k použití pro obvyklý účel a že si zachová obvyklé vlastnosti.

8.2 Záruční doba dle článku 8.1 neběží po dobu, po kterou Kupující nemůže zboží užívat pro vady, za které odpovídá Prodávající. V případě výskytu vady v záruční lhůtě se záruční lhůta prodlužuje o dobu od oznámení vady Kupujícím Prodávajícímu do uvedení Zboží do opětovného provozu v místě určeném Kupujícím.

8.3 V záruční lhůtě je Prodávající povinen odstraňovat reklamované vady, popřípadě uspokojit jiný nárok Kupujícího z vadného plnění, a to tak, že Prodávající nastoupí k odstranění závady / odstraní závady ve lhůtách požadovaných v Přílohách této Smlouvy.

Pokud není v Přílohách této Smlouvy upraveno nastoupení k odstranění závady / odstranění závady, tak platí, že Prodávající nastoupí k odstranění závady ve lhůtě nejpozději do 48 hodin od nahlášení závady Kupujícím Prodávajícímu telefonicky nebo písemně. Záruční opravy provede Prodávající na vlastní náklady bezodkladně, nejpozději do 30 kalendářních dnů od nahlášení vady Kupujícím, není-li smluvními stranami stanoveno jinak. Prodávající bere na vědomí, že k odstranění závad může nastoupit v pracovní den v době od 8:00 hodin do 16:00 hodin, případně dle písemné dohody i jindy. Nástupem na servisní zásah se rozumí dostavení se oprávněného zástupce Prodávajícího do místa plnění dle této Smlouvy za účelem odstranění oznámené závady dodaného Zboží. V případě, že konec lhůty k nástupu na odstranění připadne na dobu mimo rozmezí uvedené výše a nebude-li mezi smluvními stranami dohodnuto jinak, je Prodávající povinen nastoupit k odstranění nahlášené závady v nejbližším možném termínu (následující pracovní den).

V případě výskytu vady po dobu běhu záruční doby se záruční doba prodlužuje o dobu od oznámení závady Kupujícím Prodávajícímu po její odstranění Prodávajícím. Reklamaci lze uplatnit nejpozději do posledního dne záruční lhůty, přičemž i reklamace odeslaná v poslední den záruční lhůty se považuje za včas uplatněnou.

8.4 Oprávnění k bezplatné záruční opravě zboží zanikne v případě, kdy k závadě dojde prokazatelným mechanickým poškozením Zboží nebo prokazatelným provozováním Zboží v nevhodném prostředí. Ze záruky jsou rovněž vyjmuty vady způsobené živelnou pohromou a neodbornou manipulací se Zbožím způsobem nerespektujícím návod k použití, nadměrným opotřebením, neexistencí údržby nebo nedostatečnou či špatnou údržbou.

8.5 Prodávající se zavazuje pro účely odstranění reklamovaných vad zajistit servis Zboží po celou dobu trvání záruční lhůty. Podmínky servisu jsou uvedeny v čl. 6. a čl. 8 této Smlouvy.

8.6 Kontaktními osobami oprávněnými jednat za Kupujícího ve věcech povinností stanovených článkem 8. této Smlouvy včetně uplatňování nároků z vad Zboží jménem Kupujícího, pokud nebude Kupujícím Prodávajícímu písemně sděleno jinak, jsou osoby uvedeny u jednotlivých položek v Příloze č. 1 této Smlouvy.

Prodávající bere na vědomí, že na osobu uvedenou v článku 4. 3 této Smlouvy budou směřovány oznámení o potřebě garančního zásahu dle článku 8. této Smlouvy. Změna této osoby musí být Kupujícímu neprodleně písemně oznámena, přičemž je účinná okamžikem prokazatelného doručení tohoto písemného oznámení Kupujícímu.

9. Odstoupení od smlouvy

9.1 Odstoupit od Smlouvy lze pouze z důvodů stanovených ve Smlouvě nebo zákonem.

9.2 Od této Smlouvy může smluvní strana dotčená porušením povinnosti druhou smluvní stranou jednostranně odstoupit pro podstatné porušení této Smlouvy, přičemž za podstatné porušení této Smlouvy se zejména považuje:

a) na straně Kupujícího nezaplacení kupní ceny podle této smlouvy ve lhůtě delší 60 dní po dni splatnosti příslušné faktury,

b) na straně Prodávajícího, jestliže předmět koupě (nebo jeho část), nebude řádně dodána v dohodnutém termínu dle č. 4.1 této Smlouvy tak, aby Prodávajícímu vzniklo právo na úhradu kupní ceny (nebo její části) vystavením příslušné faktury,

c) na straně Prodávajícího, jestliže Zboží nebude mít vlastnosti deklarované prodávajícím v této smlouvě,

d) na straně Prodávajícího, jestliže ve své nabídce v rámci veřejné zakázky, která předcházela uzavření této smlouvy, uvedl informace nebo doklady, které neodpovídají skutečnosti a měly nebo mohly mít vliv na výsledek zadání veřejné zakázky.

9.3 Skončením účinnosti této Smlouvy zanikají všechny závazky smluvních stran ze Smlouvy. Skončením účinnosti nebo jejím zánikem nezanikají nároky na náhradu újmy a zaplacení smluvních pokut sjednaných pro případ porušení smluvních povinností vzniklé před skončením účinnosti Smlouvy, a ty závazky smluvních stran, které podle Smlouvy nebo vzhledem ke své povaze mají trvat i nadále nebo u kterých tak stanoví zákon.

10. Společná a závěrečná ustanovení

10.1 Smlouva nabývá platnosti dnem jejího uzavření, tj. dnem podpisu smlouvy oprávněnými zástupci obou smluvních stran. Smlouva nabývá účinnosti dnem jejího uzavření, jde-li o smlouvu podléhající zveřejnění v registru smluv dle zákona č. 340/2015 Sb., pak teprve dnem zveřejnění v registru smluv.

10.2 Nedílnou součástí této Smlouvy jsou následující přílohy:

- Příloha č. 1 Technická specifikace předmětu veřejné zakázky
- Příloha č. 2 Technická specifikace předmětu veřejné zakázky
- Příloha č. 3 Technická specifikace předmětu veřejné zakázky
- Příloha č. 4 Technická specifikace předmětu veřejné zakázky
- Příloha č. 5 Technická specifikace předmětu veřejné zakázky

10.3 Smluvní pokuty uplatňované dle této Smlouvy jsou splatné do 30 (třiceti) dní od data, kdy byla povinné straně doručena písemná výzva k zaplacení smluvní pokuty ze strany oprávněné strany, a to na účet oprávněné strany uvedený v záhlaví této Smlouvy.

10.4 Veškeré změny či doplnění Smlouvy lze učinit pouze na základě písemné dohody smluvních stran. Takové dohody musí mít podobu datovaných, číslovaných a oběma smluvními stranami podepsaných dodatků Smlouvy.

10.5 Nastanou-li u některé ze smluvních stran skutečnosti bránící řádnému plnění této Smlouvy, je povinna to ihned bez zbytečného odkladu oznámit druhé straně a vyvolat jednání zástupců Kupujícího a Prodávajícího.

10.6 Vztahuje-li se důvod neplatnosti jen na některé ustanovení Smlouvy, je neplatným pouze toto ustanovení, pokud z jeho povahy, obsahu anebo z okolností, za nichž bylo sjednáno, nevyplývá, že jej nelze oddělit od ostatního obsahu Smlouvy.

10.7 Ve věcech touto Smlouvou výslovně neupravených se bude tento smluvní vztah řídit ustanoveními obecně závazných právních předpisů, zejména zákonem a předpisy souvisejícími.

10.8 Smluvní strany budou vždy usilovat o smírné urovnání případných sporů vzniklých ze Smlouvy. Případné spory vzniklé z této Smlouvy budou řešeny podle platné právní úpravy věcně a místně příslušnými orgány České republiky. Smluvní strany sjednávají ve smyslu ustanovení § 89a zákona č. 99/1963 Sb., občanského soudního řádu, ve znění pozdějších předpisů, pro spory vyplývající z této Smlouvy či s touto Smlouvou související místní příslušnost Okresního soudu Plzeň – město, případně Krajského soudu v Plzni.

10.9 Kupující deklaruje a Prodávající bere na vědomí, že Kupující není ve vztazích vyplývajících z této Smlouvy podnikatelem.

10.10 Tato smlouva se podepisuje oběma smluvními stranami elektronicky pomocí uznávaného elektronického podpisu.

10.11 Smluvní strany prohlašují, že si Smlouvu před jejím podpisem přečetly a s jejím obsahem bez výhrad souhlasí. Smlouva je vyjádřením jejich pravé, skutečné, svobodné a vážné vůle. Na důkaz pravosti a pravdivosti těchto prohlášení připojují oprávnění zástupci smluvních stran své uznávané elektronické podpisy.

Dne (viz elektronický podpis)
Za Kupujícího:

Západočeská univerzita v Plzni
doc. Dr. RNDr. Miroslav Holeček
rektor
podepsáno elektronicky

Dne (viz elektronický podpis)
Za Prodávajícího:

Networksys a.s.
xxx

Výpočetní technika (III.) 093-2020 (VT-(III.)-093-2020)

Příloha_c._1_Kupni_smlouvy_technicka_specifikace_VT-(III.)-093-2020

Vyplní se automaticky
Vyplní dodavatel

					[DOPLNÍ DODAVATEL]							[DOPLNÍ DODAVATEL]		
Položka	Název	Množství	Měrná jednotka [MJ]	Popis	Obchodní název + typ	Fakturace	Financováno z projektových finančních prostředků	Obchodní podmínky NAD RÁMEC STANDARDNÍCH obchodních podmínek	Kontaktní osoba k převzetí zboží	Místo dodání	MAXIMÁLNÍ CENA za měrnou jednotku (MJ) v Kč bez DPH	NABÍDKOVÁ CENA za měrnou jednotku (MJ) v Kč bez DPH	NABÍDKOVÁ CENA CELKEM v Kč bez DPH	VYHOVUJE / NEVYHOVUJE
1	24 portový přepínač s 1 Gb uplink porty	1	ks	Specifikace viz Priloha_c._2_Kupni_smlouvy_technicka_specifikace_VT-(III.)-093-2020.pdf	C9200L-24T-4G-E Catalyst 9200L 24-port data, 4 x 1G,	Samostatná faktura	NE	Dodání zboží do místa plnění do 90 kalendářních dnů od dojití výzvy k plnění smlouvy. Rozšiřující podmínky viz Priloha_c._5_Kupni_smlouvy_technicka_specifikace_VT-(III.)-093-2020.pdf	xxx	Univerzitní 20, 301 00 Plzeň, Centrum informatizace a výpočetní techniky , místnost UI 420	54 873,00 Kč	50 872,00 Kč	50 872,00 Kč	VYHOVUJE
2	24 portový PoE+ přepínač s 10 Gb uplink porty	1	ks		C9200L-24P-4X-E Catalyst 9200L 24-port PoE+, 4 x 10G,						74 500,00 Kč	73 721,00 Kč	73 721,00 Kč	VYHOVUJE
3	48 portový přepínač s 1 Gb uplink porty	2	ks		C9200L-48T-4G-E Catalyst 9200L 48-port data, 4 x 1G,						71 000,00 Kč	70 320,00 Kč	140 640,00 Kč	VYHOVUJE
4	48 portový přepínač s 10 Gb uplink porty	1	ks		C9200L-48T-4X-E Catalyst 9200L 48-port data, 4 x 10G						59 000,00 Kč	58 024,00 Kč	58 024,00 Kč	VYHOVUJE
5	48 portový PoE+ přepínač s 10 Gb uplink porty	3	ks		C9200L-48P-4X-E Catalyst 9200L 48-port PoE+, 4 x 10G,						94 000,00 Kč	93 644,00 Kč	280 932,00 Kč	VYHOVUJE
6	48 portový PoE+ přepínač s 1 Gb uplink porty	12	ks		C9200L-48P-4G-E Catalyst 9200L 48-port PoE+, 4 x 1G,						77 000,00 Kč	76 782,00 Kč	921 384,00 Kč	VYHOVUJE
7	48 portový přepínač s 1 Gb uplink porty	3	ks		C9200L-48T-4G-E Catalyst 9200L 48-port data, 4 x 1G,						62 271,00 Kč	60 038,00 Kč	180 114,00 Kč	VYHOVUJE
8	24 portový fanless přepínač	1	ks	Specifikace viz Priloha_c._3_Kupni_smlouvy_technicka_specifikace_VT-(III.)-093-2020.pdf	C1000-24T-4G-L Catalyst 1000 24port GE, 4x1G SFP	Samostatná faktura					14 000,00 Kč	13 661,00 Kč	13 661,00 Kč	VYHOVUJE
9	24 portový fanless přepínač s PoE	2	ks		C1000-24P-4G-L Catalyst 1000 24port GE, POE, 4x1G						20 000,00 Kč	19 800,00 Kč	39 600,00 Kč	VYHOVUJE
10	16 portový fanless přepínač s PoE	3	ks		C1000-16FP-2G-L Catalyst 1000 16port GE, Full POE						23 000,00 Kč	22 458,00 Kč	67 374,00 Kč	VYHOVUJE
11	8 portový fanless přepínač s PoE	7	ks		C1000-8FP-2G-L Catalyst 1000 8port GE, Full POE, 2x1G						11 000,00 Kč	10 855,00 Kč	75 985,00 Kč	VYHOVUJE
12	Bezdrátový přístupový bod s interními anténami	26	ks	Specifikace viz Priloha_c._4_Kupni_smlouvy_technicka_specifikace_VT-(III.)-093-2020.pdf	C9120AXI-E Cisco Catalyst 9120AX Series	Samostatná faktura					22 500,00 Kč	21 053,00 Kč	547 378,00 Kč	VYHOVUJE
13	Bezdrátový přístupový bod s externími anténami	2	ks		C9120AXE-E Cisco Catalyst 9120AX Series						24 000,00 Kč	23 664,00 Kč	47 328,00 Kč	VYHOVUJE
14	Montážní kryt pro instalaci AP na stěnu	2	ks		Oberon 1016-00						5 250,00 Kč	5 250,00 Kč	10 500,00 Kč	VYHOVUJE

Informace pro dodavatele: Pokud se dodavateli při zadávání jednotkových cen objeví text - "NEVYHOVUJE", znamená to překročení stanovené maximální nepřekročitelné nabídkové ceny, a to znamená nesplnění podmínek stanovených Zadavatelem. Pokud bude nabídka v této podobě podána Zadavateli, bude při posouzení vyřazena.

V případě, že se dodavatel při předání zboží na některá uvedená tel. čísla nedovolá, bude v takovém případě volat tel. xxx.

CELKOVÁ MAXIMÁLNÍ CENA za celou VZ v Kč BEZ DPH	CELKOVÁ NABÍDKOVÁ CENA v Kč bez DPH
2 566 686,00 Kč	2 507 513,00 Kč

Požadované technické parametry dodávky

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

- 24 portový přepínač s 1 Gb uplink porty (1 ks).
- 24 portový PoE+ přepínač s 10 Gb uplink porty (1 ks).
- 48 portový přepínač s 1 Gb uplink porty (2 ks).
- 48 portový přepínač s 10 Gb uplink porty (1 ks).
- 48 portový PoE+ přepínač s 10 Gb uplink porty (3 ks).
- 48 portový PoE+ přepínač s 1 Gb uplink porty (12 ks).
- 48 portový přepínač s 1 Gb uplink porty (3 ks).

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/	ano

multicast rámců na portu v procentech	
Protokol IP	
IP alias (více IP síti 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/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

Tabulka povinných požadavků pro 24 portový přepínač s 1 Gb uplink porty (1 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
Počet stohovacích modulů pro přepínače ve stejném racku	2
Minimální délka stohovacích kabelů každého modulu	3 m

Tabulka povinných požadavků pro 24 portový PoE+ přepínač s 10 Gb uplink porty (1 ks)

Požadavek na funkcionalitu	**Minimální požadavky**
Počet RJ-45 portů 10/100/1000	24
Počet uplink portů a jejich typ	4x 10GE SFP+
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	350 W
Schopnost poskytovat PoE napájení připojeným zařízením i během restartu přepínače	ano
Stohování požadováno	ano
Počet stohovacích modulů pro přepínače ve stejném racku	2
Minimální délka stohovacích kabelů každého modulu	3 m

Tabulka povinných požadavků pro 48 portový přepínač s 1 Gb uplink porty (2 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
Počet stohovacích modulů pro přepínače ve stejném racku	2
Minimální délka stohovacích kabelů každého modulu	50 cm

Tabulka povinných požadavků pro 48 portový přepínač s 10 Gb uplink porty (1 ks)

Požadavek na funkcionalitu	Minimální požadavky
Počet RJ-45 portů 10/100/1000	48
Počet uplink portů a jejich typ	4x 10GE SFP+
Stohování požadováno	ano
Počet stohovacích modulů pro přepínače ve stejném racku	2
Minimální délka stohovacích kabelů každého modulu	50 cm

Tabulka povinných požadavků pro 48 portový PoE+ přepínač s 10 Gb uplink porty (3 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
Schopnost poskytovat PoE napájení připojeným zařízením i během restartu přepínače	ano
Počet uplink portů a jejich typ	4x 10GE SFP+
Požadovaný počet a typ transceiverů	2 ks, 10GBase AOC, SFP+, 3m
Stohování požadováno	ano
Minimální délka stohovacího kabelu	1 m

Tabulka povinných požadavků pro 48 portový PoE+ přepínač s 1 Gb uplink porty (12 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
Schopnost poskytovat PoE napájení připojeným zařízením i během restartu přepínače	ano
Počet uplink portů a jejich typ	4x 1GE SFP
Stohování požadováno	ano
Minimální délka stohovacího kabelu	50 cm

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

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 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 zneužiti (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 zatižení 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 RANCID[1] 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[2] 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[3], umožňující paralelní vykonávání příkazů, a NeDi.

Správa bezdrátové sítě

Na ZČU je provozována bezdrátová síť eduroam[4], 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[5].
Pro správu a konfiguraci bezdrátových přístupových bodů je využíváno centralizované řešení. Jako centrální prvky jsou použity čtyři bezdrátové řadiče[6] pracující v režimu active/standby, které jsou schopny současně spravovat až 1100 AP. K udržení konzistentní konfigurace obou bezdrátových řadičů je používán specializovaný software[7].

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

[1] http://www.shrubbery.net/rancid/
[2] http://nedi.ch/
[3] Vlastní otevřený systém založený na využiti výsledků diplomových prací studentů FAV.
[4] http://www.eduroam.cz
[5] http://freeradius.org
[6] Dva bezdrátové řadiče Cisco Wireless LAN Controller (WLC) 5520 pro 600 AP a dva bezdrátové řadiče Cisco Wireless LAN Controller (WLC) 5508 pro 400 AP.
[7] Cisco Prime Infrastructure verze 3.5 pro 1000 uzlů provozovaný ve virtualizovaném prostředí.
[8] http://sauron.jyu.fi/
[9] Vlastní otevřený systém založený na využiti výsledků diplomových prací studentů FAV.
[10] http://www.netdisco.org/

adres za konkrétními fyzickými porty jednotlivých přepínačů, informace o SMB atd.[11]) s možnosti 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[12], 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[13], 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[14].
Pro non-stop historii sledování základních L2 provozních charakteristik aktivních komunikačních prvků všech prostředí pomocí SNMP[15] (typicky zatižení 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[16] a Torrus[17] 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[18] sondy (kolejní intranet) se zpracovávají jednak nevzorkované pomocí produkčního IPv4 software Caligare Flow Inspector/CFI[19] a jednak vzorkované 1:10 pomocí testovacího IPv4/IPv6 software FTAS[20].
Pro monitorování historie latence/jitteru/ztrátovosti paketů (typicky VoIP subsystému) se používá aktivní nástroj Smokeping[21].
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[22] 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

---

[11] Z bezpečnostních důvodů se však záměrně nevyužívají integrované služby manipulace se stavy portů přepínačů vyžadující SNMP přístup pro zápis.
[12] http://www.nagios.org/
[13] http://www.nagios.org/
[14] http://www.mikrotik.com/thedude.php
[15] Konfigurace aktivních prvků pouze v režimu pro čtení s povolenými IP adresami management stanic dle ACL.
[16] http://cricket.sourceforge.net/
[17] http://torrus.org/
[18] http://www.invea.cz/produkty-sluzby/flowmon/flowmon-sondy
[19] http://www.caligare.com/
[20] 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
[21] http://oss.oetiker.ch/smokeping/
[22] http://www.zenoss.com/solution/network-monitoring

systémem zpracování Syslog hlášení z aktivních prvků OSSEC[23] a pro SNMP trapy systémem Zenoss Core.
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 podsíti zajišťuje software ARPwatch[24].
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 vypnuti daného portu na přístupovém prvku (typicky nejblíže místu svého vzniku podle typu komunikačního prvku) je řízeno pomocí nástroje NetSpy [25]. Tento vlastní nástroj také poskytuje další potřebné podpůrné administrátorské funkce jako např. automatickou detekci neregistrovaných zařízení, vyhledání různých konfliktních síťových stavů, management VLAN/IP podsíti atd.
Vzdálený administrátorský přístup ke všem aktivním síťovým prvkům je zajištěn pouze[26] pomocí SSH protokolu s autentizací/autorizací protokolem TACACS+ z předdefinovaných povolených bezpečných podsíti/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.

[23]http://www.ossec.net/
[24]http://www.securityfocus.com/tools/142
[25]Vlastní otevřený systém založený na využiti výsledků diplomových prací studentů FAV.
[26]S výjimkou menšího počtu zastaralých přepínačů, které SSH nepodporují a jsou postupně podle finančních možnosti nahrazovány.

Požadované technické parametry dodávky

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

- 24 portový fanless přepínač (1 ks).
- 24 portový fanless přepínač s PoE (2 ks).
- 16 portový fanless přepínač s PoE (3 ks).
- 8 portový fanless přepínač s PoE (7 ks).

Tabulka povinných požadavků pro všechny požadované přepínače

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Třída zařízení	L2 přepínač
Formát zařízení	fixní konfigurace
Bezvětrákové provedení	ano
Desktopové provedení	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	256
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
Multicast/broadcast storm control - hardwarové omezení poměru unicast/ multicast rámců na portu v procentech	ano
Protokol IP	
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
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
Syslog	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
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ano

Tabulka povinných požadavků pro 24 portový fanless přepínač (1 ks)

Požadavek na funkcionalitu	Minimální požadavky
Počet RJ-45 portů 10/100/1000	24
Počet uplink portů a jejich typ	4x 1GE SFP

Tabulka povinných požadavků pro 24 portový fanless přepínač s PoE (2 ks)

Požadavek na funkcionalitu	Minimální požadavky
Počet RJ-45 portů 10/100/1000	24
Počet uplink portů a jejich typ	4x 1GE SFP
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	190 W
Schopnost poskytovat PoE napájení připojeným zařízením i během restartu přepínače	ano

Tabulka povinných požadavků pro 16 portový fanless přepínač s PoE (3 ks)

Požadavek na funkcionalitu	Minimální požadavky
Počet RJ-45 portů 10/100/1000	16
Počet uplink portů a jejich typ	2x 1GE SFP
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	240 W
Schopnost poskytovat PoE napájení připojeným zařízením i během restartu přepínače	ano

Tabulka povinných požadavků pro 8 portový fanless přepínač s PoE (7 ks)

Požadavek na funkcionalitu	Minimální požadavky
Počet RJ-45 portů 10/100/1000	8
Počet uplink portů a jejich typ	2x 1GE SFP
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	120 W
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 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 zneužiti (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 zatižení 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 RANCID[1] 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

[1] http://www.shrubbery.net/rancid/

přehledných sumárních změny) všech aktivních komunikačních prvků Cisco pomocí systému NeDi[2] 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[3], umožňující paralelní vykonávání příkazů, a NeDi.

Správa bezdrátové sítě

Na ZČU je provozována bezdrátová síť eduroam[4], 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[5].
Pro správu a konfiguraci bezdrátových přístupových bodů je využíváno centralizované řešení. Jako centrální prvky jsou použity čtyři bezdrátové řadiče[6] pracující v režimu active/standby, které jsou schopny současně spravovat až 1100 AP. K udržení konzistentní konfigurace obou bezdrátových řadičů je používán specializovaný software[7].

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[8] v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet[9] 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[10] 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 adres za konkrétními fyzickými porty jednotlivých přepínačů, informace o SMB atd.[11]) s možnosti 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[12], 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.

---

[2] http://nedi.ch/
[3] Vlastní otevřený systém založený na využiti výsledků diplomových prací studentů FAV.
[4] http://www.eduroam.cz
[5] http://freeradius.org
[6] Dva bezdrátové řadiče Cisco Wireless LAN Controller (WLC) 5520 pro 600 AP a dva bezdrátové řadiče Cisco Wireless LAN Controller (WLC) 5508 pro 400 AP.
[7] Cisco Prime Infrastructure verze 3.5 pro 1000 uzlů provozovaný ve virtualizovaném prostředí.
[8] http://sauron.jyu.fi/
[9] Vlastní otevřený systém založený na využiti výsledků diplomových prací studentů FAV.
[10] http://www.netdisco.org/
[11] Z bezpečnostních důvodů se však záměrně nevyužívají integrované služby manipulace se stavy portů přepínačů vyžadující SNMP přístup pro zápis.
[12] http://www.nagios.org/

Pro sledování non-stop dostupnosti na úrovni služeb pro systém VoIP ZČU se používá systém Nagios[13], 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[14].
Pro non-stop historii sledování základních L2 provozních charakteristik aktivních komunikačních prvků všech prostředí pomocí SNMP[15] (typicky zatižení 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[16] a Torrus[17] 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[18] sondy (kolejní intranet) se zpracovávají jednak nevzorkované pomocí produkčního IPv4 software Caligare Flow Inspector/CFI[19] a jednak vzorkované 1:10 pomocí testovacího IPv4/IPv6 software FTAS[20].
Pro monitorování historie latence/jitteru/ztrátovosti paketů (typicky VoIP subsystému) se používá aktivní nástroj Smokeping[21].
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[22] 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[23] a pro SNMP trapy systémem Zenoss Core.
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 podsíti zajišťuje software ARPwatch[24].
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 vypnuti daného portu na přístupovém prvku (typicky nejblíže místu svého vzniku podle typu komunikačního prvku) je řízeno pomocí nástroje NetSpy[25]. Tento vlastní nástroj také poskytuje další potřebné podpůrné administrátorské funkce jako např. automatickou detekci neregistrovaných zařízení, vyhledání různých konfliktních síťových stavů, management VLAN/IP podsíti atd.

[13] http://www.nagios.org/
[14] http://www.mikrotik.com/thedude.php
[15] Konfigurace aktivních prvků pouze v režimu pro čtení s povolenými IP adresami management stanic dle ACL.
[16] http://cricket.sourceforge.net/
[17] http://torrus.org/
[18] http://www.invea.cz/produkty-sluzby/flowmon/flowmon-sondy
[19] http://www.caligare.com/
[20] 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
[21] http://oss.oetiker.ch/smokeping/
[22] http://www.zenoss.com/solution/network-monitoring
[23] http://www.ossec.net/
[24] http://www.securityfocus.com/tools/142
[25] Vlastní otevřený systém založený na využiti výsledků diplomových prací studentů FAV.

Vzdálený administrátorský přístup ke všem aktivním síťovým prvkům je zajištěn pouze[26] pomocí SSH protokolu s autentizací/autorizací protokolem TACACS+ z předdefinovaných povolených bezpečných podsíti/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.

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

Požadované technické parametry dodávky

Předmětem dodávky jsou aktivní síťové prvky dle technických podmínek uvedených níže

- 26 ks bezdrátových přístupových bodů s interními anténami.
- 2 ks bezdrátových přístupových bodů s externími anténami.
- 2 ks montážních krytů pro instalaci AP na stěnu.

Tabulka povinných požadavků pro bezdrátový přístupový bod s interními anténami (požadováno 26 ks)

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
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
Protokoly fyzické vrstvy	
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 radiového signálu	ano
Minimální počet inzerovaných SSID (BSSID)	8/rádiové rozhraní
Rádio podporující BLE 5.0, ZigBee a Target Wake Time (TWT)	ano
Bezpečnost	
Certifikát s lokální platnosti pro nasazení PKI	ano
Fyzické zabezpečení/zamknuti 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

Tabulka povinných požadavků pro bezdrátový přístupový bod s externími anténami (požadovány 2 ks)

Požadavek na funkcionalitu	**Minimální požadavky**
Základní vlastnosti	
Typ zařízení	bezdrátový přístupový bod
Montáž	na strop nebo na stěnu
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	dipólová, odpojitelná, naklápěcí, dvoupásmová
Zisk anténypro pásmo 2,4 Ghz / 5 GHz	2 dBi / 4 dBi
Počet antén	4
Podpora stávajících centralizovaných řadičů bezdrátové sítě	ano
Podpora systému centralizované správy bezdrátových řadičů	ano
Fyzická přenosová rychlost celé bezdrátové části	5 Gb/s
Protokoly fyzické vrstvy	
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 radiového signálu	ano
Minimální počet inzerovaných SSID (BSSID)	8/rádiové rozhraní
Rádio podporující BLE 5.0, ZigBee a Target Wake Time (TWT)	ano
Bezpečnost	
Certifikát s lokální platnosti pro nasazení PKI	ano
Fyzické zabezpečení/zamknuti 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

Tabulka povinných požadavků pro montážní kryt pro instalaci AP na stěnu (požadovány 2 ks)

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ krytu	nekovový montážní	
Rozměry (š x v x h) mm	305 x 460 x 132	
Klíčkem uzamykatelná dvířka	ano	
Instalace krytu	na stěnu	
Možnost polepu krytu fólií	ano	
Kompatibilita s bezdrátovým přístupovým bodem s externími anténami poptávaným v této ZD	ano	
Instalace AP pomocí nastavitelného držáku	ano	
Montážní šrouby a klíč součásti dodávky	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 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 zneužiti (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 RANCID[1] 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[2] 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[3], umožňující paralelní vykonávání příkazů, a NeDi.

Správa bezdrátové sítě

Na ZČU je provozována bezdrátová síť eduroam[4], 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[5]. Pro správu a konfiguraci bezdrátových přístupových bodů je využíváno centralizované

[1] http://www.shrubbery.net/rancid/

[2] http://nedi.ch/

[3] Vlastní otevřený systém založený na využiti výsledků diplomových prací studentů FAV.

[4] http://www.eduroam.cz

[5] http://freeradius.org

řešení. Jako centrální prvky jsou použity čtyři bezdrátové řadiče[6] pracující v režimu active/standby, které jsou schopny současně spravovat až 1600 AP. K udržení konzistentní konfigurace obou bezdrátových řadičů je používán specializovaný software[7].

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[8] v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet[9] 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[10] 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 adres za konkrétními fyzickými porty jednotlivých přepínačů, informace o SMB atd.[11]) s možnosti 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[12], 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[13], 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[14].

Pro non-stop historii sledování základních L2 provozních charakteristik aktivních komunikačních prvků všech prostředí pomocí SNMP[15] (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[16] a Torrus[17] pracujících nad RRD databázemi.

---

[6] Dva bezdrátové řadiče Cisco Wireless LAN Controller (WLC) 5520 pro 1000 AP a dva bezdrátové řadiče Cisco Wireless LAN Controller (WLC) 5508 pro 400 AP.

[7] Cisco Prime Infrastructure verze 3.8 pro 4000 uzlů provozovaný ve virtualizovaném prostředí.

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

[9] Vlastní otevřený systém založený na využiti výsledků diplomových prací studentů FAV.

[10] http://www.netdisco.org/

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

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

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

[14] http://www.mikrotik.com/thedude.php

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

[16] http://cricket.sourceforge.net/

[17] http://torrus.org/

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[18] sondy (kolejní intranet) se zpracovávají jednak nevzorkované pomocí produkčního IPv4 software Caligare Flow Inspector/CFI[19] a jednak vzorkované 1:10 pomocí testovacího IPv4/IPv6 software FTAS[20].
Pro monitorování historie latence/jitteru/ztrátovosti paketů (typicky VoIP subsystému) se používá aktivní nástroj Smokeping[21].
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[22] 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[23] a pro SNMP trapy systémem Zenoss Core.
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 podsíti zajišťuje software ARPwatch[24].
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 vypnuti daného portu na přístupovém prvku (typicky nejblíže místu svého vzniku podle typu komunikačního prvku) je řízeno pomocí nástroje NetSpy[25]. Tento vlastní nástroj také poskytuje další potřebné podpůrné administrátorské funkce jako např. automatickou detekci neregistrovaných zařízení, vyhledání různých konfliktních síťových stavů, management VLAN/IP podsíti atd.
Vzdálený administrátorský přístup ke všem aktivním síťovým prvkům je zajištěn pouze[26] pomocí SSH protokolu s autentizací/autorizací protokolem TACACS+ z předdefinovaných povolených bezpečných podsíti/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.

[18] http://www.invea.cz/produkty-sluzby/flowmon/flowmon-sondy
[19] http://www.caligare.com/
[20] 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
[21] http://oss.oetiker.ch/smokeping/
[22] http://www.zenoss.com/solution/network-monitoring
[23] http://www.ossec.net/
[24] http://www.securityfocus.com/tools/142
[25] Vlastní otevřený systém založený na využiti výsledků diplomových prací studentů FAV.
[26] S výjimkou menšího počtu zastaralých přepínačů, které SSH nepodporují a jsou postupně podle finančních možnosti nahrazovány.

Požadavky na záruku za jakost

- Zadavatel požaduje originální a nová zařízení určená pro evropský trh, licencovaná ve jménu Zadavatele tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce.
- Dodavatel je povinen s dodávkou doložit oficiální potvrzení zastoupení výrobce o určení dodávaných dílů a zařízení (seznamu výrobních čísel). Výrobní čísla svázaná s identitou koncového zákazníka (ZČU) doloží dodavatel na požádání.
- Všechna dodaná síťová zřízení musí být 100% kompatibilní se zařízeními používanými v současné době, spolupracovat s jejich konfigurací a nastavením a musí zajistit kontinuální provoz stávající počítačové sítě bez vynaložení dodatečných nákladů.
- Dodavatel poskytne Zadavateli po dobu trvání servisní podpory (36 měsíců) autorizovaný přístup pro stahování nových verzí programového vybavení (SW releases) a autorizovaný přístup do servisního a asistenčního centra výrobce pro řešení vzniklých problémů.
- Dodavatel se dále zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení.
- V databázi výrobce musí být Zadavatel veden jako první uživatel zboží.
- Nabídka bude zahrnovat **záruku za jakost po dobu 36 měsíců** od podpisu dodacích listů oběma smluvními stranami.
- **Záruka za jakost bude zahrnovat:**
  - výměnu vadného dílu nebo zařízení do 10 pracovních dnů od nahlášení závady zástupcem Zadavatele,
  - nárok na bezplatnou instalaci všech nových verzí firmware v rozsahu dodané licence.
- Veškeré podmínky a kritéria poptávky musí být splněny.