ZVÄZOK 3
OPIS PREDMETU ZÁKAZKY

OBSAH

1 ÚVOD

Navrhované riešenie ICT infraštruktúry STU vychádza z analýzy existujúceho stavu infraštruktúry, pričom sa zameriava na zachovanie funkčnosti ICT infraštruktúry z dvoch zásadných pohľadov:

- Migrácia na nové technológie a zriadenia (technologická obnova zariadení) s maximálnym využitím existujúcich zariadení
- Dosiahnutie maximálnej možnej priepustnosti (výkonu) ICT infraštruktúry STU
- Konečný stav ICT infraštruktúry a nové služby

Migračný stav nastáva vždy pri zapojení akéhokoľvek nového prvku ICT do existujúcej infraštruktúry. Tu je potrebné zvažovať:

- Fyzické možnosti zapojenia nových zariadení (racky, kabeláž, el. napájanie)
- Funkčné vlastnosti zariadení, aby všetky nové zariadenia boli plne kompatibilné z existujúcou infraštruktúrou na všetkých dotknutých komunikačných vrstvách. Nekompatibilita ktoréhokoľvek zariadenia a funkcionality na dotknutej komunikačnej vrstve s existujúcou infraštruktúrou môže spôsobiť pokles celkovej priepustnosti a dočasnú alebo aj trvalú nefunkčnosť celej ICT infraštruktúry.

Konečný stav ICT infraštruktúry vyplýva zo smerovania infraštruktúry k novým technológiám a ich použitiu v infraštruktúre STU. Preto je potrebné zaistiť, aby všetky prvky LAN siete boli navzájom kompatibilné s existujúcimi ako aj najnovšími technológiami na riadenie prístupu koncových zariadení do siete, monitoringom telemetrických dát z infraštruktúry, bezpečnostnými systémami pre kontrolu stavu zariadenia pred prístupom do siete, operatívnym monitoringom umožňujúcim proaktívne riešenie problémov skôr ako ich používateľ spozoruje, bezpečnostným monitoringom ako aj analytickými systémami komunikačných protokolov. Je potrebné aby aktívne prvky siete mohli byť centralizovane spravované a umožňovali ľahký inventarizačný prehľad a upgrade firmware-u na zariadeniach, čo umožňuje zjednodušenie a rýchlejšie nasadenie upgrade procedúr pri bezpečnostných upgradoch aktívnych prvkov siete.

2 POŽIADAVKY NA NOVÉ RIEŠENIE

Požiadavky na nové riešenie zahŕňajú body, ktoré boli identifikované ako potrebné riešiť v rámci upgrade celej infraštruktúry fakulty. Boli identifikované nasledujúce zásadné potreby:

- Zvýšenie celkovej priepustnosti a dostupnosti siete s využitím súčasných štandardov do rýchlostí 100GE
- Oddelenie dátového centra od kostrovej vrstvy
- Použiť platformy, kde výrobcom nebolo deklarované ukončenie podpory a teda nebude problém s reklamáciou prípadne výmenou zariadenia v prípade poruchy
- Realizovať L2/L3 sieť ako homogénnu infraštruktúru, aby nevznikali problémy pri nekompatibilite protokolov týchto vrstiev (napr. STP, MEC, FRRP)
- Citlivé platformy realizovať ako vysoko dostupné
    - centrálny firewall pre pripojenie do siete Internet
    - core
    - DC prepínače pre zapojenie dátových rozhraní serverových platforiem
    - Agregačné L3 prepínače v jednotlivých blokoch
    - bezdrôtové kontroléry
- Vykonať rozšírenie pokrytia a update/upgrade WIFI infraštruktúry, kde súčasný kontrolér a nové riešenie budú poskytovať vzájomný roaming pre klientov (plynulý prechod klienta medzi AP riadenými rôznymi kontrolérmi)
- Navrhnúť prvky a topologické riešenie bezpečnostnej infraštruktúry podľa súčasných bezpečnostných štandardov
- Implementácia IP telefónie nahrádzajúcej súčasné PBX riešenie
- V maximálnej možnej miere využiť súčasné komponenty LAN infraštruktúry
- Využitie prístupových bodov
- Využitie DC prepínača, resp. rozširujúcich FEX modulov
- Napájacie káble sa požadujú dodať s vidlicou do klasickej zásuvky

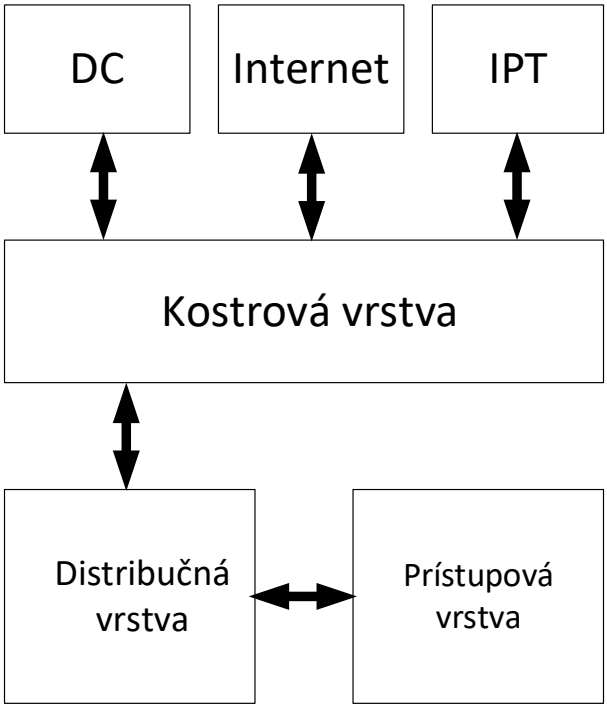
Pozn.

Nevyhnutná podmienka realizácie nového riešenia je rekonštrukcia pasívnej kabeláže, vybudovanie nových dátových rozvádzačov s ukončenými optickými trasami a požadovanými elektrickými rozvodmi. Uvedené je realizované v rámci aktuálneho projektu revitalizácie budovy FEI STU.

3 NÁVRH CIEĽOVÉHO STAVU

3.1 TOPOLÓGIA NAVRHOVANÉHO RIEŠENIA

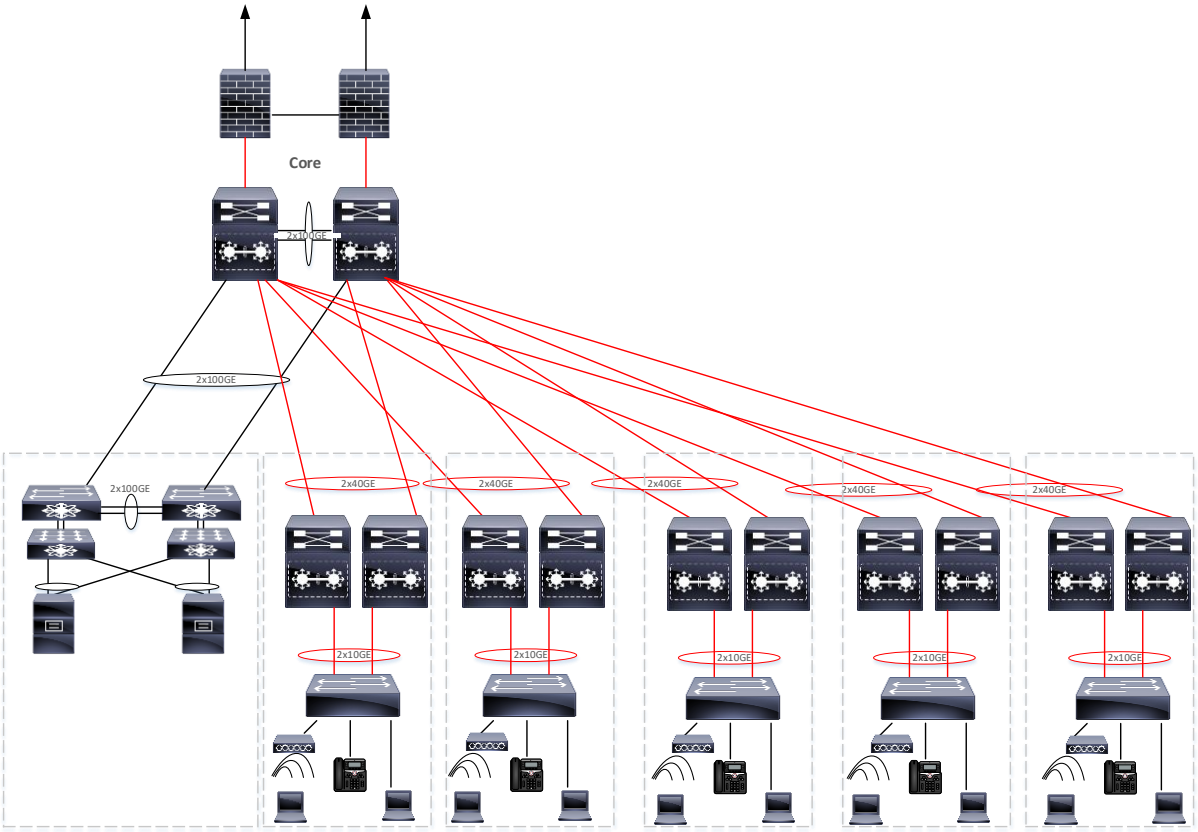
Z pohľadu topológie nedochádza k zásadným zmenám vo vnútri LAN siete. Stále zostane zachovaný hierarchický dizajn pozostávajúci z kostrovej, distribučnej a prístupovej vrstvy. Zásadnejšia zmena nastáva v DC, kde sa rozdelí kombinovaná funkcia kostrovej vrstvy a dátového centra na dva samostatné moduly. Schematicky bude sieť rozdelená do nasledovných modulov.



Obrázok 1 Schematické rozdelenie LAN siete

Kostrové prepínače ako aj prepínače dátového centra budú umiestnené v novej centrálnej serverovni, kde sa nachádza aj pripojenie do Internetu (do SANET-u cez FW). Vzájomné prepojenie kostrových a DC prepínačov bude realizované v rámci serverovne pomocou 100GE prepojov využitím pasívnych metalických a aktívnych AOC káblov.

Z jednotlivých blokov fakulty budú pripojené optickou, single módovou trasou distribučné prepínače rýchlosťou 40GE. Každý distribučný prepínač agreguje prístupové prepínače z jednotlivých poschodí v danom bloku, a zabezpečuje im pripojenie o kapacite 2x10GE cez optické prepojenia.



Obrázok 2 Topológia navrhovaného riešenia LAN FEI STU

3.2 POUŽITÉ PROTOKOLY V CIEĽOVOM STAVE LAN

Primárnym smerovacím protokolom použitým v LAN sieti, s ohľadom na kompatibilitu s existujúcimi zariadeniami, maximálnu priepustnosť novej ICT infraštruktúry a bezproblémovú migráciu zo súčasného riešenia bude EIGRP.

EIGRP odosiela iba prírastkové aktualizácie, čím sa významne znižuje pracovné zaťaženie smerovača a množstvo údajov, ktoré je potrebné preniesť. EIGRP je dynamický smerovací protokol, pomocou ktorého smerovače automaticky zdieľajú informácie o trase. Okrem smerovacej tabuľky používa EIGRP na ukladanie informácií aj tzv. Tabuľku susedov (uchováva záznamy o IP adresách smerovačov, ktoré majú priame fyzické spojenie s týmto smerovačom) a tzv. Tabuľku topológie (ukladá trasy, ktoré sa naučila zo susedných smerovacích tabuliek). Na rozdiel od smerovacej tabuľky, tabuľka topológie neukladá všetky cesty, ale iba cesty, ktoré boli určené EIGRP. Tabuľka topológie tiež zaznamenáva metriky pre každú z uvedených trás EIGRP, uskutočniteľného nástupcu a následníkov. Informácie v tabuľke topológie môžu byť vložené do smerovacej tabuľky smerovača a potom môžu byť použité na presmerovanie prevádzky. Ak sa sieť zmení (napríklad fyzické spojenie zlyhá alebo sa odpojí), cesta sa stane nedostupnou. EIGRP je navrhnutý tak, aby zistil tieto zmeny a pokúsi sa nájsť novú cestu k cieľu. Stará cesta, ktorá už nie je dostupná, sa odstráni zo smerovacej tabuľky. Na rozdiel od väčšiny protokolov diaľkového vektorového smerovania, EIGRP neprenáša všetky údaje v smerovacej tabuľke smerovača, keď sa vykoná zmena, ale prenesie iba zmeny, ktoré boli vykonané od poslednej aktualizácie smerovacej tabuľky. EIGRP neposiela svoju smerovaciu tabuľku pravidelne, ale posiela údaje smerovacej tabuľky iba vtedy, keď nastala skutočná zmena. Keď je

smerovač so systémom EIGRP pripojený k inému smerovaču, ktorý tiež používa EIGRP, dochádza k výmene informácií medzi týmito dvoma smerovačmi, vytvárajú vzťah, známy ako susedstvo a v tomto čase sa medzi oboma smerovačmi vymieňa celá smerovacia tabuľka. Po dokončení výmeny sa odosielajú už iba rozdielové zmeny. Táto skutočnosť zabezpečí maximálnu možnú priepustnosť siete.

Na detekciu prípadných problémov optických prepojov na fyzickej vrstve s ohľadom na súčasné platformy sa bude využívať UDLD (Unidirectional Link Detection), primárnym protokolom slúžiacim na prevenciu proti vzniku slučiek bude súčasne použitý RPVST+.

Unidirectional Link Detection (UDLD) je protokol vrstvy dátového spojenia (Layer 2) na monitorovanie fyzickej konfigurácie káblov a detekciu jednosmerných spojení. UDLD dopĺňa protokol Spanning Tree, ktorý sa používa na elimináciu prepínacích slučiek.

Protokol Rapid Per VLAN Spanning Tree Plus (RPVST+) – Vlastné vylepšenie IEEE 802.1w RSTP od spoločnosti Cisco. Podobne ako PVST+ umožňuje vytvoriť aj jednu inštanciu spanning-tree na VLAN. Konvergencia siete je rýchlejšia s RPVST+.

V sieti je definované značné množstvo VLAN, ktorých distribúciu na jednotlivé prístupové prepínače zabezpečuje VTP protokol, ktorý za bude aj naďalej využívať.

VLAN Trunking Protocol (VTP) je protokol šíriaci definíciu virtuálnych lokálnych sietí (VLAN) v celej lokálnej sieti. Na tento účel prenáša VTP informácie o VLAN do všetkých prepínačov v doméne VTP. Reklamy VTP je možné posielať cez 802.1Q a ISL trunky. VTP zabezpečuje konzistenciu konfigurácie VLAN naprieč sieťou vrstvy 2, dynamickú distribúciu pridaných VLAN cez sieť a Plug-and-play konfiguráciu pri pridávaní nových VLAN

Súčasná implementácia bezdrôtovej siete používa Cisco prístupové body, odporúčame preto použiť prístupové prepínače podporujúce CDP pre korektné vyjednanie PoE napájania.

Návrh cieľového stavu počíta aj s využitím IP telefónie, preto je potrebné, aby nové zariadenia podporovali 802.1x multidomain autentifikáciu, čo zabezpečí autentifikáciu prístupu do siete zvlášť pre IP Telefón a zvlášť pre PC zapojené do LAN portu telefónu.

Pre budúce využitie v bezpečnostnom monitoringu musia zariadenia podporovať Netflow v9, resp. IPFIX (nie samplovaný).

Všetky zariadenia musia podporovať RADIUS autentifikáciu a autorizáciu, ako aj systém riadenia prístupu TACACS+.

Terminal Access Controller Access-Control System Plus (TACACS+) je protokol vyvinutý spoločnosťou Cisco a vydaný ako otvorený štandard od roku 1993. Hoci je odvodený od TACACS, TACACS+ je samostatný protokol, ktorý sa zaoberá službami autentifikácie, autorizácie a účtovania (AAA). TACACS+ je rozšírenie TACACS, ktoré šifruje celý obsah každého paketu.

3.3 KOSTROVÁ VRSTVA

Kostru siete navrhujeme ako redundantnú dvojicu prepínačov vzájomne tvoriacich jeden logický prvok siete (jeden control plane) s vysokou priepustnosťou a minimálnym oneskorením. Prepínač bude disponovať optickými šachtami podporujúcimi rýchlosti 1/10/25 GE , ako aj 40/100 GE porty pre vzájomné prepojenie, pre pripojenie dátových centier a distribučné prepínače.

Takýto centrálny kostrový prepínač agreguje distribučné prepínače v jednotlivých blokoch fakulty, vzájomne prepojených LACP prepojmi o rýchlosti 2 x 40GE pomocou technológie Multichassis Etherchannel(MEC).

Dátové centrum by bolo pripojené na kostrovú vrstvu cez 2 x 100GE rozhrania.

Prepínače by mali podporovať automatické riadenie a nastavovanie v softvérovo definovanej sieti, vedieť posielať telemetrické merania pre optimálne prestavenie siete v reálnom čase a vedieť detegovať problémové nastavenia v sieti pre rýchlu diagnostiku problémov pripojenia v sieti.

Samozrejmosťou by mali byť redundantné napájacie zdroje a ventilátory, všetky podporujúce hot-swap (výmenu komponentov počas behu zariadenia).

Odporúčané parametre pre kostrové prepínače sú uvedené v dokumente Opis_pozadovanych_zariadeni_s_fazami_VV.xlsx, v záložke Kostrovy_prepinač. Odporúčame nasadiť dva kusy kostrových prepínačov.

3.4 DISTRIBUČNÁ VRSTVA

Úlohou distribučnej vrstvy je agregovať spojenia z prepínačov prístupovej vrstvy a zabezpečovať rýchle prepojenie na kostrovú vrstvu. Nakoľko agregujú značný počet prístupových prepínačov, je dôležité, aby sa jednalo o spoľahlivú, tzv. fault tolerant architektúru s vysokou priepustnosťou.

Distribučné prepínače na jednotlivých blokoch navrhujeme vytvoriť dvojicou prepínačov tvoriacich jeden logický prepínač (single control plane). Prepínače by mali poskytovať vyššiu hustotu optických portov (minimálne 24), s podporou rýchlosti 1/10/25GE na access portoch, a 40/100GE na uplink portoch.

Samozrejmosťou budú prepojenia na kostrovú vrstvu a prepojenia z prístupových prepínačov cez LACP a MEC.

Prepínače by mali byť schopné spúšťať priamo na prepínači kontajnerizované aplikácie tretích strán pre rozšírenie funkcionality (napr. performance monitoring, resp. bezpečnostné aplikácie), a mali by podporovať skriptovací programovací jazyk Python.

Prepínače by mali podporovať automatické riadenie a nastavovanie v softvérovo definovanej sieti, vedieť posielať telemetrické merania pre optimálne prestavenie

siete v reálnom čase a vedieť detegovať problémové nastavenia v sieti pre rýchlu diagnostiku problémov pripojenia v sieti.

Odporúčané parametre pre distribučné prepínače sú uvedené v dokumente Opis_pozadovanych_zariadeni_s_fazami_VV.xlsx, v záložke Distribučný_prepínač. Odporúčame nasadiť dva kusy distribučných prepínačov v každom agregačnom rozvídzači na prízemí blokov, t.j. 12ks distribučných prepínačov.

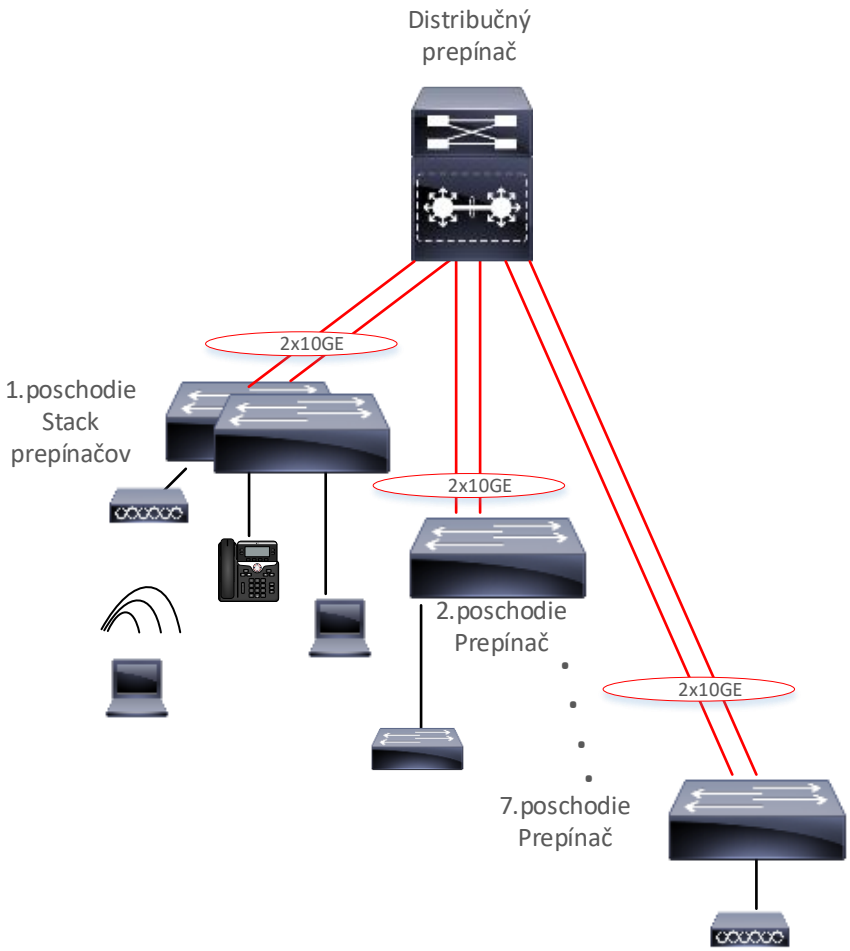
3.5 PRÍSTUPOVÁ VRSTVA

3.5.1 LAN

Úlohou prístupovej vrstvy je zabezpečiť vysokú hustotu portov určených pre klientske stanice, IP telefóny, bezdrôtové prístupové body a iné koncové body (kamery, čítačky kariet a pod.). Samozrejmosťou by mala byť podpora napájania zariadení cez ethernet (PoE),

Na základe vyššie spomenutých informácií by prístupové prepínače podľa požiadavky na počet portov mali mať 24, resp. 48 100/1000 Base-T portov s plnou podporou pre PoE+ štandard na každom porte, s optickými uplink portami podporujúcimi 10GE pripojenie na distribúciu . Prepínače by mali byť schopné vytvoriť stoh prepínačov tvoriacich jeden logický celok (single control plane) v prípade potreby vysokej hustoty portov.

Prístupové prepínače budú umiestnené na každom poschodí v rámci bloku, a budú redundantným optickým prepojom pripojené na distribučný prepínač umiestnený na prízemí bloku (cez 2x10GE).



Obrázok 3 Pripojenie prístupových prepínačov na distribúciu

Prístupové prepínače by mali podporovať automatické riadenie a nastavovanie v softvérovo definovanej sieti, vedieť posielať telemetrické merania pre optimálne prestavenie siete v reálnom čase a vedieť detegovať problémové nastavenia v sieti pre rýchlu diagnostiku problémov pripojenia v sieti.

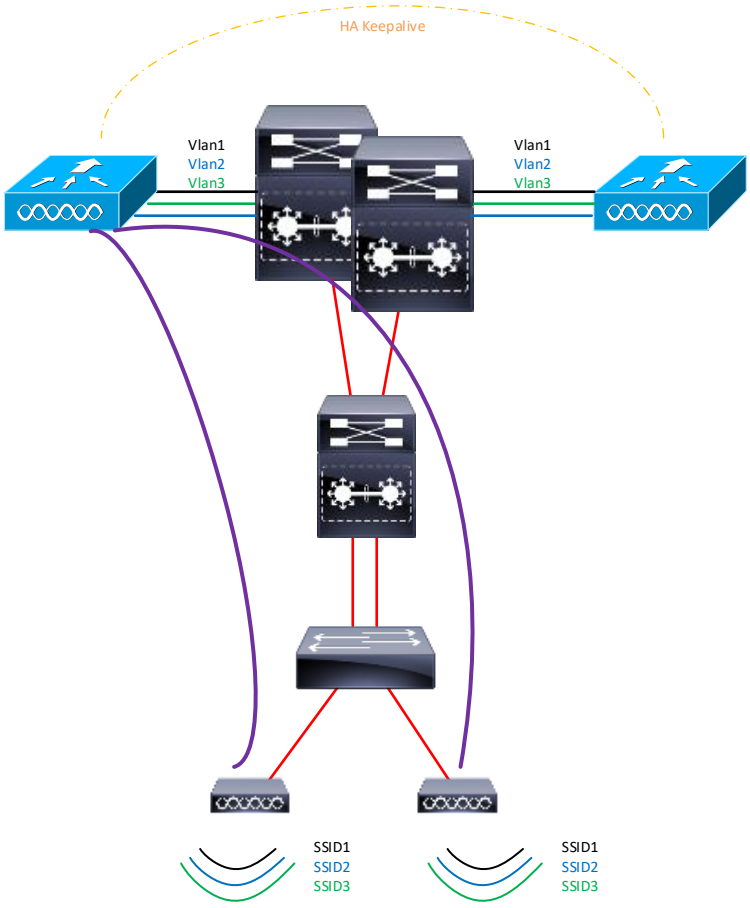
Odporúčané parametre pre prístupové prepínače sú uvedené v dokumente Opis_pozadovanych_zariadeni_s_fazami_VV.xlsx, v záložke Prístupový_prepínač. Odporúčame nasadiť jeden prístupový prepínač v každom koncovom rozvádzači, a to 48 portový, kde sa nachádza 42U rozvádzač, resp. 24 portový v uzloch, kde sa nachádza malý rozvádzač. v, t.j. celkovo 25 24-portových a 21 48-portových prepínačov.

3.5.2 Bezdrôtová sieť

Predĺžením dosahu sieťovej konektivity prístupovej vrstvy pre koncové systémy je bezdrôtová sieť. Niektoré, v súčasnosti používané komponenty bezdrôtovej infraštruktúry sa už nepredávajú, resp. majú vyhlásený End of Sale, napriek tomu sú stále výrobcom podporované a ešte niekoľko rokov podporované budú.

Preto odporúčame pokračovať v pokrytí budov FEI STU bezdrôtovým wifi signálom poskytujúcim pripojenie do LAN siete pomocou dvojice centrálnych riadiacich prvkov bezdrôtových prístupových bodov s plnou podporou pre sa štandard WiFi-6 (802.11 ax).

Dva bezdrôtové kontroléry budú tvoriť HA pár, kde na aktívny prvok budú zaregistrované všetky prístupové body v centrálnom režime. Sekundárny kontrolér bude v stave hot standby kde v prípade výpadku aktívneho kontroléra vďaka riešeniu Statefull switchover preberie registráciu všetkých AP na seba bez výpadku klientskych spojení.



Obrázok 4 Zapojenie bezdrôtových kontrolérov

Nové bezdrôtové kontroléry by mali poskytovať možnosť spolupracovať so súčasným riešením a zabezpečovať hladký, bezproblémový roaming klientov medzi prístupovými bodmi ukončenými na nových a starých kontroléroch (tzv. IRCM).

Novo implementované bezdrôtové prístupové body budú podporovať štandard 802.11 ax, t.j. budú podporovať všetky potrebné funkcie ako:

- Uplink/downlink OFDMA
- BSS coloring
- MU-MIMO
- Target wake time
- Modulácia 1024 QAM
- Podpora WPA3

Odporúčame dva typy prístupových bodov umiestnených v priestoroch:

- s vysokou koncentráciou užívateľov – prízemie + prednáškové sály, prístupové body s internými anténami s podporou technológie FRA (flexible radio asignment, dual 5GHz radio), rádia v konfigurácii až do 4x4:4 a samostatný RF ASIC pre analýzu bezdrôtového prostredia. Minimálna kombinovaná prenosová rýchlosť na AP je 5Gbps.
- s nižšou koncentráciou užívateľov – poschodia jednotlivých blokov, prístupové body s internými anténami s rádiami v konfigurácii 2x2:2.

Celé riešenie by malo podporovať automatickú ochrana pred interferenciami v sieti, možnosť vizualizovať body rušenia a automaticky mitigovať rouge AP v sieti, kde neautorizovaný užívateľ v sieti narušuje rádiové vysielanie a môže tak zvýšiť riziko výpadkov siete.

Odporúčané parametre pre bezdrôtový kontrolér sú uvedené v dokumente Opis_pozadovanych_zariadeni_s_fazami_VV.xlsx, v záložke WLC. Odporúčame 2 kusy kontrolérov.

Odporúčané parametre pre bezdrôtový prístupových bodov sú uvedené v dokumente Opis_pozadovanych_zariadeni_s_fazami_VV.xlsx, v záložke AP_high (40 ks s vysokou koncentráciou užívateľov) a AP_low (87ks s nižšou koncentráciou užívateľov).

3.6 DÁTOVÉ CENTRUM

V dátových centrách (DC) odporúčame nasadenie dvojice prepínačov tvoriacich spolu jeden data plane podporujúcich 100 GE rozhrania na uplink portoch smerujúcich do LAN siete. Pre pripojenie serverov, resp. pre pripojenie zdieľaných diskových úložísk budú slúžiť optické rozhrania 10/25 Gbps.

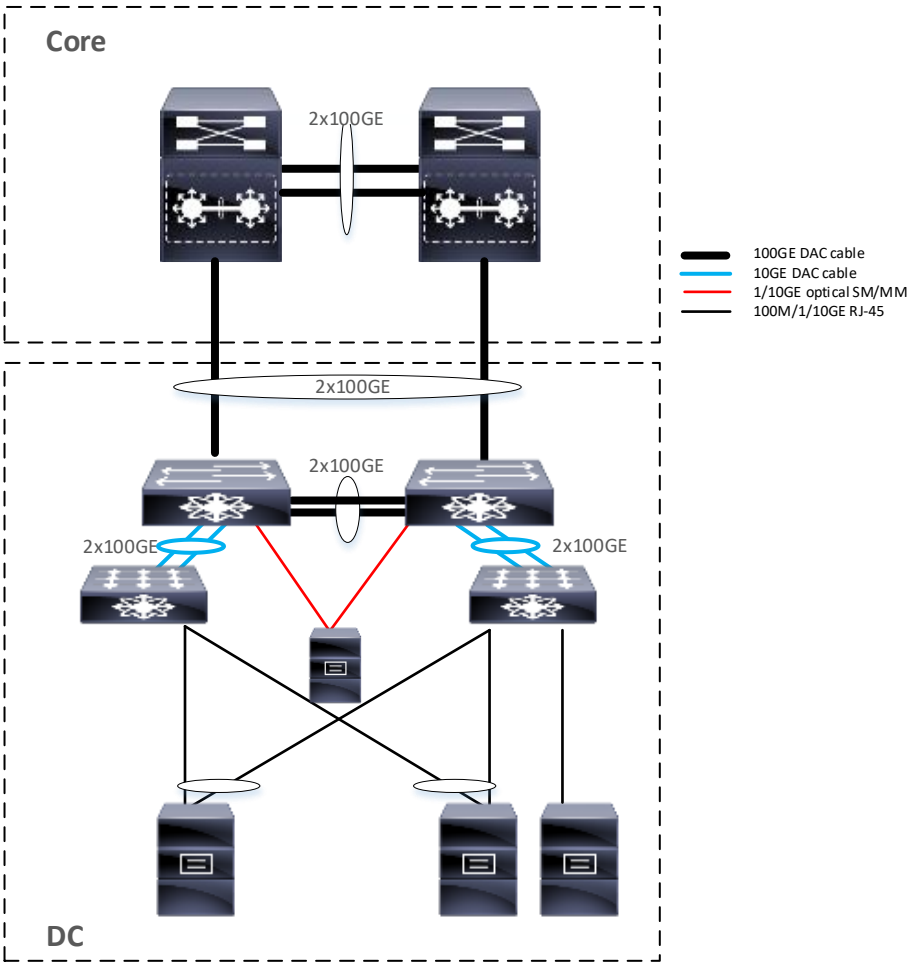
Prepínače by mali poskytovať funkcionality ako je napr. podpora RoCE, LAN a SAN konvergenciu, MAC Sec,, pokročilé L3 protokoly (OSPF, BGP, PIM-SM, SSM), podporu SDN a pod.

V DC odporúčame nasadenie dvojice prepínačov umožňujúcich redundantné pripojenie koncových zariadení (serverov, dátových úložísk) v móde active/active , t.j. vytváranie LACP spojenia cez dvojicu prepínačov (MEC).

Uplink prepojenie na kostru siete je realizované cez 2x100 GE rozhrania, vzájomné prepojenie DC prepínačov by malo byť realizované cez 2x100 GE prepoj (AOC káble).

Keďže nie všetky súčasné zariadenia v DC FEI STU podporujú optické rozhrania, a aj v budúcnosti bude vždy potreba RJ-45 rozhraní, DC prepínače budú rozšírené o prepínače podporujúce metalické rozhrania 100M/1/2.5/5/10GE, s ktorými budú tvoriť jeden logický celok. Vzájomné prepojenie týchto rozširujúcich prepínačov na DC, tzv. rodičovské prepínače bude realizované cez 100GE rozhrania. Samozrejmosťou je podpora active/active pripojenia koncových systémov aj cez rozširujúce prepínače.

Odporúčané parametre pre DC prepínače sú uvedené v dokumente Opis_pozadovanych_zariadeni_s_fazami_VV.xlsx, v záložke DC_prepínač, a ich rozširujúcich prepínačov v záložke DC_-rozširujúci prepínač. Odporúčame nasadiť dva DC prepínače a dva rozširujúce prepínače.



Obrázok 5 Schematické zapojenie DC

4 MANAŽMENT SIEŤOVEJ INFRAŠTRUKTÚRY

V riešení navrhujeme manažmentovový nástroj na správu drôtovej a bezdrôtovej siete, ktorý môže pomôcť podporiť komplexnú správu sieťových technológií a služieb, ktoré sú rozhodujúce pre fungovanie organizácie. Manažovací nástroj bude poskytovať intuitívne webové grafické používateľské rozhranie (GUI), ku ktorému je možné pristupovať odkiaľkoľvek v rámci siete a poskytuje úplný prehľad o stave a využívaní siete.

Manažovací nástroj poskytuje komplexnú správu životného cyklu, prehľadnosť zabezpečenia a možnosti riešenia problémov v rámci siete - od používateľa vo vzdialenej lokalite, cez sieť WAN až po dátové centrum, umožňuje efektívnejšie a efektívnejšie spravovať sieť, takže môžete dosiahnuť najvyššiu úroveň výkonu káblovej a bezdrôtovej siete, zabezpečenie služieb a spokojnosť koncových používateľov so zameraním na aplikácie.

Manažment by mal poskytovať:

- Manažment HW a SW inventáru, centralizované konfiguračné nástroje a syslog.

- Monitorovanie a zaznamenávanie odoziev a dostupnosti siete.
- Real– time manažment zariadenia a linky ako aj manažment prevádzky na porte, analýzu a reporting.
- Objavovanie nových zariadení v sieti, pohľady na topológiu, sledovanie koncových zariadení.
- Centralizovaný systém pre zber a zdieľanie informácií o zariadeniach naprieč konvergovanou sieťou, všetkými manažment aplikáciami a zvýšenie vedomosti o zmenách v sieti.
- Analýzu chýb v reálnom čase v sieti s ľahko nasaditeľnými vzormi podľa zariadení zohľadňujúcimi best practice.
- Workflow engine, ktorý poskytuje návody krok za krokom pre systémové nastavenie a riešenie problémov zariadení.
- Zvýšenie celkovej dostupnosti siete zjednodušením konfigurácie a rýchlej identifikácie a nápravy sieťového problému.
- Maximalizovanie bezpečnosti siete s využitím integrácie so servismi kontrolu prístupu a auditu zmien na úrovni siete.
- Eliminácia a skrátenie výpadkov kritických IT služieb.
- Vytvorenie koncepcií štandardného monitoringu pre jednotlivé oblasti podpory a zefektívnenie práce pracovníkov dohľadového centra ako aj získavanie vstupných údajov pre SLM.
- Získanie a vyhodnotenie údajov pre kapacitné plánovanie konvergovanej siete.
- Grafické znázornenie pokrytia importovaných pôdorysov budov bezdrôtovým signálom.
- Zobrazovanie aktuálneho stavu zariadení WLAN siete ako aj štatistiky využívania WLAN siete.

Odporúčaná funkcionalita pre manažment sieťovej infraštruktúry je uvedená v dokumente Opis_pozadovanych_zariadeni_s_fazami_VV.xlsx, v záložke Manažment.

5 BEZPEČNOSTNÁ INFRAŠTRUKTÚRA

V rámci bezpečnostnej infraštruktúry sa bude riešiť obnova alebo nasadenie kontroly niekoľkých oblastí:

- Doplnenie HA firewall riešenia

Do budúcna navrhujeme sa zamyslieť aj nad nadstavbami bezpečnostného riešenia, ako sú napríklad:

- Ochrana mail komunikácie.
- Ochrana web komunikácie.
- Ochrana na úrovni DNS.

5.1 FIREWALL

Firewall, ako hlavný bod vstupu do komunikačnej infraštruktúry FEI STU odporúčame doplniť o redundantnú jednotku, ktorá by pracovala so súčasným firewallom v režime Active/Standby pre zabezpečenie vysokej dostupnosti. t.j. v prípade výpadku primárneho prvku by bez výpadkov prevzala všetky otvorené spojenia. Rovnako navrhujeme rozšíriť funkcionalitu s použitím technológie NGFW (next generation firewall) FTD (Firepower Threat Defense).

Funkcie realizované na vyslednom firewall riešení:

- Základná statefull ochrana realizovaných komunikačných tokov.
- IPS
- Ukončovanie VPN pripojení pre vzdialených pracovníkov (RA VPN).
- Ukončovanie L2L VPN pripojení (aktuálne sa nepoužíva), ak by v budúcnosti táto požiadavka vznikla.
- Ochrana proti malware (anti malware protection).
- Manažment tohto FW realizovaný cez dedikovaný manažment server (korelácia logov a udalostí, informácie a type a objeme realizovanej komunikácie atď).

Pre vytvorenie Active/standby zapojenia je potrebné implementovať zhodný firewall, ako je v súčasnosti implementovaný, t.j. Cisco Firepower FPR2130-NGFW-K9 s Threat Defense Threat Protection License (3Y).

5.2 OCHRANA MAIL KOMUNIKÁCIE

Ochrana mailovej komunikácie navrhujeme cez bezpečnostné mail brány umiestnené v DMZ sieti ako prvok vložený medzi vonkajšie mail servery v Internete a interné mail servery fakulty. Navrhujeme použitie mailových brán ako fyzických serverov z riešenia Cisco ESA (Email Security Appliance).

Výhodami využitia technológie ESA s použitím virtualizácie sú:

- Vysoký stupeň ochrany pred nežiadúcou mail komunikáciou
- Vysoký podiel zachytených nežiadúcich mailov “catch rate” – na úrovni 97%.

- Nízke percento tzv. “false-positive”.
- Ochrana proti malware v mail komunikácii
- Vysoké percento zachytených malware mailov pre tzv. “Day Zero” útoky.
- Analýza neznámych súborov.
- Centralizovaná karanténa pre používateľov na dedikovanom serveri.
- Nezávislosť na špecifickom HW, v prípade potreby vyššieho výkonu možnosť navýšenia zdrojov alebo vytvorenie novej inštancie virtuálne ESA servera.

Z pohľadu zapojenia do sieťovej komunikácie by riešenie bolo nasadené podobne ako fungujú súčasné mail servery, kedy by v DNS zázname boli na tieto servery namapované MX definície.

5.3 OCHRANA WEB KOMUNIKÁCIE

Ochrana web komunikácie používateľov je navrhovaná cez bezpečnostné web brány zapojené v DMZ sieti ako medzičlánok v komunikácii do siete Internet. Navrhujeme použitie web brán ako fyzických serverov z produktovej rodiny Cisco WSA (Web Security Gateway).

- Výhodami využitia WSA s použitím virtualizácie sú:
- Možnosť fungovania v režime transparentného proxy.
- Možnosť fungovania v režime explicitného proxy.
- Pravidlá pre filtrovanie na základe URL alebo kategórie URL.
- Kategorizáciu URL realizuje permanentne výrobca technológie, jej výsledky sú aplikované na WSA platformy pravidelne.
- Anti-malware ochrana.
- SSL offload – v prípade potreby je možné rozbaliť a prekontrolovať SSL komunikáciu.
- Identifikácia útokov na základe štatistického modelovania a dynamického učenia v čase.
- Centralizovaný manažment politík na dedikovanom manažment server.

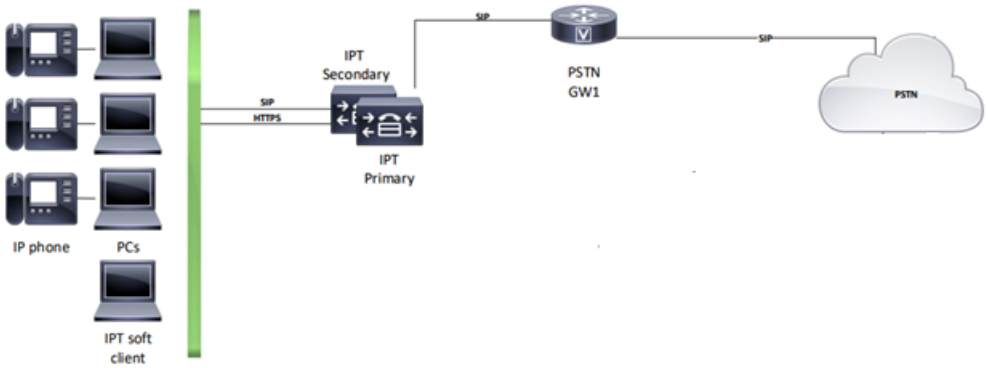
Pre niektoré platformy alebo toky je výhodnejší využitie systému explicitného proxy, pre iné (guest access) transparentného proxy. Výhodou je možnosť využitia oboch mechanizmov v jednom čase.

6 IPT PLATFORMA

Pre obnovu tradičnej PBX telefónie bude zvolené riešenie postavené na IP, ktoré poskytuje viaceré výhody, ako napríklad:

- Využitie rovnakej kabeláže pre PC a IPT
- Integrovaný prepínač v telefóne umožňuje zapojit koncové PC za telefón – šetrí porty na prístupovom prepínači
- Napájanie telefónov z prepínača pomocou PoE
- Flexibilita nastavení na softvérovej ústredni
- Redundancia ústredne
- podpora jednotného prihlásenia sa do systému (SSO)
- natívna podpora IM (Instant Messaging)
- podpora video-telefónie
- podpora šifrovania hovorov aj s certifikátmi podnikovej certifikačnej autority
- zdieľanie telefónnych klapiek

Správne nasadenie IPT riešenia pozostáva z hlasovej brány, systému centrálnej logiky a koncových zariadení.



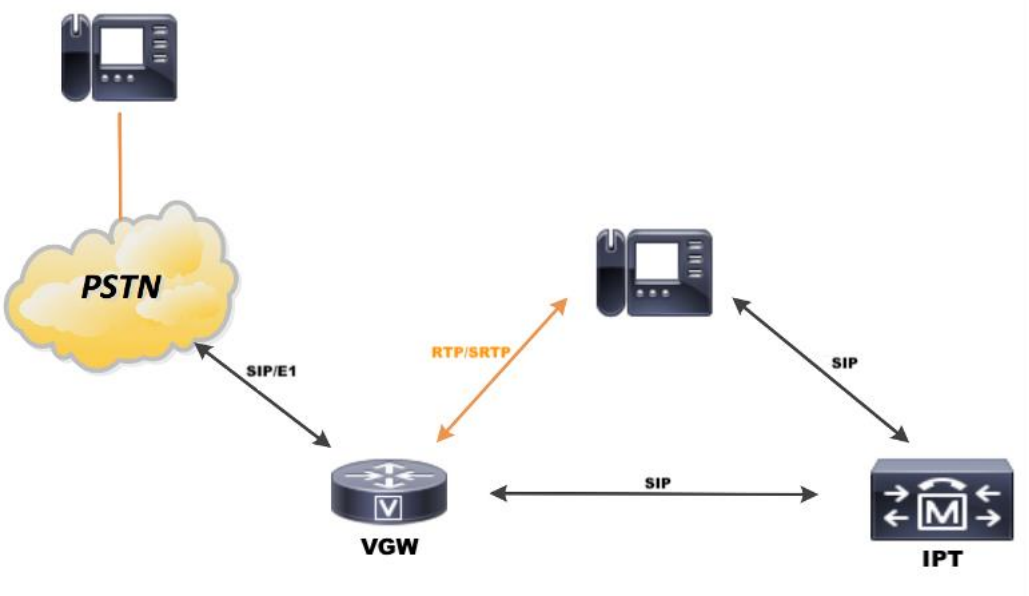
Obrázok 6 Schematické zapojenie komponentov IPT

6.1 HLASOVÁ BRÁNA

Na prestup do PSTN (verejnej telefónnej siete) bude potrebné zariadenie, a to hlasový smerovač, ktorý zabezpečí IP komunikáciu voči poskytovateľovi hlasových služieb.

Prepoj s operátorom (poskytovateľom verejnej telefónnej siete) sa predpokladá prostredníctvom SIP trunk-u.

Pre tieto potreby navrhujeme hlasovú bránu - smerovač, ktorý je licenčné nastavený tak, aby umožňoval paralelne 30 hlasových spojení s operátorom. Daný prvok nie je licenčne ani hardvérovo nastavený redundantne. Hlasové brány budú nakonfigurované ako vstupno / výstupné zariadenia z/do PSTN.



Obrázok 7 Znázornenie komunikácie externého hovoru na IP telefón

Obrázok znázorňuje prípad ak volajúci z ľubovoľného telefónu v PSTN sieti volá do IPT systému. Hlasová brána využíva SIP/E1 rozhranie pre prichádzajúce a tiež odchádzajúce hovory smerom k poskytovateľovi hlasových služieb. Okrem tohto pripojenia bude mať hlasová brána aj IPT prepojenie potrebné pre správne smerovanie hovorov, a to SIP trunk. Po prijatí hovoru bude mať IP telefón nadviazané dve pripojenia, registračné pomocou SIP protokolu na IPT a média pripojenie na telefón volajúceho s využitím RTP resp. SRTP protokolu.

6.2 SYSTÉM CENTRÁLNEJ LOGIKY

Návrh komunikačnej platformy sa dá logicky rozdeliť na tri základné prvky:

- hardvérová platforma
- softvérové riadiace entity

Tieto prvky sú medzi sebou prepojené a navzájom sa dopĺňajú. Pri ich výbere boli zohľadnené a dodržané výrobcom definované požiadavky a odporúčania. Vďaka tomu návrh garantuje kompatibilitu medzi jednotlivými prvkami a zároveň garantuje funkčnosť riešenia s ohľadom na dodržanie bezpečnostných odporúčaní.

Hardvérová platforma pozostáva z dvoch fyzicky na sebe nezávislých serverov. Hardvérová konfigurácia daných serverov je na základne výrobcom definovaných odporúčaní, pre komunikačné platformy do tisíc používateľov. Dané zariadenia laicky povedane slúžia ako „podvozok“ pre komunikačnú platformu. Sú dodávané nie len s výrobcom požadovaným a optimalizovaným výpočtovým výkonom ale aj s požadovaným virtuálnym prostredím ESXi 7.X. Charakteristika zariadení umožňuje od seba oddeliť prevádzkovú komunikáciu v rámci komunikačnej platformy a manažment komunikáciu hardvérovej platformy. Z dôvodu prerozdelenia prevádzkovej záťaže ale aj z dôvodu zvýšenia dostupnosti komunikačnej služby, návrh pozostáva z dvoch fyzických serverov. Za účelom zvýšenia dostupnosti služby sú servery okrem toho ešte dodávane so sekundárnymi zdrojmi.

Softvérové riadiace entity budú existovať vo virtuálnom prostredí v rámci dodávanej hardvérovej platformy. Vybraná hardvérová platforma umožňuje klastrové nasadenie (z dôvodu prerozdelenia záťaže a zvýšenia dostupnosti riešenia) virtuálnych entít CUCM, IM&P, EXP-C a EXP-E. Stručný popis a charakteristika daných virtuálnych entít je v nasledovnej tabuľke:

Entita	Základný popis zariadenia
CUCM	CUCM (Cisco Unified Communications Manager) je SIP IP PBX (Cisco telefónna a video ústredňa), pracujúca v režime B2B UA (Back-to-Back User Agent) a dá sa považovať za „srdce“ celého riešenia. CUCM je zodpovedný za registráciu Cisco zariadení do centrálneho riadiaceho systému, definuje hlavné konfiguračné parametre pre zariadenia a procesuje smerovanie hovorov.
IM&P	IM&P (Instant Messaging & Presence) je XMPP/SIP klaster, ktorý umožňuje softvérovým klientom Cisco Jabber výmenu rýchlych správ, súborov a sledovanie prezenčného status (online-offline-away-DND).
EXP-C	EXP-C (Cisco Expressway- CORE) je tzv. firewall traversal komponent - konkrétne jeho interná entita. Entita je potrebná pre SIP/H323 spojenia s externými subjektami (ako napr. Webex) prostredníctvom internetu ako napr. video hovory (nie hovory cez verejnú sieť). Entitu je možné použiť aj pre potreby pripojenia zariadenia do internej siete bez VPN (napr. SW klient Cisco Jabber). Obojsmerná video komunikácia, ktorá nemá zvyšovať bezpečnostné riziká, (otváranie príliš veľa portov na firewall-och) z pravidla vyžaduje riešenie bezpečného prechodu video prevádzky cez firewall - tzv. firewall traversal. EXP-C teda slúži pre účely bezpečného prístupu do internetu cez firewall, ako aj prijímanie video hovorov z internetu - t.j. spätný smer. Tento prístup je potrebný napr. pre potreby B2B (Business-to-Business) hovorov s externými subjektami.
EXP-E	EXP-E (Cisco Expressway- EDGE) je tzv. firewall traversal komponent - konkrétne jeho externá entita. Celé riešenie bezpečného prechodu cez firewall totiž pozostáva z 2 entít - internej (EXP-C) a externej (EXP-E), ktoré využívajú podobných princípov fungovania ako je koncept reverzného proxy servera. Spolu s EXP-C, EXP-E zabezpečuje uskutočňovanie a príjem B2B hovorov s externými subjektami. EXP-E je v tomto riešení jediná entita ktorá disponujú verejnou IP adresou a má priamu konektivitu do internetu (či už majú alokovanú priamo verejnú IP adresu, alebo majú 1:1 statický NAT na definovanú verejnú IP adresu). Pre bezpečnú šifrovanú prevádzku vyžaduje bezpečnostný certifikát podpísaný verejnou certifikačnou autoritou (daný certifikát nie je súčasťou dodávky).

Jednotlivé komponenty (riadiace entity ale aj koncové komunikačné zariadenia) je možné medzi sebou bezpečne a šifrovane prepojiť prostredníctvom HTTPS, TLS a SRTP štandardov. Licenčne je platforma nastavená formou subskripcie na 36 mesiacov pre 400 zariadení. Za zariadenie môžeme počítať Cisco IP telefón alebo softvérového klienta Cisco Jabber. Platforma je bezpečne prepojiteľná s Webex cloud platformou.

6.3 KONCOVÉ ZARIADENIA

Ako koncové komunikačné zariadenia navrhujeme dve kategórie telefónov. Jeden typ pre bežného užívateľa, druhý, manažérsky pre vybraných užívateľov, resp. pre asistentov (resp. vrátnikov), keďže by vedel podporovať aj rozširujúce, asistentské moduly. Stručná charakteristika daných zariadení je v nasledovnej tabuľke:

Užívateľský telefón:

Parameter	
Obrázok	
Displej	Čiernobiely, 3,5“ 396x162 pixel
Zabudovaný prepínač	10/100/1000
Programovateľné tlačidlá	4
POE class	1

Manažérsky telefón:

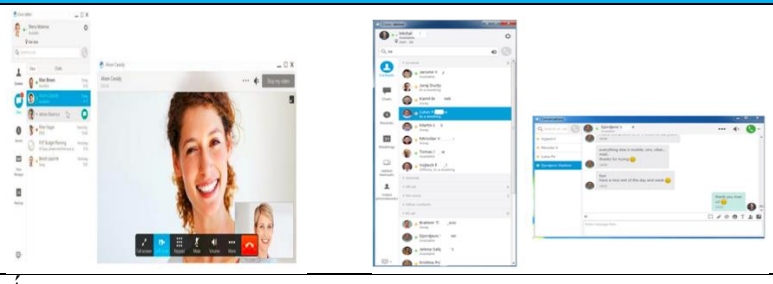
Parameter	
Obrázok	
Displej	farebný, 5“ 800 x 480
Zabudovaný prepínač	10/100/1000
Programovateľné tlačidlá	5
POE class	3
Podpora video	NIE
Podpora rozširujúci panel	8800 A KEM

Rozširujúci modul:

Parameter	
Obrázok	
Displej	Farebný, 3,5“ 320x480
Počet stánok	2
Programovateľné tlačidlá na jednu stránku	14
Prepojiteľnosť	Cisco IP Phone 8851 a 8861

Ako alternatívu k stolovému IP telefónu môže byť použitý softvérový IP telefón. Softvérový klient je aplikácia pre zjednotenú komunikáciu, ktorá zjednodušuje komunikáciu a zvyšuje produktivitu zjednotením funkcií zabezpečenia, zasielania

správ, videa, hlasu, hlasových správ, zdieľania obrazovky a konferencií bezpečne do jedného klienta na osobnom počítači. Aplikácia softvérového klienta pre podporované operačné systémy poskytuje vysoko bezpečnú a spoľahlivú komunikáciu. So softvérovým klientom je možné efektívne komunikovať a spolupracovať odkiaľkoľvek, kde máte bezpečné pripojenie do materskej organizácie.

Parameter	
Obrázok	
Audio / Video hovory	Áno
Možnosť ovládať IP telefón	Áno
Možnosť vymieňania správ	Áno, v rámci platformy
Možnosť vymieňania súborov	Áno, v rámci platformy
Možnosť zdieľať obrazovku	Áno, v rámci platformy
Podpora	Windows 10 / MAC

7 NÁVRH POKRYTIA BEZDRÔTOVEJ SIETE

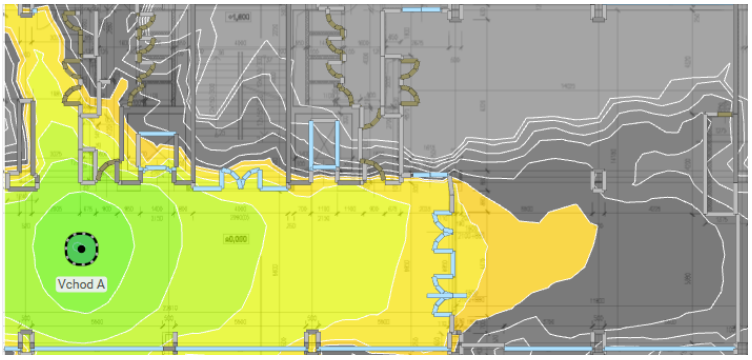
7.1 SIMULÁCIA POKRYTIA

Na základe simulácie pokrytia budovy FEI STU bezdrôtovým signálom bol vyhotovený návrh rozmiestnenia bezdrôtových prístupových bodov (AP) na jednotlivých poschodiach v blokoch FEI STU. Nasledujúce kapitoly zobrazujú pozíciu, kde by mali byť umiestnené bezdrôtové prístupové body a tabuľka zobrazuje sumár koľko prístupových bodov bude umiestnených v jednotlivých blokoch a poschodiach.

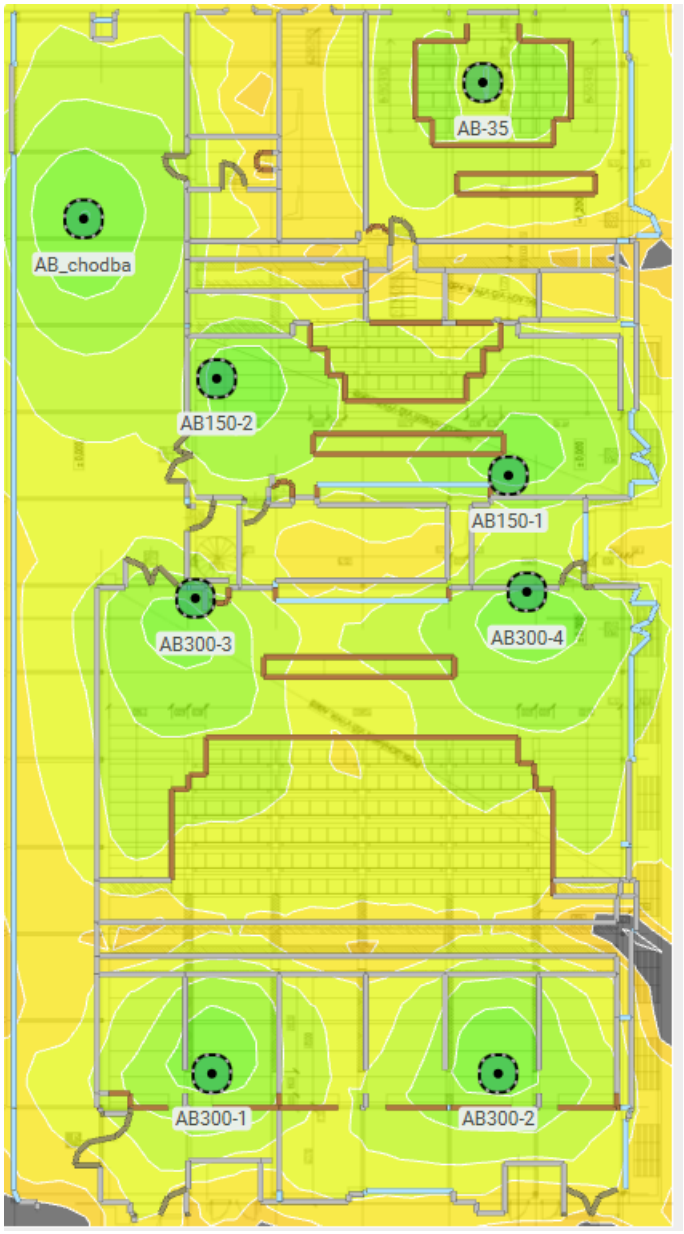
#Posch.	Blok A #AP	Blok B #AP	Blok C #AP	Blok D #AP	Blok E #AP	Blok T
Prizemie	9	9	12	7	1	5
1	6	5	6	5	6	
2	6	4	4	4	5	
3	4	3	3	3	4	
4	3	3	4	3	3	
5	3	2	3	2	3	
6	2	2	2	2	2	
7	2	2	2	3	2	
8	2		2			
Pocet AP	**37**	**30**	**38**	**29**	**26**	**5**

7.2 PRÍZEMIE

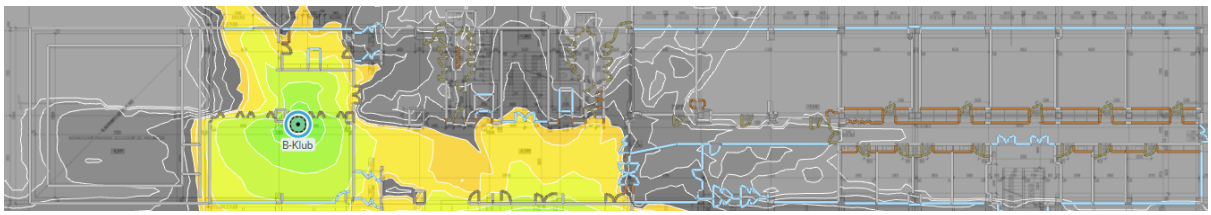
7.2.1 Blok A



7.2.2 Blok AB

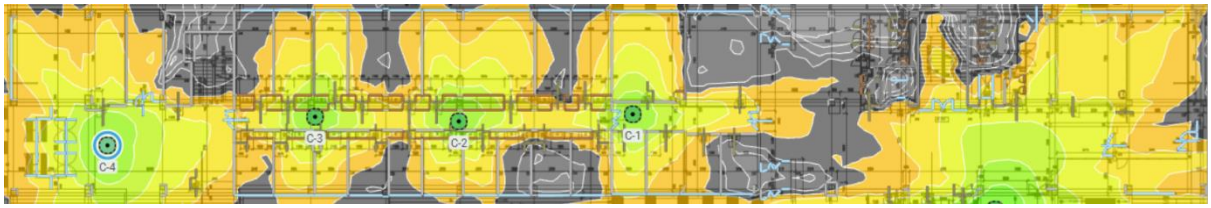


7.2.3 Blok B



7.2.4 Blok BC

7.2.5 Blok C

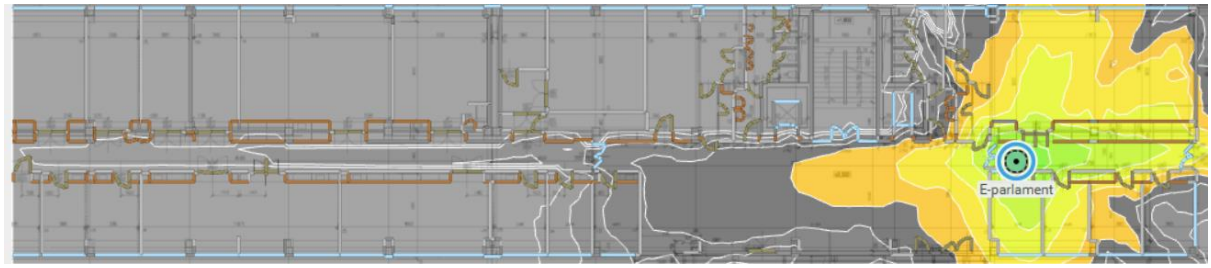


7.2.6 Blok CD

7.2.7 Blok D

7.2.8 Blok DE

7.2.9 Blok E

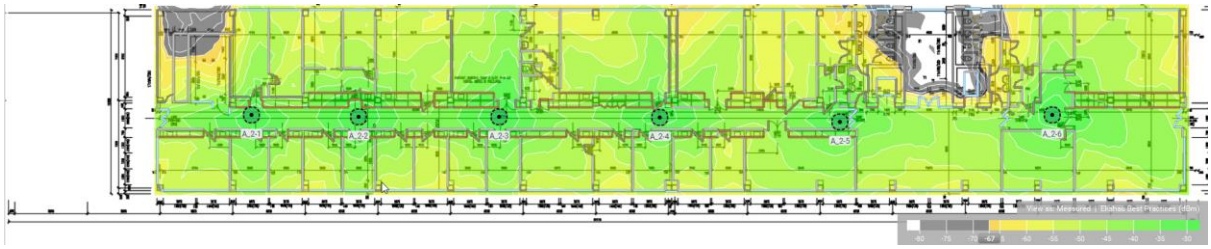


7.3 POSCHODIA

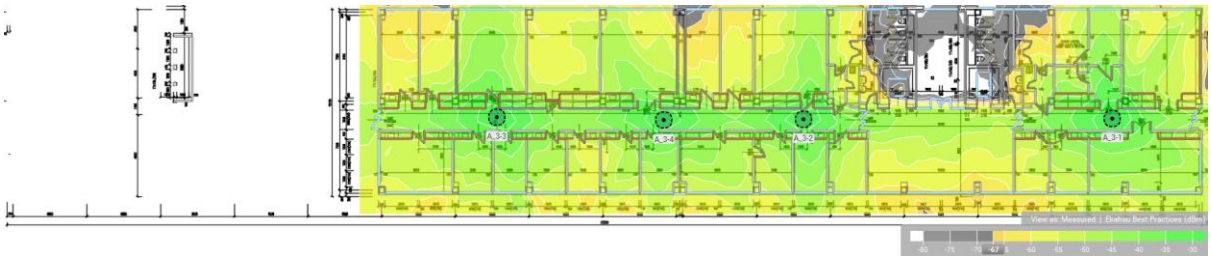
7.3.1 Blok A

7.3.2 1.Poschodie

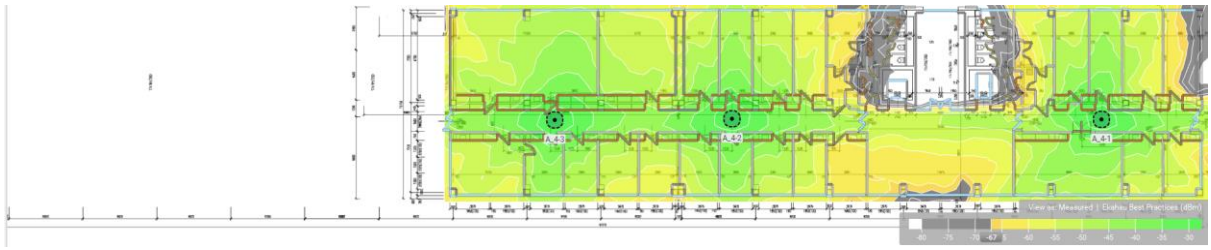
7.3.3 2.Poschodie



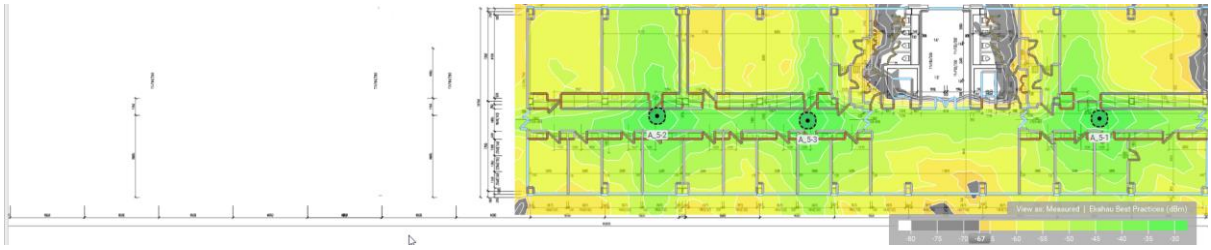
7.3.4 3.Poschodie



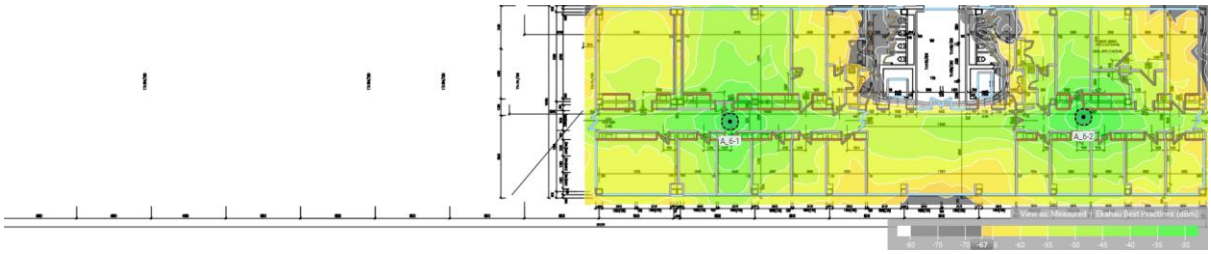
7.3.5 4.Poschodie



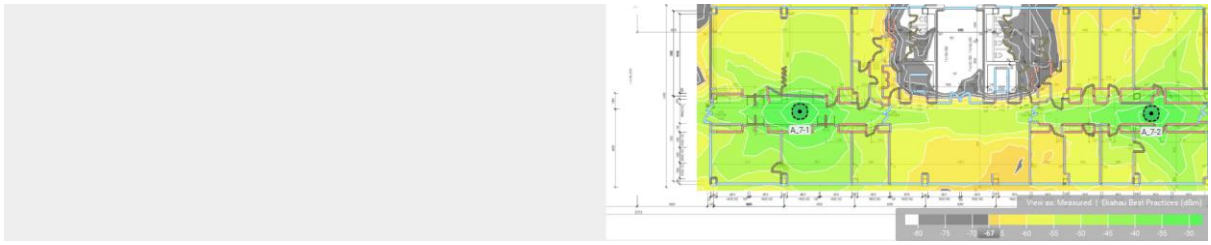
7.3.6 5.Poschodie



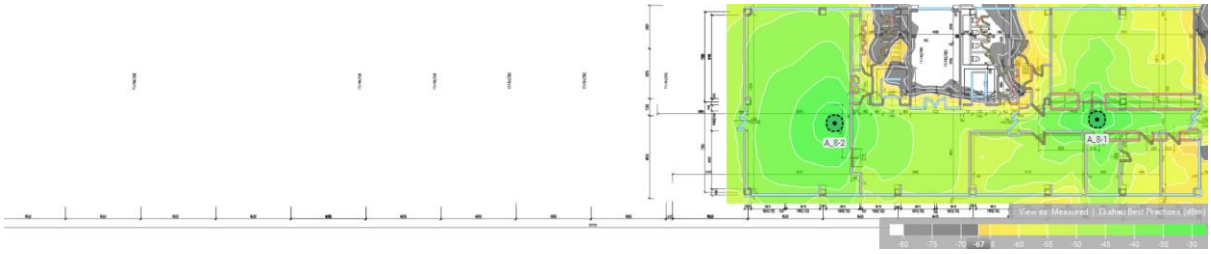
7.3.7 6.Poschodie



7.3.8 7.Poschodie

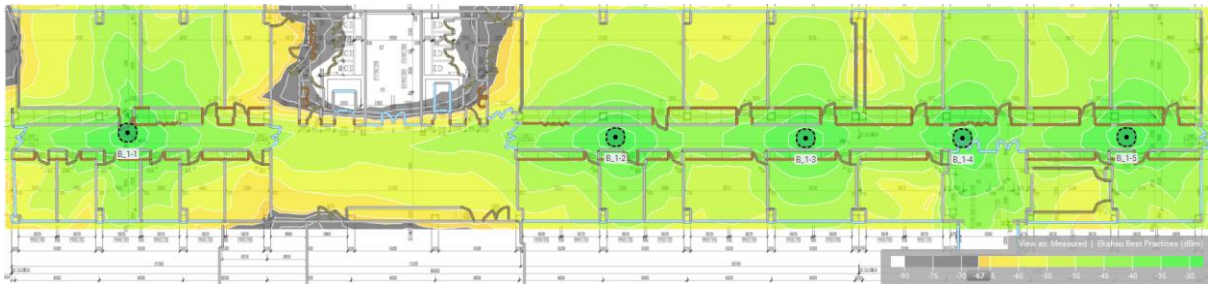


7.3.9 8.Poschodie

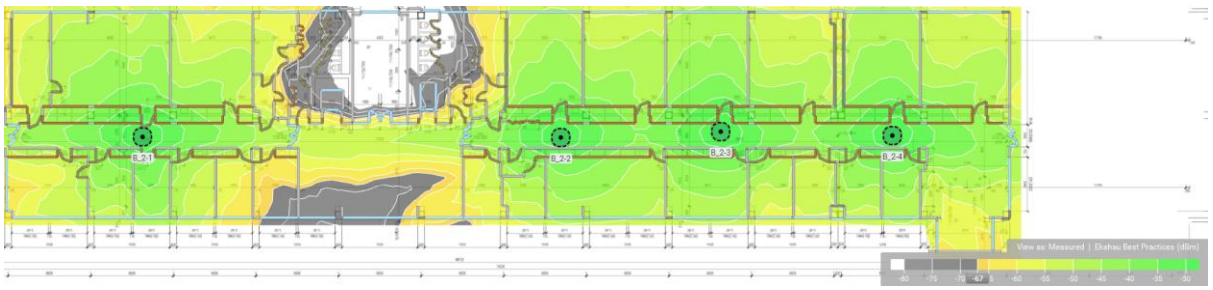


7.4 BLOK B

7.4.1 1.Poschodie

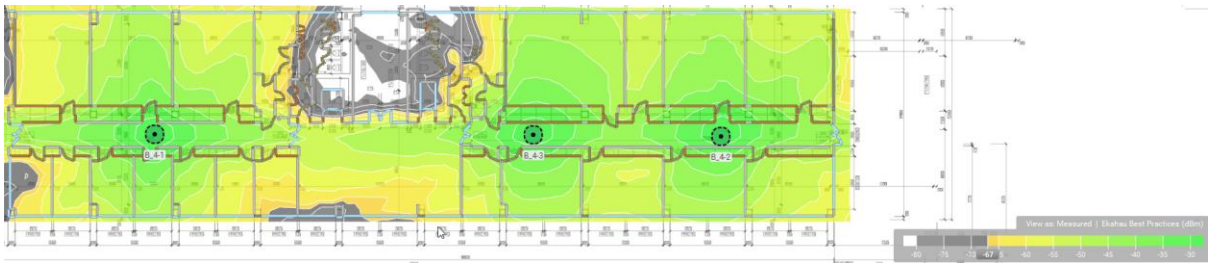


7.4.2 2.Poschodie

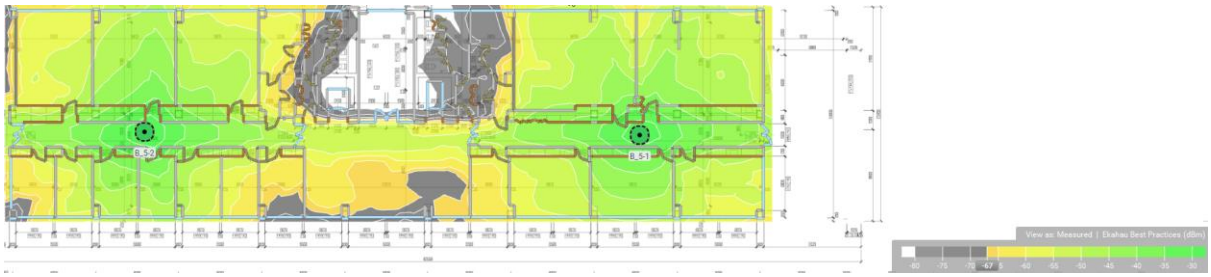


7.4.3 3.Poschodie

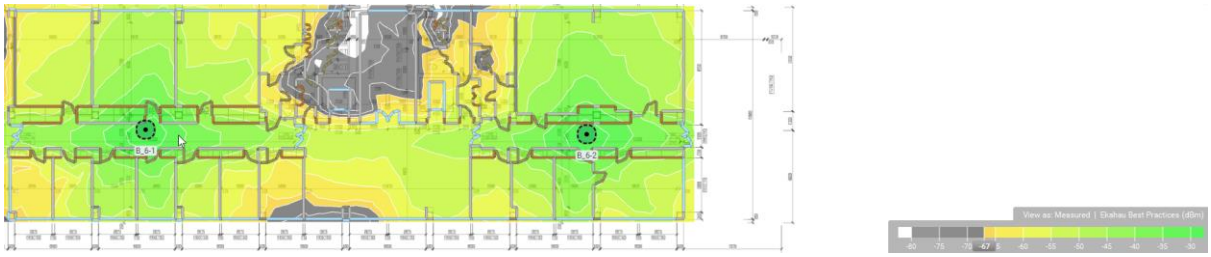
7.4.4 4.Poschodie



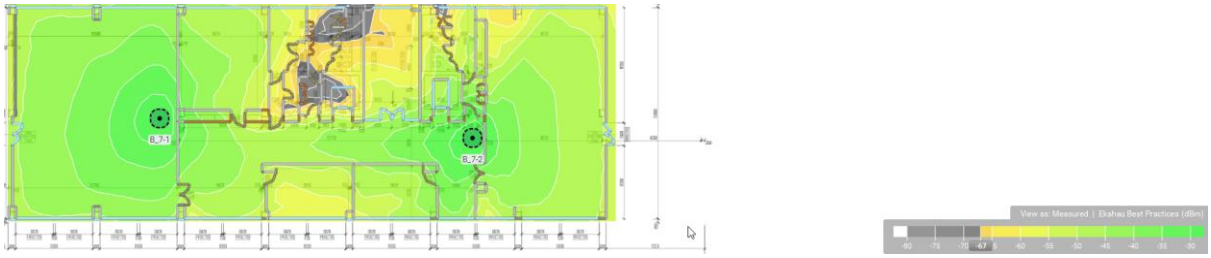
7.4.5 5.Poschodie



7.4.6 6.Poschodie

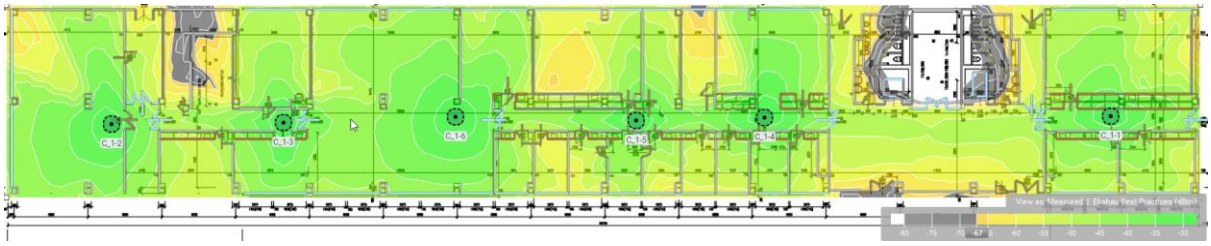


7.4.7 7.Poschodie

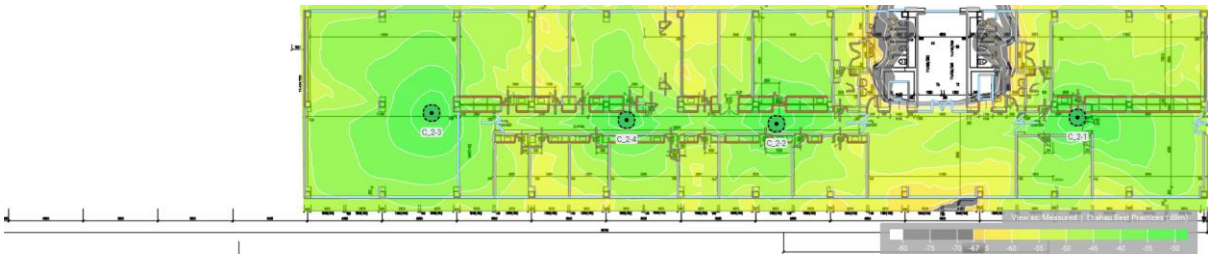


7.5 BLOK C

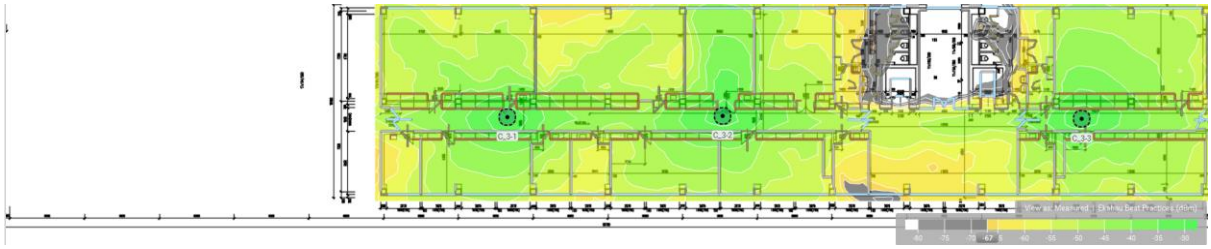
7.5.1 1.Poschodie



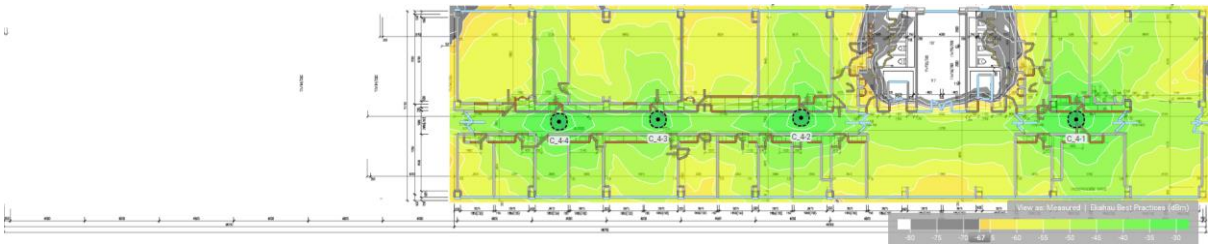
7.5.2 2.Poschodie



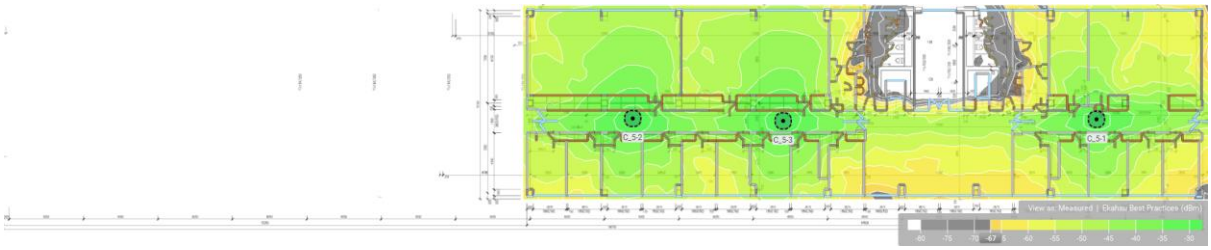
7.5.3 3.Poschodie



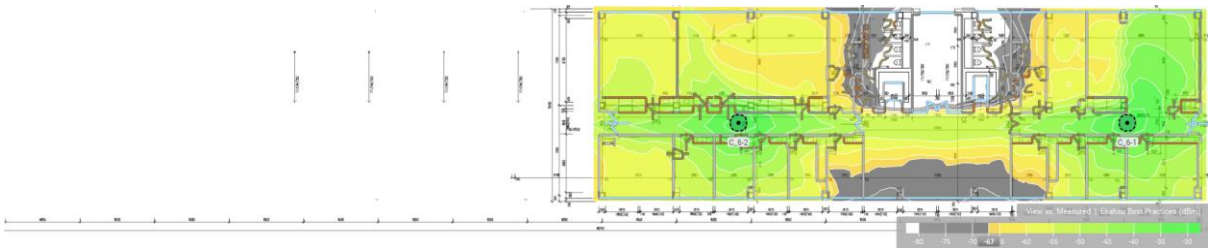
7.5.4 4.Poschodie



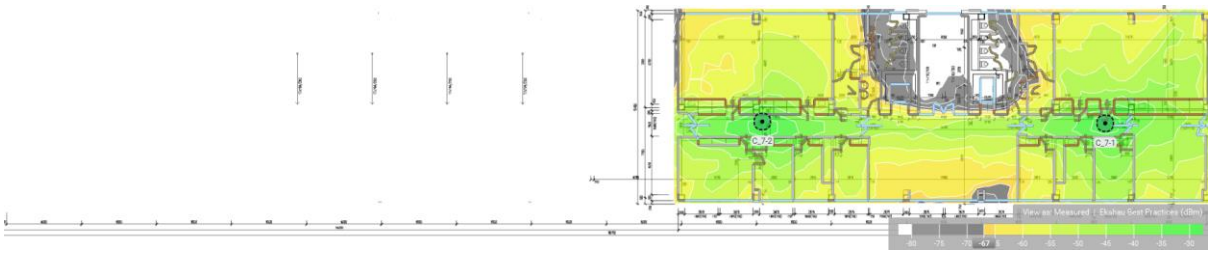
7.5.5 5.Poschodie



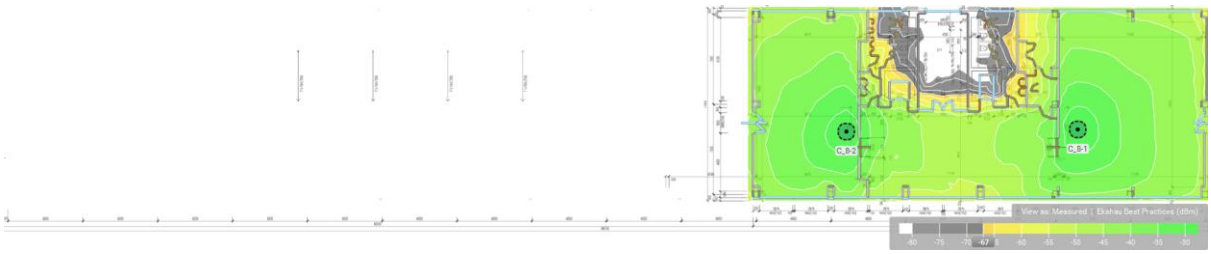
7.5.6 6.Poschodie



7.5.7 7.Poschodie

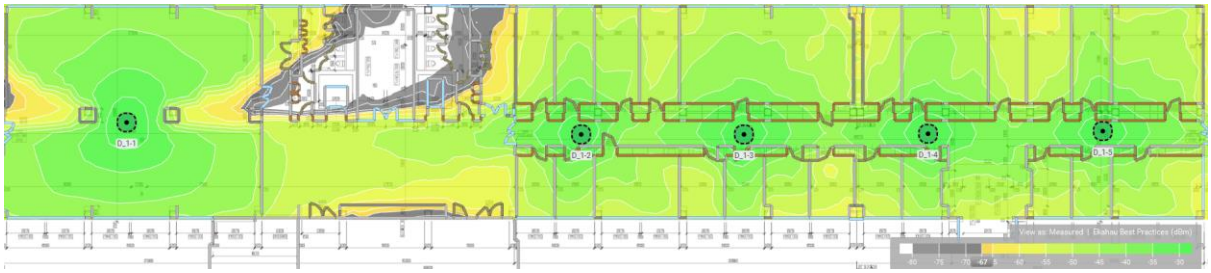


7.5.8 8.Poschodie

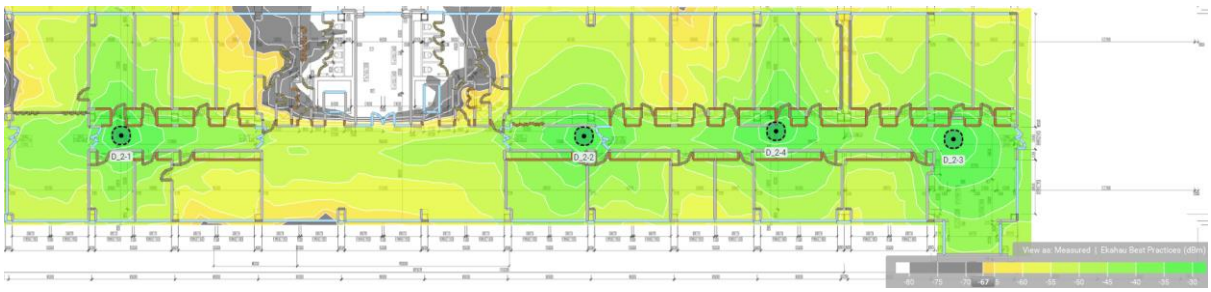


7.6 BLOK D

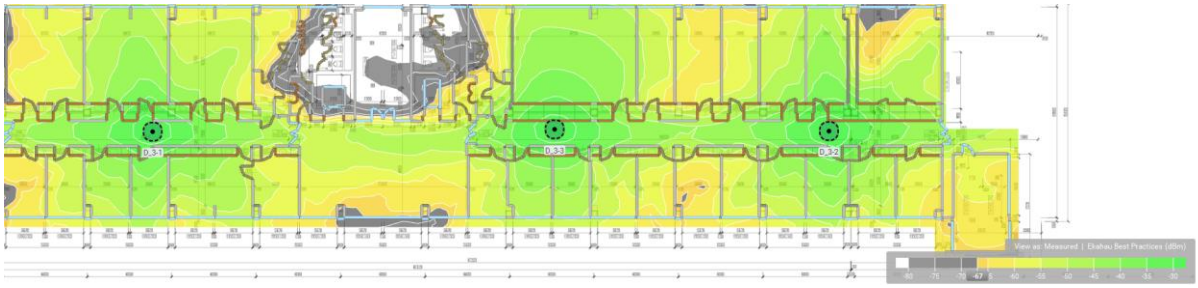
7.6.1 1.Poschodie



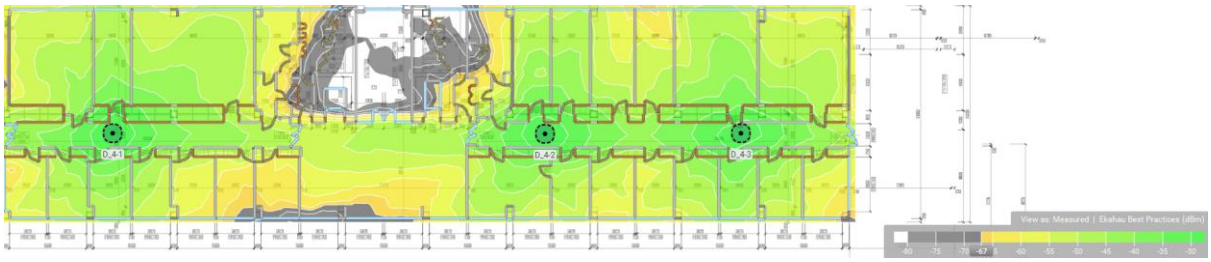
7.6.2 2.Poschodie



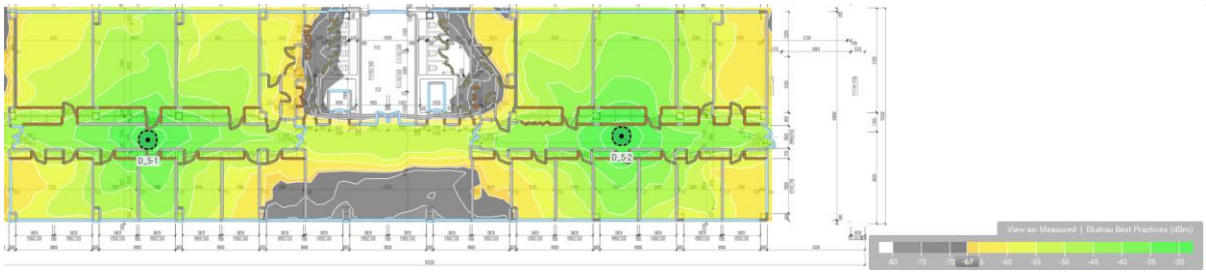
7.6.3 3.Poschodie



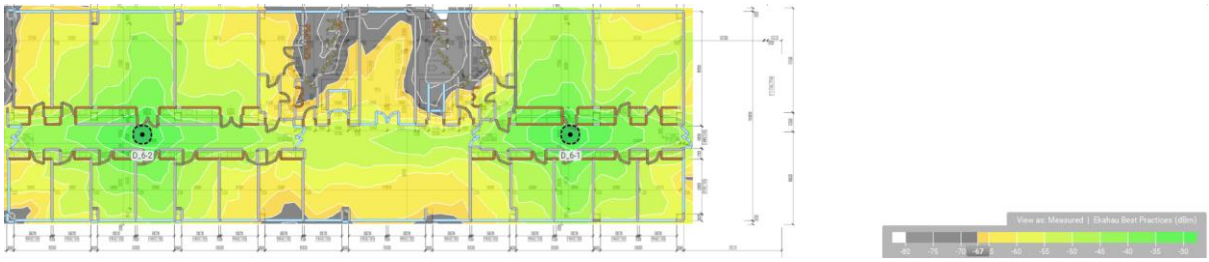
7.6.4 4.Poschodie



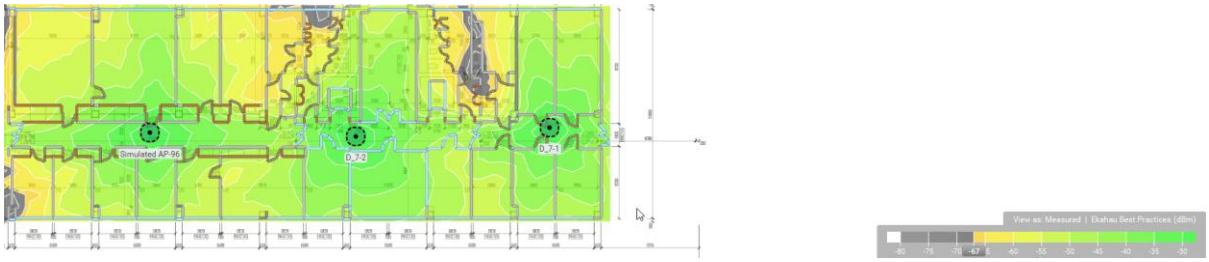
7.6.5 5.Poschodie



7.6.6 6.Poschodie

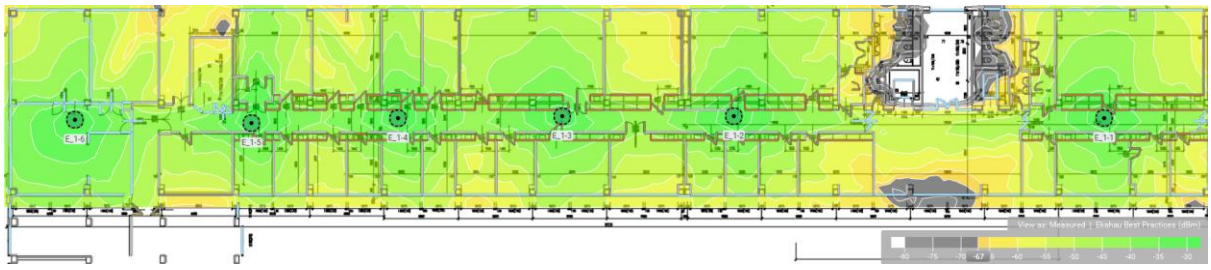


7.6.7 7.Poschodie

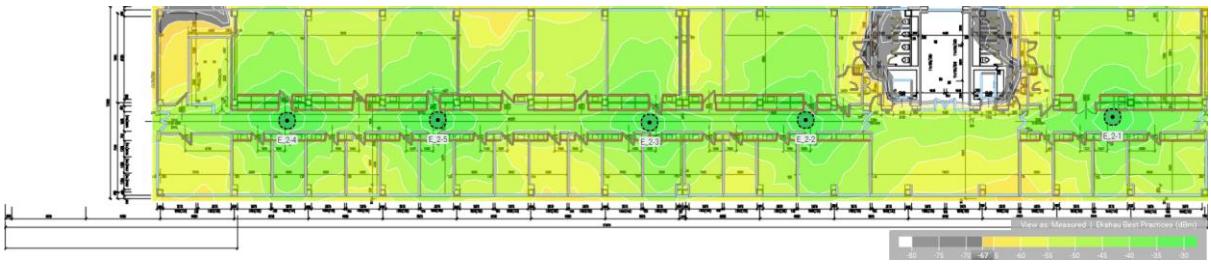


7.7 BLOK E

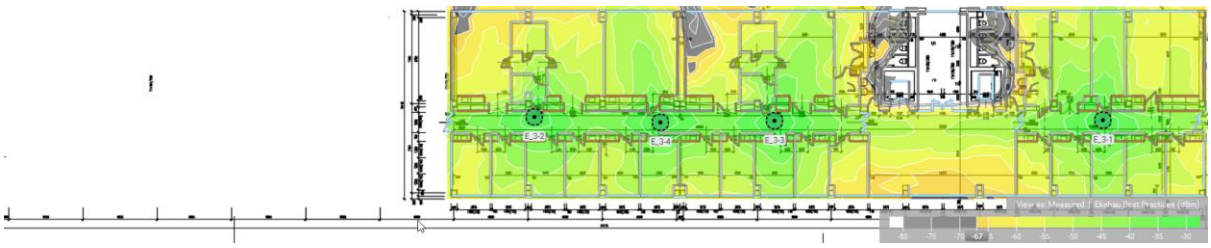
7.7.1 1.Poschodie



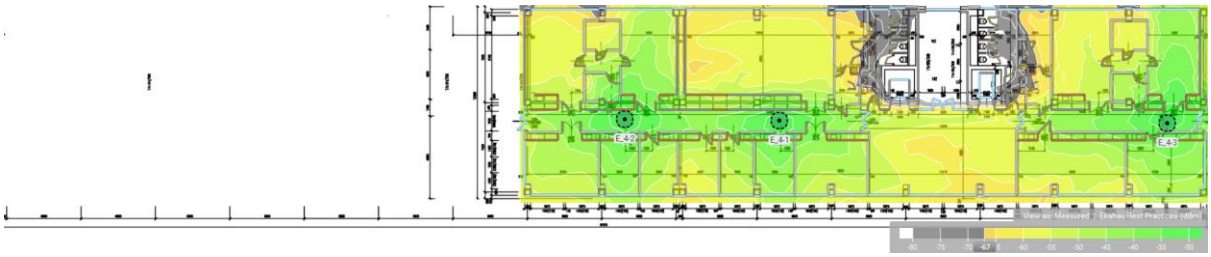
7.7.2 2.Poschodie



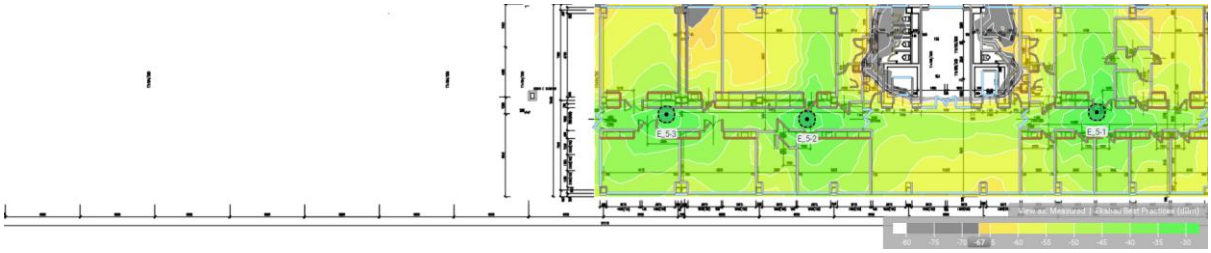
7.7.3 3.Poschodie



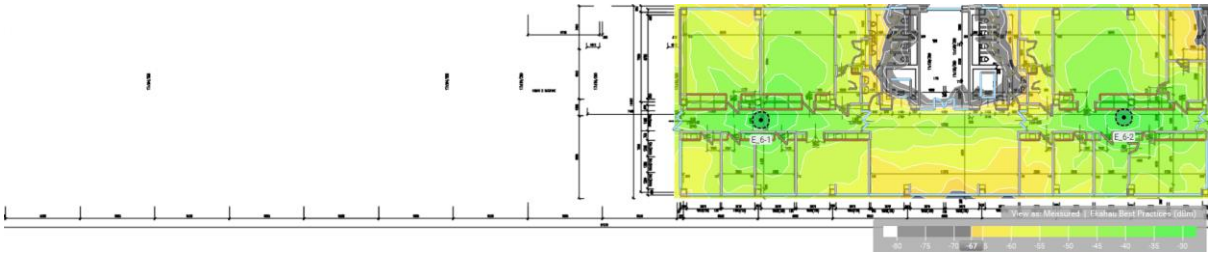
7.7.4 4.Poschodie



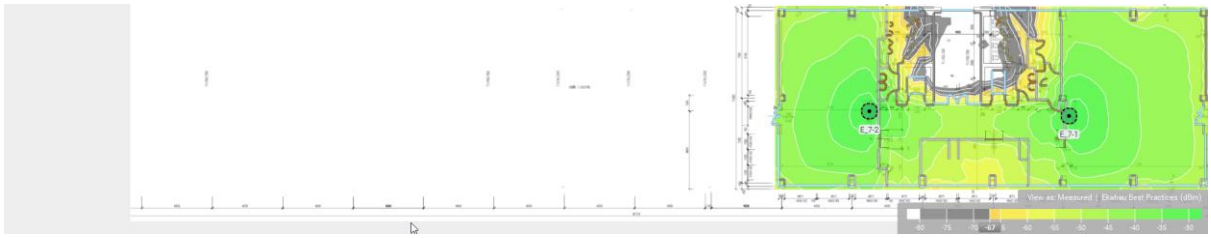
7.7.5 5.Poschodie



7.7.6 6.Poschodie



7.7.7 7.Poschodie



8 IMPLEMENTÁCIA RIEŠENIA

8.1 I.FÁZA – VYBUDOVANIE LAN CORE A DC

V prvej fáze prebehne fyzická inštalácia, vzájomné prepojenia a oživenie hlavných komponentov siete:

- Kostrové prepínače
- DC prepínače vrátane extenderov
- Prístupové prepínače pre hlavnú serverovňu
- bezdrôtové kontroléry
- riadiace komponenty IPT
- sekundárny FW

Úlohou prvej fázy je vybudovanie robustnej kostry siete, ktorá bude pozostávať z dvoch fyzických prepínačov tvoriacich jeden logický celok so spoločným control aj data plane, kedy výpadok jedného prepínača nijako neovplyvní funkčnosť druhého. Vzájomné prepojenie dvoch kostrových prepínačov bude realizované minimálne cez dva 100GE prepoje a separátnym prepojením zabezpečujúcim ochranu pred vznikom duálnej GW v prípade výpadku / prerušenia dátových liniek medzi kostrovými prepínačmi.

Samozrejmosťou je vytvorenie všetkých potrebných L2 VLAN, zabezpečenie ich šírenia na potrebné downlink porty (smerom na distribúcie realizované v nasledovných fázach), predpríprava na migráciu L3 rozhraní a smerovania zo starého kostrového prepínača, a ich vzájomné prepojenie.

Vytvorenia modulu DC zahŕňa implementáciu dvojice tzv. parent prepínačov a ich metalických extenderov pomocou 100GE liniek a ich pripojenie priamo na kostru siete. Samozrejmosťou je povolenie šírenia potrebných L2 VLAN určených pre dátové centrum na DC prepínače. Všetky prepojenia medzi infraštruktúrnymi zariadeniami musia byť realizované pomocou technológie LACP.

Vytvorenie HA páru bezdrôtových kontrolérov pre zabezpečenie redundancie súčasných, podporovaných prístupových bodov (AP) a prípravu pre pripájanie nových AP je úlohou pripojenia nových kontrolérov. V tomto bode je nutné implementovať všetky potrebné nastavenia ako sú napr.:

- Sieťové nastavenia
- RF parametre bezdrôtového prostredia
- Vytvorenie a zabezpečenie potrebných SSID
- zabezpečiť bezproblémový roaming klientov medzi existujúcim WLC a novým HA párom

Pre potreby IPT je úlohou z prevádzkovať riadiace komponenty riešenia (IP telefónna ústredňa,

Implementácia nového FW zahŕňa nastavenie všetkých potrebných zabezpečení a pripojenie nového FW k starému tak, aby vytvorili HA pár.

8.2 II.FÁZA – DISTRIBÚCIA BLOKU A

Úlohou II.Fázy je vytvorenie distribučnej vrstvy pre blok A, ktorá bude mať za úlohu agregovanie prístupových prepínačov v danom bloku a zabezpečiť ich rýchle dátové prepojenie na kostrovú vrstvu a zdroje umiestnené v DC alebo Internete.

Distribúcia bude pozostávať z dvoch fyzických, optických prepínačov tvoriacich jeden logický celok so spoločným control aj data plane, kedy výpadok jedného prepínača nijako neovplyvní funkčnosť druhého, a nakoľko všetky prepojenia medzi prístupovou vrstvou, ako aj pripojenia na kostrovú vrstvu budú realizované redundantne, nedôjde ani k výpadku pripojenia koncových systémov.

Vzájomné prepojenie dvoch kostrových prepínačov bude realizované minimálne cez dva 100GE prepoje a separátnym prepojením zabezpečujúcim ochranu pred vznikom duálnej GW v prípade výpadku / prerušenia dátových liniek medzi distribučnými prepínačmi.

Kostrová vrstva bude pripojená cez 2x40GE rozhrania, prístupové prepínače budú pripojené cez 2x10GE rozhrania.

Samozrejmosťou je vytvorenie všetkých potrebných L2 VLAN pre daný segment LAN siete, zabezpečenie ich šírenia na potrebné uplink/downlink porty, zabezpečenie optimálnej topológie STP.

8.3 III.FÁZA – DISTRIBÚCIA BLOKU B

Úlohou III.Fázy je vytvorenie distribučnej vrstvy pre blok B, ktorá bude mať za úlohu agregovanie prístupových prepínačov v danom bloku a zabezpečiť ich rýchle dátové prepojenie na kostrovú vrstvu a zdroje umiestnené v DC alebo Internete.

Distribúcia bude pozostávať z dvoch fyzických, optických prepínačov tvoriacich jeden logický celok so spoločným control aj data plane, kedy výpadok jedného prepínača nijako neovplyvní funkčnosť druhého, a nakoľko všetky prepojenia medzi prístupovou vrstvou, ako aj pripojenia na kostrovú vrstvu budú realizované redundantne, nedôjde ani k výpadku pripojenia koncových systémov.

Vzájomné prepojenie dvoch kostrových prepínačov bude realizované minimálne cez dva 100GE prepoje a separátnym prepojením zabezpečujúcim ochranu pred vznikom duálnej GW v prípade výpadku / prerušenia dátových liniek medzi distribučnými prepínačmi.

Kostrová vrstva bude pripojená cez 2x40GE rozhrania, prístupové prepínače budú pripojené cez 2x10GE rozhrania.

Samozrejmosťou je vytvorenie všetkých potrebných L2 VLAN pre daný segment LAN siete, zabezpečenie ich šírenia na potrebné uplink/downlink porty, zabezpečenie optimálnej topológie STP.

8.4 IV.FÁZA – DISTRIBÚCIA BLOKU C

Úlohou IV.Fázy je vytvorenie distribučnej vrstvy pre blok C, ktorá bude mať za úlohu agregovanie prístupových prepínačov v danom bloku a zabezpečiť ich rýchle dátové prepojenie na kostrovú vrstvu a zdroje umiestnené v DC alebo Internete.

Distribúcia bude pozostávať z dvoch fyzických, optických prepínačov tvoriacich jeden logický celok so spoločným control aj data plane, kedy výpadok jedného prepínača nijako neovplyvní funkčnosť druhého, a nakoľko všetky prepojenia medzi prístupovou vrstvou, ako aj pripojenia na kostrovú vrstvu budú realizované redundantne, nedôjde ani k výpadku pripojenia koncových systémov.

Vzájomné prepojenie dvoch kostrových prepínačov bude realizované minimálne cez dva 100GE prepoje a separátnym prepojením zabezpečujúcim ochranu pred vznikom duálnej GW v prípade výpadku / prerušenia dátových liniek medzi distribučnými prepínačmi.

Kostrová vrstva bude pripojená cez 2x40GE rozhrania, prístupové prepínače budú pripojené cez 2x10GE rozhrania.

Samozrejmosťou je vytvorenie všetkých potrebných L2 VLAN pre daný segment LAN siete, zabezpečenie ich šírenia na potrebné uplink/downlink porty, zabezpečenie optimálnej topológie STP.

8.5 V.FÁZA – DISTRIBÚCIA BLOKU D

Úlohou V.Fázy je vytvorenie distribučnej vrstvy pre blok D, ktorá bude mať za úlohu agregovanie prístupových prepínačov v danom bloku a zabezpečiť ich rýchle dátové prepojenie na kostrovú vrstvu a zdroje umiestnené v DC alebo Internete.

Distribúcia bude pozostávať z dvoch fyzických, optických prepínačov tvoriacich jeden logický celok so spoločným control aj data plane, kedy výpadok jedného prepínača nijako neovplyvní funkčnosť druhého, a nakoľko všetky prepojenia medzi prístupovou vrstvou, ako aj pripojenia na kostrovú vrstvu budú realizované redundantne, nedôjde ani k výpadku pripojenia koncových systémov.

Vzájomné prepojenie dvoch kostrových prepínačov bude realizované minimálne cez dva 100GE prepoje a separátnym prepojením zabezpečujúcim ochranu pred vznikom duálnej GW v prípade výpadku / prerušenia dátových liniek medzi distribučnými prepínačmi.

Kostrová vrstva bude pripojená cez 2x40GE rozhrania, prístupové prepínače budú pripojené cez 2x10GE rozhrania.

Samozrejmosťou je vytvorenie všetkých potrebných L2 VLAN pre daný segment LAN siete, zabezpečenie ich šírenia na potrebné uplink/downlink porty, zabezpečenie optimálnej topológie STP.

8.6 VI.FÁZA – DISTRIBÚCIA BLOKU E

Úlohou VI.Fázy je vytvorenie distribučnej vrstvy pre blok E, ktorá bude mať za úlohu agregovanie prístupových prepínačov v danom bloku a zabezpečiť ich rýchle dátové prepojenie na kostrovú vrstvu a zdroje umiestnené v DC alebo Internete.

Distribúcia bude pozostávať z dvoch fyzických, optických prepínačov tvoriacich jeden logický celok so spoločným control aj data plane, kedy výpadok jedného prepínača nijako neovplyvní funkčnosť druhého, a nakoľko všetky prepojenia medzi prístupovou vrstvou, ako aj pripojenia na kostrovú vrstvu budú realizované redundantne, nedôjde ani k výpadku pripojenia koncových systémov.

Vzájomné prepojenie dvoch kostrových prepínačov bude realizované minimálne cez dva 100GE prepoje a separátnym prepojením zabezpečujúcim ochranu pred vznikom duálnej GW v prípade výpadku / prerušenia dátových liniek medzi distribučnými prepínačmi.

Kostrová vrstva bude pripojená cez 2x40GE rozhrania, prístupové prepínače budú pripojené cez 2x10GE rozhrania.

Samozrejmosťou je vytvorenie všetkých potrebných L2 VLAN pre daný segment LAN siete, zabezpečenie ich šírenia na potrebné uplink/downlink porty, zabezpečenie optimálnej topológie STP.

8.7 VII.FÁZA – DISTRIBÚCIA BLOKU T

Úlohou VII.Fázy je vytvorenie distribučnej vrstvy pre blok T, ktorá bude mať za úlohu agregovanie prístupových prepínačov v danom bloku a zabezpečiť ich rýchle dátové prepojenie na kostrovú vrstvu a zdroje umiestnené v DC alebo Internete.

Distribúcia bude pozostávať z dvoch fyzických, optických prepínačov tvoriacich jeden logický celok so spoločným control aj data plane, kedy výpadok jedného prepínača nijako neovplyvní funkčnosť druhého, a nakoľko všetky prepojenia medzi prístupovou vrstvou, ako aj pripojenia na kostrovú vrstvu budú realizované redundantne, nedôjde ani k výpadku pripojenia koncových systémov.

Vzájomné prepojenie dvoch kostrových prepínačov bude realizované minimálne cez dva 100GE prepoje a separátnym prepojením zabezpečujúcim ochranu pred vznikom duálnej GW v prípade výpadku / prerušenia dátových liniek medzi distribučnými prepínačmi.

Kostrová vrstva bude pripojená cez 2x40GE rozhrania, prístupové prepínače budú pripojené cez 2x10GE rozhrania.

Samozrejmosťou je vytvorenie všetkých potrebných L2 VLAN pre daný segment LAN siete, zabezpečenie ich šírenia na potrebné uplink/downlink porty, zabezpečenie optimálnej topológie STP.

8.8 VIII.FÁZA – PRÍSTUPOVÁ VRSTVA BLOKU A

Úlohou VIII.Fázy je vytvorenie prístupovej vrstvy pre blok A, ktorá bude mať za úlohu pripojenie koncových klientov, bezdrôtových AP, IP telefónov, IP kamier a pod. do LAN siete. Prepínače budú pripojené cez 2x10GE optické rozhrania na distribúciu v danom bloku cez technológiu LACP.

Samozrejmosťou je vytvorenie všetkých potrebných L2 VLAN pre daný prístupový prepínač, zabezpečenie ich šírenia na potrebné uplink/downlink porty, zabezpečenie optimálnej topológie STP. Rovnako je potrebné zabezpečiť rozpoznávanie koncových zariadení a v prípade potreby im zabezpečiť PoE, správne QoS parametre, resp. priradenie do požadovanej VLAN.

8.9 IX.FÁZA – PRÍSTUPOVÁ VRSTVA BLOKU B

Úlohou IX.Fázy je vytvorenie prístupovej vrstvy pre blok B, ktorá bude mať za úlohu pripojenie koncových klientov, bezdrôtových AP, IP telefónov, IP kamier a pod. do LAN siete. Prepínače budú pripojené cez 2x10GE optické rozhrania na distribúciu v danom bloku cez technológiu LACP.

Samozrejmosťou je vytvorenie všetkých potrebných L2 VLAN pre daný prístupový prepínač, zabezpečenie ich šírenia na potrebné uplink/downlink porty, zabezpečenie optimálnej topológie STP. Rovnako je potrebné zabezpečiť rozpoznávanie koncových zariadení a v prípade potreby im zabezpečiť PoE, správne QoS parametre, resp. priradenie do požadovanej VLAN.

8.10 X.FÁZA – PRÍSTUPOVÁ VRSTVA BLOKU C

Úlohou X.Fázy je vytvorenie prístupovej vrstvy pre blok C, ktorá bude mať za úlohu pripojenie koncových klientov, bezdrôtových AP, IP telefónov, IP kamier a pod. do LAN siete. Prepínače budú pripojené cez 2x10GE optické rozhrania na distribúciu v danom bloku cez technológiu LACP.

Samozrejmosťou je vytvorenie všetkých potrebných L2 VLAN pre daný prístupový prepínač, zabezpečenie ich šírenia na potrebné uplink/downlink porty, zabezpečenie optimálnej topológie STP. Rovnako je potrebné zabezpečiť rozpoznávanie koncových

zariadení a v prípade potreby im zabezpečiť PoE, správne QoS parametre, resp. priradenie do požadovanej VLAN.

8.11 XI.FÁZA – PRÍSTUPOVÁ VRSTVA BLOKU D

Úlohou XI.Fázy je vytvorenie prístupovej vrstvy pre blok D, ktorá bude mať za úlohu pripojenie koncových klientov, bezdrôtových AP, IP telefónov, IP kamier a pod. do LAN siete. Prepínače budú pripojené cez 2x10GE optické rozhrania na distribúciu v danom bloku cez technológiu LACP.

Samozrejmosťou je vytvorenie všetkých potrebných L2 VLAN pre daný prístupový prepínač, zabezpečenie ich šírenia na potrebné uplink/downlink porty, zabezpečenie optimálnej topológie STP. Rovnako je potrebné zabezpečiť rozpoznávanie koncových zariadení a v prípade potreby im zabezpečiť PoE, správne QoS parametre, resp. priradenie do požadovanej VLAN.

8.12 XII.FÁZA – PRÍSTUPOVÁ VRSTVA BLOKU E

Úlohou XII.Fázy je vytvorenie prístupovej vrstvy pre blok E, ktorá bude mať za úlohu pripojenie koncových klientov, bezdrôtových AP, IP telefónov, IP kamier a pod. do LAN siete. Prepínače budú pripojené cez 2x10GE optické rozhrania na distribúciu v danom bloku cez technológiu LACP.

Samozrejmosťou je vytvorenie všetkých potrebných L2 VLAN pre daný prístupový prepínač, zabezpečenie ich šírenia na potrebné uplink/downlink porty, zabezpečenie optimálnej topológie STP. Rovnako je potrebné zabezpečiť rozpoznávanie koncových zariadení a v prípade potreby im zabezpečiť PoE, správne QoS parametre, resp. priradenie do požadovanej VLAN.

8.13 XIII.FÁZA – PRÍSTUPOVÁ VRSTVA BLOKU T

Úlohou XIII.Fázy je vytvorenie prístupovej vrstvy pre blok T, ktorá bude mať za úlohu pripojenie koncových klientov, bezdrôtových AP, IP telefónov, IP kamier a pod. do LAN siete. Prepínače budú pripojené cez 2x10GE optické rozhrania na distribúciu v danom bloku cez technológiu LACP.

Samozrejmosťou je vytvorenie všetkých potrebných L2 VLAN pre daný prístupový prepínač, zabezpečenie ich šírenia na potrebné uplink/downlink porty, zabezpečenie optimálnej topológie STP. Rovnako je potrebné zabezpečiť rozpoznávanie koncových zariadení a v prípade potreby im zabezpečiť PoE, správne QoS parametre, resp. priradenie do požadovanej VLAN.

8.14 XIV.FÁZA – ROZŠÍRENIE BEZDRÔTOVÉHO POKRYTIA

Úlohou XIV.Fázy je rozšíriť pokrytie fakulty bezdrôtovým signálom. Je potrebné fyzicky umiestniť bezdrôtové prístupové body (AP) na lokality podľa prediktívneho návrhu rozmiestnenia, zabezpečiť ich pripojenie do LAN siete a:

- Zabezpečiť automatické pripojenie na WLC
- Priradiť AP požadované RF parametre
- Priradiť AP potrebné WLAN a Policy profily
- Priradiť pre AP špecifické parametre

8.15 XV.FÁZA – IP TELEFÓNIA

Úlohou XV. Fázy je zabezpečiť kompletnú výmenu tradičnej telefónie na IP telefónne riešenie, t.j. rozmiestnenie IP telefónov a zabezpečenie ich pripojenia do LAN a IPT ústredne, priradenia špecifických nastavení ako meno, klapka a pod. samozrejmosťou je sfunkčnenie dodaných kolaboračných nástrojov.

8.16 XVI. FÁZA – MANAŽMENT

Úlohou XVI. Fázy je implementácia komplexného manažmentového nástroja, t.j. import všetkých požadovaných komponentov do tohto nástroja, import máp, nastavenie konfiguračnej zálohy zariadení a pod.