Opis predmetu zákazky: Definícia služieb zabezpečovania prevádzky, údržby a ďalšieho rozvoja riešenia LAN/WLAN a dátovej konektivity WAN

„Definícia služieb RPŠ“

Príloha 01b

december 2024

Obsah

1 Úvod 4

1.1 Cieľ dokumentu a širší kontext 4

1.2 Obsah dokumentu 4

1.3 Definície a výklad pojmov 4

1.4 Spôsob kategorizácie služieb 6

1.4.1 Kontinuálne (priebežne poskytované) služby 6

1.4.2 Ad hoc služby 6

1.4.3 Pravidelné služby 6

1.5 Proaktívny a reaktívny vznik incidentu 6

1.5.1 Proaktívne meranie 7

1.5.2 Reaktívny vznik incidentu 7

1.6 Riadenie zmien 7

1.6.1 Postup Riadenia zmeny 7

2 Katalóg služieb 9

2.1 Služby zabezpečovania prevádzky riešenia LAN/WLAN 9

2.1.1 Zabezpečovanie pokrytia WLAN 10

2.1.2 Zabezpečovanie pokrytia LAN 15

2.1.3 Zabezpečovanie priepustnosti v sieti WLAN 17

2.1.4 Zabezpečovanie priepustnosti v sieti LAN 20

2.1.5 Zabezpečovanie pripájania a výmeny CPE 25

2.1.6 Zaisťovanie sieťovej bezpečnosti WLAN 26

2.1.7 Zaisťovanie sieťovej bezpečnosti LAN 28

2.1.8 RACI matica pre služby zabezpečovania prevádzky riešenia LAN/WLAN 30

2.2 Služby zabezpečovania WAN konektivity 32

2.2.1 Zabezpečovanie primárnej dátovej konektivity a jej zálohy 32

2.2.2 RACI matica pre služby zabezpečovania WAN konektivity 37

2.3 Služby manažmentu a monitoringu riešenia LAN/WLAN/WAN 38

2.3.1 Poskytovanie služieb centralizovaného riešenia správy a dohľadu (CRSD) priamo RPŠ – Alternatíva 1 38

2.3.2 Poskytovanie služieb centralizovaného riešenia správy a dohľadu poskytovaná RPŠ prostredníctvom služieb NCU (NCU-CRSD) – Alternatíva 2 49

2.3.3 Meranie spokojnosti koncového používateľa služieb a náprava 62

2.3.4 RACI matica pre služby manažmentu a monitoringu riešenia LAN/WLAN/WAN 65

2.4 Služby podpory prevádzky a údržby riešenia LAN/WLAN/WAN 66

2.4.1 Poskytovanie služieb RPŠ – ServiceDesk, evidencie a spracovania ticketov 67

2.4.2 Riešenie incidentov 70

2.4.3 Riešenie iných požiadaviek používateľov 76

2.4.3.1 Žiadosť o informáciu 76

2.4.3.2 Mimoriadne situácie 77

2.4.4 Oznamovanie a odsúhlasovanie plánovaných výpadkov 77

2.4.5 Zabezpečovanie údržby a homogenity LAN/WLAN a súladu s dokumentáciou 79

2.4.5.1 Zabezpečovanie aktualizácii a testovania 79

2.4.5.2 Zabezpečovanie súladu s metodickými usmerneniami 80

2.4.5.3 Zabezpečovanie komunikácie s časťou siete v správe školy 80

2.4.5.4 Zabezpečovanie súladu dokumentácie 80

2.4.6 RACI matica pre služby podpory, prevádzky a údržby riešenia LAN/WLAN/WAN 81

2.5 Služby reportingu o stave a využívaní riešenia LAN/WLAN/WAN a kvality 82

2.5.1 Vytváranie správy o histórii pripojených zariadení 82

2.5.2 Vytváranie správy o poskytnutom výkone za zvolené obdobie 84

2.5.3 Vytváranie správy o intruzívnom meraní kapacity WAN 86

2.5.4 Vytvorenie analýzy trendov a problémov 87

2.5.5 Zaisťovanie kompatibility reportovania s nástrojmi NCU 89

2.5.6 RACI matica pre služby reportingu o stave a využívaní riešenia LAN/WLAN/WAN a kvality 91

2.6 Služby opcie – Náhrada služieb NCU 92

2.6.1 Poskytovanie služieb Service Desk - Helpdesk, Ticketing 92

2.6.2 Poskytovanie sieťových služieb a sieťovej bezpečnosti 93

3 Prílohy 96

3.1 Zoznam skratiek 96

3.2 Zoznam obrázkov 98

3.3 Zoznam tabuliek 98

# Úvod

## Cieľ dokumentu a širší kontext

Špecifikácia služieb definuje požiadavky na telekomunikačné služby poskytované školám v pôsobnosti RPŠ (Regionálny partner školy) podľa špecifikácie obstarávateľa - **Ministerstvo školstva výskumu vývoja a mládeže SR** (ďalej len: MŠVVaM SR, MŠ, Ministerstvo, rezort, obstarávateľ) pre dosiahnutie požadovaných štandardov IKT (Informačné a komunikačné technológie). Telekomunikačné služby sú poskytované na komponentoch infraštruktúry ktoré dodá a vybuduje v lokalitách škôl RPŠ spolu s dodávkou potrebných licencií a podpory od výrobcu zariadení. Dodané riešenie v lokalitách škôl prepojí s Národným Centrálnym uzlom (NCU) a zabezpečí akceptačné testovanie riešenia tak aby boli spĺňané definované požiadavky a ich merateľné parametre na služby uvedené v katalógu služieb tohto dokumentu. Po akceptácii riešenia vykonaním akceptačného testovania, odstránim nedostatkov a teda aj potvrdením každého požadovaného merateľného parametra s definovanou metrikou prechádza riešenie do prevádzky RPŠ. RPŠ poskytuje služby zabezpečovania prevádzky, údržby a ďalšieho rozvoja LAN/WLAN/WAN riešenia v školách regiónu na požadované obdobie podľa zmluvy.

## Obsah dokumentu

**Kategorizácia služieb –** Definuje typy poskytovaných služieb podľa spôsobu ich poskytovania:

* kontinuálne,
* pravidelné,
* ad-hoc.

**Katalóg služieb** - Špecifikácia požiadaviek na služby uvádza najmä definíciu poskytovaných služieb pre lokality škôl, metriky merateľných parametrov služieb a ostatné nevyhnutné požiadavky pre zabezpečovanie plynulej prevádzky.

## Definície a výklad pojmov

| **Pojem** | **Vysvetlenie** |
| --- | --- |
| **Udalosť** | Udalosťou rozumieme akúkoľvek zmena stavu infraštruktúry, ktorá môže mať vplyv na poskytovanie služieb. Môže byť plánovaná alebo neplánovaná, avšak nie vždy má priamy negatívny vplyv na služby. Slúži ako signalizácia potenciálnej situácie, ktorú je potrebné sledovať. Udalosť môže byť automaticky/proaktívne detegovaná (napr. výpadok spojenia automatickým monitorovacím systémom), nahlásená oprávnenou osobou používateľa siete alebo manuálne zadaná pracovníkom RPŠ, pracovníkom NCU. Požiadavky oprávnenej osoby typu: žiadosť o informáciu, zmenu, sú rovnako evidované ako udalosť. |
| **Ticket** | Je akýkoľvek zaznamenaný záznam o interakcii medzi oprávnenou osobou používateľa a prevádzkovateľom služieb. Slúži ako základný nástroj na sledovanie, správu a riešenie rôznych udalostí. |
| **Problém** | Je podstatná príčina jedného alebo viacerých incidentov. Zatiaľ čo incident predstavuje konkrétny výskyt poruchy, problém je koreňová príčina týchto porúch. |
| **Incident** | Je akákoľvek neplánovaná udalosť, ktorá spôsobuje, alebo má potenciál spôsobiť, prerušenie alebo podstatné zníženie kvality požadovaných služieb, hodnoty parametrov služieb nedosahujú požadovanú úroveň, negatívny vplyv na používateľov pre porušenie definovaných požiadaviek na služby. |
| **Požiadavka na zmenu** | Je formálna žiadosť o autorizáciu na vykonanie zmeny v IT službách, systémoch alebo infraštruktúre. Táto zmena môže byť plánovaná alebo nútená a môže mať vplyv na kvalitu, dostupnosť alebo zabezpečovanie služieb. |
| **Požiadavka o informáciu** | Je formálna žiadosť na poskytnutie informácie o poskytovaných službách, ich nastavení parametrov služieb, atď. |
| **RPŠ – Service Desk** | Je súbor organizačných, technických a personálnych prostriedkov pre zabezpečenie poskytovania služieb podpory prevádzky a údržby riešenia v pôsobnosti RPŠ. |
| **NCU – Service Desk** | Je súbor organizačných, technických a personálnych prostriedkov pre zabezpečenie poskytovania služieb podpory prevádzky a údržby riešenia v pôsobnosti NCU. Znamená aj súbor technických, organizačných a personálnych prostriedkov pre zabezpečenie poskytovania služieb kontaktu a podpory prostredníctvom hlasovej komunikácie s využitím verejnej telefónnej siete, pomocou internetového portálu a mailovej adresy. |
| **Centrálny ticketing portál (CTP)** | Centrálny portál zriadený a prevádzkovaný dodávateľom služieb NCU. Portál slúži ako základný centrálny nástroj na sledovanie, správu a riešenie ticketov, reportovania kvality. Portál je dostupný cez štandardné webové rozhranie pre RPŠ agentov, NCU agentov, ŠKOLY a rezort. |
| **Severity** | Definuje závažnosť nesúladu služby a vplyv nesúladu služby na používateľov. |
| **Pripájaný bod** | Je označenie pre každé miesto, ktoré poskytuje možnosť fyzického pripojenia do siete používateľa – RJ.45 v učebni a WiFi AP. |
| **Nesúlad služby** | V prípade že parametre služby nedosahuje požadované hodnoty alebo služba nie je v súlade s definíciou požiadaviek na službu. |
| **Čas nesúladu ()** | Predstavuje celkový čas trvania nesúladu služby v mesiaci počas prevádzkovej doby služby. Čas nesúladu služby sa počíta od vzniku udalosti/nahlásenia problému oprávnenou osobou používateľa, od času odhalenia nedostupnosti poskytovateľom služieb RPŠ, poskytovateľom služieb NCU (podľa toho čo nastane skôr). Čas nesúladu končí obnovením súladu služby. Čas kedy hodnoty merateľných parametrov a definícia požiadaviek na službu neboli dodržané z:  1/príčin na strane objednávateľa alebo,  2/z dôvodu plánovaných prác ktoré sú v súlade s požiadavkami,  nebude započítavaný do času nedostupnosti služby. Časy sa počítajú na celé minúty. |
| **Súlad služby** | Služba spĺňa hodnoty merateľných parametrov a spĺňa definíciu požiadaviek na službu |
| **Prevádzkový čas služby ()** | Predstavuje celkový čas prevádzky služby v mesiaci v ktorom sa vyžaduje garancia dosahovania hodnôt parametrov služby a definovaných požiadaviek na službu. Časy sa počítajú na celé minúty. |
| **Čas opravy nesúladu (TTR)** | Predstavuje celkový čas od vzniku udalosti o nesúlade služby až po nápravu služby. Časy sa počítajú na celé minúty. |
| **Požadovaný čas opravy nesúladu (RTTR)** | Predstavuje požadovaný celkový čas od vzniku udalosti o nesúlade služby až po nápravu služby. Časy sa počítajú na celé minúty. Požadované časy sú definované podľa severity nesúladu. |
| **Dostupnosť služby** | Dostupnosť sa vyjadrí v % zaokrúhlene na dve desatinné miesta. |
| **Prevádzková doba poskytovania služieb** | Je časové obdobie v ktorom sa vyžaduje garancia dosahovania hodnôt parametrov služby a definovaných požiadaviek na službu |
| **Chrbticová sieť LAN** | Je sieť v lokalite školy medzi CPE a akýmkoľvek switchom, medzi switchmi |
| **Riešiteľ incidentu** | Rola obsadená aktuálne zodpovednou stranou za pridelený ticket. |
| **RACI matica** | Predstavuje rozdelenie zodpovedností pri plnení úloh. RACI matica rozdeľuje zodpovednosti medzi Školu, RPŠ, NCU a MŠVVaM pričom prvky RACI matice predstavujú:   * **R** (Responsible) – je zodpovedný za danú činnosť * **A** (Accountable) - je zodpovedný za výsledok a overenie danej činnosti * **C** (Consulted) – je konzultovaný o činnosti * **I** (Informed) - je informovaný o výsledku, priebehu činnosti |

Tabuľka 1: Zoznam pojmov

## Spôsob kategorizácie služieb

### Kontinuálne (priebežne poskytované) služby

Kontinuálne služby sú také, ktoré dodávateľ poskytuje súvisle, počas celého trvania zmluvy. Objednávateľ uhrádza za tieto služby fixný poplatok pre dané obdobie (s možným znížením poplatku z dôvodu penalizácie).

### Ad hoc služby

Ad-hoc služby sú také, ktoré sa vykonávajú na vyžiadanie resp. sú spustené automaticky z dôvodu zaznamenania udalosti v sieti. Typicky ide o služby operačnej prevádzky riešenia, riešenia incidentov a požiadaviek. Takouto službou je aj zvýšená prevádzková podpora pri mimoriadnych situáciách.

### Pravidelné služby

Pravidelnú služby sú také, ktoré sú vykonávané na pravidelnej báze. Typicky služby generovania reportov, služby údržby (SW upgrade), reportovanie kvality vykonávaných služieb a vyhodnocovanie dostupnosti za uplynulé obdobie.

## Proaktívny a reaktívny vznik incidentu

V opise služieb nižšie je definovaný vznik incidentu na základe proaktívneho merania alebo reaktívne nahlásením.

### Proaktívne meranie

Proaktívne meranie predstavuje priebežné sledovanie stavu merateľných parametrov a požiadaviek na službu. Prebieha kontinuálne (v definovaných intervaloch) a automatizovane. Pri zistení nesúladu meraného parametra s dohodnutou úrovňou parametrov je automaticky otvorený ticket.

### Reaktívny vznik incidentu

Reaktívny vznik incidentu je na základe nahlásenej udalosti pri podozrení nesúladu služby s požadovanými parametrami.

Reaktívne riešenie incidentu je obvykle iniciované na základe podozrenia školy, prípadne aj NCU alebo RPŠ.

Priebeh riešenia je nasledovný:

1. Nahlásenie udalosti, evidencia vo forme nového ticketu.
2. Klasifikácia na úrovni NCU.
3. Klasifikácia a začatie riešenia do 60 minút na úrovni RPŠ (ak bolo pridelené RPŠ).
4. RPŠ do 2 hodín vzdialene preverí, či ide o incident. Vzdialené preverenie môže vyžadovať aj súčinnosť zamestnanca školy na mieste. V prípade potvrdenia incidentu je ďalší postup podľa služieb riadenia incidentov. V prípade nepotvrdenie (služby sú v súlade s požiadavkami) je ticket uzavretý.
5. V prípade, že nie je možné preverenie na diaľku, zabezpečí RPŠ preverenie na mieste do 5 pracovných dní. V prípade potvrdenia incidentu je ďalší postup podľa služieb riadenia incidentov. V prípade nepotvrdenia nesúladu (služby sú v súlade s požiadavkami) je ticket uzavretý a škola môže požiadať o ďalšie takéto preverenie rovnakého podozrenia na nesúlad služby na mieste najskôr nasledujúci mesiac v prípade že si to vyžaduje výjazd na školu.

## Riadenie zmien

Proces Riadenia zmien zabezpečí, aby zmeny v poskytovaných službách, či už na požiadavku používateľa alebo s dôvodu údržby a aktualizácie zo strany RPŠ, boli plánované, schválené a implementované kontrolovaným spôsobom, minimalizujúc pritom riziká a negatívne dopady na prevádzku. Tento proces sa týka zmien v službách v rozsahu zmluvy alebo objednávky, ktorých cena je v zmluve určená alebo sa dá určiť na základe zmluvy.

### Postup Riadenia zmeny

O zmenu môže požiadať riaditeľ školy, ním poverená osoba alebo zástupca obstarávateľa.

Po prijatí žiadosti o zmenu NCU alebo RPŠ vytvorí ticket, kde bude evidovaná žiadosť, následná komunikácia, realizácia zmeny až po jej akceptáciu. Ak má zmena vplyv na obsah zadanej objednávky, výsledkom postupu Riadenia zmeny je zmena objednávky.

Postup Riadenia zmien sa spravuje týmito princípmi:

* zmeny musia prechádzať jasne definovaným procesom, ktorý zahŕňa podanie žiadosti o zmenu, hodnotenie, schvaľovanie, plánovanie, implementáciu, testovanie a zavedenie do prevádzky,
* zmeny sú klasifikované podľa ich potenciálneho vplyvu na prevádzku (nízky, stredný, vysoký) z dôvodu prispôsobenia procesu schvaľovania a kontroly jednotlivým typom zmien,
* každá zmena musí byť podrobená dôkladnému hodnoteniu rizík, aby sa identifikovali potenciálne negatívne dopady a prijali potrebné opatrenia na ich minimalizáciu,
* zmeny musia byť schválené oprávnenými osobami, ktoré majú potrebné znalosti a autoritu,
* pre každú zmenu musí byť vypracovaný detailný plán, ktorý špecifikuje všetky potrebné činnosti, zdroje a časové harmonogramy,
* zmeny musia byť implementované podľa schváleného plánu,
* po implementácii musí byť vykonané primerané testovanie,
* po úspešnom testovaní je zmena zavedená do pravidelnej prevádzky,
* celý proces riadenia zmien musí byť dôkladne zdokumentovaný v príslušnom tickete, aby bolo možné sledovať históriu zmien a vyhodnocovať ich účinnosť,
* o zmenách musia byť primerane informovaní zástupcovia školy, MŠVVaM SR a poskytovateľ služieb NCU.

# Katalóg služieb

Katalóg služieb je detailný popis požadovaných služieb, pričom sú tieto služby rozdelené do nasledujúcich základných kategórii:

* služby zabezpečovania prevádzky riešenia LAN/WLAN,
* služby zabezpečovania WAN konektivity školy,
* služby manažmentu a monitoringu riešenia LAN/WLAN/WAN,
* služby reportingu o stave a využívaní riešenia LAN/WLAN/WAN,
* služby podpory prevádzky a údržby riešenia LAN/WLAN/WAN,
* opcia – služby sieťovej bezpečnosti a service desk pre školy.

## Služby zabezpečovania prevádzky riešenia LAN/WLAN

Prevádzka služieb LAN/WLAN zahŕňa riešenia na zabezpečenie spoľahlivej a efektívnej sieťovej infraštruktúry. Tieto služby pokrývajú všetky aspekty súvisiace s plánovaním, inštaláciou, údržbou a optimalizáciou sietí LAN (Local Area Network) a WLAN (Wireless Local Area Network). Cieľom je zabezpečiť, aby lokalita mala počas celej prevádzkovej doby poskytovania služieb stabilné, rýchle sieťové pripojenie s požadovaným pokrytím a kapacitou, ktoré podporuje každodenné operácie a dlhodobé technologické ciele obstarávateľa a v neposlednom rade sieťovú bezpečnosť.

Prevádzka služieb bezpečnosti LAN/WLAN plní funkciu ochrany pred hrozbami, neoprávneným prístupom, implementáciu mechanizmov chrániacich dostupnosť služby, zaručujúcich integritu, dôvernosť a dostupnosť sieťových služieb pomocou moderných šifrovacích technológií, autentifikačných protokolov a segmentáciou siete.

### Zabezpečovanie pokrytia WLAN

| **Zabezpečovanie pokrytia siete WLAN - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Zabezpečovanie pokrytia siete WLAN |
| **Kategória** | | | | Služby zabezpečovania prevádzky riešenia LAN/WLAN |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Služba pokrytia WLAN zahŕňa zabezpečenie bezdrôtového pripojenia v interiérových a exteriérových priestoroch podľa požiadaviek školy v súlade s požiadavkami štandardu. Cieľom je dosiahnuť optimálne a zabezpečené WiFi pokrytie s bezpečnosťou riadenia prístupu do siete, ktoré umožní spoľahlivé pripojenie zariadení a udržanie tohto pripojenia pri pohybe používateľov medzi rôznymi oblasťami (tam kde je to možné – t.j. Inštalované WiFi AP poskytujú dostatočný prienik rádiového pokrytia). |
| **Zabezpečovanie pokrytia siete WLAN - detailná definícia požiadaviek na službu** | | | | |
| * WiFi 6 2.4 GHz (IEEE 802.11 b/g/n/ax) a 5 GHz (IEEE 802.11 a/n/ac/ax), * UL/DL MU-MIMO (MU-MIMO v odchádzajúcom smere (Uplink) ako aj prichádzajúcom smere (Downlink) ), * OFDMA v odchádzajúcom smere (Uplink) ako aj prichádzajúcom smere (Downlink), * Minimálne 2x2:2 spatial streams avšak s povinnosťou dosahovať uvedené merateľné parametre služieb, * IEEE 802.11e/WMM, * podpora U-APSD (Power save), * IEEE 802.1p, resp. podpora QoS, CoS * IEEE 802.11r, * IEEE 802.1Q – Wlan tagovanie – jednotlivé SSID siete sú mapované do rôznych VLAN, * WPA2-Preshared key, WPA2-Enterprise s IEEE 802.1X, * WPA3-Preshared key, WPA3-Enterprise s IEEE 802.1X, * EAP-TLS,  EAP-TTLS, EAP-MSCHAPv2, * band steering – podpora funkcionality AP, ktorá preferuje pripojenie klientov k 5Ghz, * rate limit – WiFi AP musí podporovať nastavenie limitovanie rýchlosti obslužných rámcov (management frames) buď na základe jednotlivých pásiem alebo na základe jednotlivých SSID, * RX-SOP – zariadenie podporuje konfiguráciu minimálnych prahových hodnôt RSSI potrebných na dekódovanie a demodulovanie dátových rámcov pre efektívne využitie spektra, * podpora min. 15 aktívnych SSID, * podpora mapovania týchto SSID do VLAN (IEEE 802.1Q), * per SSID definícia PSK alebo 802.1x/RADIUS, * automatizované nezávislé zapínanie a vypínanie jednotlivých SSID podľa predom určeného časového harmonogramu, * Guest WiFi - SSID pre pripojenie návštevníkov školy, s kompletnou izoláciou pripojených guest zariadení (nemožnosť komunikovať medzi pripojenými guest zariadeniami)   , * zabudované antény na WiFi AP v interiéri, * možnosť vypnúť svetelnú signalizáciu na AP, * dedikované rádio pre 2,4 Ghz, dedikované rádio pre 5 Ghz, * spektrálna analýza 2,4 a 5 Ghz pásma (real-time, bez ovplyvnenia dátovej prevádzky WiFi klientov), * funkcie Wireless IDS , * Nezáväzne podpora Mesh – WiFi AP podporuje automatizované vytvorenie MESH typu prepojenia bod-bod, bod-multibod s automatickým vyhľadávaním susedov v oboch rádiových pásmach (2.4 Ghz a 5Ghz) , * teplotný rozsah -20 až 55 C a IP67 krytie AP určených pre inštaláciu v exteriéri, * je povolené využívanie len frekvencií a vyžarovacích výkonov schválených pre SR. * V rámci zabezpečovania služieb RPS očakávame, poskytovanie prevádzky komplexných služieb súvisiacich s pokrytím WiFi, ktoré zahŕňajú: * poskytovanie pokrytia WiFi interiérových, exteriérových učebni, chodieb podľa IKT štandardu, * pokrytie WiFi signálom nie je nižšie ako -70dBm RSSI a zároveň nižšie ako 25 dB SNR, pričom:   + hodnota -70 dBm RSSI je hodnota úrovne signálu zaznamenaná na strane WiFi indoor AP smerom od WiFi klienta, platná pre pásmo 2.4 aj 5 GHz,   + hodnota 25 dB SNR je hodnota odstupu signálu od šumu zaznamenaná na strane WiFi indoor AP smerom od WiFi klienta, platná pre pásmo 2.4 aj 5 GHz   + hodnota RSSI a SNR na strane AP musí byť nameraná pri umiestnení WiFi klienta v strede učebne, a v štyroch najvzdialenejších miestach od stredu, vo výške 90 cm od podlahy   + WiFi klientom sa myslí mobilné zariadenie kategórie smart phone alebo tablet   + jeden WiFi indoor AP je pritom určený na pokrytie maximálne takého počtu učební, ktorého súčet počtu žiakov nepresahuje 50,   + všetky vyššie uvedené podmienky musia byť splnené súčasne, * WiFi klient nachádzajúci sa v mieste určenom na využitie opisovanej WLAN služby musí byť schopný pripojiť sa do WLAN siete do 10 000ms, pričom za úspešné pripojenie považujeme splnenie nasledovných krokov:   + asociáciu WiFi klienta k AP,   + autentifikáciu klienta,   + priradenie IP adresy a DNS servera,   + Schopnosť komunikovať do siete internet,   + POZNÁMKA: Za E2E dosahovanie požiadavky nesú prevádzkovú zodpovednosť ako RPŠ tak aj NCU na prvkoch vo svojej zodpovednosti. Dodávateľ RPŠ a NCU sú povinní spoločne identifikovať a odstrániť nedostatky spôsobujúce nesúlad služby tak aby celková hodnota parametra v súčte cez všetky prvky nepresiahla požadované hodnoty. * ak to situácia umožňuje, t.j. inštalované WiFi AP poskytujú dostatočný vzájomný prienik rádiového pokrytia, čas potrebný na prechod medzi AP je maximálne 3 sekundy. * Meranie WiFi pokrytia a jeho optimalizácia, meranie interferencií:   + Zobrazenie sily signálu (RSSI) v dBm a odstupu signálu od šumu (SNR) v dB WiFi pripojenia z pohľadu pripojeného WiFi klienta, aby boli dosiahnuté hodnoty definované v službe pokrytia WiFi.   + Meranie vyťaženia jednotlivých kanálov v pásmach 2.4 Ghz a 5 Ghz s možnosťou manuálneho a automatického ladenia kanálov podľa aktuálnej interferencie v okolí.   + Meranie času potrebného na prechod WiFi klienta medzi prístupovými bodmi v miestach s dostatočným prienikom rádiového pokrytia.   + Meranie a zobrazovanie interferencií v pásme 2.4 a 5 Ghz v reálnom čase, bez dopadu na obsluhovanie WiFi klientov schopné určiť prítomnosť zdrojov rušenia v blízkosti zvoleného AP a tieto zdroje (ak sú to WiFi AP) identifikovať – SSID, BSSID (MAC).   + Zabezpečovanie optimalizácie šírky pásma smerovaním klientov do menej zaťaženého pásma 5GHz (Band steering). | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | Škola |
| **Iné zainteresované strany** | | | NCU |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 97% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | 1/ Podľa dostupnosti služby, kde do Čas nesúladu sú započítavané trvania Nesúladu služby so severitou 1, 2  2/ Podľa služby: Riešenie incidentov |
| **Doba vyhodnocovania** | | | | 1 krát mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Pokrytie vnútorných priestorov učební a chodieb |
| **Definícia** | | Plné sieťové pokrytie pre bezproblémové pripojenie klientov a udržanie pripojenia pre všetky pripájané body typu AP |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne |
| **Požadovaná hodnota** | **Jednotka** | % |
| **Minimum** | 100 |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 2** | **Názov:** | | Pokrytie vonkajších priestorov – vonkajšie učebne |
| **Definícia** | | Plné sieťové pokrytie pre bezproblémové pripojenie klientov a udržanie pripojenia pre všetky pripájané body typu AP vonkajší |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne |
| **Požadovaná hodnota** | **Jednotka** | % |
| **Minimum** | 100 |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 3** | **Názov:** | | Sila signálu vo vnútorných priestoroch učebne v definovanej výške na frekvenciách v definícii služby |
| **Definícia** | | Intenzita signálu na zabezpečenie primeraného pripojenia vo vnútorných priestoroch |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ s podporou Školy |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | dBm |
| **Minimum** | -77 |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 4** | **Názov:** | | Pokrytie vonkajších priestorov – vonkajšie učebne |
| **Definícia** | | Intenzita signálu na zabezpečenie primeraného pripojenia pre vonkajšie učebne |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ s podporou Školy |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | dBm |
| **Minimum** | -80 |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 5** | **Názov:** | | Odstupu signál od šumu SNR vo vnútorných priestoroch |
| **Definícia** | | Minimálna hodnota odstupu signálu od šumu (signál, ktorý nevie dekódovať rádio pripojeného klienta) |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ s podporou Školy |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | dBm |
| **Minimum** | 20 |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 6** | **Názov:** | | Čas potrebný na pripojenie WiFi klienta |
| **Definícia** | | Maximálny čas medzi spustením pripojenia klienta k zvolenému SSID až po schopnosť komunikovať do siete internet, musí byť na prvkoch v pôsobnosti RPŠ zabezpečený tak aby E2E parameter v celej DigiNET sieti spĺňala požadovanú hodnotu 10 000 ms |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | ms |
| **Minimum** | nie je obmedzené |
| **Maximum** | 15 000 |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |

Tabuľka 2: Zabezpečovanie pokrytia siete WLAN – definícia požiadaviek na službu

### Zabezpečovanie pokrytia LAN

| **Zabezpečovanie pokrytia siete LAN - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Zabezpečovanie pokrytia siete LAN |
| **Kategória** | | | | Služby zabezpečovania prevádzky riešenia LAN/WLAN |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Služba zabezpečovania pokrytia siete LAN zahŕňa zabezpečenie káblového sieťového pripojenia v interiérových priestoroch – učebne. Štandard vyžaduje službu pokrytia – 2 RJ45 zásuvka v každej učebni. Cieľom je dosiahnuť optimálne LAN pokrytie ktoré umožní spoľahlivé pripojenie zariadení pomocou fyzických káblových pripojení a bezpečnosť riadenia prístupu do siete. |
| **Zabezpečovanie pokrytia siete LAN - detailná definícia požiadaviek na službu** | | | | |
| RPŠ poskytuje prevádzku komplexných služieb súvisiacich s pokrytím LAN ktoré zahŕňajú nasledujúce činnosti:   * poskytuje káblové pripojenia v učebniach, * zabezpečuje zakončenia jednoznačne označenou 2x zásuvkou RJ45 v každej učebni (pripájané body LAN), * zabezpečuje, aby boli AP napájané priamo alebo patch káblom zo samostatnej zásuvky RJ45 dovedenej výhradne pre účely pripojenia AP (pripájané body AP), * poskytovanie manažovaných prepínačov s podporou napájania PoE (Power over Ethernet) pre účely pripojenia AP, * zabezpečenie plného pokrytia požadovanej kapacity PC miest učební informatiky, pričom každý počítač v učebni musí mať LAN pripojenie. * Zabezpečuje káblové prepojenie aktívnych prvkov v sieti * Zabezpečuje budovanie pasívnej infraštruktúry v lokalitách škôl, Vybudovaná kabeláž na škole však musí byť schopná v budúcnosti podporovať rýchlosti 10 Gbit/s. Z tohto dôvodu je v prípade inštalácie metalickej kabeláže požadovaná minimálne Cat6A a v prípade potreby inštalácie optickej kabeláže môže byť použitá OM4 ak to maximálna vzdialenosť Switch-Switch umožňuje. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | Škola |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 97% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | 1/ Podľa dostupnosti služby, kde do Čas nesúladu sú započítavané trvania Nesúladu služby so severitou 1, 2  2/ Podľa služby: Riešenie incidentov |
| **Doba vyhodnocovania** | | | | 1 krát mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Počet funkčných RJ45 zásuviek v každej učebni |
| **Definícia** | | Dostupnosť služieb na minimálne dvoch RJ45 zásuvkách v každej učebni pre káblové pripojenie zariadení. |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Switche proaktívne, reaktívne |
| **Požadovaná hodnota** | **Jednotka** | ks |
| **Minimum** | 2 x počet učební |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 2** | **Názov:** | | Maximálny výstupný výkon PoE |
| **Definícia** | | Každý PoE port pre pripojenie AP port musí byť schopný dodávať energiu podľa štandardu IEEE 802.3af |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | W |
| **Minimum** | 15,4 |
| **Maximum** |  |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 3** | **Názov:** | | Dostupnosť služieb pre RJ45 prípojky PC v PC učebni |
| **Definícia** | | Zabezpečenie plného pokrytia požadovanej kapacity učební informatiky pre taký počet PC/NTBK pre ktoré je učebňa určená. |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | ks |
| **Minimum** | Kapacita PC/NTBK učebne informatiky |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Severity 3 |

Tabuľka 3: Zabezpečovanie pokrytia siete LAN – definícia požiadaviek na službu

### Zabezpečovanie priepustnosti v sieti WLAN

| **Zabezpečovanie priepustnosti v sieti WLAN - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Zabezpečovanie priepustnosti v sieti WLAN |
| **Kategória** | | | | Služby zabezpečovania prevádzky riešenia LAN/WLAN |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Priepustnosť v kontexte WLAN sa vzťahuje na rýchlosť, akou sa užitočné údaje úspešne prenášajú z jedného bodu do druhého v rámci lokálnej siete. Je to metrika na posúdenie výkonnosti a efektívnosti siete v lokalite školy. Nasledujúce parametre definujú minimálnu a očakávanú priepustnosť pre poskytované služby WLAN, ako aj požiadavky na technické možnosti zabezpečiť férové a rovnomerné využívanie služby viacerými používateľmi, aby nedochádzalo k nadmernému vyťažovaniu neopodstatnenou prevádzkou. |
| **Zabezpečovanie priepustnosti v sieti WLAN - detailná definícia požiadaviek na službu** | | | | |
| RPŠ poskytuje prevádzku komplexných služieb súvisiacich s priepustnosťou v sieti WLAN. Štandardom služby pritom je:   * pripojenie WiFi AP metalickým rozhraním RJ45, rýchlosť min. 1 Gbit/s k LAN prepínaču, * IEEE 802.11e/WMM, * band steering – podpora funkcionality AP, ktorá preferuje pripojenie klientov k 5Ghz, * rate limit – WiFi AP musí podporovať nastavenie minimálnej prenosovej rýchlosť obslužných rámcov (management frames) buď na základe jednotlivých pásiem alebo na základe jednotlivých SSID, * RX-SOP – zariadenie musí podporovať konfiguráciu minimálnych prahových hodnôt RSSI, * shaping dátovej prevádzky umožňujúci na jednotlivé SSID definovať kapacitné limity, ktoré umožnia:   + možnosť definovať download a upload maximá pripojených klientov k danému SSID,   + definovať download a upload maximá agregovane pre jednotlivé SSID, * rýchlosť prenosu dát v pásme 2.4 a aj 5 Ghz, pri šírke kanála 20 Mhz a 2 spatial-streams meraného od WIFI AP k jedinému (1) WiFi klientovi kategórie smart phone alebo tablet 100 Mbps, pričom meranie musí byť uskutočnené medzi klientom a WIFI AP, alebo softvérom, ktorý zvolí RPŠ, * rýchlosť prenosu dát v pásme 2.4 a aj 5 Ghz, pri šírke kanála 20 Mhz a 2 spatial-streams meraného medzi päťdesiatimi (50) WiFi klientami kategórie smart phone alebo tablet 3 Mbps medzi klientom a WIFI AP, alebo softvérom, ktorý zvolí RPŠ, * Podporovaná schopnosť merania rýchlosti pripojených klientov – tzn., realizovať testy priepustnosti medzi WiFi klientom a AP, * schopnosť RPŠ monitorovať akou rýchlosťou (data rate) je konkrétny WiFi klient pripojený. * Schopnosť RPŠ vykonávať real-time spektrálnu analýzu 2,4 a 5 Ghz pásma bez ovplyvnenia dátovej prevádzky WiFi klientova odhaliť interferencie ako aj kvantifikovať mieru využitia (utlizácie) všetkých kanálov príslušného spektra 2.4 a 5 Ghz, priemerovanú za min. posledných 60 sekúnd. Hodnoty utilizácie všetkých dostupných rádiových kanálov v pásme 2.4 Ghz a 5 Ghz určené ako aritmetický priemer meraní za posledných min.60 sekúnd nesmú prekročiť hodnotu 70% | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | Škola |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 99,5% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | 1/ Podľa dostupnosti služby, kde do Čas nesúladu sú započítavané trvania Nesúladu služby so severitou 1, 2  2/ Podľa služby: Riešenie incidentov |
| **Doba vyhodnocovania** | | | | 1 krát mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Priepustnosť na 1 klienta v pásmach 2.4 Ghz a 5 Ghz |
| **Definícia** | | Rýchlosť prenosu dát dostupná pre jedného klienta voči AP, resp. testovaciemu SW |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ s podporou školy |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Mbit/s |
| **Minimum** | 90 |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 2** | **Názov:** | | Priepustnosť pri počte 50 klientov v pásmach 2.4 Ghz a 5 Ghz |
| **Definícia** | | Priepustnosť na 1 používateľa pri počte maximálne 50 klientov na AP v pásmach 2.4 Ghz a 5 Ghz |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ s podporou školy |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Mbit/s |
| **Minimum** | 2 |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 3** | **Názov:** | | Agregovaná priepustnosť pre jeden pripájaný bod AP |
| **Definícia** | | Celková rýchlosť prenosu dát dostupná pre všetkých používateľov a zariadenia pripojené na AP |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Mbit/s |
| **Minimum** | 900 |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 4** | **Názov:** | | Minimálna priepustnosť z AP do siete LAN |
| **Definícia** | | Minimálna priepustnosť do siete LAN z prístupového bodu |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Mbit/s |
| **Minimum** | 900 |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |

Tabuľka 4: Zabezpečovanie priepustnosti v sieti WLAN – definícia požiadaviek na službu

### Zabezpečovanie priepustnosti v sieti LAN

| **Zabezpečovanie priepustnosti v sieti LAN - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Zabezpečovanie priepustnosti v sieti LAN |
| **Kategória** | | | | Služby zabezpečovania prevádzky riešenia LAN/WLAN |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Priepustnosť v LAN sieti sa vzťahuje na rýchlosť, akou sa údaje úspešne prenášajú z jedného bodu do druhého v rámci lokálnej siete. Je to metrika na posúdenie výkonnosti a efektívnosti siete. |
| **Zabezpečovanie priepustnosti v sieti LAN - detailná definícia požiadaviek na službu** | | | | |
| V rámci zabezpečovania služieb RPŠ obstarávania očakávame, že vybraný dodávateľ poskytuje prevádzku komplexných služby súvisiacich s priepustnosťou v sieti LAN. Štandardom služby pritom je:   * pripojenie WiFi AP (indoor aj outdoor) ako aj klientskych pracovných staníc (PC) rýchlosťou 1 Gbit/s k switchu, * prepojenie switchov medzi sebou (v prípade, že to vyžaduje topológia zapojenia) rýchlosťou min. 1 Gbit/s, * prepojenie switcha (resp. switchov – podľa riešenia topológie zapojenia) na CPE prvok rýchlosťou min. 1 Gbit/s, * switch podporuje prenosovú kapacitu pri plnom obsadení všetkých portov, * schopnosť RPŠ v reálnom čase skontrolovať vyťaženie switcha:   + prevádzkou sumárne, min. za posledný deň, týždeň a mesiac,   + prevádzkou na jednotlivých portoch, min. za posledný deň, týždeň a mesiac:     - objem dát prenesených v prichádzajúcom smere, odchádzajúcom smere a celkovo,     - aktuálnu rýchlosť dátových tokov na jednotlivých portoch v smere prichádzajúcom, odchádzajúcom, * schopnosť on-line real-time merania latencie a stratovosti medzi switchmi, * schopnosť on-line real-time merania latencie a stratovosti medzi switchom a AP, * schopnosť on-line real-time merania latencie a stratovosti medzi switchom a CPE. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | Škola |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 99,5% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | 1/ Podľa dostupnosti služby, kde do Čas nesúladu sú započítavané trvania Nesúladu služby so severitou 1, 2  2/ Podľa služby: Riešenie incidentov |
| **Doba vyhodnocovania** | | | | 1 krát mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Agregovaná priepustnosť pre každú učebňu |
| **Definícia** | | Celková rýchlosť prenosu dát dostupná pre všetky zariadenia pripojené v učebni |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ s podporou školy |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Mbit/s |
| **Minimum** | 900 |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 2** | **Názov:** | | Individuálna priepustnosť pre každý port RJ45 |
| **Definícia** | | Podporovaná prenosová kapacita pre každé pripojené zariadenie prostredníctvom RJ45 rozhrania. |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ s podporou školy |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Mbit/s |
| **Minimum** | 900 |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 3** | **Názov:** | | Priepustnosť v core sieti LAN |
| **Definícia** | | Podporovaná prenosová kapacita medzi portami LAN infraštruktúry: medzi miestom pripojenia CPE a všetkými ostatnými LAN prepínačmi |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Gbit/s |
| **Minimum** | 1 |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 4** | **Názov:** | | Latencia v sieti LAN |
| **Definícia** | | Čas potrebný na prenos dátového paketu z jedného bodu do druhého v rámci siete |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | ms |
| **Minimum** | nie je obmedzené |
| **Maximum** | 5 |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 5** | **Názov:** | | Stratovosť paketov v sieti LAN |
| **Definícia** | | Percento stratených dátových paketov v rámci prenosu v sieti |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | % |
| **Minimum** | nie je obmedzené |
| **Maximum** | 0,1 |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |
| **Metrika 6** | **Názov:** | | Podporovaná prenosová kapacita pre novobudovanú pasívnu infraštruktúru v lokalite školy |
| **Definícia** | | Vybudovaná kabeláž na škole je schopná podporovať rýchlosti 10 Gbit/s. RPŠ zabezpečuje pokrytie pasívnou infraštruktúrou v súlade s požiadavkou podpory budúcich prenosov 10 Gbit/s |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | 24/7 |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Gbit/s |
| **Minimum** | 10 |
| **Maximum** | nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa rozsahu postihnutých pripájaných bodov definovaných podľa služby: Riešenie incidentov. Riešiteľ incidentu definuje a overí počet postihnutých pripájaných bodov a urči správnu severitu nesúladu. |

Tabuľka 5: Zabezpečovanie priepustnosti v sieti LAN – definícia požiadaviek na službu

Kvalitatívne parametre priepustnosti LAN služby RPŠ preukáže/potvrdí uvedením že spĺňa požadované požiadavky na služby a hodnoty merateľných parametrov pri akceptovaní riešenia v lokalite školy. Tieto parametre môže overiť meraním, ktoré musí obsahovať hodnoty nameraných požadovaných parametrov:

* meranie rýchlosti, latencie a stratovosti medzi zvoleným LAN portom každej učebne a LAN portom najbližšie k CPE,
* meranie rýchlosti, latencie a stratovosti medzi každým switchom vzájomne (zo zvoleného portu),

### Zabezpečovanie pripájania a výmeny CPE

| **Zabezpečovanie pripájania a výmeny CPE - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Zabezpečovanie pripájania a výmeny CPE |
| **Kategória** | | | | Služby zabezpečovania prevádzky riešenia LAN/WLAN |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Služby RPŠ pre zabezpečovanie on-site podpory zariadenia CPE umiestneného v lokalite školy, kontinuálne napájaného a pripojeného k WAN portom RPŠ a pripojeného k centrálnemu prepínaču lokality školy. |
| **Zabezpečovanie pripájania a výmeny CPE - detailná definícia požiadaviek na službu** | | | | |
| * RPŠ zabezpečuje on-site podporu pre poskytovateľa služieb NCU pre zariadenie CPE dodávaného poskytovateľom služieb NCU. * Zabezpečuje po dohode a usmernení s poskytovateľom služieb NCU výmenu CPE v lokalite školy pri riešení udalostí v sieti. * RPŠ udržiava potrebnú úroveň spare parts CPE dodávaných poskytovateľom služieb NCU. * RPŠ zabezpečuje skladovú adresu na ktorú mu dodáva poskytovateľ služieb NCU v potrebných kusoch CPE spare parts s podpisovaním akceptačného protokolu prijatých CPE zariadení. * Zasiela zariadenie CPE na opravu na adresu skladu poskytovateľa služieb NCU. * Zabezpečuje pripájanie CPE k centrálnemu switchu a k WAN portom, zabezpečuje napájanie CPE zariadenia. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | NCU |
| **Iné zainteresované strany** | | | Škola |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | N/A |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa času v tickete |
| **Doba vyhodnocovania** | | | | Po uzavretí ticketu |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Výmena zariadenia CPE |
| **Definícia** | | Zabezpečenie výmeny zariadenia CPE v lokalite školy |
| **Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | N/A |
| **Požadovaná hodnota** | **Jednotka** | pracovný deň od nahlásenia/identifikácie |
| **Minimum** | nie je obmedzené |
| **Maximum** | 1 |
| **Severita Nesúladu služby** | | Severity 1 |

Tabuľka 6: Zabezpečovanie pripájania a výmeny CPE – definícia požiadaviek na službu

### Zaisťovanie sieťovej bezpečnosti WLAN

| **Zaisťovanie sieťovej bezpečnosti WLAN - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Zaisťovanie sieťovej bezpečnosti WLAN |
| **Kategória** | | | | Služby zabezpečovania prevádzky riešenia LAN/WLAN |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Zaisťovanie sieťovej bezpečnosti WLAN zahŕňa implementáciu bezpečnostných opatrení nevyhnutných pre ochranu citlivých údajov, zaručenie kontinuity služieb a v spolupráci s NCU zabezpečenie spoľahlivého prístupu pre relevantných používateľov siete, vrátane zamestnancov školy(učitelia a iný personál), študentov a hostí. |
| **Zaisťovanie sieťovej bezpečnosti WLAN - detailná definícia požiadaviek na službu** | | | | |
| * WPA2-Preshared key, WPA2-Enterprise s IEEE 802.1X, * WPA3-Preshared key, WPA3-Enterprise s IEEE 802.1X, * WPA3 - Enhanced Open (OWE) - šifrovanie dát bez potreby tradičnej autentifikácie, * DHCP a RA Guard - schopnosť zariadenia zabezpečiť, že pre dané SSID rozdáva IP adresy pre klientov len definovaný legitímny DHCP server, * schopnosť priraďovať VLAN tag pre používateľov pripojených ku konkrétnemu SSID, * schopnosť priraďovať rôzne VLAN tagy pre rôzne AP, pričom sa zachová rovnaké SSID, * schopnosť priraďovať VLAN tag na používateľskej báze za predpokladu použitia Radius servera, * RPŠ sa riadi nastavením segmentov a mapovaním do segmentov podľa požiadaviek/inštrukcií NCU, * RPŠ pre služby centrálnej autentifikácie používateľov školy pre overenie a riadenia ich prístupu do siete WLAN v lokalite školy spolupracuje s NCU a podľa metodických usmernení, * RPŠ pre služby lokálnej autentifikácie používateľov školy pre overenie a riadenia ich prístupu do siete WLAN v lokalite školy spolupracuje s NCU a podľa metodických usmernení, * Guest WiFi – kompletná izolácia pripojených guest zariadení (nemožnosť komunikovať medzi pripojenými guest zariadeniami), * podpora blokovania (firewallingu) pre jednotlivé SSID, umožňujúca nastavenie aby:   + klienti pripojení k danému SSID mohli komunikovať len na zvolené cieľové IP adresy a porty, * nepretržitá klasifikácia WiFi AP ako autorizované, susedné alebo neautorizované (rogue), pričom služba umožňuje detegovať:   + pripojenie neautorizovaného WiFi AP do spravovanej siete LAN,   + vyžarovanie rovnakého SSID aké poskytuje služba WiFi neautorizovaným WiFi AP,   + DOS útoky spôsobený zasielaním nadmerného množstva deautentifikačných, disasociačných a manažment rámcov.   + Reagovať na hrozby nasledovne:     - zablokovaním neautorizovaného WiFi AP pripojeného do spravovanej siete LAN RPŠom,     - zaslaním emailu zodpovedným osobám, vytvorením Syslog informácie, a zaznamenaním eventu v manažmente WLAN riešenia. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | Škola, NCU |
| **Iné zainteresované strany** | | | NCU |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | N/A |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa služby: Riešenie incidentov |
| **Doba vyhodnocovania** | | | |  |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Sieťová bezpečnosť |
| **Definícia** | | V súlade s požiadavkami popísaných v definícii služby |
| **Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | N/A |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO v súlade |
| **Maximum** | N/A |
| **Severita Nesúladu služby** | | Severity 2 |

Tabuľka 7: Zaisťovanie sieťovej bezpečnosti WLAN – definícia požiadaviek na službu

### Zaisťovanie sieťovej bezpečnosti LAN

| **Zaisťovanie sieťovej bezpečnosti LAN - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Zaisťovanie sieťovej bezpečnosti LAN |
| **Kategória** | | | | Služby zabezpečovania prevádzky riešenia LAN/WLAN |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Zaisťovanie sieťovej bezpečnosti LAN zahŕňa implementáciu bezpečnostných opatrení nevyhnutných pre ochranu citlivých údajov, zaručenie kontinuity služieb a zabezpečenie spoľahlivého a autentifikovaného prístupu pre relevantných používateľov siete v spolupráci s NCU. |
| **Zaisťovanie sieťovej bezpečnosti LAN - detailná definícia požiadaviek na službu** | | | | |
| Štandardom služby je:   * IEEE 802.1X, RADIUS, * podpora autentifikácie v režime:   + Single host – na porte sa pripája a autentifikuje jediný používateľ,   + Multi domain – na porte sa pripájajú a autentifikujú zariadenia z rôznych VLAN domén – napr. IP Telefón a za ním PC, * multi Auth – na porte sa pripájajú viacerí používatelia, pričom každý je autentifikovaný zvlášť, * dynamické prideľovanie VLAN na základe Radius autentifikácie, * voľba pridelenej VLAN pri zamietnutí autentifikácie, * podpora MAB – MAC Authentication Bypass – overovanie MAC adresy pripojeného zariadenia voči RADIUS serveru, v prípade, že zariadenie nedisponuje 802.1X suplicant softvérom, * MAB musí byť možné nastaviť ako záložný mechanizmus, ak zlyhá 802.1X, * MAC filter adries na porte:   + Static-MAC-list - možnosť pre každý port prepínača definovať zoznam min. 15 povolených MAC adries,   + Sticky-MAC - možnosť sa na porte naučiť povolený počet MAC adries – min.15, ktoré budú následne zapamätané a do budúcna povolené, * Radius Accounting – sledovanie pripojených klientov, RFC 2869, * preverovanie dostupnosti Radius servera – switch musí kontrolovať dostupnosť Radius služby, * v prípade nedostupnosti Radius servera, možnosť definície záložnej fall-back VLAN do ktorej bude zariadenie priradené, * SYSLOG – logovanie udalostí na definovaný Syslog server, * ACL IPv4 – možnosť definovať access-control-list na obmedzenie prevádzky v definovanej VLAN na základe definície zdroja: IP adresa (resp. rozsah), protokol (TCP,UDP), port a cieľa: IP adresa (resp. rozsah), port, * DHCP snooping a Dynamická inšpekcia ARP – bezpečnostný mechanizmus vynucujúci že ARP odpovede od klientov sú v zhode s mapovaním na ich DHCP pridelenú IP adresu, * STP ochranné mechanizmy:   + Root Guard,   + BPDU Guard,   + Loop Guard, * RPŠ sa riadi nastavením segmentov a mapovaním do segmentov podľa požiadaviek/inštrukcií NCU, * RPŠ pre služby centrálnej autentifikácie používateľov školy pre overenie a riadenia ich prístupu do siete LAN v lokalite školy spolupracuje s NCU podľa metodických usmernení, * RPŠ pre služby lokálnej autentifikácie používateľov školy pre overenie a riadenia ich prístupu do siete LAN v lokalite školy spolupracuje s NCU podľa metodických usmernení. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | Škola, NCU |
| **Iné zainteresované strany** | | | NCU |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | N/A |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa služby: Riešenie incidentov |
| **Doba vyhodnocovania** | | | | N/A |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Sieťová bezpečnosť |
| **Definícia** | | V súlade s požiadavkami popísaných v definícii služby |
| **Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | N/A |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO v súlade |
| **Maximum** | N/A |
| **Severita Nesúladu služby** | | Severity 2 |

Tabuľka 8: Zaisťovanie sieťovej bezpečnosti LAN – definícia požiadaviek na službu

### RACI matica pre služby zabezpečovania prevádzky riešenia LAN/WLAN

| **Popis činnosti** | **Škola** | **RPŠ** | **NCU** | **MŠVVaM** |
| --- | --- | --- | --- | --- |
| Dodržiavanie požadovanej hodnoty merateľného parametra**: Čas potrebný na pripojenie klienta WiFi** na prvkoch v pôsobnosti RPŠ | I | A,R | C | I |
| Dodržiavanie požadovanej hodnoty merateľného parametra**: Čas potrebný na pripojenie klienta WiFi** na prvkoch v pôsobnosti NCU | I | C | A,R | I |
| Odstraňovanie nedostatkov identifikovaných na strane školy | A,R | C | I | I |
| Odstraňovanie nedostatkov identifikovaných na strane RPŠ | C | A,R | I | I |
| Odstránenie cudzieho zariadenia spôsobujúceho nameranú interferenciu v priestoroch školy | A,R | C | I | N/A |
| Sprístupnenie priestorov, sprevádzanie, súčinnosť pri plánovaní a riešení problémov | R | C | N/A | A |
| Dodanie CPE na centrálny sklad NCU a zapečenie potrebných kusov na distribúciu pre RPŠ, distribúcia na RPŠ | N/A | C | A,R | N/A |
| Distribúcia, Inštalácia v centrálnom rozvádzači a napájanie CPE na škole | I | A,R | C | N/A |
| Konfigurácia a správa CPE | I,C | C | A,R | N/A |
| Správa a údržba aktívnych a pasívnych prvkov riešenia | C | A,R | N/A | N/A |
| Zabezpečenie prvkov riešenia LAN/WLAN proti krádeži a poškodeniu treťou osobou | A,R | C | N/A | N/A |
| Identifikácia, odstraňovanie a náprava bezpečnostných hrozieb, nedostatkov a incidentov v riešení v pôsobnosti RPŠ | I | A,R | C | I |
| Zablokovanie prístupu k neovereným SSID definovaným školou v priestoroch pokrytia službou DigiNET, ktoré sú detegované zariadeniami v správe RPŠ v rámci sieťovej infraštruktúry školy | A,R | C,I | N/A | N/A |

Tabuľka 9: RACI matica pre služby zabezpečovania prevádzky riešenia LAN/WLAN

## Služby zabezpečovania WAN konektivity

Cieľom služieb dátovej konektivity škôl je zabezpečovanie kvalitného dátové pripojenie škôl s dostatočnou priepustnosťou odvodenou na základe počtu používateľov na škole a zabezpečením každoročného nárastu prenosových rýchlosti, zabezpečovanie služieb LAN/WLAN a NCU s požadovanými hodnotami parametrov.

Služba podporuje realizácie privátnej siete k Centrálnemu uzlu pre zabezpečenie centrálnych služieb bezpečnosti a bezpečného prechodu konektivity škôl do internetu.

### Zabezpečovanie primárnej dátovej konektivity a jej zálohy

| **Zabezpečovanie primárnej dátovej konektivity a jej zálohy - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Zabezpečovanie dátovej konektivity a jej zálohy |
| **Kategória** | | | | Služby zabezpečovania WAN konektivity školy |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | V rámci zabezpečovania služieb konektivity RPŠ poskytuje prevádzku komplexných služieb dátovej konektivity na pripojenie škôl k NCU s  parametrami: rýchlosť pripojenia, dostupnosť pripojenia, latencia a požiadavkou ročné navyšovanie rýchlosti. |
| **Zabezpečovanie primárnej dátovej konektivity a jej zálohy - detailná definícia požiadaviek na službu** | | | | |
| * WAN rozhraním dátovej konektivity školy (primárnym aj záložným) sa myslí fyzický port na dedikovanom zariadení poskytovateľa konektivity. * WAN rozhrania sú využívane CPE zariadením dodávaným dodávateľom NCU. * WAN rozhranie školy je odovzdávané na sieťovej úrovni L2 alebo L3. * RPS odovzdáva WAN rozhranie na metalickom Ethernete typu 1000BaseT; zodpovedajúce požadovanej rýchlosti pripojenia lokality. * Zabezpečovanie konektivity primárne optickými prístupovými technológiami, odporúčame preferovanie optickej technológie v prípade že je lokalita školy v jej pokrytí. Alternatívne rádiovými prístupovými technológiami, prípadne takými metalickými prístupovými technológiami, ktoré zabezpečia potrebné prenosové rýchlosti. * Zabezpečovanie prenosových rýchlosti dátového pripojenia Downlink/Uplink školy na WAN rozhraní.  Požadovaná hodnota rýchlosti pripojenia v prvom roku je uvedená v tejto tabuľke nižšie. V prípade ak dátové pripojenie školy nebude na základe intruzívnych meraní dosahovať požadovanú hodnotu metriky Yn prenosovej rýchlosti, považuje sa to za Nesúlad služby. Profil WAN konektivity je určený pre každú školu podľa počtu požívateľov v prvom roku začatia poskytovania služieb ak nie je uvedený vyšší. * Požadovaná rýchlosť uplink je minimálne 25% z požadovanej downlink rýchlosti. V prípade ak dátové pripojenie školy nebude na základe intruzívnych meraní dosahovať požadovanú hodnotu metriky Yn prenosovej rýchlosti, považuje sa to za Nesúlad služby. Profil WAN konektivity je určený pre každú školu podľa počtu požívateľov v prvom roku začatia poskytovania služieb ak nie je uvedený vyšší. * Požadujeme navyšovanie požadovanej rýchlosti WAN konektivity o 15% ročne. Zabezpečovanie navyšovania požadovanej rýchlosti z predchádzajúceho školského roku je o 15%. K navýšeniu musí prísť pred začatím nového školského roku. K navýšeniu nedochádza pri dosiahnutí 1000 Mbit/s, resp. ak už škola podľa uvedeného počtu používateľov už požadovanú rýchlosť v danom roku spĺňa. * **Požadované rýchlostné profily:**      * RPŠ zabezpečuje, aby na celej trase od WAN rozhrania školy až do odovzdania dátovej prevádzky v NCU, prípadne na trase medzi školami, nedochádzalo k strate požadovanej prenosovej rýchlosti. * V prípade že škola aktuálne využíva vyššiu ako požadovanú rýchlosť dátového pripojenia podľa základného modelu riešenia, táto zvýšená požiadavka bude uvedená pre danú školu. Povinnosťou RPŠ bude zabezpečovať na škole zodpovedajúcu rýchlosť. Zároveň platí požiadavka 15% navyšovania rýchlosti ročne, avšak len v prípade že škola pre predpokladaný počet používateľov na škole v príslušnom roku podľa tabuľky vyššie, ešte nedosahuje minimálne požadovanú rýchlosť. * Potvrdzovanie navýšenia požadovanej rýchlosti vždy k 2. septembru vykonaním intruzívneho merania prenosovej rýchlosti podľa služby: „Vytváranie správy o intruzívnom meraní kapacity linky“. * V prípade že je to v lokalite technicky možné bez navýšenia ceny služby poskytovať aj vyššiu prenosovú rýchlosť, obstarávateľ požaduje od RPŠ aby neobmedzoval rýchlostný profil WAN konektivity a dosahoval najvyššiu možnú priepustnosť. Typicky: dátová konektivita je odovzdávaná na 1Gbit/s optickom interface ale RPŠ ju redukuje napríklad na 150 Mbit/s. * Poskytovanie záložného dátového pripojenia v prípade výpadku primárnej konektivity počas Prevádzkovej doby služby. Záložná konektivita je poskytovaná až do momentu zabezpečenia Súladu služby primárnej dátovej konektivity – obnovenia pripojenia. * V prípade prechodu školy na záložnú konektivitu RPŠ zabezpečuje že kapacita záložného pripojenia je výhradne poskytovaná pre časť LAN/WLAN určenej pre pedagógov, zamestnancov školy. * Adresa odovzdávania dátovej prevádzky školy do NCU (miesto prepojenia RPŠ a NCU) je na spoločnej dohode prevádzkovateľa služieb NCU a RPŠ. * Prepojenie RPŠ a NCU je riešené georedundantne. * RPŠ zabezpečuje dostatočnú kapacitu linky pre pripojenie na NCU tak aby nedochádzalo k degradácii prenosových rýchlosti z lokalít škôl. * Poznámka: celková kapacita georedundantného prepojenia je výsledkom počtu škôl ktoré RPŠ obsluhuje. RPŠ a poskytovateľ služieb NCU ju odvodia v spolupráci na základe požadovaných kapacít podľa pasportov obsluhovaných škôl. * RPŠ a NCU spoločne navyšujú kapacitu pri dosiahnutí 80% maximálnej kapacity prepojenia RPŠ a NCU. * Poskytovanie bezpečnej komunikácie. Pripojenie je šifrované a prostredníctvom šifrovacích protokolov požadujeme selektívne definovať bezpečnostné parametre, definovať spôsob utajenia prenosu, spôsob verifikácie odosielateľa a spôsob algoritmického zabezpečenia celistvosti prenášaných dát. * Pripojenie pre vybraných požívateľov do DigiNET bude možné aj z Internetu cez IPSEC VPN klienta, ako vzdialený prístup. Vzdialený prístup bude zabezpečovať poskytovateľ služieb NCU. * Podpora site-to-site IPSec pre minimálne 2 paralelne zostavené tunely s priepustnosťou do maximálnej rýchlosti konkrétnej školy.   Meranie skutočnej priepustnosti WAN konektivity.   * Meraná je priepustnosť medzi Školou a RPŠ (alebo NCU) v oboch smeroch. * Automatické meranie zabezpečí RPŠ pravidelne 1x za kvartál mimo Prevádzkovej doby služby, napríklad večer, aby meranie neobmedzilo dátovú prevádzku školy v čase vyučovania. * Škola môže v prípade pochybností o priepustnosti WAN pripojenia 1x mesačne požiadať aj o mimoriadne meranie v rámci Prevádzkovej doby služby. Škola navrhne minimálne 72 hodín vopred čas vykonania merania, RPŠ uskutoční meranie a informuje školu o výsledku a zapracuje do reportu. Škola je povinná akceptovať dočasné prerušenie WAN konektivity v čase vykonávania tohto mimoriadneho intruzívneho merania. * V prípade požadovaného automatického navýšenia kapacity WAN pripojenia k prvému septembru (k začiatku nového školského roka) bude nová priepustnosť potvrdená meraním. Meranie musí byť vykonane v pracovný deň každú hodinu od 8:00 do 14:00 pred začiatkom školského roka a výsledkom merania bude priemerná hodnota z týchto meraní. Meranie je vykonávané minimálne každú hodinu v 3h intervale. * Z pohľadu priority zabezpečovania služieb RPŠ požadujeme v prvých etapách realizácie zriadenia služieb od RPŠ v lokalite školy prioritne riešiť prípravu realizácie a zriaďovanie WAN konektivity škôl a to najmä z dôvodu možnej technickej a najmä časovej náročnosti zriadenia konektivity.   Akceptácia služieb RPŠ   * V prípade potreby a technickej pripravenosti zo strany RPŠ môže obstarávateľ požiadať RPŠ o zabezpečenie pripojenia lokality školy do siete internet. RPŠ teda bude v prípade potreby na požiadavku obstarávateľa pomocou konektivity zabezpečovať prístup školy priamo do siete internet, až do úspešného zriadenia a akceptácie všetkých požadovaných služieb v lokalite. * Obstarávateľ teda môže RPŠ akceptovať WAN konektivitu samostatne v prípade že na nej bude na požiadavku obstarávateľa dočasne RPŠ zabezpečovať službu pripojenia na Internet. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | Škola, NCU, RPŠ |
| **Iné zainteresované strany** | | | NCU |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | 97% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | 1/ Podľa dostupnosti služby  2/ Podľa služby: Riešenie incidentov |
| **Doba vyhodnocovania** | | | | 1 krát mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Aktuálny stav primárnej konektivity |
| **Definícia** | | Využívanie a status dátového pripojenia WAN na rozhraním školy |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne |
| **Požadovaná hodnota** | **Jednotka** | Mbit/s |
| **Minimum** | Plynulá dátová prevádzka školy bez obmedzení pri požadovanom profile linky |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Severity 1 |
| **Metrika 2** | **Názov:** | | Rýchlosť odozvy (latencia) |
| **Definícia** | | Čas potrebný na prenos dátového paketu z jedného bodu do druhého v milisekundách. |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne a reaktívne |
| **Požadovaná hodnota** | **Jednotka** | ms |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 50 |
| **Severita Nesúladu služby** | | Severity 2 |
| **Metrika 3** | **Názov:** | | Minimálne dostupná prenosová rýchlosť Downlink/Uplink primárnej konektivity podľa intruzívneho merania |
| **Definícia** | | Minimálne dostupná rýchlosť na WAN rozhraním školy |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne a reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Mbit/s |
| **Minimálne dostupná rýchlosť = 90% požadovanej rýchlosti** | |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Severity 1 |

Tabuľka 10: Zabezpečovanie primárnej dátovej konektivity – definícia požiadaviek na službu

| **Zabezpečovanie záložnej dátovej konektivity - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | Škola, NCU, RPŠ |
| **Iné zainteresované strany** | | | NCU |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | |  |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Poľa času v tickete o zaznamenaní spustenia služby náhradného riešenia výpadku primárnej dátovej konektivity |
| **Doba vyhodnocovania** | | | | 1 krát mesačne v prípade že nastane využitie zálohy. |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Aktivácia záložného pripojenia od výpadku primárneho pripojenia |
| **Definícia** | | Doba do ktorej je potrebné aktivovať záložné dátové pripojenie školy pri výpadku primárneho pripojenia v čase mimoriadnych situácií |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne a reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Minúty |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 30 |
| **Severita Nesúladu služby** | | N/A |

Tabuľka 11: Zabezpečovanie primárnej dátovej konektivity a jej zálohy- detailná definícia požiadaviek na službu

### RACI matica pre služby zabezpečovania WAN konektivity

| **Popis činnosti** | **Škola** | **RPŠ** | **NCU** | **MŠVVaM** |
| --- | --- | --- | --- | --- |
| Poskytovanie vzdialeného prístupu do siete školy podľa potrieb školy | C | C | A,R |  |
| Prepnutie na záložnú konektivitu v prípade výpadku primárnej linky a zabezpečenie dátovej konektivity v príslušných častiach siete | I | R | A,R | I |
| Dohoda s poskytovateľmi pripojenia a prevádzkovateľmi pokrytia na adrese školy | C | A,R | C | N/A |

Tabuľka 12: RACI matica pre služby zabezpečovania WAN konektivity

## Služby manažmentu a monitoringu riešenia LAN/WLAN/WAN

Služby monitoringu a manažmentu siete zabezpečujú sledovanie a správu siete LAN a WLAN, pričom poskytujú ucelený obraz o prevádzkovom stave inštalovanej infraštruktúry a služby.

V tejto sekcii obstarávateľ definuje požiadavky na služby v dvoch alternatívach. Služby sú definované s rovnakou úrovňou kvality a špecifikáciou. Cieľom obstarávateľa je aby RPŠ spĺňal kritéria pre obe alternatívy pričom obstarávateľ na základe výsledku obstarávania definuje alternatívu ktorou bude RPŠ služby poskytovať.

* Alternatíva 1: RPŠ poskytuje služby centralizovaného riešenia správy a dohľadu prostredníctvom systémov vo vlastnej zodpovednosti.
* Alternatíva 2: RPŠ Poskytuje služby centralizovaného riešenia správy a dohľadu prostredníctvom služieb NCU (NCU-CRSD). NCU-CRSD je obstarávané samostatnou súťažou. Obstarávateľ obstaráva NCU-CRSD tak aby pomocou nich vedel RPŠ poskytovať služby v rovnakej kvalite a uvádza podporované prvky. Systémy sú prevádzkované poskytovateľom služieb NCU ku ktorým RPŠ pristupuje za účelom poskytovania služieb podľa tohoto opisu predmetu zákazky.

### Poskytovanie služieb centralizovaného riešenia správy a dohľadu (CRSD) priamo RPŠ – Alternatíva 1

| **Poskytovanie služieb centralizovaného riešenia správy a dohľadu (CRSD) priamo RPŠ - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Poskytovanie centralizovaného riešenia správy a dohľadu |
| **Kategória** | | | | Služby manažmentu a monitoringu riešenia LAN/WLAN |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Centralizované riešenie správy a dohľadu (ďalej len CRSD), súvisí s prevádzkou, monitorovaním, správou, údržbou sieťového riešenia, atď. Takáto služba umožní čo najefektívnejšie nasadenie riešenia, jeho správu, monitorovanie a diagnostiku. |
| **Poskytovanie služieb centralizovaného riešenia správy a dohľadu (CRSD) priamo RPŠ - detailná definícia požiadaviek na službu** | | | | |
| **Poskytovanie služieb CRSD**  Poskytovanie centralizovaného riešenia správy a dohľadu (ďalej len CRSD), súvisiaceho s prevádzkou, správou a údržbou sieťového riešenia.  Centralizovanou službou sa myslí spravidla jedno grafické prostredie (GUI) poskytujúce ucelenú funkcionalitu, dostupné vzdialene a on-line pre všetky relevantné organizácie prostredníctvom web klienta (štandardný internetový browser).  Služba je zabezpečovaná podľa nasledujúcich kritérií:   * Je neprípustné v kombinácii so službami NCU umiestňovanie serverov alebo akýchkoľvek dedikovaných kontrolérov do prostredia/lokality školy. RPŠ môže CRSD  vybudovať alebo inak zabezpečiť jeho prevádzku v private cloud prostredí, resp. On-premises dátové centrum alebo public cloud prostredí. Predložené CRSD riešenie musí byť:   + garantované vo funkčnom stave a podporujúce pridávanie funkcionality do produktov WiFi AP a switche zo strany ich výrobcov (ak títo budú pridávať nové vlastnosti) po celú dĺžku trvania prevádzky,   + prevádzkované na lokalitách určených RPŠ – napr. private cloud, on-premises dátové centrum, na náklady RPŠ,   + pri prevádzkovaní v public cloud prostredí, hostovanom v EU, garantujúcom požadovanú dostupnosť, na náklady RPŠ,   + dostupná vzdialene v reálnom čase, pričom musí byť možný prístup do grafického GUI prostredia zabezpečujúci náhľad prevádzkových a výkonnostných parametrov minimálne pre nasledovných určených pracovníkov:     - zamestnanci RPŠ     - zamestnanci školy/poverení pracovníci školy     - zamestnanci zriaďovateľa školy     - zamestnanci MŠVVaM SR a poverená osoba pre prípadný audit     - zamestnanci poskytovateľa NCU   CRSD služba musí vykonávať funkcie WiFi kontroléra – tzn., musí:   * vykonávať registráciu WiFi prístupových bodov, * zabezpečovať centrálne konfiguráciu všetkých AP, * zbierať informácie od jednotlivých AP vo vzťahu k frekvenciám použitým susedným AP, * minimalizovať interferenciu, nastavovať vysielací výkon a kanál, * vykonávať rádiofrekvenčné plánovanie (RRM) s cieľom maximalizovať kvalitné pokrytie signálom, * v prípade výpadku kontroléra zabezpečovať aby aktuálne pripojení klienti/používatelia nestratili prístup k službám WLAN.   RPŠ je povinný sa o dodané prvky infraštruktúry – WiFi a Switche starať pomocou CRSD, a to minimálne z pohľadu úvodného nastavenia,  úpravy a optimalizácií nastavení v čase, upgrade-ov OS/firmware aktívnych prvkov, dohľadu a monitoringu a riešení problémov.  Vzhľadom na očakávanú veľkosť projektu sa požaduje, aby CRSD nástroj podporoval API RESTFUL služby, ktoré musia:   * byť verejne zdokumentované, * dostupné počas celej doby trvania zmluvného vzťahu, * byť dostupné vzdialene a real-time, * poskytnúť informácie o konfiguráciách (WiFi AP a prepínačov), * poskytnúť informácie o pripojených zariadeniach v sieti (klientov), * chránené unikátnym API kľúčom s možnosťou revokácie.   **Služba onboardingu zariadení LAN/WLAN**  Z dôvodu jednoduchosti a rýchlosti nasadenia, budúceho rozširovania, urýchlenia výmen pokazených zariadení, minimalizácie ľudskej chyby ako aj ďalších dôvodov sa požaduje, aby dodané sieťové zariadenia - WiFi access point-y (indoor a outdoor) a switche podporovali a boli nasadené v režime ZTP – Zero Touch Provisioning.  Režimom ZTP sa myslí najmä:   * Schopnosť nového zariadenia bez predchádzajúcej konfigurácie sa po zapnutí a pripojení ku sieti poskytujúcej DHCP pridelenie adresy automatizovaným a zabezpečeným spôsobom prihlásiť do CRSD a stiahnuť si svoju konfiguráciu s ktorou má byť prevádzkované, bez potreby vykonávania predchádzajúcej konfigurácie (bez potreby tzv. pre-staging-u). Zároveň je možné vytvárať konfiguračné šablóny, zabezpečujúce konzistenciu konfigurácií. * Pri onboardingu zariadení sa navyše musia automaticky stiahnuť potrebné aktualizácie firmvéru a bezpečnostné záplaty, odporúčané výrobcom týchto zariadení. * Dodané riešenie CRSD musí za týmto účelom takéto ZTP služby umožňovať.   **Služba konfigurácie zariadení LAN/WLAN**  CRSD musí poskytovať centralizovanú službu správy konfigurácii umožňujúcu minimálne nasledovné:   * kompletnú konfiguráciu WiFi AP a switchov bez nutnosti používať iné nástroje, * priradiť zariadeniam popisné označenie/meno, * priradiť Ethernet rozhraniam switchov popisné označenia, * konfigurovať zariadenia:   + individuálnym spôsobom   + prostredníctvom konfiguračných šablón umožňujúcich aplikovať zvolené nastavenia hromadným spôsobom – napr. pre všetky AP, prepínače * špecificky pre WiFi musí byť možné nastaviť hromadne:   + pre skupinu zvolených AP:     - frekvenčné pásmo na ktorom sú dostupné dané SSID – 2.4 Ghz, 5Ghz, obe, band steering,     - vysielací výkon v zvolenom frekvenčnom pásme,     - minimálnu povolenú rýchlosť,     - šírku pásma vysielacieho kanálu – 20/40/80 Mhz (5Ghz pásmo),   + pre každé SSID individuálne parametre:     - časový harmonogram dostupnosti zvoleného SSID,     - či je zvolené SSID verejne inzerované alebo skryté,     - na ktorých AP je SSID inzerované,     - bezpečnostné parametre:       * PSK / IEEE 802.1X,       * WPA2 /WPA3,       * Vynucovanie DHCP pridelenej IP adresy klienta od definovaných DHCP serverov     - do ktorej VLAN je bridge-ované,   + povolenie/zakázanie L2 izolácie klientov,   + ACL umožňujúci dodatočné blokovanie zvolených cieľov – IP adresa, Protokol, Port   + shaping dátovej prevádzky umožňujúci na jednotlivé SSID definovať kapacitné limity, ktoré umožnia:     - možnosť definovať download a upload maximá pripojených klientov k danému SSID,     - definovať download a upload maximá agregovane pre jednotlivé SSID, * špecificky pre Switche musí byť možné nastaviť hromadne:   + zapnutie/vypnutie skupiny portov,   + povolenie/zakázanie PoE skupiny portov,   + časový harmonogram zapínania/vypínania skupiny portov,   + Access VLAN ID resp. Trunk a povolené VLAN ID, Native VLAN ID skupiny portov,   + rýchlosť, duplex skupín portov,   + Rapid STP mechanizmy: BPDU Guard, Loop Guard, Root Guard skupiny portov,   + Prístupovú politiku skupiny portov:     - Radius IEEE802.1X, MAB, MAB fallback ak zlyhá 802.1X,     - Radius accounting,     - Režim: Single Host, Multi Domain, Multi Auth,     - VLAN ID pri zamietnutí autentifikácie,     - VLAN ID pri nedostupnosti Radius servera. * Viditeľnosť a topológia siete a prvkov, ich dostupnosť atď..   Náhľad topológie je kľúčový pre efektívnu správu a monitorovanie siete, pretože poskytuje komplexný prehľad o fyzickej a logickej štruktúre siete. Služba musí disponovať schopnosťou poskytnúť ucelený pohľad na celú sieťovú infraštruktúru, zahŕňajúcu zobrazenie inštalovaných LAN a WLAN prvkov, teda prepínačov a WiFi AP. Služba disponuje podporou LLDP protokolu, ktorý je štandardom pre výmenu informácií o priamych susedných sieťových zariadeniach a umožňuje tak zariadeniam v sieti automaticky objavovať a zdieľať informácie o sebe so susednými zariadeniami.  Služba musí automatizovane vytvárať typologické zobrazenie aktuálneho zapojenia sieťovej infraštruktúry, umožňujúce jednoducho identifikovať:   * topológiu zapojenia s menom/popisom zariadení, * chybový stav zariadenia (ak taký nastal), * ktoré zariadenia sú vzájomne prepojené, * konkrétny port na prepínači, kde je pripojené AP so zobrazením:   + rýchlosť portu,   + vyťaženie portu, * Služba topológie musí byť dostupná okrem RPŠ dostupná cez GUI štandardných browserov aj pre poverených pracovníkov školy, MŠVVaM SR a NCU. * Interferencie a cudzie prvky:   + Pre bezproblémovú prevádzku najmä WLAN siete je kľúčové byť schopný odhaliť prítomnosť rušenia (interferencie) a cudzích prvkov. Za týmto účelom je vhodné vykonávať periodickú spektrálnu analýzu, ktorá jednak tieto zdroje rušenia identifikuje, ale poskytuje tiež údaje potrebné k automatickému alebo manuálnemu preladeniu na iný kanál, prípadne úpravu výkonu. Vzhľadom na časovú náročnosť spektrálnej analýzy je požadované aby túto funkciu vykonávala oddelená časť WiFi AP, aby nedochádzalo k ovplyvňovaniu užitočnej prevádzky. Ďalšou úlohou je pri identifikácii cudzích prvkov aj schopnosť posúdiť, či predstavujú bezpečnostnú hrozbu.   + Štandardom služby je:     - Dedikované rádio pre 2,4 Ghz, Dedikované rádio pre 5 Ghz,     - spektrálna analýza 2,4 a 5 Ghz pásma (real-time, bez ovplyvnenia dátovej prevádzky WiFi klientov) a schopnosť odhaliť interferencie ako aj kvantifikovať mieru využitia (utlizácie) všetkých kanálov príslušného spektra 2.4 a 5 Ghz, priemerovanú za min. posledných 60 sekúnd,     - meranie a zobrazovanie interferencií v pásme 2.4 a 5 Ghz v reálnom čase, bez dopadu na obsluhovanie WiFi klientov schopné určiť prítomnosť zdrojov rušenia v blízkosti zvoleného AP a tieto zdroje (ak sú to WiFi AP) identifikovať – SSID, BSSID (MAC), * Wireless IDS – intrusion detection system:   + nepretržitá klasifikácia WiFi AP ako autorizované, susedné alebo neautorizované (rogue), pričom služba umožňuje:     - detegovať:       * pripojenie neautorizovaného WiFi AP do spravovanej siete LAN,       * vyžarovanie rovnakého SSID aké poskytuje služba WiFi neautorizovaným WiFi AP,       * DOS útoky spôsobený zasielaním nadmerného množstva de-autentifikačných, disasociačných a manažment rámcov,     - reagovať:       * zamedzením pripojenie sa na neautorizované WiFi AP,       * zablokovaním prístupu k neovereným SSID definovaným školou, ktoré sú detegované spravovanými WiFi AP v rámci sieťovej infraštruktúry školy,       * zaslaním emailu zodpovedným osobám, Syslog informácie, zaznamenaním eventu v manažmente WLAN riešenia.   Správa inventára   * Inventory manažment poskytuje v rámci služby detailný prehľad o všetkých inštalovaných LAN, WLAN zariadeniach, prípadne licenciách, nevyhnutných pre centralizovanú správu siete RPŠ. Okrem potreby RPŠ slúžia tieto informácie na účely auditu inštalácie a tiež kontroly dodržania regulačných požiadaviek (napr. inštalované WiFi AP sú v súlade s požiadavkami TÚ SR/ETSI) * V rámci služby Inventory manažmentu je nevyhnutné poskytnúť nasledovné informácie o zariadeniach: * MAC adresa, sériové číslo, model, aktuálny firmware, stav pripojenia, licencia. * Pre účely kontroly prístupu k monitoringu a manažmentu siete je nevyhnutné, aby služba umožňovala rozdelenie kompetencií v rámci administrátorských účtov. Služba teda definuje, aký typ administrátora má k inventarizácií zariadení prístup. * Služba musí byť prístupná real-time online formou GUI prostredníctvom štandardných browserov pre poverených zamestnancov RPŠ, školy, NCU a MŠVVaM SR. Musí tiež umožňovať tieto dáta exportovať (priamo z GUI a tiež formou API) aspoň v jednom z formátov CSV, XML, JSON, pre potreby archivácie a ďalšieho spracovania. * Monitoring   Služba musí umožňovať centralizovaný vzdialený online dohľad aktívnych sieťových prvkov – WiFi AP indoor, WiFi AP outdoor, prepínače prostredníctvom web klienta (štandardný internetový prehliadač) a používateľov.  Monitoring Služba CRSD pozostáva z nasledovných kategórií:   * monitorovanie dostupnosti a stavu prvkov infraštruktúry, * stav aktívnych prvkov (WiFi AP, prepínače), * zobrazenie „zdravotného“ skóre siete, ktoré sa vzťahuje na pripojené zariadenia a rovnako tak sieťové prvky LAN a WLAN s možnosťou výberu konkrétnej metriky, ktorá ovplyvnila skóre.   Monitoring prepínačov:   * zobrazenie dostupnosti / nedostupnosti zariadenia, * zobrazenie grafickej reprezentácie prepínača s rozmiestnením portov zodpovedajúcim realite, na ktorom je zrejmé:   + ktoré porty sú aktuálne pripojené, odpojené porty,   + ktoré pripojené porty poskytujú PoE napájanie, * zobrazenie mena/popisu prepínača, * počet aktuálne pripojených klientov, * zobrazenie zoznamu pripojených zariadení (wired klientov) za zvolené časové obdobie, min. 30 dní spätne, * zoznam pripojených zariadení musí poskytovať minimálne nasledovné informácie:   + port prepínača, MAC adresa klienta, VLAN ID,   + zobrazenie informácií o nastavení a štatistikách portov switchu, minimálne nasledovné informácie:     - vlan ID, Trunk a native vlan ID a zoznam povolených VLAN (ak je zapnutý trunk),     - administratívny stav (port zapnutý/vypnutý), výsledná rýchlosť linky, duplex, alokácia PoE výkonu, * informácie o Spanning-Tree-protokole – min:   + či je port v stave prepúšťajúci alebo blokujúci používateľskú prevádzku,   + Spanning-Tree Root – ktorý switch je root, * počítadlá za zvolené časové obdobie, min. 30 dní spätne:   + prenesený objem dát na porte v smere prijatom,   + prenesený objem dát na porte v smere odoslanom, * LLDP zoznam susedov, * množstvo alokovaného PoE výkonu z celkového PoE budgetu prepínača.   Monitoring WiFi AP:   * zobrazenie dostupnosti / nedostupnosti zariadenia, * zobrazenie prevádzky Uplink/Downlink v reálnom čase pre vybrané AP, * zobrazenie informácií pre aktuálne pripojených klientov, ako napr.:   + meno zariadenia, IP adresa, MAC adresa, VLAN, asociované SSID,   + dĺžka pripojenia, množstvo prenesených dát, sila signálu, aktuálny kanál a jeho šírka,   + percentuálne vyťaženie jednotlivých kanálov v 2.4Ghz a 5 Ghz pásme,   + zobrazenie aktuálne spotreby AP, dĺžky prevádzky AP, * pre vybrané SSID je dôležité sledovať nasledovné údaje o výkone bezdrôtovej služby WiFi s dopadom na vybrané problematické AP a klientov:   + schopnosť prešetriť čas potrebný na pripojenie k prístupovému bodu,   + sledovanie priemernej latencie, straty paketov a kvalitu signálu SNR pre klientov,   + monitorovanie dostupnosti služieb ako RADIUS, DNS.   Bezpečnostný monitoring:   * Udalosti súvisiace prevádzkou 802.1x, napríklad:   + autentifikácia používateľa,   + deautentifikáciou používateľa,   + vypršanie času odozvy (time-out) RADIUS servera,   + vypršanie času odozvy (time-out) klienta,   + zlyhanie autentifikácie,   + detekcia a upozorňovanie na pokusy o neoprávnený prístup.   Reaktívne monitorovanie používateľa pripojeného v sieti:   * vyhľadanie konkrétneho zariadenia (klienta) aby bolo možné pre WiFi určiť: * na ktoré AP je pripojené, * od kedy je pripojené, * ako vyťažuje sieť za zvolené časové obdobie, * na ktoré destinácie komunikuje a koľko na ne prenieslo dát, * na ktoré SSID, pásmo (2.4 Ghz alebo 5 Ghz), silu signálu s ktorou je zariadenie videné zo strany AP, * vyhľadanie konkrétneho zariadenia (klienta) aby bolo možné pre wired určiť:   + na ktorý switch a port je pripojené,   + od kedy je pripojené,   + ako vyťažuje sieť za zvolené časové obdobie,   + na ktoré destinácie komunikuje a koľko na nich prenieslo dát.   Monitorovanie používateľských aktivít:   * koľko bolo za zvolené časové obdobie pripojených zariadení pomocou WiFi, * koľko bolo za zvolené časové obdobie pripojených zariadení cez drôtový ethernet, * ktoré pripojené WiFi zariadenia preniesli koľko dát za zvolené časové obdobie, * ktoré pripojené drôtové zariadenia preniesli koľko dát za zvolené časové obdobie, * ktoré zariadenie prenieslo za zvolené časové obdobie najviac dát, * IP adresa pripojených zariadení, * typ zariadenia a jeho OS, * zobrazenie aktívnych aj neaktívnych zariadení, ktoré sa pripojili za posledných 30 dní.   **Upozornenia**  CRSD monitoring musí umožňovať na definované ciele na základe metodického usmernenia Ministerstva zasielať upozornenia týkajúce sa najmä zmien, výpadkov a kritických stavov. Medzi monitorované udalosti, v reakcii na ktoré sú zasielané upozornenia musí patriť:   * zmena konfiguračných parametrov AP, switchov a firewallu, * detekcia cudzieho WiFi AP, * WiFi AP sa stalo nedostupným, * switch sa stal nedostupným, * bola zistená prítomnosť nelegitímneho DHCP servera.   Medzi definované ciele, na ktoré je možné odosielať upozornenia musí patriť:   * definovaný zoznam emailových adries – napríklad adresy zvolených zamestnancov školy, * minimálne 2 Webhook HTTPS adresy, kde budú notifikácie odosielané formou HTTP POST metódy.   **Ochrana centrálneho monitoring nástroja**  Centralizované riešenie správy a dohľadu (CRSD) siete obsahuje dôveryhodné informácie, ktoré sú určené pre vybraných správcov a zainteresované osoby podľa príslušného rozdelenia právomocí. Dodaná služba preto musí poskytnúť zabezpečenie takéhoto nástroja kombináciou viacvrstvovej bezpečnosti. Tieto opatrenia garantujú dôveru používateľov.  V rámci zabezpečovania služieb RPŠ očakávame, že vybraný dodávateľ poskytne zabezpečený prístup do RPŠ monitoring nástroja nasledovne:   * všetka komunikácia medzi používateľmi a CRSD je šifrovaná (šifrovanie data in-motion), * CRSD podporuje dvojfaktorovú autentifikáciu, ktorá pridáva dodatočnú vrstvu ochrany tým, že vyžaduje nielen heslo, ale aj druhý faktor, ako je potvrdenie identity pomocou mobilnej aplikácie alebo kódom, obdržaným cez SMS/email, * služba podporuje SAML SSO, čo umožňuje integráciu s externými autentifikačnými systémami a centralizovanú správu prístupu, * prístup k nástroju je riadený na základe rolí (RBAC – Role based access control), čo umožňuje priradiť rôzne úrovne prístupu používateľom podľa ich úlohy a zodpovedností, a to nasledovne:   + privilégia na zmeny (read-write), privilégia na čítanie (read-only) pre rôznych používateľov – zamestnanci RPŠ, zamestnanci NCU, zamestnanci školy a pod.,   + aby bolo možné zriadiť administrátora, ktorý bude mať prístup do monitoring nástroja pre celú školu: WiFi AP a prepínače na všetkých adresách školy,   + administrátora, ktorý bude mať prístup do monitoring nástroja pre WiFi AP a switche na len danej adrese školy,   + pre zvolených pracovníkov školy, zriaďovateľa a MŠVVaM SR, NCU musí byť možné zriadiť read-only prístupy, * prístup k dátam CRSD je možné poskytnúť pomocou API prístupu, ktorý je zabezpečený unikátnym API kľúčom (s možnosťou odvolať/zrušiť už vytvorený kľúč), * možnosťou zadefinovať IP adresné rozsahy, z ktorých je povolené prihlásenie sa do monitoring-ového nástroja, * dáta obsiahnuté v monitorovacom nástroji sú šifrované (šifrovanie data at-rest), navyše monitoring spĺňa požiadavky GDPR (General Data Protection Regulation), * audit Log - CRSD automatizovane zaznamenáva všetky prístupy a akcie vykonané používateľmi, čo umožňuje administrátorom sledovať aktivity a identifikovať potenciálne bezpečnostné incidenty.   **Audit Log**  Za účelom editovateľnosti vykonaných konfiguračných zmien spolu s autorom zmien musí CRSD automatickým spôsobom tieto zmeny zaznamenávať – Audit Log.  Štandardom služby pritom je:   * držanie záznamov o administratívnych zmenách vykonaných za obdobie min. 3 mesiacov spätne, * záznamy musia jasne definovať ktorý konkrétny administrátor vykonal ktorú zmenu, * popis čoho sa zmena týkala, * detail pôvodného nastavenia, * detail nového (zmeneného nastavenia), * export Audit Logu do jedného z formátov: XML, JSON, CSV. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | RPŠ, Škola, NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1 krát mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Poskytovanie centralizovaného riešenia správy a dohľadu |
| **Definícia** | | Zabezpečovanie služieb nástroja CRSD podľa definície a jeho GUI, API, služieb exportovania, ochrany, atď. |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO poskytuje definované služby |
| **Maximum** | N/A |
| **Severita Nesúladu služby** | | N/A |
| **Metrika 2** | **Názov:** | | Poskytovanie zabezpečeného prístup do CRSD |
| **Definícia** | | Zabezpečovanie dostatočnej kapacity počtu prístupov používateľom |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 33% z počtu obsluhovaných lokalít škôl |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa dostupnosť služby |
| **Metrika 3** | **Názov:** | | Poskytovanie zabezpečeného prístup do CRSD |
| **Definícia** | | Zabezpečovanie dostatočnej kapacity konkurentných prístupov |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 33% z počtu obsluhovaných lokalít škôl |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa dostupnosť služby |

Tabuľka 13: Poskytovanie centralizovaného riešenia správy a dohľadu – definícia požiadaviek na službu

### Poskytovanie služieb centralizovaného riešenia správy a dohľadu poskytovaná RPŠ prostredníctvom služieb NCU (NCU-CRSD) – Alternatíva 2

V tejto kapitole je uvedená špecifikácia ktorá je súťažená v samostatnej súťaži pre poskytovateľa služieb NCU, v špecifikácii sú rovnako uvedené aktívne prvky ktoré sú podporované týmito službami.

| **Poskytovanie služieb centralizovaného riešenia správy a dohľadu prostredníctvom NCU-CRSD - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Poskytovanie centralizovaného riešenia správy a dohľadu |
| **Kategória** | | | | Služby manažmentu a monitoringu riešenia LAN/WLAN |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Centralizované riešenie správy a dohľadu (ďalej len CRSD), súvisí s prevádzkou, monitorovaním, správou, údržbou sieťového riešenia, atď. Takáto služba umožní čo najefektívnejšie nasadenie riešenia, jeho správu, monitorovanie a diagnostiku. |
| **Poskytovanie služieb centralizovaného riešenia správy a dohľadu prostredníctvom NCU-CRSD** | | | | |
| **Poskytovanie služieb NCU-CRSD**  Poskytovanie centralizovaného riešenia správy a dohľadu (ďalej len NCU-CRSD), súvisiaceho s prevádzkou, správou a údržbou sieťového riešenia.  Centralizovanou službou sa myslí spravidla jedno grafické prostredie (GUI) poskytujúce ucelenú funkcionalitu, dostupné vzdialene a on-line pre všetky relevantné organizácie prostredníctvom web klienta (štandardný internetový browser).  Služba je zabezpečovaná podľa nasledujúcich kritérií:   * Je neprípustné v kombinácii so službami NCU umiestňovanie serverov alebo akýchkoľvek dedikovaných kontrolérov do prostredia/lokality školy. NCU môže NCU-CRSD vybudovať alebo inak zabezpečiť jeho prevádzku napríklad v private cloud prostredí, resp. On-premises dátové centrum alebo public cloud prostredí. Predložené CRSD riešenie musí podporovať:   + garantované vo funkčnom stave a podporujúce pridávanie funkcionality do produktov WiFi AP a switche zo strany ich výrobcov (ak títo budú pridávať nové vlastnosti) po celú dĺžku trvania prevádzky,   + prevádzkované na lokalitách určených NCU – napr. private cloud, on-premises dátové centrum, na náklady NCU,   + pri prevádzkovaní v public cloud prostredí, hostovanom v EU, garantujúcom požadovanú dostupnosť, na náklady NCU,   + dostupná vzdialene v reálnom čase, pričom musí byť možný prístup do grafického GUI prostredia zabezpečujúci management, prevádzku a ostatné prevádzkové funkcionality určené pre RPŠ na zabezpečenie služieb prevádzky v lokalitách škôl minimálne pre nasledovných určených pracovníkov:     - zamestnanci a administrátori RPŠ,     - zamestnanci NCU,   + dostupná vzdialene v reálnom čase, pričom musí byť možný prístup do grafického GUI prostredia zabezpečujúci náhľad prevádzkových a výkonnostných parametrov minimálne pre nasledovných určených pracovníkov:     - zamestnanci školy/poverení pracovníci školy,     - zamestnanci zriaďovateľa školy,     - zamestnanci MŠVVaM SR a poverená osoba pre prípadný audit,     - zamestnanci poskytovateľa NCU.   **NCU-CRSD** služba musí vykonávať funkcie WiFi kontroléra – tzn., musí:   * vykonávať registráciu WiFi prístupových bodov, * zabezpečovať centrálne konfiguráciu všetkých AP, * zbierať informácie od jednotlivých AP vo vzťahu k frekvenciám použitých susedným AP, * minimalizovať interferenciu, nastavovať vysielací výkon a kanál, * vykonávať rádiofrekvenčné plánovanie (RRM) s cieľom maximalizovať kvalitné pokrytie signálom, * v prípade výpadku kontroléra zabezpečovať aby aktuálne pripojení klienti/používatelia nestratili prístup k službám WLAN.   RPŠ je povinný sa o dodané prvky infraštruktúry – WiFi a Switche starať pomocou NCU-CRSD v súlade s metodickým usmernením NCU, a to minimálne z pohľadu nastavenia,  úpravy a optimalizácií nastavení v čase, upgrade-ov OS/firmware aktívnych prvkov, dohľadu a monitoringu a riešení problémov.  Vzhľadom na očakávanú veľkosť projektu sa požaduje, aby NCU-CRSD nástroj podporoval API RESTFUL služby, ktoré musia:   * byť verejne zdokumentované, * dostupné počas celej doby trvania zmluvného vzťahu, * byť dostupné vzdialene a real-time, * poskytnúť informácie o konfiguráciách (WiFi AP a prepínačov), * poskytnúť informácie o pripojených zariadeniach v sieti (klientov), * chránené unikátnym API kľúčom s možnosťou revokácie.   **Služba onboardingu zariadení LAN/WLAN**  Z dôvodu jednoduchosti a rýchlosti nasadenia, budúceho rozširovania, urýchlenia výmen pokazených zariadení, minimalizácie ľudskej chyby ako aj ďalších dôvodov sa požaduje, aby dodané sieťové zariadenia - WiFi access point-y (indoor a outdoor) a switche podporovali a boli nasadené v režime ZTP – Zero Touch Provisioning.  Režimom ZTP sa myslí najmä:   * Schopnosť nového zariadenia bez predchádzajúcej konfigurácie sa po zapnutí a pripojení ku sieti poskytujúcej DHCP pridelenie adresy automatizovaným a zabezpečeným spôsobom prihlásiť do NCU-CRSD a stiahnuť si svoju konfiguráciu s ktorou má byť prevádzkované, bez potreby vykonávania predchádzajúcej konfigurácie (bez potreby tzv. pre-staging-u). Zároveň je možné vytvárať konfiguračné šablóny, zabezpečujúce konzistenciu konfigurácií. * Pri onboardingu zariadení sa navyše musia automaticky stiahnuť potrebné aktualizácie firmvéru a bezpečnostné záplaty, odporúčané výrobcom týchto zariadení. * Dodané riešenie NCU-CRSD musí za týmto účelom takéto ZTP služby umožňovať.   **Služba konfigurácie zariadení LAN/WLAN**  NCU-CRSD musí poskytovať centralizovanú službu správy konfigurácii umožňujúcu minimálne nasledovné:   * kompletnú konfiguráciu WiFi AP a switchov, * priradiť zariadeniam popisné označenie/meno, * priradiť Ethernet rozhraniam switchov popisné označenia, * konfigurovať zariadenia:   + individuálnym spôsobom   + prostredníctvom konfiguračných šablón umožňujúcich aplikovať zvolené nastavenia hromadným spôsobom – napr. pre všetky AP, prepínače * špecificky pre WiFi musí byť možné nastaviť hromadne:   + pre skupinu zvolených AP:     - frekvenčné pásmo na ktorom sú dostupné dané SSID – 2.4 Ghz, 5Ghz, obe, band steering,     - vysielací výkon v zvolenom frekvenčnom pásme,     - maximálnu povolenú rýchlosť,     - šírku pásma vysielacieho kanálu – 20/40/80 Mhz (5Ghz pásmo),   + pre každé SSID individuálne parametre:     - časový harmonogram dostupnosti zvoleného SSID,     - či je zvolené SSID verejne inzerované alebo skryté,     - na ktorých AP je SSID inzerované,     - bezpečnostné parametre:       * PSK / IEEE 802.1X,       * WPA2 /WPA3,       * Vynucovanie DHCP pridelenej IP adresy klienta od definovaných DHCP serverov     - do ktorej VLAN je bridge-ované,   + povolenie/zakázanie L2 izolácie klientov,   + ACL umožňujúci dodatočné blokovanie zvolených cieľov – IP adresa, Protokol, Port   + shaping dátovej prevádzky umožňujúci na jednotlivé SSID definovať kapacitné limity, ktoré umožnia:     - možnosť definovať download a upload maximá pripojených klientov k danému SSID,     - definovať download a upload maximá agregovane pre jednotlivé SSID, * špecificky pre Switche musí byť možné nastaviť hromadne:   + zapnutie/vypnutie skupiny portov,   + povolenie/zakázanie PoE skupiny portov,   + časový harmonogram zapínania/vypínania skupiny portov,   + Access VLAN ID resp. Trunk a povolené VLAN ID, Native VLAN ID skupiny portov,   + rýchlosť, duplex skupín portov,   + Rapid STP mechanizmy: BPDU Guard, Loop Guard, Root Guard skupiny portov,   + Prístupovú politiku skupiny portov:     - Radius IEEE802.1X, MAB, MAB fallback ak zlyhá 802.1X,     - Radius accounting,     - Režim: Single Host, Multi Domain, Multi Auth,     - VLAN ID pri zamietnutí autentifikácie,     - VLAN ID pri nedostupnosti Radius servera. * Viditeľnosť a topológia siete a prvkov, ich dostupnosť atď..   Služba musí automatizovane vytvárať typologické zobrazenie aktuálneho zapojenia sieťovej infraštruktúry, umožňujúce jednoducho identifikovať:   * topológiu zapojenia s menom/popisom zariadení, * chybový stav zariadenia (ak taký nastal), * ktoré zariadenia sú vzájomne prepojené, * konkrétny port na prepínači, kde je pripojené AP so zobrazením:   + rýchlosť portu,   + vyťaženie portu, * Služba topológie musí byť okrem pre RPŠ dostupná cez GUI štandardných browserov aj pre poverených pracovníkov školy, MŠVVaM SR a NCU. A to v minimálne kapacite počtu prístupov v počte 33% obsluhovaných lokalít škôl. * Interferencie a cudzie prvky:   + Pre bezproblémovú prevádzku najmä WLAN siete je kľúčové byť schopný odhaliť prítomnosť rušenia (interferencie) a cudzích prvkov. Za týmto účelom je vhodné vykonávať periodickú spektrálnu analýzu, ktorá jednak tieto zdroje rušenia identifikuje, ale poskytuje tiež údaje potrebné k automatickému alebo manuálnemu preladeniu na iný kanál, prípadne úpravu výkonu. Vzhľadom na časovú náročnosť spektrálnej analýzy je požadované aby túto funkciu vykonávala oddelená časť WiFi AP, aby nedochádzalo k ovplyvňovaniu užitočnej prevádzky. Ďalšou úlohou je pri identifikácii cudzích prvkov aj schopnosť posúdiť, či predstavujú bezpečnostnú hrozbu.   + Štandardom služby je:   + dedikované rádio pre 2,4 Ghz, Dedikované rádio pre 5 Ghz,   + spektrálna analýza 2,4 a 5 Ghz pásma (real-time, bez ovplyvnenia dátovej prevádzky WiFi klientov) a schopnosť odhaliť interferencie ako aj kvantifikovať mieru využitia (utlizácie) všetkých kanálov príslušného spektra 2.4 a 5 Ghz, priemerovanú za min. posledných 60 sekúnd,   + meranie a zobrazovanie interferencií v pásme 2.4 a 5 Ghz v reálnom čase, bez dopadu na obsluhovanie WiFi klientov schopné určiť prítomnosť zdrojov rušenia v blízkosti zvoleného AP a tieto zdroje (ak sú to WiFi AP) identifikovať – SSID, BSSID (MAC), * Wireless IDS – intrusion detection system:   + nepretržitá klasifikácia WiFi AP ako autorizované, susedné alebo neautorizované (rogue), pričom služba umožňuje:     - detegovať:       * pripojenie neautorizovaného WiFi AP do spravovanej siete LAN,       * vyžarovanie rovnakého SSID aké poskytuje služba WiFi neautorizovaným WiFi AP,       * DOS útoky spôsobený zasielaním nadmerného množstva de-autentifikačných, disasociačných a manažment rámcov,     - reagovať:       * zamedzením pripojenie sa na neautorizované WiFi AP,       * zablokovaním prístupu k neovereným SSID definovaným školou, ktoré sú detegované spravovanými WiFi AP v rámci sieťovej infraštruktúry školy,       * zaslaním emailu zodpovedným osobám, Syslog informácie, zaznamenaním eventu v manažmente WLAN riešenia.   Správa inventára   * Inventory manažment poskytuje v rámci služby detailný prehľad o všetkých inštalovaných LAN, WLAN zariadeniach, prípadne licenciách, nevyhnutných pre centralizovanú správu siete RPŠ. Okrem potreby RPŠ slúžia tieto informácie na účely auditu inštalácie a tiež kontroly dodržania regulačných požiadaviek (napr. inštalované WiFi AP sú v súlade s požiadavkami TÚ SR/ETSI). * V rámci služby Inventory manažmentu je nevyhnutné poskytnúť nasledovné informácie o zariadeniach: * MAC adresa, sériové číslo, model, aktuálny firmware, stav pripojenia, licencia. * Pre účely kontroly prístupu k monitoringu a manažmentu siete je nevyhnutné, aby služba umožňovala rozdelenie kompetencií v rámci administrátorských účtov. Služba teda definuje, aký typ administrátora má k inventarizácií zariadení prístup. * Služba musí byť prístupná real-time online formou GUI prostredníctvom štandardných browserov pre poverených zamestnancov RPŠ, školy, NCU a MŠVVaM SR. Musí tiež umožňovať tieto dáta exportovať (priamo z GUI a tiež formou API) aspoň v jednom z formátov CSV, XML, JSON, pre potreby archivácie a ďalšieho spracovania.   Monitoring  Služba musí umožňovať centralizovaný vzdialený online dohľad aktívnych sieťových prvkov – WiFi AP indoor, WiFi AP outdoor, prepínače prostredníctvom web klienta (štandardný internetový prehliadač) a používateľov.  Služba musí umožňovať centralizovaný vzdialený online zber monitoring informácii WiFi AP indoor, WiFi AP outdoor, prepínače prostredníctvom štandardizovaného rozhrania.  Monitoring Služba NCU-CRSD pozostáva z nasledovných kategórií:   * monitorovanie dostupnosti a stavu prvkov infraštruktúry, * stav aktívnych prvkov (WiFi AP, prepínače),   Monitoring prepínačov:   * zobrazenie dostupnosti / nedostupnosti zariadenia, * zobrazenie grafickej reprezentácie prepínača s rozmiestnením portov zodpovedajúcim realite, na ktorom je zrejmé:   + ktoré porty sú aktuálne pripojené, odpojené porty,   + ktoré pripojené porty poskytujú PoE napájanie, * zobrazenie mena/popisu prepínača, * počet aktuálne pripojených klientov, * zobrazenie zoznamu pripojených zariadení (wired klientov) za zvolené časové obdobie, min. 30 dní spätne, * zoznam pripojených zariadení musí poskytovať minimálne nasledovné informácie:   + port prepínača, MAC adresa klienta, VLAN ID,   + zobrazenie informácií o nastavení a štatistikách portov switchu, minimálne nasledovné informácie:     - vlan ID, Trunk a native vlan ID a zoznam povolených VLAN (ak je zapnutý trunk),     - administratívny stav (port zapnutý/vypnutý), výsledná rýchlosť linky, duplex, alokácia PoE výkonu, * informácie o Spanning-Tree-protokole – min:   + či je port v stave prepúšťajúci alebo blokujúci používateľskú prevádzku,   + Spanning-Tree Root – ktorý switch je root, * počítadlá za zvolené časové obdobie, min. 30 dní spätne:   + prenesený objem dát na porte v smere prijatom,   + prenesený objem dát na porte v smere odoslanom, * LLDP zoznam susedov, * množstvo alokovaného PoE výkonu z celkového PoE budgetu prepínača.   Monitoring WiFi AP:   * zobrazenie dostupnosti / nedostupnosti zariadenia, * zobrazenie prevádzky Uplink/Downlink v reálnom čase pre vybrané AP, * zobrazenie informácií pre aktuálne pripojených klientov, ako napr.:   + meno zariadenia, IP adresa, MAC adresa, VLAN, asociované SSID,   + dĺžka pripojenia, množstvo prenesených dát, sila signálu, aktuálny kanál a jeho šírka,   + percentuálne vyťaženie jednotlivých kanálov v 2.4Ghz a 5 Ghz pásme,   + zobrazenie aktuálne spotreby AP, dĺžky prevádzky AP, * pre vybrané SSID je dôležité sledovať nasledovné údaje o výkone bezdrôtovej služby WiFi s dopadom na vybrané problematické AP a klientov:   + schopnosť prešetriť čas potrebný na pripojenie k prístupovému bodu,   + sledovanie priemernej latencie, straty paketov a kvalitu signálu SNR pre klientov,   + monitorovanie dostupnosti služieb ako RADIUS, DNS.   Bezpečnostný monitoring:   * Udalosti súvisiace prevádzkou 802.1x, napríklad:   + autentifikácia používateľa,   + deautentifikáciou používateľa,   + vypršanie času odozvy (time-out) RADIUS servera,   + vypršanie času odozvy (time-out) klienta,   + zlyhanie autentifikácie,   + detekcia a upozorňovanie na pokusy o neoprávnený prístup.   Reaktívne monitorovanie používateľa pripojeného v sieti:   * vyhľadanie konkrétneho zariadenia (klienta) aby bolo možné pre WiFi určiť:   + na ktoré AP je pripojené,   + od kedy je pripojené,   + ako vyťažuje sieť za zvolené časové obdobie,   + na ktoré destinácie komunikuje a koľko na ne prenieslo dát,   + na ktoré SSID, pásmo (2.4 Ghz alebo 5 Ghz), silu signálu s ktorou je zariadenie videné zo strany AP,   + vyhľadanie konkrétneho zariadenia (klienta) aby bolo možné pre wired určiť:     - na ktorý switch a port je pripojené,     - od kedy je pripojené,     - ako vyťažuje sieť za zvolené časové obdobie,     - na ktoré destinácie komunikuje a koľko na nich prenieslo dát.   Monitorovanie používateľských aktivít:   * koľko bolo za zvolené časové obdobie pripojených zariadení pomocou WiFi, * koľko bolo za zvolené časové obdobie pripojených zariadení cez drôtový ethernet, * ktoré pripojené WiFi zariadenia preniesli koľko dát za zvolené časové obdobie, * ktoré pripojené drôtové zariadenia preniesli koľko dát za zvolené časové obdobie, * ktoré zariadenie prenieslo za zvolené časové obdobie najviac dát, * IP adresa pripojených zariadení, * typ zariadenia a jeho OS, * zobrazenie aktívnych aj neaktívnych zariadení, ktoré sa pripojili za posledných 30 dní.   Poznámka: v prípade zberu reportinových dát z NCU-CRSD môže RPŠ spolupracovať s NCU na príprave a vytváraní reportov v jednotnom formáte.  **Upozornenia**  NCU-CRSD monitoring musí umožňovať na definované ciele na základe metodického usmernenia Ministerstva zasielať upozornenia týkajúce sa najmä zmien, výpadkov a kritických stavov. Medzi monitorované udalosti, v reakcii na ktoré sú zasielané upozornenia musí patriť:   * zmena konfiguračných parametrov AP, switchov a firewallu, * detekcia cudzieho WiFi AP, * WiFi AP sa stalo nedostupným, * switch sa stal nedostupným, * bola zistená prítomnosť nelegitímneho DHCP servera.   Medzi definované ciele, na ktoré je možné odosielať upozornenia musí patriť:   * definovaný zoznam emailových adries – napríklad adresy zvolených zamestnancov školy, * minimálne 2 Webhook HTTPS adresy, kde budú notifikácie odosielané formou HTTP POST metódy.   **Ochrana centrálneho monitoring nástroja**  Centralizované riešenie správy a dohľadu (NCU-CRSD) siete obsahuje dôveryhodné informácie, ktoré sú určené pre vybraných správcov a zainteresované osoby podľa príslušného rozdelenia právomocí. Dodaná služba preto musí poskytnúť zabezpečenie takéhoto nástroja kombináciou viacvrstvovej bezpečnosti. Tieto opatrenia garantujú dôveru používateľov.  V rámci zabezpečovania služieb RPŠ očakávame, že vybraný dodávateľ poskytne zabezpečený prístup do RPŠ monitoring nástroja nasledovne:   * všetka komunikácia medzi používateľmi a NCU-CRSD je šifrovaná (šifrovanie data in-motion), * NCU-CRSD podporuje dvojfaktorovú autentifikáciu, ktorá pridáva dodatočnú vrstvu ochrany tým, že vyžaduje nielen heslo, ale aj druhý faktor, ako je potvrdenie identity pomocou mobilnej aplikácie alebo kódom, obdržaným cez SMS/email, * služba podporuje SAML SSO, čo umožňuje integráciu s externými autentifikačnými systémami a centralizovanú správu prístupu, * prístup k nástroju je riadený na základe rolí (RBAC – Role based access control), čo umožňuje priradiť rôzne úrovne prístupu používateľom podľa ich úlohy a zodpovedností, a to nasledovne:   + privilégia na zmeny (read-write), privilégia na čítanie (read-only) pre rôznych používateľov – zamestnanci RPŠ, zamestnanci NCU, zamestnanci školy a pod.,   + aby bolo možné zriadiť administrátora, ktorý bude mať prístup do monitoring nástroja pre celú školu: WiFi AP a prepínače na všetkých adresách školy,   + administrátora, ktorý bude mať prístup do monitoring nástroja pre WiFi AP a switche na len danej adrese školy,   + pre zvolených pracovníkov školy, zriaďovateľa a MŠVVaM SR, musí byť možné zriadiť read-only prístupy, * prístup k dátam **NCU-CRSD** je možné poskytnúť pomocou API prístupu, ktorý je zabezpečený unikátnym API kľúčom (s možnosťou odvolať/zrušiť už vytvorený kľúč), * možnosťou zadefinovať IP adresné rozsahy, z ktorých je povolené prihlásenie sa do monitoring-ového nástroja, * dáta obsiahnuté v monitorovacom nástroji sú šifrované (šifrovanie data at-rest), navyše monitoring spĺňa požiadavky GDPR (General Data Protection Regulation), * audit Log - NCU-CRSD automatizovane zaznamenáva všetky prístupy a akcie vykonané používateľmi, čo umožňuje administrátorom sledovať aktivity a identifikovať potenciálne bezpečnostné incidenty.   **Audit Log**  Za účelom editovateľnosti vykonaných konfiguračných zmien spolu s autorom zmien musí NCU-CRSD automatickým spôsobom tieto zmeny zaznamenávať – Audit Log.  Štandardom služby pritom je:   * držanie záznamov o administratívnych zmenách vykonaných za obdobie min. 3 mesiacov spätne, * záznamy musia jasne definovať ktorý konkrétny používateľ vykonal ktorú zmenu, * popis čoho sa zmena týkala, * detail pôvodného nastavenia, * detail nového (zmeneného nastavenia), * export Audit Logu do jedného z formátov: XML, JSON, CSV.   **NCU-CRSD podporuje minimálne integráciu nasledovných prvkov**   |  |  | | --- | --- | | **Fortinet WLAN** | | | **Model zariadenia** | **Špecifikácia** | | **802.11be Wi-Fi 7** |  | | FAP-441K | 4x4 Indoor quad-radio 11be 6Ghz Capable APs | | FAP-443K | 4x4 Indoor quad-radio 11be 6Ghz Capable APs | | FAP-241K | 2x2 Indoor quad-radio 11be 6Ghz Capable APs | | FAP-243K | 2x2 Indoor quad-radio 11be 6Ghz Capable APs | | **802.11ax Wi-Fi 6E** |  | | FAP-431G | 4x4 Indoor tri-radio 11ax 6Ghz Capable APs | | FAP-432G | 4x4 Ruggedized Tri-radio indoor/outdoor 11ax (6Ghz) Capable APs | | FAP-433G | 4x4 Indoor tri-radio 11ax 6Ghz Capable APs | | FAP-231G | 2x2 Indoor tri-radio 11ax 6Ghz Capable APs | | FAP-233G | 2x2 Indoor tri-radio 11ax 6Ghz Capable APs | | FAP-234G | 2x2 Ruggedized Tri-radio indoor/outdoor 11ax (6Ghz) Capable APs | | **802.11ax Wi-Fi 6** |  | | FAP-831F | 8x8 Indoor tri-radio 11ax AP | | FAP-433F | 4x4 Indoor tri-radio 11ax APs | | FAP-432F | 4x4 Ruggedized indoor/outdoor tri-radio 11ax AP | | FAP-431F | 4x4 Indoor tri-radio 11ax APs | | FAP-234F | 2x2 Ruggedized indoor/outdoor tri-radio 11ax AP | | **Fortinet LAN** | | | **Model zariadenia** | **Špecifikácia zariadenia a portov** | | FortiSwitch-108F | 7x GE RJ45, 1x GE/POE-PD RJ45 + 2x GE SFP | | FortiSwitch-108F-POE | 8x (802.3af/at) GE RJ45 + 2x GE SFP | | FortiSwitch-108F-FPOE | 8x (802.3af/at) GE RJ45 + 2x GE SFP | | FortiSwitch-108E-FPOE | 8x (802.3af/at) GE RJ45 + 2x GE SFP | | FortiSwitch-110G-FPOE | 2x 5G/2.5G/1G/100M [PoE bt], 8x 2.5G/1G/100M/10M RJ45 [PoE at/af], 4x 10G/1G/100 SFP+/SFP | | FortiSwitch-124F | 24x GE RJ45 and 4x 10GE SFP+ | | FortiSwitch-124F-POE | 24x GE RJ45 and 4x 10GE SFP+ [12x 802.3af/at] | | FortiSwitch-124F-FPOE | 24x GE RJ45 and 4x 10GE SFP+ [24x 802.3af/at] | | FortiSwitch-148F | 48x GE RJ45 and 4x 10GE SFP+ | | FortiSwitch-148F-POE | 48x GE RJ45 and 4x 10GE SFP+ [24x 802.3af/at] | | FortiSwitch-148F-FPOE | 48x GE RJ45 and 4x 10GE SFP+ [48x 802.3af/at] | | **CISCO WLAN** | | | **Model zariadenia** | **Špecifikácia** | | **Catalyst** |  | | 9105AX (I/W) | Wi-Fi 6 (802.11ax), 2x2 UL/DL MU-MIMO with two spatial streams | | 9115AX (I/E) | Wi-Fi 6 (802.11ax), 4x4 DL MU-MIMO with four spatial streams | | 9120AX (I/E/P) | Wi-Fi 6 (802.11ax), 4x4 DL MU-MIMO with four spatial streams | | 9130AX (I/E) | Wi-Fi 6 (802.11ax), 8x8 UL/DL MU-MIMO with eight spatial streams | | 9136 (I) | Wi-Fi 6E (802.11ax), 8x8 UL/DL MU-MIMO with eight spatial streams | | 9162 (I) | Wi-Fi 6E (802.11ax), 2x2 UL/DL MU-MIMO with two spatial streams | | 9164 (I) | Wi-Fi 6E (802.11ax), 4x4 UL/DL MU-MIMO with four spatial streams | | 9166 (I/D1) | Wi-Fi 6E (802.11ax), 4x4 UL/DL MU-MIMO with four spatial streams | | 9124AX (I/D/E) | Wi-Fi 6 (802.11ax), 4x4:4 UL/DL MU-MIMO with four spatial streams | | 9163 (E) | Wi-Fi 6E (802.11ax), 2x2 DL MU-MIMO with two spatial streams | | IW9167 (I/E) | Wi-Fi 6E (802.11ax), 4x4 UL/DL MU-MIMO with four spatial streams | | **Aironet** |  | | 1815 (I/W/M/T) | 802.11ac Wave 2 with 2x2:2 MU-MIMO | | **CISCO LAN** | | | **Model zariadenia** | **Špecifikácia** | | Catalyst C9200L-24P-4G | 24-port full PoE+, 4 x 1G fixed uplinks | | Catalyst C9200L-24T-4G | 24-port data only, 4 x 1G fixed uplinks | | Catalyst C9200L-48P-4G | 48-port full PoE+, 4 x 1G fixed uplinks | | Catalyst C9200L-48T-4G | 48-port data only, 4 x 1G fixed uplinks | | Catalyst C9200L-48PL-4G | 48-port partial PoE+, 4 x 1G fixed uplinks | | Catalyst C9200L-24P-4X | 24-port full PoE+, 4 x 1/10G fixed uplinks | | Catalyst C9200L-24T-4X | 24-port data only, 4 x 1/10G fixed uplinks | | Catalyst C9200L-48P-4X | 48-port full PoE+, 4 x 1/10G fixed uplinks | | Catalyst C9200L-48T-4X | 48-port data only, 4 x 1/10G fixed uplinks | | Catalyst C9200L-48PL-4X | 48-port partial PoE+, 4 x 1/10G fixed uplinks | | Catalyst C9200CX-8P-2X2G | 8-port full PoE+; 2x 1G copper, 2x 10G SFP+ fixed uplinks | | Catalyst C9200CX-12P-2X2G | 12-port PoE+; 2x 1G copper, 2x 10G SFP+ fixed uplinks | | Catalyst C9200CX-12T-2X2G | 12-port data only; 2x 1G copper, 1x 1G CU PD 802.3bt Class 6, 2x 10G SFP+ fixed uplinks | | | | | |
| **Účastníci** | **Poskytovateľ** | | | NCU, RPŠ |
| **Používateľ** | | | RPŠ, Škola, NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1 krát mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Poskytovanie centralizovaného riešenia správy a dohľadu |
| **Definícia** | | Zabezpečovanie služieb nástroja NCU-CRSD podľa definície a jeho GUI, API, služieb exportovania, ochrany, atď. |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne |
| **Požadovaná hodnota** | **Jednotka** | % |
| **Minimum** | 99,9% |
| **Maximum** | N/A |
| **Severita Nesúladu služby** | | Severita 1 |
| **Metrika 2** | **Názov:** | | Poskytovanie zabezpečeného prístup do NCU-CRSD |
| **Definícia** | | Zabezpečovanie dostatočnej kapacity počtu prístupov používateľom |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 33% z počtu obsluhovaných lokalít škôl |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa dostupnosť služby |
| **Metrika 3** | **Názov:** | | Poskytovanie zabezpečeného prístup do NCU-CRSD |
| **Definícia** | | Zabezpečovanie dostatočnej kapacity konkurentných prístupov |
| **Meranie/Monitorovanie** | **Vykonávateľ** | NCU |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne alebo reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 33% z počtu obsluhovaných lokalít škôl |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Podľa dostupnosť služby |

Tabuľka 14: Poskytovanie služieb centralizovaného riešenia správy a dohľadu prostredníctvom NCU-CRSD – definícia požiadaviek na službu

### Meranie spokojnosti koncového používateľa služieb a náprava

| **Meranie spokojnosti koncového používateľa služieb, objektívna analýza - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Meranie spokojnosti koncového používateľa služieb, objektívna analýza |
| **Kategória** | | | | Služby manažmentu a monitoringu riešenia LAN/WLAN |
| **Typ** | | | | Pravidelná |
| **Cieľ** | | | | Prevádzka služieb merania spokojnosti koncového používateľa sa vykonávala za účelom zistenia kvality služieb a následného zlepšenia služieb poskytovaných koncovým používateľom (školám). Nasledovná definícia uvádza pre celkový kontext definíciu služieb poskytovateľa NCU aj RPŠ. |
| **Meranie spokojnosti koncového používateľa služieb, objektívna analýza - detailná definícia požiadaviek na službu** | | | | |
| Služby súvisiacich meraním spokojnosti koncového používateľa, zahŕňajú nasledujúce činnosti:   * zber a analýza údajov používateľskej skúsenosti – subjektívna analýza, * zber a analýza údajov používateľskej skúsenosti – objektívna analýza, * reporty z analýzy, * optimalizácia siete na základe analýzy.   Štandardom služby pritom je:   * subjektívna analýza - pravidelný dotazníkový zber používateľskej skúsenosti na základe ich subjektívneho hodnotenia, realizovaný poskytovateľom služieb NCU:   + min. 2x ročne, rovnomerne rozdelené,   + formou odoslania internetového linku na formulár (zo strany NCU), ktorý následne rozpošle riaditeľ školy na zamestnancov, ktorí sa zapájajú na dobrovoľnej báze, * formulár musí skúmať spokojnosť a používateľskú skúsenosť používateľov min. vo vzťahu k WLAN konektivite a LAN konektivite, na škále od 1 – 5 (5=najlepšia skúsenosť) a to minimálne s ohľadom na:   + rýchlosť WLAN,   + pokrytie WLAN,   + rýchlosť LAN,   + rýchlosť práce s Internetom, * formulár musí tiež dávať priestor vložiť ku každej otázke vlastný text, a obsahovať časť s voľným textovým poľom, * vyhodnotenie dotazníkov musí NCU po spracovaní zasielať poverenej osobe na MŠVVaM SR a RPŠ, * za účelom štandardizácie zberu dát má MŠVVaM SR právo zmeniť a určiť presné formulácie dotazníkových otázok resp. znenie celého formuláru, aby boli tieto porovnateľné pre všetky školy, * v prípade, že používatelia vo vzťahu k skúmaným otázkam udelia počet bodov 1 a 2, opakovane dva krát po sebe vo vzťahu k príbuznej veci, musí RPŠ pristúpiť k objektívnej analýze, * objektívna analýza – objektívny zber parametrov kvality práce používateľov formou získavania metrík z reálnej používateľskej prevádzky ako aj formou syntetickej (umelo generovanej) dátovej prevádzky:   + min. v trvaní 10 dní, v reakcii na nízky počet bodov (1 a 2),   + posúdenie metrík konektivity k zvoleným web službám, min. však nasledovné:     - syntetické testy generujúce pravidelnú dátovú prevádzku min 1x za 30 min. voči: používateľmi označenej „problematickej“ web-stránke a kontrolnej web-stránke (určenej RPŠ) a kontrolnej web-stránke určenej MŠVVaM SR, s meraním min. nasledovného:       * dostupnosť web-stránky z lokality školy (áno – nie),       * celkový čas odpovede, rýchlosť DNS odpovede (sekundy resp. msek),       * meranie priepustnosti pripojenia voči web-stránke v kbps (Mbps),       * meranie percenta stratovosti paketov a oneskorenia voči serveru web-stránky,     - metriky z analýzy reálnej používateľskej prevádzky zachytenej z konkrétnej pracovnej stanice používateľa hlásiaceho problém, min 1x za 30 min (ak je stanica zapnutá) voči: používateľmi označenej „problematickej“ web-stránke a kontrolnej web-stránke (určenej RPŠ) a kontrolnej web-stránke určenej MŠVVaM SR, s meraním min. nasledovného:       * dostupnosť web-stránky z lokality školy (áno – nie),       * celkový čas odpovede, rýchlosť DNS odpovede (sekundy resp. msek),       * meranie priepustnosti pripojenia voči web-stránke v kbps (Mbps),       * meranie percenta stratovosti paketov a oneskorenia voči serveru web-stránky,       * stratovosti paketov voči DNS serveru a východiskovej bráne (default gw),       * latencie paketov voči DNS serveru a východiskovej bráne,       * pri WiFi – rýchlosť pripojenia k AP (data-rate), * Výsledkom vyhodnotenia objektívnej analýzy musí byť potvrdenie resp. vyvrátenie hlásených problémov a implementácia zmien, ktoré budú týmto problémom predchádzať, pokiaľ tieto nie sú preukázateľne mimo kompetencie NCU a RPŠ. Výsledky skúmania a zmien musí RPŠ do 30 dní po skončení Objektívnej analýzy oznámiť povereným pracovníkom NCU, oprávnenej osobe školy a MŠVVaM SR na pripomienkovanie, prípadne ďalej riešiť na eskalačných stretnutiach. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ, NCU |
| **Používateľ** | | | RPŠ, Škola, NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | Podľa výsledkov merania prieskumu viď definícia vyššie |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | Podľa výsledkov merania prieskumu viď definícia vyššie |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Objektívna analýza |
| **Definícia** | | Objektívna analýza na základe merania reálnej a syntetickej prevádzky podľa popisu vyššie |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Proaktívne a reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | Definované podľa nízkeho bodového hodnotenia zo subjektívnej analýzy |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | N/A |

Tabuľka 15: Meranie spokojnosti koncového používateľa služieb, objektívna analýza – definícia požiadaviek na službu

### RACI matica pre služby manažmentu a monitoringu riešenia LAN/WLAN/WAN

| **Popis činnosti** | **Škola** | **RPŠ** | **NCU** | **MŠVVaM** |
| --- | --- | --- | --- | --- |
| Monitorovanie napĺňania kritérií a požiadaviek služieb RPŠ | I | R | A | I |
| Merania napĺňania kritérií a požiadaviek služieb RPŠ | I | R | A | I |
| Poskytovanie parametrov pre NCU | N/A | R | A | I |
| Škola je povinná akceptovať dočasné prerušenie WAN konektivity v čase vykonávania mimoriadneho intruzívneho merania | A,R | N/A | N/A | N/A |
| Vykonávanie intruzívneho merania WAN konektivity | C,I | A,R | C,I | N/A |
| Prevádzka systémov pre poskytovanie služieb centralizovaného riešenia správy a dohľadu poskytovaná RPŠ prostredníctvom služieb NCU-CRSD |  | C,I | A,R |  |
| Prevádzka systémov pre poskytovanie služieb centralizovaného riešenia správy a dohľadu (CRSD) priamo RPŠ |  | A,R | C,I |  |

Tabuľka 16: RACI matica pre služby manažmentu a monitoringu riešenia LAN/WLAN/WAN

## Služby podpory prevádzky a údržby riešenia LAN/WLAN/WAN

Služby prevádzkovej podpory sú koordinované RPŠ a vykonávané aj v spolupráci s prevádzkovateľom služieb NCU a so školami. Služba je poskytovaná najmä prostredníctvom operačného strediska RPŠ - Service Desk. Jeho hlavnou úlohou je prijímať, spracovávať a riešiť požiadavky, otázky a problémy používateľov v súvislosti s prevádzkou služieb siete škôl.

Poznámka: Udalosti sú vo forme ticketov ako prvý kontakt s používateľmi zaznamenávané a riadené v centrálnom ticketing portály (CTP) zriadenom v operačnom stredisku dodávateľa služieb NCU - Service Desk. NCU - Service Desk je centrálnym bodom, ktorý poskytuje okrem iných služieb aj centrálnu podporu používateľom siete ako prvý bod kontaktu a centrálny nástroj pre riadenie a evidenciu udalostí. Jeho hlavnou úlohou je prijímať, spracovávať a riešiť požiadavky, otázky a problémy používateľov v súvislosti s prevádzkou služieb siete.

Služby RPŠ- Service Desku sú najmä nasledovné:

* správa a evidencia priebehu riešenia udalostí, incidentov, problémov prostredníctvom ticketov v centrálnom ticketing portály,
* riadenie incidentov,
* riadenie žiadostí o služby a informácie,
* riadenie problémov,
* riadenie zmien,
* správa znalostí,
* logovanie,
* reporting a výpočet kreditov za nedodržanie SLA,
* správu plánovaných prác a výpadkov,
* eskalácia podľa dohodnutých eskalačných postupov,
* technická podpora pre NCU,
* L1,L2, L3 prevádzková podpora on-site/off-site lokalít škôl.

### Poskytovanie služieb RPŠ – ServiceDesk, evidencie a spracovania ticketov

| **Poskytovanie služieb RPŠ – ServiceDesk - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Poskytovanie služieb RPŠ – ServiceDesk |
| **Kategória** | | | | Služby podpory prevádzky a údržby riešenia LAN/WLAN/WAN |
| **Typ** | | | | Ad-hoc |
| **Cieľ** | | | | Služby prevádzkovej podpory sú koordinované a poskytovaná najmä prostredníctvom operačného strediska RPŠ - Service Desk. Jeho hlavnou úlohou je prijímať, spracovávať a riešiť požiadavky, otázky a problémy používateľov v súvislosti s prevádzkou služieb siete. |
| **Poskytovanie služieb RPŠ – ServiceDesk - detailná definícia požiadaviek na službu** | | | | |
| RPŠ prevádzkuje službu správy a evidencie priebehu riešenia udalostí, incidentov, problémov v reálnom čase prostredníctvom ticketov využívaním CTP v prevádzke dodávateľa NCU. CTP je webový nástroj prístupný cez štandardný webový prehliadač. NCU vystaví API na ktoré sa môže RPŠ integrovať pre implementáciu automatizácie preberania a aktualizácie ticketov z vlastného nástroja.  Povinnosťou RPŠ je prijímať, zadávať a aktualizovať udalosti z a do centrálneho ticketing portálu.  V prípade že RPŠ bude využívať aj vlastný Portál RPŠ je povinný v reálnom čase replikovať informácie do centrálneho ticketing portálu. V prípade integrácie RPŠ portálu s CTP, NCU vystaví rozhranie (napr. API) a jeho špecifikáciu kam sa môže RPŠ integrovať. NCU poskytne dokumentáciu rozhrania, stavov ticketov a ich prechodov a poskytne integračnú podporu RPŠ.  CTP umožní:   * zadanie udalosti Národným centrálnym uzlom, samotným RPŠ, oprávnenou osobou školy, ministerstvom * kategorizácia udalosti, * Informácie o stave udalosti, riešení, aktivitách a uzavretí, * tvorbu reportov, filtrovanie, * komentovanie priebehu riešenia udalosti, zmena stavu a časove stopy každej zmeny.   Služby RPŠ prevádzky sú poskytované v Slovenskom jazyku  Každá udalosť je zaevidovaná v CTP a pridelené jej číslo ticketu, pod ktorým bude zaznamenaný celý priebeh riešenia. Udalosť môže vzniknúť:   * nahlásením na centrálny portál NCU - Service Desk, * automaticky/proaktívne RPŠ alebo NCU (napr. automatickou detekciou výpadku, proaktívny monitoring), * manuálne operátorom RPŠ, manuálne operátorom NCU.   Po zaevidovaní udalosti, ju operátor RPŠ klasifikuje (ak už nebol klasifikovaný operátorom NCU – Service Desk) a začne riešiť v zmysle dohodnutého postupu. Udalosť môže byť klasifikovaná ako:   * incident, * problém, * žiadosť o informáciu, * žiadosť o zmenu, * plánovaný výpadok * iná požiadavka.   Každá zmena stavu ticketu je zaznamená na centrálnom portáli. Dotknutá škola bude informovaná aj mailom o podstatných zmenách stavu riešenia ticketu a jeho uzatvorení aj o plánovaných prácach začatí prác a ich ukončení. Kontaktné informácie a oprávnené osoby nahlasuje škola pri akceptácii riešenia, informácie je RPŠ povinný odovzdať NCU.  **Ostatné služby – Service review meetings**  Service Review Meeting (SREV) slúži na pravidelné hodnotenie a zlepšovanie poskytovaných služieb. Jeho cieľom je zabezpečiť, aby služby spĺňali očakávania škôl a objednávateľa. Účastníkmi stretnutia sú RPŠ, NCU, Ministerstvo. V prípade potreby môže Ministerstvo prizvať zástupcu/zástupcov dotknutých lokalít škôl. Predmetom stretnutia bude najmä:   * hodnotenie kvality dodaných služieb, analýza kľúčových ukazovateľov výkonnosti, porovnanie s cieľmi a identifikácia odchýlok, * zhrnutie spätnej väzby získanej od škôl, identifikácia oblastí na zlepšenie, * analýza incidentov: preskúmanie významných incidentov, identifikácia príčin a navrhovanie preventívnych opatrení, * hodnotenie nových požiadaviek: diskusia o nových požiadavkách, * plánovanie zmien: diskusia o plánovaných zmenách v službách a ich vplyve, * stretnutie iniciuje RPŠ a bude sa konať mesačne počas prvých 6 mesiacov poskytovania služieb a následne štvrťročne. RPŠ zabezpečí primeranú účasť pracovníkov zodpovedných za poskytované služby. Mimoriadne Service review meeting môže iniciovať Ministerstvo v prípade opakovaných, podstatných porušení hodnôt parametrov a definície služieb.   Z každého stretnutia bude vytvorený zápis so zhrnutím obsahu, zoznamom identifikovaných problémov a príležitostí, prijatých rozhodnutí, zoznamom úloh, zodpovedných osôb a termínov. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | RPŠ, Škola, NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | | NCU |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | N/A |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | N/A |
| **Doba vyhodnocovania** | | | | N/A |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | RPŠ – Service Desk zabezpečovaný |
| **Definícia** | | Je zabezpečovaná podľa požiadaviek vyššie |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | N/A |
| **Požadovaná hodnota** | **Jednotka** | boolean |
| **Minimum** | ÁNO je zabezpečovaná |
| **Maximum** | N/A |
| **Severita Nesúladu služby** | | N/A |
| **Merateľné parametre** | **Metrika 2** | **Názov:** | | Doba spracovania ticketu |
| **Definícia** | | Čas od prijatia, prevzatia do zaevidovania a kategorizácie |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | minúta |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 60 |
| **Severita Nesúladu služby** | | Service review meeting eskalácia |

Tabuľka 17: Poskytovanie služieb RPŠ – ServiceDesk - detailná definícia požiadaviek na službu

### Riešenie incidentov

A group of white labels

Description automatically generated

Obrázok 1: Proces zadávania a riešenia incidentu

| **Riešenie incidentov RPŠ - ServiceDesk - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Riešenie incidentov RPŠ- ServiceDesk |
| **Kategória** | | | | Služby podpory prevádzky a údržby riešenia LAN/WLAN/WAN |
| **Typ** | | | | Ad-hoc |
| **Cieľ** | | | | Služby riadenia/riešenia incidentov |
| **Riešenie incidentov RPŠ - ServiceDesk** **- detailná definícia požiadaviek na službu** | | | | |
| Riadenie incidentov zahŕňa najmä:   * registráciu a kategorizáciu podľa severity: zaznamenávanie všetkých nahlásených udalostí, * priorizácia: určenie naliehavosti incidentov na základe ich dopadu na zákazníka a prevádzku, * riešenie: podľa potreby vzdialené, na mieste, výmenu zariadenia za nové, výjazd servisného technika apod. a sledovanie ich riešenia až do úplného vyriešenia, * komunikácia: informovanie zákazníkov o stave a zmene stavu ich požiadaviek a poskytovanie pravidelných aktualizácií. * Proaktívne informovanie používateľov pri proaktívne vytvorenom incidente z monitoringu RPŠ pri identifikovaní Nesúladu so službou taktiež pri podstatnej zmene stavu incidentu   Incidenty sú podľa závažnosti Nesúladu služby a vplyv Nesúladu služby na používateľov definované takto:   * **Severity 1**: Celá škola bez pripojenia alebo Nesúlad služby na celej škole - LAN, WLAN, WAN. Výpadok centrálneho switchu školy, routra apod. Nesúlad služieb pre viac ako 50% aktívnych prvkov. * **Severity 2**: Výpadok časti školy alebo Nesúlad služby pre <50%, školy napr. chodbový switch alebo viacero AP na škole. * **Severity 3**: Nesúlad služieb jedného aktívneho prvku spôsobujúci nedostupnosť služieb pre skupinu používateľov (napr. 1 AP alebo 1 switch) * **Severity 4**: Nesúlad služieb jedného alebo niekoľkých pripájaných bodov LAN v učebniach, jedného alebo niekoľkých portov na switchi apod.   RPŠ začne s diagnostikou a  odstraňovaním incidentu do 60 minút (viď metrika služby RPŠ-ServiceDesk) od vzniku udalosti nahlásením používateľom, proaktívnou/automatickou alebo manuálnou detekciou. Stav riešenia a vykonané kroky budú priebežne aktualizované v tickete v CTP. V prípade, že nie je možne incident odstrániť na diaľku, vyšle RPŠ na miesto inštalácie servisného technika.  RPŠ si vytvorí primerané skladové zásoby náhradných dielov pre potreby výmeny chybných zariadení na mieste a vhodne ich rozmiestni s ohľadom na počet a umiestnenie škôl a servisných technikov s cieľom plnenia dostupnosti a požiadaviek na odstránenie Nesúladu.  V prípade chybného zariadenia ho technik na mieste vymení za funkčné pre zabezpečenie Súladu služby.  **Požiadavky na odstraňovanie Nesúladu služby podľa severity:**  **Incident severity 1**: RTTR - Odstránenie nasledujúci pracovný deň od identifikácie/nahlásenia  **Incident severity 2**: RTTR - Odstránenie najneskôr tretí pracovný deň od identifikácie/nahlásenia  **Incident severity 3**: RTTR - Odstránenie najneskôr piaty pracovný deň od identifikácie/nahlásenia  **Incident severity 4**: RTTR - Odstránenie najneskôr desiaty pracovný deň od identifikácie/nahlásenia  Časy uvedené vyššie sa predlžujú:   * o dobu neposkytnutia súčinnosti na základe povinností používateľa, * o plánované výpadky podľa definície požiadaviek na služby plánovania výpadkov, * o dočasné prerušenie poskytovania služby na žiadosť Používateľa/Objednávateľa, * o dočasné prerušenie poskytovania služby z dôvodu zmeny prevádzkových parametrov okruhu resp. služby na žiadosť Používateľa/Objednávateľa (zmena rýchlosti a pod.), * z dôvodu prekládky služieb na žiadosť Používateľa/Objednávateľa a pod., * o prerušenie spôsobené Používateľom alebo dôvodom na strane Používateľa napr. spôsobené nevhodným používaním zariadení RPŠ alebo ich odpojením, spôsobené výpadkom elektrického napájania, * neumožnenie prístupu technických pracovníkov poskytovateľa služieb RPŠ do priestorov, v ktorých je umiestnená infraštruktúra alebo pripájaný bod, * o dobu zapríčinenú nefunkčnosťou (aj opakujúcou sa) koncových zariadení, ktoré sú v správe školy, * o prerušenie z dôvodu nepredvídateľných a neodvrátiteľných udalostí (Vis Major).   **Povinnosti používateľa**  Poverená osoba školy je povinná poskytovať súčinnosť pri odstraňovaní incidentu podľa požiadaviek RPŠ. Súčinnosť môže spočívať vo vzdialenej podpore (napr. telefonicky poskytne informáciu o výpadky el. energie, stave kontroliek na zariadení, vizuálnej kontrole zariadení, kabeláže apod.). Súčinnosť pri podpore na mieste môže spočívať v sprístupnení budovy a miest inštalácie, uskladnení zariadení a pod.  V prípade neposkytovania potrebnej súčinnosti sa budú časy uvedené v RTTR predlžovať o dobu neposkytovania súčinnosti a takéto predĺženie nebude považované za porušenie RTTR (napr. ak kontaktná osoba neberie telefón, nie je na mieste a nie je schopná poskytnúť súčinnosť, nie je ochotná sprístupniť v požadovanom čase miesto inštalácie a pod).  **Riadenie problémov (Problem management)**  Cieľom riadenia problémov je identifikácia a odstránenie základných príčin opakujúcich sa incidentov, prevencia budúcich incidentov a zlepšenie celkovej dostupnosti a spoľahlivosti služieb.  Riadenie problémov môže iniciovať RPŠ, NCU, škola alebo MŠ. Problém môže byť uzatvorený iba so súhlasom toho kto ho inicioval.  RPŠ musí mať implementovaný systém riadenia problémov v zmysle ITIL alebo obdobný, ktorý zahŕňa minimálne:   * analýzu incidentov a identifikácia opakujúcich sa incidentov, * identifikáciu základnej príčiny (root cause), * navrhovanie a implementácia trvalých riešení, * aktualizácia znalostnej bázy, * implementácia prípadných potrebných zmien v konfigurácii, * preventívne opatrenia.   **Eskalácie**  Pravidlá pre eskalácie definujú postup, ako sa bude riešiť situácia, keď poskytované služby nespĺňajú dohodnuté parametre. Cieľom eskalácií je urýchlenie procesu identifikácie a odstránenia porúch, zvýšenie transparentnosti, zlepšenie komunikácie, vytvorenie jasných kanálov komunikácie medzi poskytovateľom a zákazníkom a minimalizácia negatívnych dôsledkov výpadkov alebo zhoršenia kvality služieb.  Eskalačné postupy sa aplikujú pre incidenty Severity 1 a Severity 2 po uplynutí stanovenej doby po nesplnení parametrov pre daný incident alebo pri značnom množstve dotknutých škôl, hromadných výpadkoch.   * Eskalácia 1. úrovne:   + Eskalácia na vedúceho Servis desk   + Incident Severity 1 neodstránený v dohodnutom čase * Eskalácia 2. úrovne:   + Eskalácia na CTO alebo obdobné   + Incident Severity 1 neodstránený 2. pracovný deň po dohodnutom čase, alebo   + Incident Severity 1 súčasne na viac ako 25 školách po dobu 1 pracovného dňa * Eskalácia 3. úrovne:   + Eskalácia na CEO RPŠ   + Incident Severity 1 neodstránený 4. pracovný deň po dohodnutom čase, alebo   + Incident Severity 1 súčasne na viac ako 50 školách po dobu 1 pracovného dňa   O eskalácii bude upovedomený mailom zodpovedná oprávnená osoba školy ako aj Ministerstvo a uvedením kontaktov na vedúceho pracovníka ktorému bola situácia eskalovaná. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | Škola |
| **Iné zainteresované strany** | | | NCU |
| **Prevádzková doba** | | | | pracovné dni 6:00 – 18:00 |
| **Minimálna Dostupnosť služby** | | | | N/A |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa času v tickete |
| **Doba vyhodnocovania** | | | | Po uzavretí ticketu |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | RTTR Merateľné ukazovatele pre odstraňovanie Nesúladu služby podľa severity |
| **Definícia** | | Severity 1 |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | N/A |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | pracovný deň od nahlásenia/identifikácie |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 1 |
|  | |  |
| **Metrika 2** | **Názov:** | | RTTR Merateľné ukazovatele pre odstraňovanie Nesúladu služby podľa severity |
| **Definícia** | | Severity 2 |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | N/A |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | pracovný deň od nahlásenia/identifikácie |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 3 |
|  | |  |
| **Metrika 3** | **Názov:** | | RTTR Merateľné ukazovatele pre odstraňovanie Nesúladu služby podľa severity |
| **Definícia** | | Severity 3 |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | N/A |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | pracovný deň od nahlásenia/identifikácie |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 5 |
|  | |  |
| **Metrika 4** | **Názov:** | | RTTR Merateľné ukazovatele pre odstraňovanie Nesúladu služby podľa severity |
| **Definícia** | | Severity 4 |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | N/A |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | pracovný deň od nahlásenia/identifikácie |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 10 |
|  | |  |

Tabuľka 18: Riešenie incidentov RPŠ – ServiceDesk - detailná definícia požiadaviek na službu

### Riešenie iných požiadaviek používateľov

#### Žiadosť o informáciu

Škola môže požiadať prostredníctvom NCU Helpdesku o rôzne ďalšie relevantné informácie súvisiace s poskytovanými službami. NCU žiadosť zaeviduje v tickete, priamo odpovie alebo presunie riešenie na RPŠ. RPŠ v primeranom čase zašle požadovanú informáciu.

#### Mimoriadne situácie

Mimoriadna situácia je vopred ohlásené časové obdobie v ktorom sú požadované zvýšené nároky na dostupnosť a kvalitu služieb zo strany RPŠ. V prípade mimoriadnej situácie môže Ministerstvo žiadať o spustenie posilnenia prevádzky. Ide napríklad o prevádzku v čase volieb v budove školy, maturít, testovania deviatakov, živelných katastrof a odstraňovania ich následkov a podobne.

Mimoriadna situácia môže byť vyhlásená na jednej, niekoľkých alebo aj všetkých školách.

Mimoriadnu situáciu oznámi Ministerstvo alebo Škola RPŠ a to minimálne 1 mesiac vopred, o výnimočných prípadoch urgentnej mimoriadnej situácie aj v skrátenej lehote.

Celkové trvanie mimoriadnych situácií môže byť maximálne 10 dní na jednej škole v jednom školskom roku.

Počas trvania mimoriadnej situácie RPŠ zabezpečí prednostné spracovanie na ServiceDesk-u, prednostné odstraňovanie incidentov na mieste, priorizáciu liniek daných škôl a ďalšie požadované primerané opatrenia.

Počas mimoriadnej situácie môže Ministerstvo žiadať o zmenu konfigurácie v sieti tak aby bol uprednostňovaný istý typ služby, časť siete resp. zapnutá časť siete a ostatné blokované a zabezpečená zmena smerovania v sieti.

### Oznamovanie a odsúhlasovanie plánovaných výpadkov

| **Plánované výpadky - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Plánované výpadky |
| **Kategória** | | | | Služby podpory prevádzky a údržby riešenia LAN/WLAN/WAN |
| **Typ** | | | | Ad-hoc |
| **Cieľ** | | | | Táto časť definuje požiadavky na úrovne služieb v súvislosti s plánovanými výpadkami. Cieľom je zabezpečiť, aby plánované výpadky mali minimálny vplyv na prevádzku škôl a aby boli všetky relevantné informácie poskytnuté včas a transparentne. |
| **Plánované výpadky - detailná definícia požiadaviek na službu** | | | | |
| **Plánovaný výpadok:** Dočasné prerušenie/Nesúlad poskytovania aspoň časti služieb, ktoré je vopred naplánované a ohlásené RPŠ.  **Okno údržby:** Časový úsek, počas ktorého môže dôjsť k plánovanému výpadku:   * pracovné dni medzi 16:00 a 06:00 a počas víkendov 00:00 – 23:59   **Oznámenie o plánovanom výpadku:** Informácie poskytuje RPŠ škole a na NCU-ServiceDesk, vytvorí príslušný typ udalosti v CTP o nadchádzajúcom plánovanom výpadku, ktorá obsahuje dátum, čas začiatku a predpokladaný čas ukončenia výpadku.  Oznámenie o plánovanom výpadku bude obsahovať nasledujúce informácie:   * dátum a čas začiatku plánovaného výpadku, * predpokladaný čas ukončenia plánovaného výpadku, * dôvod plánovaného výpadku, * vplyv plánovaného výpadku na poskytované služby, * kontaktné informácie pre prípad otázok.   **Urgentný plánovaný výpadok:** V mimoriadnych situáciách, keď s bezpečnostných alebo iným závažných dôvodov nie je možné dodržať časy uvedené vyššie. Ak to urgencia vyžaduje, vo výnimočných prípadoch je ho možné zrealizovať aj mimo Okna údržby. Oznámenie potom musí obsahovať aj zdôvodnenie Urgentného plánovaného výpadku.  Po ukončení výpadku RPŠ oznámi ukončenie plánované výpadku.  V prípade že navrhovaný čas plánovaného výpadku bude pre školu v značne nevyhovujúcom čase, môže požiadať zmenu času vykonania plánovanej práce a RPŠ zváži možnosť vyhovieť požiadavke.  V prípade že výpadok bude oznámený podľa podmienok, nebude podliehať pokutám inak sa bude na neho nahliadať ako na Incident ak nastane v prevádzkovej dobe služby. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | Škola, NCU |
| **Iné zainteresované strany** | | | NCU |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | N/A |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa času v tickete |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Oznámenie o plánovanom výpadku vopred |
| **Definícia** | | Požadovaný čas oznámenia plánovaného výpadku |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | N/A |
| **Požadovaná hodnota** | **Jednotka** | hodina |
| **Minimum** | 72 vopred |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Service review meeting |
| **Merateľné parametre** | **Metrika 2** | **Názov:** | | Oznámenie o urgentnom plánovanom výpadku vopred |
| **Definícia** | | Požadovaný čas oznámenia urgentného plánovaného výpadku |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | N/A |
| **Požadovaná hodnota** | **Jednotka** | hodina |
| **Minimum** | 2 vopred |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Service review meeting |
| **Merateľné parametre** | **Metrika 3** | **Názov:** | | Požiadavka na trvanie plánovaného výpadku |
| **Definícia** | | Maximálna dĺžka plánovaného výpadku |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | pracovné dni medzi 16:00 a 06:00 a počas víkendov 00:00 – 23:59 |
| **Spôsob** | N/A |
| **Požadovaná hodnota** | **Jednotka** | hodina |
| **Minimum** | Nie je obmedzené |
| **Maximum** | 5 |
| **Severita Nesúladu služby** | | Podľa služby: Riešenie incidentov; a teda rozsahu počtu postihnutých bodov v prípade že plánovaný výpadok presiahol okno údržby do štandardnej prevádzkovej doby služieb. |

Tabuľka 19: Plánované výpadky – definícia požiadaviek na službu

### Zabezpečovanie údržby a homogenity LAN/WLAN a súladu s dokumentáciou

#### Zabezpečovanie aktualizácii a testovania

RPŠ musí mať zavedený systém pre riadenie záplat (patchov) a aktualizácií. Systém musí zabezpečiť pravidelné sledovanie publikovaných aktualizácie prevádzkované prvky IT infraštruktúry a rozhodnúť o ich nasadení. Okrem sledovania vydaných aktualizácií sa musia pravidelne (minimálne raz za mesiac) monitorovať a posudzovať ich zraniteľnosti.

Aktualizácie sa nasadzujú na základe vyhodnotenia rizík a kontrolovaným spôsobom. Inštalácia aktualizácií musí byť riadená iba Špecialistom/Administrátorom zodpovedným za daný systém a to kontrolovaným spôsobom tak, aby bezpečnostná záplata nespôsobila funkčné výpadky služieb. Deploy zmien musí byť riadne otestovaný. Aktualizácie a meny musia byť pred inštaláciou adekvátne otestované za účelom overenia ich funkčnosti a vplyvu na prevádzku a bezpečnosť. Zároveň musí byť pripravená aj stratégia vrátenia zmeny v prípade neočakávaných problémov.

RPŠ pred implementáciou opráv softvéru, implementácie zmien HW, SW, konfigurácie v školskej sieti vykoná všetky potrebné testy. V prípade požiadavky oprávnenej osoby školy, Ministerstva, poskytne správu o testovaní. Zástupcovia školy, Ministerstva, NCU majú právo zúčastniť sa testov ak o to požiadajú.

#### Zabezpečovanie súladu s metodickými usmerneniami

Vyžadujeme od RPŠ aby dlhodobo koordinoval konfigurácie služieb/nastavenia služieb v súlade s usmerneniami NCU resp. metodickými usmerneniami Ministerstva s cieľom zabezpečenia homogenity nastavení a udržateľnosti zmien v školských sieťach. Úlohou poskytovateľa služieb NCU je formalizovať prevádzkový a konfiguračný poriadok ktorý formálne schvaľuje Ministerstvo a úlohou RPŠ je sa ním riadiť.

#### Zabezpečovanie komunikácie s časťou siete v správe školy

Súčasťou služieb RPŠ je dlhodobé zabezpečovanie funkčnosti prepojenia medzi riešením RPŠ a existujúcou časťou siete školy, ktorého prepojenie vykonal podľa požiadaviek školy pri akceptácii riešenia na škole a jeho prechode riešenia RPŠ do prevádzky.

#### Zabezpečovanie súladu dokumentácie

Súčasťou služieb RPŠ je priebežne aktualizovať dizajn a dokumentáciu riešenia a služieb.

Dokumentácia odovzdaná pri akceptácii riešenia do prevádzky musí byť aktualizovaná po každej významnej zmene v systéme počas nasadzovania a životného cyklu projektu.

Aktualizovať zoznam aktívnych prvkov na škole minimálne v rozsahu: Výrobca, Typ, SN, dátum inštalácie, evidencia EoS a EoL zariadenia.

Zabezpečovať správu licencii ktoré prislúchajú k nainštalovaným prvkom riešenia.

Aktualizovať v prípade zmien a doplnení pasívnej infraštruktúry do plánu budovy. Umiestnenia pasívnych prvkov.

Udržiavať označenie: káblov, koncoviek, portov a prepojení.

Všetky časti dokumentácie sú aktualizované v digitálnej podobe na lokalite definovanej Ministerstvom. Dokumentácia musí byť v Slovenskom jazyku.

Hodnota parametra

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Aktualizácia dokumentácie riešenia a služieb |
| **Definícia** | | Požadovaný čas vykonania aktualizácie dokumentácie |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Dni |
| **Minimum** | 5 |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Severita 4, Eskalácia |

### RACI matica pre služby podpory, prevádzky a údržby riešenia LAN/WLAN/WAN

| **Popis činnosti** | **Škola** | **RPŠ** | **NCU** | **MŠVVaM** |
| --- | --- | --- | --- | --- |
| Bezodkladné nahlasovanie udalosti používateľom | A,R | R | I | n/a |
| Poskytovanie súčinnosti používateľa pri klasifikácii a riešení udalostí 8.00 – 17.00 počas pracovných dní | A,R | C | C | n/a |
| Prevádzka NCU – Service Desku | N/A | N/A | A,R | N/A |
| Evidencia udalostí, aktuálnosť informácií ticketov | I | R | A,R | I |
| Klasifikácia udalosti | C | R | A,R | I |
| Detekcia udalostí | I | A,R | R | I |
| Spolupráca s NCU pri riešení problémov | N/A | A,R | N/A | N/A |
| Odstránenie incidentu v pôsobnosti RPŠ | I | R | A,I | I |
| Vzdialená podpora, súčinnosť, podpora na mieste | R | C | I | A |
| Sklad HW, výmena HW na mieste, RMA, výjazd servisného technika | I | A,R | I | I |
| Oznámenie o plánovanom výpadku | I | A,R | C | I |
| Oznámenie o neplánovanom výpadku | I | A,R | I | I |

Tabuľka 20: RACI matica pre služby podpory, prevádzky a údržby riešenia LAN/WLAN/WAN

## Služby reportingu o stave a využívaní riešenia LAN/WLAN/WAN a kvality

Prevádzka služieb reportingu poskytuje komplexné a automatizované správy a analýzy týkajúce sa výkonu siete, stavu zariadení, používaní siete klientami a kvality poskytovaných služieb. RPŠ odovzdáva reporty Ministerstvu na určenú sieťovú lokalitu a do NCU na ďalšie spracovanie. RPŠ pripravuje reporty v požadovanom formáte podľa metodického usmernenia Ministerstva.

### Vytváranie správy o histórii pripojených zariadení

| **Vytváranie správy o histórii pripojených zariadení - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Vytváranie správy o histórii pripojených zariadení |
| **Kategória** | | | | Služby reportingu o stave a využívaní riešenia LAN/WLAN/WAN a kvality |
| **Typ** | | | | Pravidelná |
| **Cieľ** | | | | Z dôvodu zabezpečenia efektívneho využitia siete, služba reportingu musí poskytnúť funkciu 30-dňovej histórie, ktorá uchováva a zobrazuje údaje o sieťových aktivitách zariadení pripojených v sieti |
| **Zabezpečovanie údržby a homogenity LAN/WLAN - detailná definícia požiadaviek na službu** | | | | |
| Historické dáta musia obsahovať minimálne nasledovné informácie:   * status klienta (online/off-line), * meno/popis zariadenia, * kedy bol pripojený v sieti (prvý a posledný krát), * vyťaženie siete za zvolené obdobie (2H až 30 dní), * typ klienta (výrobca, Operačný systém), * IPv4/IPv6 adresa, MAC adresa, * na ako porte prepínača alebo WiFi AP je/bol pripojený, * VLAN ID, * používateľ (za predpokladu 802.1X), * aktuálne pripojené SSID, šírka kanálu, schopnosti WiFi štandardu (802.11). * Služba poskytuje vygenerovanie reportu vo formáte CSV, XML a JSON, dostupné cez GUI alebo API rozhranie. Vygenerované si sťahuje v požadovanej periodicite a granularite NCU. Miesto sa určí po vzájomnej dohode RPŠ a poskytovateľa služieb NCU. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | Škola, NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | História |
| **Definícia** | | Dostupnosť histórie s funkcionalitou podľa požiadaviek na službu v požadovanej granularite/periodicite |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 1x mesačne |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Eskalácie |

Tabuľka 21: Vytváranie správy o histórii pripojených zariadení – definícia požiadaviek na službu

### Vytváranie správy o poskytnutom výkone za zvolené obdobie

| **Performance report za zvolené obdobie - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Performance report za zvolené obdobie |
| **Kategória** | | | | Služby reportingu o stave a využívaní riešenia LAN/WLAN/WAN a kvality |
| **Typ** | | | | Pravidelná |
| **Cieľ** | | | | Súhrnná správa slúži pre kapacitné plánovanie, vytváranie konsolidovaných reportov pre rezort, vynucovanie súladu s využívaním konektivity, kvality služieb, fakturáciu. |
| **Performance report za zvolené obdobie - detailná definícia požiadaviek na službu** | | | | |
| **Vytváranie správy o vyťažení LAN/WLAN**  Súhrnná správa slúži pre kapacitné plánovanie a vynucovanie súladu s využívaním konektivity  Funkcia musí umožňovať na požiadanie online vytvorenie súhrnných správ ohľadne využívania infraštruktúry. Špecificky musí umožňovať za zvolené časové obdobie (min 3 mesiace spätne) získať minimálne nasledovné informácie:   * celkové množstvo prenesených dát upload, * celkové množstvo prenesených dát download, * určiť špičky v dátových prenosoch, * priemerný počet pripojených zariadení denne, * určiť najvyužívanejšie SSID z pohľadu počtu klientov, * určiť najvyužívanejšie SSID z pohľadu množstva dátových prenosov , * určiť WiFi AP zariadenia najviac vyťažené z pohľadu počtu klientov, * určiť WiFi AP zariadenia najviac využité z pohľadu množstva dátových prenosov, * určiť switche najviac využité z pohľadu množstva dátových prenosov, * vyťaženie konkrétneho portu na switchi, * určiť spotrebu PoE napájania na konkrétnych prepínačoch, * určiť klientske zariadenia pripojené k sieti WiFi a wired najviac využité z pohľadu množstva dátových prenosov, * určiť najpoužívanejšie aplikačné kategórie (produktivita, emaily, sociálne siete atď.).   Funkcia musí umožňovať odoslanie súhrnnej správy na definované emailové adresy.  Funkcia musí umožňovať automatizáciu odosielania súhrnnej správy za zvolené obdobie (min. týždenne a mesačne) na definované emailové adresy.  **Vyťaženie WAN linky**  S cieľom zabezpečiť optimálne využívanie WAN konektivity, služby reportingu musia poskytovať funkciu zbierania a zobrazenia údajov o vyťažení WAN pripojenia. Služba reportingu musí poskytovať prehľad o aktuálnom a historickom využití WAN linky, a to z hľadiska prenesených dát, počtu paketov a ďalších relevantných parametrov. Reporty musia obsahovať minimálne tieto informácie:   * celkové vyťaženie WAN linky: priemerná, maximálna a minimálna prenosová rýchlosť za zvolené obdobie počas celej doby poskytovania služieb, * Upozornenia: možnosť nastavenia prahových hodnôt pre vyťaženie WAN linky a generovanie notifikácií na oprávnenú osobu školy, poskytovateľa služieb NCU v prípade ich porušenia.   Funkcia musí umožňovať odoslanie súhrnnej správy na definované emailové adresy.  Funkcia musí umožňovať automatizáciu odosielania súhrnnej správy za zvolené obdobie (min. týždenne a mesačne) na definované emailové adresy  **Report kvality služieb prevádzky**   * RPŠ vypracuje všetky požadované reporty a odovzdá ich Centrálnemu uzlu najneskôr v tretí pracovný deň nasledujúceho mesiaca po skončení príslušného zúčtovacieho obdobia. Formát v akom budú reporty odovzdávané špecifikuje NCU. Report bude obsahovať aj posúdenie zhody s požadovanými hodnotami parametrov a dostupnosti. * V prípade nedodržania parametra dostupnosti ku ktorému sú dohodnuté pokuty RPŠ vypočíta a uvedie aj príslušnú pokutu. V prípade nedodržania parametra pre službu Riešenia incidentov, nesúlad sa vypočítava na základe časov podľa ticketov v centrálnom portály riadenia ticketov prevádzkovaného poskytovateľom služieb NCU. * NCU report skontroluje a najneskôr 8. pracovný deň nasledujúceho mesiaca po skončení príslušného zúčtovacieho obdobia zašle RPŠ schválenie reportu alebo pripomienky, ktoré RPŠ bez odkladne odstráni a zašle opravený report. * NCU zašle reporty 8. pracovný deň nasledujúceho mesiaca po skončení príslušného zúčtovacieho obdobia Ministerstvu, ktoré zašle prípadné pripomienky najneskôr 13. pracovný deň nasledujúceho mesiaca po skončení príslušného zúčtovacieho obdobia do RPŠ. V prípade že najneskôr 13. pracovný deň nasledujúceho mesiaca po skončení príslušného zúčtovacieho obdobia, RPŠ nedostane pripomienky považuje sa report za schválený. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | Škola, NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Dostupnosť reportov |
| **Definícia** | | Možnosť generovať performance report za zvolené obdobie s funkcionalitou podľa požiadaviek na službu |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 1x mesačne |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Eskalácie |

Tabuľka 22: Performance report za zvolené obdobie– definícia požiadaviek na službu

### Vytváranie správy o intruzívnom meraní kapacity WAN

| **Vytváranie správy o intruzívnom meraní kapacity WAN - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Vytváranie správy o intruzívnom meraní kapacity WAN |
| **Kategória** | | | | Služby reportingu o stave a využívaní riešenia LAN/WLAN/WAN a kvality |
| **Typ** | | | | Pravidelná |
| **Cieľ** | | | | Cieľom je meranie skutočnej priepustnosti WAN konektivity. |
| **Vytváranie správy o intruzívnom meraní kapacity WAN - detailná definícia požiadaviek na službu** | | | | |
| Vytváranie správy o priepustnosti WAN na základe merania podľa služby: Zabezpečovanie primárnej dátovej konektivity. Meraná bude priepustnosť medzi Školou a RPŠ (alebo NCU) v oboch smeroch.   * Výsledok merania bude súčasťou nasledujúceho mesačného reportu. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | Škola, NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x kvartálne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Dostupnosť reportov |
| **Definícia** | | Meranie a reportovanie priepustnosti WAN konektivity školy |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 1 za kvartál |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Eskalácie |

Tabuľka 23: Vytváranie správy o intruzívnom meraní kapacity WAN – definícia požiadaviek na službu

### Vytvorenie analýzy trendov a problémov

| **Vytvorenie analýzy trendov a problémov - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Vytvorenie analýzy trendov a problémov |
| **Kategória** | | | | Služby reportingu o stave a využívaní riešenia LAN/WLAN/WAN a kvality |
| **Typ** | | | | Pravidelná |
| **Cieľ** | | | | Pre účely prediktívnej údržby a optimalizácie výkonu siete je nevyhnutné vykonávať pravidelnú analýzu historických údajov. Táto analýza umožní identifikovať dlhodobé trendy, sezónne výkyvy, opakujúce sa problémy a predikovať budúce potreby siete. |
| **Vytvorenie analýzy trendov a problémov - detailná definícia požiadaviek na službu** | | | | |
| V rámci zabezpečovania tejto služby je potrebné vykonávať nasledovné činnosti:   * uchovávanie historických dát: systém musí uchovávať detailné historické dáta o prevádzke siete za dostatočne dlhé obdobie a to minimálne za posledných 30 dní, * služba identifikácie stúpajúcich alebo klesajúcich trendov v prevádzke siete, ako aj sezónne výkyvy, * detekcia anomálií: detekcia odchýlok od normálneho správania siete, ktoré môžu signalizovať potenciálne problémy, * korelácia údajov: systém musí umožniť koreláciu údajov z rôznych zdrojov (napr. vyťaženie linky, počet používateľov, poruchy zariadení) za účelom identifikácie príčin problémov, * predpovedanie: na základe historických údajov systém musí byť schopný predpovedať budúce potreby siete, napr. zvýšenú kapacitu, nové zariadenia, * grafické zobrazenie: systém musí umožňovať zobrazovať vývoj vyťaženia WAN linky za zvolené obdobie (hodina, deň, mesiac) počas celej doby poskytovania služieb, systém musí umožňovať filtrovanie škôl na základe úrovne vyťaženia primárnej konektivity v hlavnej prevádzkovej hodine, * reportovanie analýzy v dohodnutom formáte poskytovateľovi služieb Centrálneho uzlu. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | Škola, NCU, MŠVVaM SR |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Frekvencia vykonávania analýzy a správy |
| **Definícia** | | Pravidelnosť, s akou je vykonávaná automatická analýza historických údajov |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | 1x mesačne |
| **Maximum** | Nie je obmedzené |
| **Severita Nesúladu služby** | | Eskalácie |

Tabuľka 24: Vytvorenie analýzy trendov a problémov – definícia požiadaviek na službu

### Zaisťovanie kompatibility reportovania s nástrojmi NCU

| **Zaisťovanie kompatibility reportovania s nástrojmi NCU - detailná definícia požiadaviek na službu** | | | | |
| --- | --- | --- | --- | --- |
| **Názov** | | | | Zaisťovanie kompatibility reportovania s nástrojmi NCU |
| **Kategória** | | | | Služby reportingu o stave a využívaní riešenia LAN/WLAN/WAN a kvality |
| **Typ** | | | | Kontinuálna |
| **Cieľ** | | | | Okrem súhrnných reportov umožňuje systém RPŠ odosielať informácie o zariadeniach a udalostiach prostredníctvom Syslog, API a SNMP. |
| **Zaisťovanie kompatibility reportovania s nástrojmi NCU - detailná definícia požiadaviek na službu** | | | | |
| Okrem prípravy súhrnných reportov podľa usmernenia NCU umožňuje systém RPŠ odosielať informácie o zariadeniach a udalostiach prostredníctvom API  RPŠ v sieti podporuje Syslog protokol je používaný na reportovanie systémových logov a udalostí zo sieťových zariadení do centralizovaného logovacieho servera, pričom logy musia obsahovať minimálne nasledovné informácie:   * Špecificky pre prepínače:   + 802.1X: Udalosti súvisiace s autentifikáciou a deautentifikáciou klientov,   + RADIUS: Udalosti spojené s Radius protokolom,   + Spanning Tree: Udalosti súvisiace s protokolom STP,   + Switch port: Udalosti spojené so stavom portov,   + Switch status: Udalosti spojené s poskytovaním PoE a teplotou zariadenia, * Špecificky pre WiFi AP:   + 802.11: Udalosti spojené s Asociáciou a disasociáciou klientov k WiFi AP,   + 802.1X: Autentifikácia a deautentifikácia RADIUS protokolom,   + WPA: Udalosti spojené s autentifikáciou/deautentifikáciou WPA,   + Radio planning: Udalosti spojené so zmenou a šírkou pásma vyžarovaných kanálov, vysielacím výkonom,   + WiFi IPS/IDS: Udalosti spojené s bezdrôtovým DDOS útokom a iné bezpečnostné hrozby detegované AP,   + DFS: Udalosti spojené s Dynamickou selekciou kanálov (DFS),   + DHCP: Udalosti spojené s réžiou DHCP,   + IP: Detekcia IP konfliktov,   + NBAR: Upozornenie na detekciu L7 firewall pravidla,   + RADIUS: Udalosti spojené s Radius protokolom a MAB autentifikáciou.   Služba podporuje možnosť používať API volania na zhromažďovanie a export štatistík a ďalších informácií, slúžiacich na účely integrácie s externými nástrojmi, ktoré spravuje NCU.  Pre účely kompatibility a reportingu musí služba poskytovať verejne prístupné API knižnice. Táto API knižnica obsahuje minimálne nevyhnutné prevádzkové dáta, týkajúci sa sieťových prvkov a pripojených WiFi/drôtových zariadení.  Najmä však dáta o stave zariadení a klientov, ich vyťaženie a sieťové štatistiky, informácie o inventári a konfiguračné zmeny.  Funkcia musí byť dostupná pre RPŠ, tiež pre poverených pracovníkov NCU,  školy, zriaďovateľa, MŠVVaM SR.  RPŠ v sieti podporuje protokol SNMP (Simple Network Management Protocol) umožňuje sieťovým administrátorom dotazovať zariadenia na rôzne nevyhnutné informácie pre účely reportovania stavu siete.  Služba preto vyžaduje, aby zariadenia poskytovali štandardizované MIB (Management Information Base) databázy, obsahujúce hierarchicky usporiadaný zoznam objektov OID (Object Identifier).  OID predstavuje konkrétny typ informácie, ktorú môže SNMP vyžadovať od zariadení.  Nakoľko poskytovaná služba vyžaduje iba reportovanie informácií prostredníctvom SNMP, služba požaduje iba vykonávanie požiadavky typu „GET“. Neuvažuje sa teda o vykonávaní žiadnych konfiguračných zmien pomocou tohto protokolu. Protokol musí byť podporovaný verziách: SNMP v1/v2c a v3.  Keďže verzie SNMP 1 a 2 posielajú community string v nezašifrovanej podobe, služba požaduje definovanie IP adries oprávnených pristupovať k sieti pomocou protokolu SNMP.  Okrem iného služba požaduje, aby systém RPŠ poskytoval aspoň nasledovné informácie prostredníctvom SNMP:   * MAC adresa zariadenia, * sériové číslo zariadenia, * meno zariadenia a jeho produktový kód, * status zariadenia (online/offline), * posledná komunikácia zariadenia s CRSD (dátum a čas), * množstvo prenesených packetov/bytes in/out na každom fyzickom rozhraní.   Pre zasielanie okamžitých upozornení na špecifické sieťové scenáre je možné definovať SNMP Traps. Pre ochranu súkromia používajú SHA1 pre autentifikáciu a AES pre šifrovanie. | | | | |
| **Účastníci** | **Poskytovateľ** | | | RPŠ |
| **Používateľ** | | | NCU |
| **Iné zainteresované strany** | | |  |
| **Prevádzková doba** | | | | 24/7 |
| **Minimálna Dostupnosť služby** | | | | 99,9% |
| **Spôsob vyhodnocovania merateľných parametrov** | | | | Podľa dostupnosti služby |
| **Doba vyhodnocovania** | | | | 1x mesačne |
|  | | | |  |
| **Merateľné parametre** | **Metrika 1** | **Názov:** | | Dostupnosť služieb |
| **Definícia** | | Dostupnosť služieb SNMP, Syslog, API |
| **Meranie/Monitorovanie** | **Vykonávateľ** | RPŠ |
| **Čas** | Počas prevádzkovej doby |
| **Spôsob** | Reaktívne |
| **Požadovaná hodnota** | **Jednotka** | Počet |
| **Minimum** | ÁNO služby podľa definície sú podporované |
| **Maximum** | N/A |
| **Severita Nesúladu služby** | | Eskalácie |

Tabuľka 25: Zaisťovanie kompatibility reportovania s nástrojmi NCU – definícia požiadaviek na službu

### RACI matica pre služby reportingu o stave a využívaní riešenia LAN/WLAN/WAN a kvality

| **Popis činnosti** | **Škola** | **RPŠ** | **NCU** | **MŠVVaM** |
| --- | --- | --- | --- | --- |
| Definovanie štruktúry reportov | N/A | C | A,R | C |
| Príprava reportov v požadovanej štruktúre | N/A | A,R | C | N/A |
| Zasielanie reportov do NCU podľa požadovanej štruktúry do požadovaného adresára | N/A | R | A | C |
| Poskytovanie rozhrania pre NCU na zber dát pre reportovanie | N/A | A,R | C | C |
| Schvaľovanie reportov | I | I | A,R | R |

Tabuľka 26: RACI matica pre služby reportingu o stave a využívaní riešenia LAN/WLAN/WAN a kvality

## Služby opcie – Náhrada služieb NCU

Z dôvodu zabezpečovania služieb NCU samostatnou súťažou žiada obstarávateľ v prípade meškania NCU ponuku zabezpečovania Náhradných služieb NCU od RPŠ. RPŠ plní základné požiadavky na tieto služby vedené ako opcia a bude ich zabezpečovať v prípade ich objednania zo strany obstarávateľa. Cieľom služby je poskytovanie dvoch skupín náhradných služieb NCU.

* Poskytovanie náhrady centrálnych služieb podpory prevádzky, konkrétne zabezpečovania služieb Service Desk – Helpdesk určených pre nahlasovanie a riadenia ticketov používateľov služieb a náhradu služieb CTP, ktorý si bude zabezpečovať RPŠ centrálne pre lokality škôl a používateľov pre ktorých zabezpečuje poskytovanie služieb.
* Poskytovanie sieťových služieb a sieťovej bezpečnosti.

Obstarávateľ môže požiadať o zabezpečovanie oboch služieb aj samostatne.

### Poskytovanie služieb Service Desk - Helpdesk, Ticketing

* Service desk – kontakt pre nahlasovanie udalostí oprávnenou osobou školy a Ministerstvom
  + Zabezpečovanie súboru technických, organizačných a personálnych prostriedkov pre zabezpečenie poskytovania služieb kontaktu a podpory pre používateľov siete prostredníctvom hlasovej komunikácie s využitím verejnej telefónnej siete a súčasne pomocou internetového portálu a mailovej adresy.
  + Vytváranie správ o riešení incidentov, napĺňania Dostupnosti a RTTR pre tikety.
* Service desk nástroj pre riadenie ticketov RPŠ
  + Nástroj RPŠ na evidenciu a management udalostí v sieti – ticketing nástroj a možnosť pripravovania performance reportov napĺňania hodnôt parametrov služieb.

### Poskytovanie sieťových služieb a sieťovej bezpečnosti

* Bezpečný prechod školy do internetu a sieťové služby
  + zabezpečené pripojenie do siete Internet prostredníctvom peeringového centra SIX s použitím vlastného čísla autonómneho systému
  + preklad privátnych IPv4 adries na verejné IPv4
  + DNS služby
  + služby správy IP adries
    - statický IP to MAC binding
    - podpora pre 802.1X
    - podpora pre IPv4 a IPv6
  + služby správy LAN segmentov a rozdelenie prevádzky do jednotlivých sietí a aplikácia nastavení pre jednotlivé SSID
  + zabezpečovať služby CPE alebo CE
  + zabezpečovať služby riadenia prístupu používateľov k sieti LAN/WLAN
* Content filtering, Firewall, aplikačná kontrola
  + V rámci zabezpečovania služieb RPŠ verejný obstarávateľ očakáva, že vybraný dodávateľ poskytuje prevádzku komplexnej služby súvisiacej so zabezpečením firewall-ingu dimenzovanej na základe požadovanej kapacity vyplývajúcej z počtu obsluhovaných škôl
    - podpora SSL inšpekcie
    - identifikácia aplikácie bez ohľadu na port, kryptovanie (SSL alebo SSH) alebo využitie evazívnych metód a techník
    - využitie aplikačnej vrstvy a nie portu ako základu pre výber správnej bezpečnostnej politiky a aplikáciu bezpečnostných opatrení (povoliť, zakázať, povoliť v časovom okne, limitovať šírku pásma alebo filtrovať nepovolený obsah)
    - kategorizácia neidentifikovaných aplikácií
    - forenznú analýzu
    - blokovanie na základe databáz známych hrozieb, vrátane exploit, malware a spyware na všetkých portoch a bez ohľadu na spôsob alebo metódu prieniku
    - limitovanie a obmedzovanie neautorizovaného prenosu súborov alebo iných typov dát vrátane HTTP a HTTPS prenosov webového obsahu
    - identifikácia neznámych typov malware na základe aplikácie behaviorálnych analytických nástrojov
    - škálovateľný IPv4 PAT (1:N) pre preklad privátnych IPv4 adries na verejné adresy pre užívateľov siete DigiNET
    - škálovateľný IPv4 NAT (1:1) pre sieť DigiNET (požiadavka na minimálne 1 verejnú IPv4 adresu pre každú lokalitu pripojenú do siete DigiNET) pre publikovanie zdrojov zo školských DMZ
  + V rámci zabezpečovania služieb RPŠ verejný obstarávateľ požaduje, že vybraný dodávateľ poskytuje prevádzku komplexnej služby súvisiacej so zabezpečením filtrovania webového obsahu, a to najmä:
    - možnosť explicitne povoliť web stránky / zdroje elektronického obsahu, ktoré sú dôveryhodné a tie ponechať bez inšpekcie
    - možnosť vytvoriť zoznamy s web stránkami alebo URL / URI, alebo špeciálnych výrazov a kľúčových slov, ktoré budú podliehať inšpekcii
    - možnosť použiť preddefinované kategórie filtrov obsahu a podkategórie a tie podľa určenia blokovať alebo povoľovať
    - možnosť použiť verejne dostupné block listy a podľa nich blokovať alebo povoľovať obsah
    - možnosť regulovať šírku prenosového pásma pre obsah nesúvisiaci s procesom výučby
    - možnosť aktualizovať databázu kategórií a signatúr systému filtrovania minimálne 4-krát denne
    - možnosť pridať do databázy kategórií a signatúr nový záznam
    - Globálne nastavenie filtrovania obsahu musí byť realizované spôsobom blocklist prístupu k filtrovaniu, teda neznámy, nevhodný, nový a nedôveryhodný obsah je zakázaný na základe kategórií a dodaných blocklist URL na základe požiadaviek MŠVVaM SR, podľa uvedených kritérií:
      * podľa času (vyučovací čas vs. ostatný čas),
      * podľa WiFi SSID alebo LAN pripojeného užívateľa,
      * podľa skupín užívateľov (vek, žiak, učiteľ, návštevník),
      * podľa zdrojovej IP adresy alebo rozsahu adries.
    - Zároveň je nevyhnutné, aby bolo možné blokovanie granulárne definovať pre konkrétnu skupinu používateľov alebo podmienok podľa rovnakých kritérií.
    - Známy, dôveryhodný obsah by mal byť štandardne povolený. Takto nastavený proces filtrovania musí byť možné škálovať a individuálne nastavovať podľa bezpečnostných nastavení skupín z identity servera až do úrovne konkrétneho prihláseného užívateľa.
  + V rámci zabezpečovania služieb RPŠ verejný obstarávateľ očakáva, že vybraný dodávateľ poskytuje prevádzku komplexnej služby súvisiacej so zabezpečením centrálnej aplikačnej kontroly, a to najmä:
    - možnosť explicitne povoliť kategórie aplikácií a ich komunikáciu na zdroje elektronického obsahu, ktoré sú dôveryhodné a tie ponechať bez inšpekcie
    - možnosť explicitne zakázať kategórie aplikácií a ich komunikáciu na zdroje elektronického obsahu, ktoré sú nedôveryhodné alebo nežiadané pre komunikáciu siete DigiNET do Internetu
    - vytváranie profilov nastavení aplikačnej kontroly na základe požiadaviek MŠVVaM SR a uplatniť ich až do úrovne konkrétneho užívateľa
    - možnosť regulovať šírku prenosového pásma pre aplikácie nesúvisiace s procesom výučby
    - možnosť aktualizovať databázu kategórií a signatúr systému aplikačnej kontroly minimálne 1-krát týždenne
    - možnosť pridať do databázy kategórií a signatúr nový záznam.
    - Globálne nastavenie filtrovania obsahu je realizované spôsobom blocklist prístupu k aplikáciám, teda neznáme aplikácie a aplikácie predstavujúce bezpečnostné riziko by mali byť zakázané na základe požiadaviek MŠVVaM SR, podľa:
      * času (vyučovací čas, ostatný čas),
      * WiFi SSID/LAN,
      * skupín používateľov (vek, žiak, učiteľ, návštevník).
* Príprava konsolidovaných reportov za RPŠ podľa požiadaviek reportingu.

# Prílohy

## Zoznam skratiek

| **Skratka** | **Vysvetlenie** |
| --- | --- |
| ACL | Access Control List |
| AP | Access Point |
| API | Application Programming Interface |
| API RESTful | Representational State Transfer Application Programming Interface |
| BPDU | Bridge Protocol Data Unit |
| BSSID | Basic Service Set Identifier |
| CEO | Chief Executive Officer |
| CoPP | Control Plane Policing |
| CPE | Customer Premises Equipment |
| CRSD | Centralizované riešenie správy a dohľadu |
| CSV | Comm-aSeparated Values |
| CTO | Chief Technology Officer |
| CTP | Centrálny Ticketing Portál |
| NCU | Centrálny Uzol |
| DDoS | Distributed Denial of Service |
| DFS | Dynamic Frequency Selection |
| DHCP | Dynamic Host Configuration Protocol |
| DMZ | Demilitarized Zone |
| DNS | Domain Name System |
| EoL | End of Life |
| EoS | End of Service |
| ETSI | European Telecommunications Standards Institute |
| EUR | Euro |
| GDPR | General Data Protection Regulation |
| GUI | Graphical User Interface |
| HECC | Highly Equipped and Connected Classroom |
| HTTP | HyperText Transfer Protocol |
| HTTPS | HyperText Transfer Protocol Secure |
| HW | Hardvér |
| ID | Identifikátor |
| IDS | Intrusion Detection System |
| IEEE | Institute of Electrical and Electronics Engineers |
| IKT | Informačné a Komunikačné Technológie |
| IP | Internet Protocol |
| IPSEC | Internet Protocol Security |
| IT | Informačné Technológie |
| ITIL | Information Technology Infrastructure Library |
| JSON | JavaScript Object Notation |
| LAN | Local Area Network |
| LLDP | Link Layer Discovery Protocol |
| MAB | Media Access Control Authentication Bypass |
| MAC | Media Access Control |
| MD | Man-Day |
| MIB | Management Information Base |
| MŠVVaM SR | Ministerstvo školstva výskumu vývoja a mládeže SR |
| MU-MIMO | MultiUser Multiple Input Multiple Output |
| N/A | Not Applicable |
| NBAR | NetworkBased Application Recognition |
| NCU | Národný Centrálny Uzol/ Centrálny uzol |
| NTBK | Notebook |
| OID | Object Identifier |
| OS | Operačný Systém |
| OWE | Opportunistic Wireless Encryption |
| PAT | Port Address Translation |
| PC | Osobný Počítač |
| PoE | Power over Ethernet |
| POST | PowerOn SelfTest |
| PSK | PreShared Key |
| RADIUS | Remote Authentication Dial-In User Service |
| RAM | Random Access Memory |
| RBAC | RoleBased Access Control |
| RFC | Request for Comments |
| RPŠ | Regionálny Partner Školy |
| RSSI | Received Signal Strength Indicator |
| RX-SOP | Receiver Start of Packet |
| SLA | Service Level Agreement |
| SMS | Short Message Service |
| SN | Serial Number |
| SNMP | Simple Network Management Protocol |
| SNR | Signal-to-Noise Ratio |
| SR | Slovenská Republika |
| SREV | Service Review Meeting |
| SSH | Secure Shell |
| SSID | Service Set Identifier |
| SSL | Secure Sockets Layer |
| STP | Spanning Tree Protocol |
| SW | Softvér |
| SYSLOG | System Logging Protocol |
| TBD | To Be Determined |
| TÚ SR | Telekomunikačný Úrad Slovenskej Republiky |
| U-APSD | Unscheduled Automatic Power Save Delivery |
| UL/DL | Upload/Download |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WiFi | Wireless Fidelity |
| WLAN | Wireless Local Area Network |
| WMM | WiFi Multimedia |
| WPA | WiFi Protected Access |
| XML | eXtensible Markup Language |
| ZTP | Zero Touch Provisioning |

Tabuľka 27: Zoznam skratiek

## Zoznam obrázkov

[Obrázok 1: Proces zadávania a riešenia incidentu 71](#_Toc184082982)

## Zoznam tabuliek

[Tabuľka 1: Zoznam pojmov 6](#_Toc184975359)

[Tabuľka 2: Zabezpečovanie pokrytia siete WLAN – definícia požiadaviek na službu 15](#_Toc184975360)

[Tabuľka 3: Zabezpečovanie pokrytia siete LAN – definícia požiadaviek na službu 17](#_Toc184975361)

[Tabuľka 4: Zabezpečovanie priepustnosti v sieti WLAN – definícia požiadaviek na službu 20](#_Toc184975362)

[Tabuľka 5: Zabezpečovanie priepustnosti v sieti LAN – definícia požiadaviek na službu 24](#_Toc184975363)

[Tabuľka 6: Zabezpečovanie pripájania a výmeny CPE – definícia požiadaviek na službu 26](#_Toc184975364)

[Tabuľka 7: Zaisťovanie sieťovej bezpečnosti WLAN – definícia požiadaviek na službu 28](#_Toc184975365)

[Tabuľka 8: Zaisťovanie sieťovej bezpečnosti LAN – definícia požiadaviek na službu 30](#_Toc184975366)

[Tabuľka 9: RACI matica pre služby zabezpečovania prevádzky riešenia LAN/WLAN 31](#_Toc184975367)

[Tabuľka 10: Zabezpečovanie primárnej dátovej konektivity – definícia požiadaviek na službu 36](#_Toc184975368)

[Tabuľka 11: Zabezpečovanie primárnej dátovej konektivity a jej zálohy- detailná definícia požiadaviek na službu 37](#_Toc184975369)

[Tabuľka 12: RACI matica pre služby zabezpečovania WAN konektivity 38](#_Toc184975370)

[Tabuľka 13: Poskytovanie centralizovaného riešenia správy a dohľadu – definícia požiadaviek na službu 49](#_Toc184975371)

[Tabuľka 14: Poskytovanie služieb centralizovaného riešenia správy a dohľadu prostredníctvom NCU-CRSD – definícia požiadaviek na službu 62](#_Toc184975372)

[Tabuľka 15: Meranie spokojnosti koncového používateľa služieb, objektívna analýza – definícia požiadaviek na službu 65](#_Toc184975373)

[Tabuľka 16: RACI matica pre služby manažmentu a monitoringu riešenia LAN/WLAN/WAN 66](#_Toc184975374)

[Tabuľka 17: Poskytovanie služieb RPŠ – ServiceDesk - detailná definícia požiadaviek na službu 70](#_Toc184975375)

[Tabuľka 18: Riešenie incidentov RPŠ – ServiceDesk - detailná definícia požiadaviek na službu 76](#_Toc184975376)

[Tabuľka 19: Plánované výpadky – definícia požiadaviek na službu 79](#_Toc184975377)

[Tabuľka 20: RACI matica pre služby podpory, prevádzky a údržby riešenia LAN/WLAN/WAN 82](#_Toc184975378)

[Tabuľka 21: Vytváranie správy o histórii pripojených zariadení – definícia požiadaviek na službu 84](#_Toc184975379)

[Tabuľka 22: Performance report za zvolené obdobie– definícia požiadaviek na službu 86](#_Toc184975380)

[Tabuľka 23: Vytváranie správy o intruzívnom meraní kapacity WAN – definícia požiadaviek na službu 87](#_Toc184975381)

[Tabuľka 24: Vytvorenie analýzy trendov a problémov – definícia požiadaviek na službu 89](#_Toc184975382)

[Tabuľka 25: Zaisťovanie kompatibility reportovania s nástrojmi NCU – definícia požiadaviek na službu 91](#_Toc184975383)

[Tabuľka 26: RACI matica pre služby reportingu o stave a využívaní riešenia LAN/WLAN/WAN a kvality 92](#_Toc184975384)

[Tabuľka 28: Zoznam skratiek 98](#_Toc184975385)