

Príloha č. 1 k Výzve k spolupráci za účelom určenia predpokladanej hodnoty zákazky

1. Opis predmetu zákazky

Cieľom projektu EDUNET_SK je vybudovať jednotnú komunikačnú infraštruktúru pre materské, základné, stredné a špeciálne školy na Slovensku (ďalej len školy), ktorá zohľadní vyššie uvedené výzvy a zabezpečí:

- Virtuálnu privátnu sieť VPN na báze MPLS na zabezpečenie bezpečnej komunikácie zo škôl na zdroje dát a aplikácie umiestnené v dátových centrách rezortu školstva
- Centralizovaný riadený spoločný prestup pre všetky školy do siete Internet
- Prístup na Internet a VPN pre jednotlivé školy prostredníctvom technológie s najvyššou priepustnosťou, ktorá je dostupná v tej ktorej lokalite
- Bezdrôtový prístup z mobilných zariadení prostredníctvom technológie WiFi do sietí na školách. Bezdrôtový prístup má byť centrálnie spravovaný.
- Ochrana LAN sietí škôl pomocou centrálného firewallu
- Služby content a web filteringu aplikované podľa definovaných politík s dynamickým manažmentom
- Centralizované riešenie DDoS ochrany a eliminácia útokov z Internetu
- Monitoring a reporting prevádzky do a z Internetu
- Manažment internej sieťovej prevádzky do a z Dátového centra rezortu školstva
- Riešenie má zahrnúť integráciu koncových bodov, pripojených konektivitou od tretích strán (napr. SANET alebo ekvivalentných operátorov, príp. iných operátorov zazmluvnených školami)

1.1. Aktuálny stav EDU.SK

Lokality verejného obstarávateľa, základné a stredné školy, sú v súčasnosti pripojené do MPLS VPN siete poskytovanej a spravovanej spoločnosťou Slovak Telekom, a.s. Takto vybudovaná infraštruktúra poskytuje jednotlivým školám:

- VPN sieť na úrovni MPLS, komunikáciu medzi školami typu any-to-any
- centralizovaný prístup na Internet s monitoringom prevádzky
- možnosť bezdrôtového prístupu do siete na škole, pričom bezdrôtový prístup je centrálnie riadený
- Centralizované antivírusové a antispamové riešenie pre elektronickú poštu
- ochranu LAN siete na škole pomocou lokálneho firewallu.

V súčasnosti existuje 6 typov pripojenia škôl do MPLS VPN:

Typ školy	Počet škôl	Rýchlosť pripojenia
A	628	Min. 12/0,512 Mb/s
B	1485	Min. 3/0,256 Mb/s

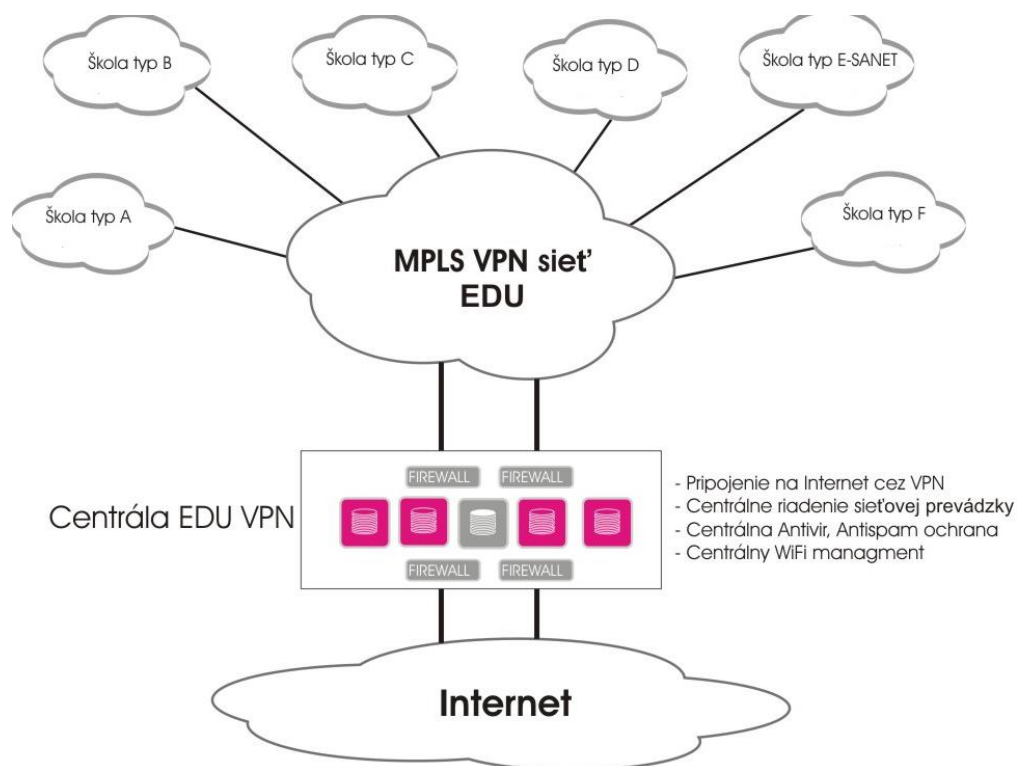
C	218	Min. 2,5/0,256 Mb/s
D	206	Min. 128/128 kb/s
E- SANET	54	100 Mb/s
F	455	Min. 2,5/0,256 Mb/s
Spolu škôl	3046	

Tabuľka 1 Aktuálne typy pripojenia do MPLS VPN (stav k 31. 12. 2014)

Všetky školy pripojené do MPLS VPN siete majú prístup do Internetu cez Centrálnu lokalitu. Tento prístup je chránený prostredníctvom firewall modulov v kostrových prepínačoch tvoriacich lokálnu komunikačnú infraštruktúru centrálnej lokality. Zároveň sú na tejto lokalite zabezpečované nasledujúce služby:

- riadenie kontroly WiFi prístupových bodov na školách
- centrálné riadenie sieťovej prevádzky
- centrálna antivírusová a antispamová ochrana
- koncentrácia IPSec tunelov na školy pripojené cez SANET

V súčasnosti implementované riešenie je znázornené na nasledujúcom obrázku:



Obrázok 1 Súčasné riešenie RIRŠ

Súčasný stav pripojenia škôl do MPLS VPN a tým aj šírka prenosového pásma k prístupu do Internetu je závislá od technológií "poslednej míle" využívaných na prístup do MPLS VPN siete.

Z hľadiska dlhodobej vízie informatizácie a digitalizácie školstva a požiadaviek na využívanie nových aplikácií pri vyučovacom procese je tento stav nevyhovujúci. Tento stav zodpovedá dostupným technológiám v čase spustenia projektu Rozvoj informatizácie regionálneho školstva - RIRŠ (Infovek II).

Podobne je to aj HW vybavením na jednotlivých školách (CPE smerovače, LAN prepínače, WiFi prístupové body), ktoré sú už morálne zastarané a výkonovo poddimenzované.

1.2. Cieľový stav EDUNET_SK

1.2.1. Popis koncepcie komunikačnej infraštruktúry EDUNET_SK

Riešenie novej komunikačnej infraštruktúry EDUNET_SK sa zameriava na pokrytie nasledujúcich kľúčových oblastí:

- rýchlosti a výkonnosti poskytovania internetových služieb pre školy
- dostupnosti a kvality konektivity do siete EDUNET_SK s garantovanou SLA (Service Level Agreement)
- bezpečnosti komunikácie v sieťovom prostredí škôl, manažment LAN a WiFi komponentov, Content Filtering, Web Filtering
- službami súvisiacimi s Internetom a Intranetom
- podporou kvality služby v sieti EDUNET_SK (QoS) pre poskytovaný content v Internete/Intranete.

S ohľadom na uvedené oblasti koncepcia novej architektúry siete EDUNET_SK kladie dôraz na:

- modularitu riešenia,
- škálovateľnosť riešenia,
- vysokú dostupnosť riešenia,
- bezpečnosť riešenia.

Základným funkčným stavebným prvkom je virtuálna privátna MPLS VPN sieť, umožňujúca:

- bezpečnú komunikáciu každý s každým pre všetky koncové body pripojené do MPLS VPN,
- bezpečnú komunikáciu do Dátového centra rezortu školstva k privátnym zdrojom (napr. online testovanie žiakov, elektronický obsah, atď.),
- podporu QoS pre aplikácie a zdroje poskytované napríklad z Dátového centra rezortu školstva,

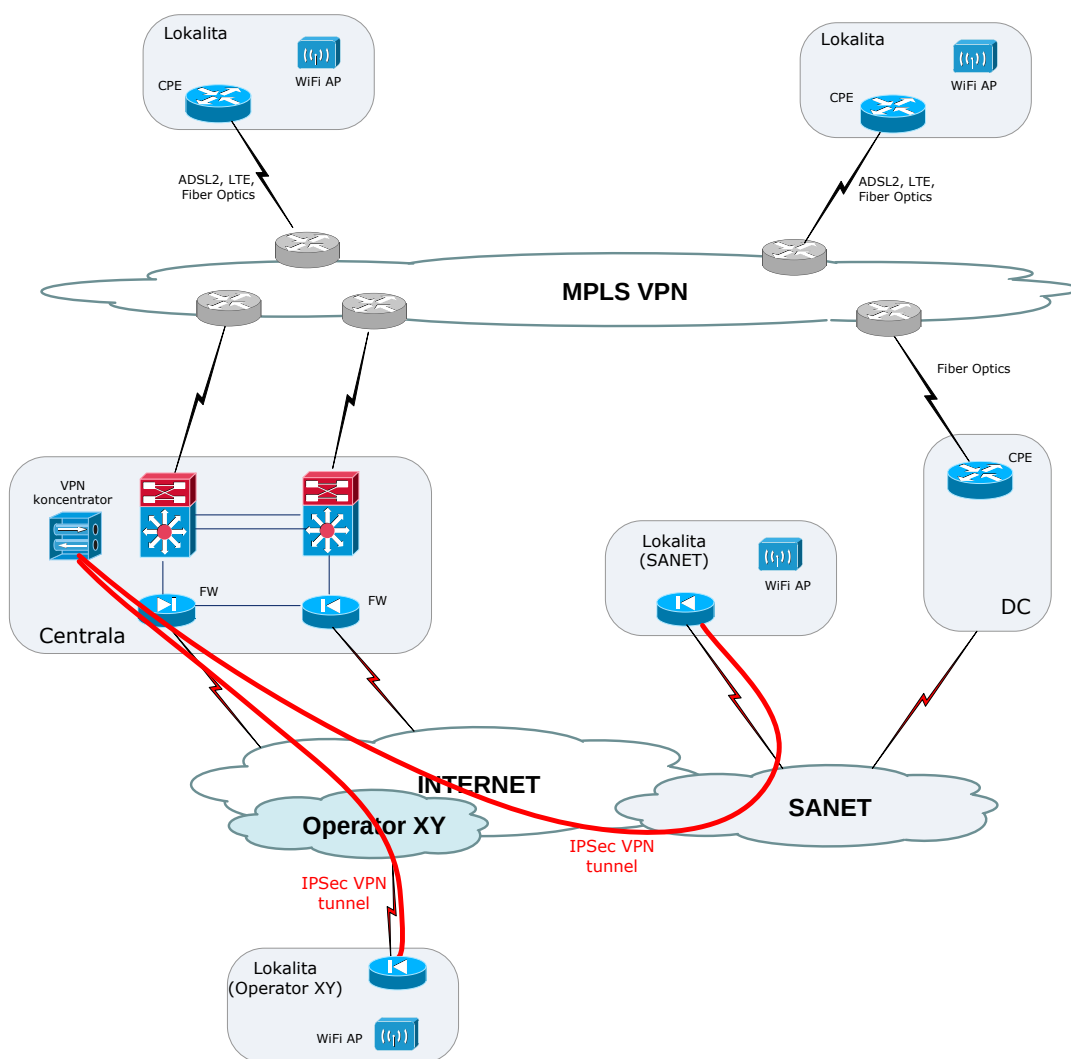
- centralizovaný prístup do Internetu.

Verejný obstarávateľ požaduje, aby MPLS VPN sieť EDUNET_SK prepájala tri kategórie koncových bodov:

- Dátové centrum rezortu školstva,
- Centrálu EDUNET_SK, zabezpečujúca a poskytujúca servisné bloky riešenia,
- školy (primárne základné a stredné, s možnosťou pripojenia materských škôl a vybraných školských zariadení).

Okrem týchto koncových bodov je dôležitá integrácia riešenia s koncovými bodmi, ktoré sú pripojené cez iného operátora (lokality priamo pripojené cez SANET, alebo školu v rámci Národného projektu Digitálne učivo na dosah).

Koncepcia architektúry EDUNET_SK je znázornená na nasledujúcom obrázku:



Obrázok 2 Koncepcia architektúry riešenia EDUNET_SK

MPLS VPN sieť bude tak stabilná ako stabilná bude MPLS sieť uchádzača. To závisí na viacerých faktoroch, ako sú napríklad:

- kapacita chrbticových a prístupových trás,
- dizajn MPLS siete (fyzický dizajn, logický dizajn, použitý HW),
- zabezpečenie siete MPLS siete.

Práve zabezpečenie MPLS siete uchádzača je veľmi dôležité. Hoci v riešení EDUNET_SK bude zabezpečenie riešené prostredníctvom "bezpečnostného modulu" v Centrále EDUNET_SK, môže dôjsť k DDoS útoku na sieť uchádzača a tým aj k výpadku služieb pre MPLS VPN sieť EDUNET_SK. Preto je dôležité, aby mal uchádzač MPLS VPN siete zabezpečenú sieť proti DDoS útokom. Ide o ochranu siete od útokov typu ako sú napríklad:

- HTTP Malformed
- DNS Malformed
- IPv4 Address Filter Lists
- IPv4 Black/White Lists
- DNS Rate Limiting
- Zombie Detection
- TCP Connection Reset (incl. L7 Slow Attack)

Ďalším dôležitým faktorom je flexibilita uchádzača implementovať do riešenia nové črty alebo úpravy riešenia na základe požiadaviek verejného obstarávateľa, ktoré môžu byť jednorazové (napr. pri testovaní žiakov). Môže ísť o plošnú implementáciu alebo úpravu QoS, kedy bude na základe požiadavky verejného obstarávateľa plošne v sieti prioritizovaná niektorá aplikácia na úkor napríklad prístupu do Internetu.

1.2.2. Centrála EDUNET_SK

Centrála EDUNET_SK predstavuje kľúčový prvok riešenia jednotnej komunikačnej infraštruktúry. Vzhľadom na vysokú dostupnosť, škálovateľnosť a flexibilitu poskytovaných služieb verejný obstarávateľ požaduje, aby Centrála EDUNET_SK bola umiestnená v dátovom centre uchádzača/ poskytovateľa MPLS VPN siete.

Vysoká dostupnosť komunikačnej infraštruktúry Centrál EDUNET_SK je funkciou:

- použitého hardvéru
- návrhu fyzickej a logickej topológie komunikačnej infraštruktúry (KI) LAN
- redundantného pripojenia k dvom PE smerovačom

Pre použitý HW pre Centrálu EDUNET_SK sa vyžadujú nasledovné vlastnosti:

- redundantné modulárne kostrové prepínače, osadené redundantnými napájacími zdrojmi pre prípad výpadku niektorej z napájacích vetiev dátovej rozvodne, v ktorej je umiestnený komponent KI
- kritické komponenty (kostrové prepínače) budú osadené redundantnými procesorovými jednotkami, eliminujúce výpadok komponentu KI pri zlyhaní primárneho riadiaceho procesora
- navrhnutý modulárny softvér riadiacich procesorových jednotiek umožňuje in-service upgrade, bez výpadku služieb, ako aj selektívne zaplätanie niektorého z bežiacich procesov v prípade vydania softvérovej záplaty
- Všetky komponenty (dátové moduly), ventilátory a duálne napájacie moduly podporujú hot swapping, čiže je ich možné pridávať, vymieňať a vyberať bez potreby prerušenia systémového napájania alebo potreby odstavenia funkčnosti softvéru alebo rozhraní
- ostatné kritické komponenty (Firewall) musia byť navrhnuté redundantne

Fyzická koncepcia komunikačnej infraštruktúry Centrály EDUNET_SK:

- jednotlivé 10GE spojnice medzi chrbticovými komponentmi KI budú ukončené na rozdielnych moduloch,
- každý komponent KI bude mať fyzicky nezávislú redundantnú trasu k chrbtici siete, každá bude ukončená na fyzicky odlišnom hardvéri.

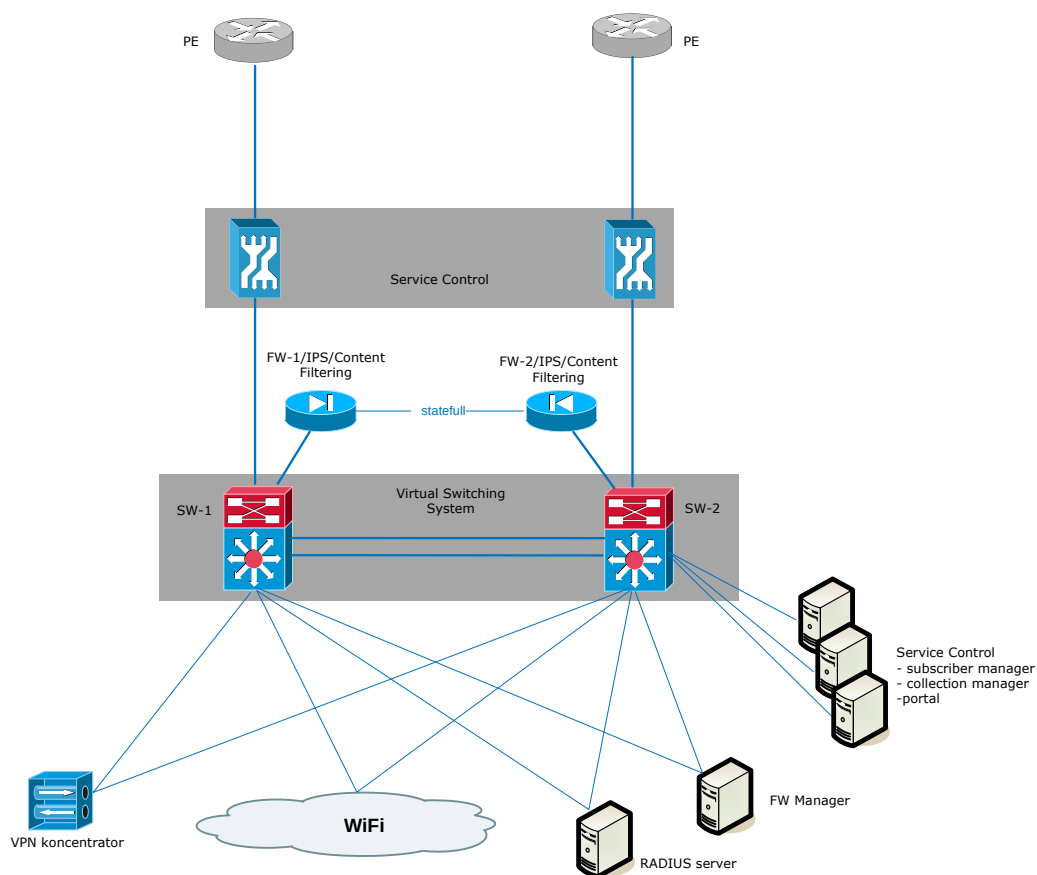
Logická koncepcia komunikačnej infraštruktúry kladie dôraz na rýchlu konvergenciu a stabilitu KI na L2 a L3:

- využitím virtuálneho prepínacieho systému sa eliminuje komplexnosť spanning tree protokolu v infraštruktúre, čím sa zvýši stabilita KI. Rapid STP protokol je len backup pre prípad chybného konfigurovania niektorého komponentu KI (v prípade ak by došlo k systémovej chybe na virtuálnom prepínači systému, aby nedošlo k vzniku L2 slučiek);
- využitím vlastnosti ukončenia etherchannelu z jedného prepínača (prístupového alebo serverovej farmy) na dvoch chrbticových prepínačoch sa dosiahne, že obidva uplinky (ich počet závisí od liniek v channely) budú vždy aktívne a využívané na prenos dát. Žiadna linka nebude blokována STP protokolom a tým nevyužívaná;
- optimalizáciou interného smerovacieho OSPF protokolu dosiahnuť rýchlu konvergenciu.

Škálovateľnosť LAN KI, podobne ako dostupnosť, je závislá od voľby hardvéru a návrhu LAN KI. Navrhnutý hardvér komponentov umožňuje ich vynikajúcu škálovateľnosť, vďaka:

- modularite hardvéru (schopnosť rozšíriť systém o nové moduly so širokou možnosťou výberu vhodných rozhraní);

- priepustnosti a prepínacieho výkonu systému (celkový prepínací výkon systému, ako aj priepustnosť systému na slot);
- funkcionalite hardvéru (počet MAC adries na systém, VLAN, SVI, L2 funkcionalita, L3 funkcionalita, ACL aplikovaná v hardvéri, napájanie pre koncové systémy,...);
- funkcionalite systémového softvéru (bezpečnosť,...).



Obrázok 3 Konceptia fyzickej topológie Centrálky EDUNET_SK

Na rozhraní prestupu zo siete EDUNET_SK do Internetu bude nasadený systém riadenia prevádzky, ktorý bude monitorovať komunikáciu klientov na školách do Internetu. Súčasťou systému musia byť systémy, pomocou ktorých budú štatistiky dátovej komunikácie prezentované zodpovedným pracovníkom.

Verejný obstarávateľ požaduje, aby smerovanie dátovej komunikácie medzi sieťou EDUNET_SK a Internetom prechádzalo centrálnymi firewallmi.

1.2.3. Zabezpečenie EDUNET_SK

Centrálny Firewall systém je jedným z kľúčových komponentov celého riešenia. Vzhľadom na požiadavku primárneho prepojenia 10Gbps s možnosťou rozširovania

podľa zvyšujúcich sa nárokov je veľmi dôležitá výkonnosť a priepustnosť firewall systému.

Základné požadované vlastnosti centrálného firewall systému v riešení:

- redundantný HW umožňujúci konfiguráciu active/standby, active/active,
- pripojenie do Internetu 10Gbps s rozšírením do 40Gbps,
- centrálny IPv4 NAT pre EDUNET_SK,
- integrované IPS (Intrusion Prevention System),
- integrovaný web/content filtering.

Vzhľadom na požadovanú funkcionálnosť a priepustnosť pri využívaní všetkých požadovaných funkcií verejný obstarávateľ požaduje použiť dostatočne robustný hardvér, aby počas prevádzky práve centrálny firewall nebol úzkym hrdlom celého riešenia, ktorý disponuje 40GE aj 10GE portami.

Verejný obstarávateľ požaduje možnosť vytvárania filtrov pre obsah z Internetu na základe požiadaviek verejného obstarávateľa.

Verejný obstarávateľ požaduje, aby v systéme bola možnosť nastavenia filtrovania obsahu a blokovanie nevhodného obsahu. Možnosť filtrovať a blokovať nevhodný obsah sa požaduje podľa:

- času (vyučovací čas, ostatný čas),
- podľa WiFi SSID/LAN,
- podľa skupín užívateľov (vek, žiak, učiteľ).

1.2.4. WiFi riešenie

Poskytovanie WiFi pripojenia pre koncové zariadenia na školách pre riešenie EDUNET_SK požaduje verejný obstarávateľ riešiť centrálnym prostredníctvom Centrálneho EDUNET_SK. Na rozdiel od riešenia prevádzkovaného v projekte RIRŠ, verejný obstarávateľ požaduje riešenie spĺňajúce nasledovné vlastnosti:

- plne riadené a manažované Cloudom, kde Cloudový riadiaci systém je out-of-band, t.j. užívateľská dátová prevádzka nie je smerovaná ani procesovaná cloudom;
- out-of-band komunikácia medzi Cloudom a bezdrôtovým bodom je kryptovaná v SSL tunely, minimálne na úrovni protokolu AES 256 a táto komunikácia slúži na konfiguráciu, prenos sieťových štatistík a update firmwaru bezdrôtových prístupových bodov;
- vysoká dostupnosť Cloudu, ale v prípade jeho nedostupnosti
 - Užívatelia ostávajú autentifikovaní
 - Dátová komunikácia prebieha bez prerušenia
 - Užívatelia môžu roamovať medzi bezdrôtovými AP
 - L7 traffic shaping pravidlá ostávajú v platnosti a sú naďalej aplikované

- RF vlastnosti bezdrôtovej siete (napr. DFS) sú bez prerušenia
- Wireless mesh routing pracuje bez prerušenia;
- Implementácia nových črt a vlastností si nevyžaduje upgrade na strane klienta ale na strane Cloudu;
- Centrálne správa firmwaru bezdrôtových AP prostredníctvom Cloudu;
- Podpora mesh WiFi infraštruktúry;
- Adaptácia na problémy súvisiace s RF pokrytím, ako je napríklad pokrytie oblastí rádiových dier;
- Bezpečnosť riešenia (autentikácia užívateľov, enkrypcia, blokovanie aplikácií na SSID báze, podpora traffic shapingu, detekcia a remedácia rogue AP a pod.);
- Podpora mobility;
- Podpora lokalizačných služieb;
- Monitoring a štatistiky (logovanie a ukladanie eventov vyhľadávanie v logoch, monitoring pripojených sieťových zariadení, štatistiky o správaní sa jednotlivých užívateľov, štatistiky podľa jednotlivých aplikácií).

Konfigurácia spôsobu autentifikácie sa požaduje na per-SSID báze. T.j. súčasne môžu byť pre rôzne SSID využívané rôzne spôsoby autentifikácie užívateľov.

Overovanie užívateľov EDUNET_SK v rámci riešenia bude realizované prostredníctvom RADIUS servera umiestneného v Centrále EDUNET_SK. Ten bude využívať databázu externého LDAP (AD) servera umiestneného v Dátovom centre rezortu školstva (bude slúžiť aj na iné aplikácie, kde sú žiaci autentifikovaní) z projektu RIAM (systém prevádzkovaný verejným obstarávateľom na správu používateľských účtov).

1.3. Traffic shaping - regulácia šírky prenosového pásma na lokalite

Na reguláciu šírky prenosového pásma pre menej dôležité aplikácie nesúvisiace s procesom výučby v školách bude aplikovaná regulácia šírky pásma – traffic shaping.

Traffic shaping bude v rámci riešenia aplikovaný dvoma spôsobmi:

- **na centrálnych FW v Centrále EDUNET_SK** budú implementované traffic profily, ktoré budú priradené jednotlivým školám. Tieto profily bude možné priradovať aj na základe časového princípu s granulárnou škálovateľnosťou nastavenia parametrov ako napr. šírka pásma pre zadané aplikácie (na základe web filtrov, ACL, ...).
- **Prostredníctvom správy Cloudu bezdrôtovej časti EDUNET_SK**, kde bude možné regulovať šírku prenosového pásma až na úroveň SSID, alebo na úroveň jednotlivého klienta, šírku prenosového pásma granulórne nastaviť pre download a upload zvlášť.

1.4. Dátové centrum rezortu školstva (DCRŠ)

V Dátovom centre rezortu školstva sú lokalizované centrálné servery služieb. Dátové centrum rezortu školstva bude pripojené do MPLS VPN minimálne prístupom 1 Gbps s možným rozšírením na 10 Gbps.

Prístup z DCRŠ do Internetu je aktuálne realizovaný vlastnými prostriedkami Dátového centra rezortu školstva – SANET s kapacitou 10Gbps (mimo EDUNET_SK).

1.5. Pripojenie koncových lokalít do EDUNET_SK

Penetrácia technológií poslednej míle na území Slovenska, určujúcich kapacitu pripojenia do MPLS VPN siete, je rozdielna. Práve toto predstavuje limitujúci faktor na šírku prenosového pásma pre jednotlivú lokalitu a tým aj rýchlosti k prístupu na Internet a Intranet.

Vzhľadom na počet užívateľov na jednotlivých lokalitách (školách) sú školy rozdelené do kategórií uvedených v nasledujúcej tabuľke:

Typ lokality	Počet škôl (lokalít)	Počet užívateľov v škole	Druh lokality	Šírka prenosového pásma (minimálna)
A	113	viac ako 600 žiakov	ZŠ, SŠ, špec. škola	200 Mbps
B	258	401-600 žiakov	ZŠ, SŠ, špec. škola	100 Mbps
C	415	251-400 žiakov	ZŠ, SŠ, špec. škola	50 Mbps
D	1238	51-250 žiakov	ZŠ, SŠ, špec. škola	20 Mbps
E	815	do 50 žiakov	ZŠ, SŠ, špec. škola	10 Mbps
F	3909		Materská škola, školské zariadenie	10 Mbps
X	546	Lokalita cez SANET, DUD, iný operátor	ZŠ, SŠ, špec. škola	100 Mbps

Tabuľka 2 Typové rozdelenie lokalít a požadovaný spôsob pripojenia

Preferovaný spôsob pripojenia lokality do MPLS VPN EDUNET_SK je prostredníctvom optických technológií (dark fiber, GPON, ...). Avšak technologická vyspelosť fyzickej infraštruktúry na území Slovenska je rôznorodá, je možné využiť aj iné technológie na prístup do MPLS VPN siete. Ide o technológie typu ADSL2, VDSL2, SHDSL, LTE, bezdrôtový prepoj bod-bod.

V prípade miest sú však dostupné aj technológie umožňujúce prístup cez optické vlákno (GPON, dark fiber). Preto ak je v danej lokalite takáto možnosť, tak verejný obstarávateľ požaduje primárne využiť takúto technológiu na prístup do MPLS VPN siete pre lokality A, B, C.

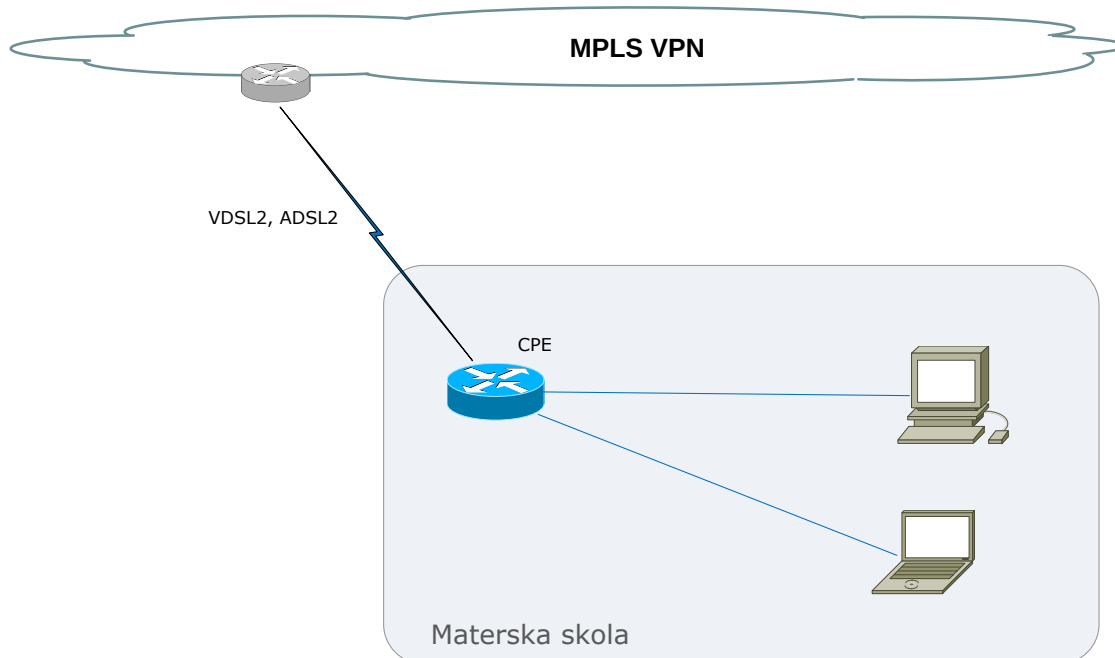
Verejný obstarávateľ požaduje 20% škôl (z typu lokality A, B a C) pripojiť do MPLS VPN prostredníctvom optických technológií.

1.5.1. Pripojenie materských škôl/ školských zariadení

Pripojenie materskej školy/ školského zariadenia do EDUNET_SK MPLS VPN bude prostredníctvom CPE smerovača zabezpečujúceho:

- smerovanie dátovej prevádzky,
- základnú sieťovú bezpečnosť v rámci lokality,
- QoS pre Internet a Intranet aplikácie,
- DHCP server pre lokálnych užívateľov.

Vzhľadom na charakter materskej školy/ školského zariadenia sa v súčasnosti nepredpokladá ich pokrytie WiFi signálom. Klientské PC budú priamo pripojené na CPE zariadenie tak, ako je to znázornené na nasledujúcom obrázku:



Obrázok 4 Pripojenie materskej školy/ školského zariadenia do EDUNET_SK

1.5.2. Pripojenie lokalít do EDUNET_SK

Pripojenie každej lokality do EDUNET_SK MPLS VPN bude prostredníctvom CPE smerovača, ktorého typ bude závislý od prístupovej technológie. CPE smerovač okrem toho zabezpečí:

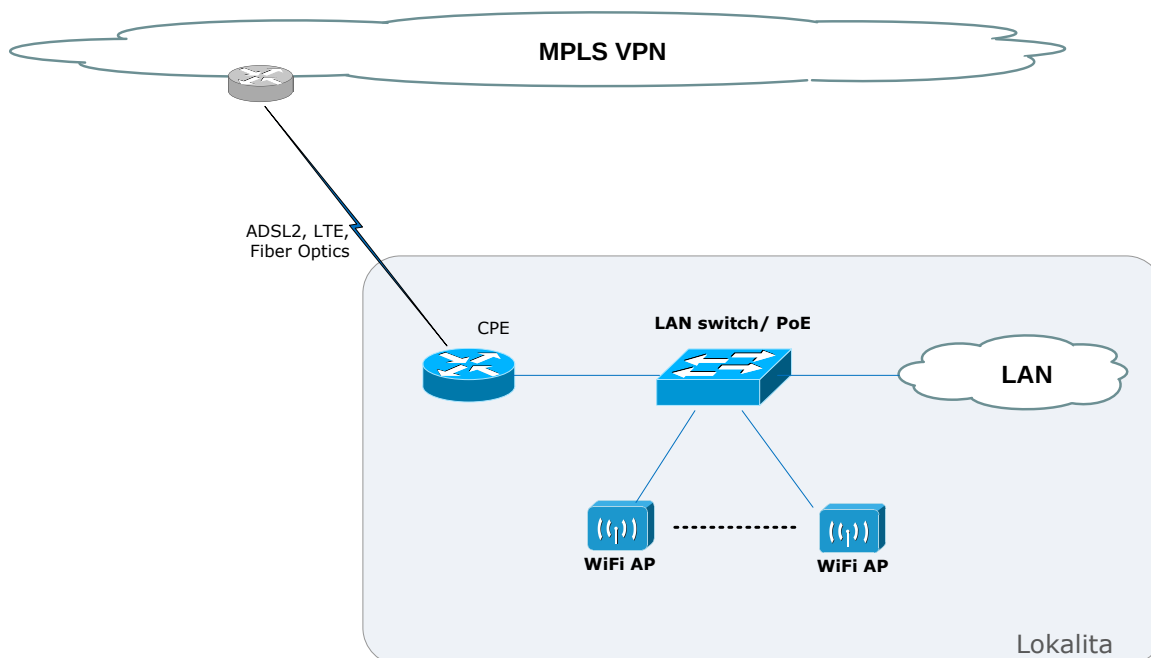
- smerovanie dátovej prevádzky,
- základnú sieťovú bezpečnosť v rámci lokality (ACL medzi VLAN sieťami),
- QoS pre Internet a Intranet aplikácie,
- DHCP server pre lokálnych užívateľov.

Na každej lokalite bude umiestnený LAN prepínač (počet portov bude závislý od typu lokality) zabezpečujúci:

- napájanie pre WiFi prístupové body,
- prepojenie na už vybudované LAN na školách,
- pripojenie systémov zabezpečujúcich fyzickú bezpečnosť (napr. IP kamerové systémy).

Správa LAN prepínača a WiFi bude spoločná prostredníctvom cloudového riešenia. Počet WiFi prístupových bodov požaduje verejný obstarávateľ riešiť samostatne pre jednotlivé lokality, pričom pred implementáciou bude dôležitá obhliadka miesta, ktorá určí požadovaný počet AP tak, aby pokrytie bezdrôtovou LAN bolo na dostatočnej úrovni.

Riešenie topológie fyzického pripojenia lokality bez rozdielu technológie poslednej míle je na nasledujúcom obrázku:



Obrázok 5 Pripojenie lokality školy do EDUNET_SK

1.5.3. Integrácia lokalít pripojených cez SANET/ cez NP DUD/ iného operátora do EDUNET_SK

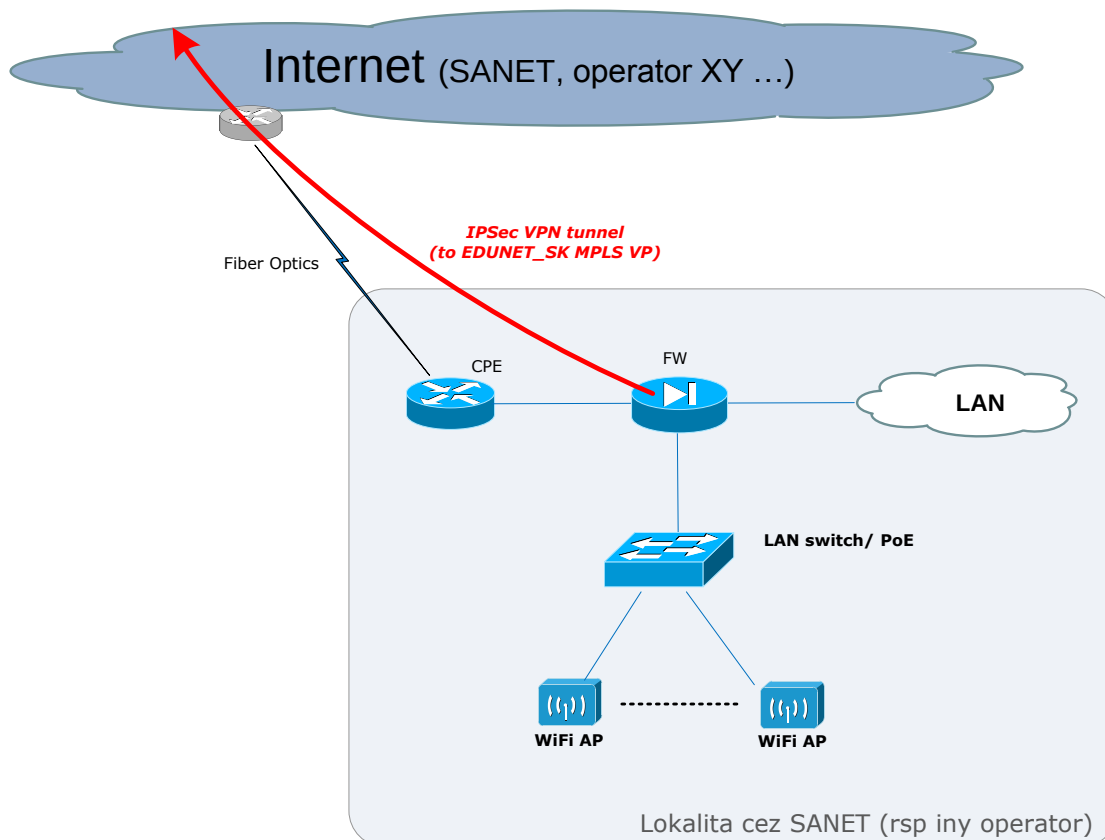
V súčasnosti je určitý počet lokalít (cca 300) pripojených do Internetu prostredníctvom SANETu resp. môžu byť v budúcnosti pripojené aj prostredníctvom iného Poskytovateľa, alebo v rámci Národného projektu Digitálne učivo na dosah (cca 220 škôl).

Ich integráciu do EDUNET_SK zabezpečuje lokálny firewall, z ktorého je vytvorený IPSec tunel do Centrály EDUNET_SK, kde je tento tunel ukončený na koncentrátore VPN.

V súčasnosti dátová komunikácia do Internetu nie je realizovaná cez žiadnu centrálnu lokalitu, teda nie je monitorovaná. V prípade zmeny a presmerovania celej komunikácie cez Centrálu EDUNET_SK treba brať do úvahy:

- lokálny FW umiestní na škole a zabezpečujúci kryptovanie celej dátovej komunikácie bude musieť byť z výkonových dôvodov vymenený.
- smerovanie celej dátovej komunikácie zvýši nároky na pripojenie Centrálne EDUNET_SK do Internetu a to obojsmerne.
- bude potrebné zabezpečiť VPN koncentrátor na Centrále EDUNET_SK z výkonových dôvodov (aby mal dostatočný výkon na kryptovanie celej dátovej komunikácie pre cca 500 škôl).
-

Navrhnuté riešenie pripojenia takýchto lokalít je znázornené na nasledujúcom obrázku:



Obrázok 6 Integrácia lokality do EDUNET_SK

1.6. Webhostingové služby pre EDUNET_SK

V súčasnosti si niektoré školy a školské zariadenia prevádzkujú webové stránky, na ktorých zdieľajú aktuálne informácie týkajúce sa života jednotlivých škôl. Vlastníctvo a správa fyzických serverov si však vyžaduje nároky na odborný personál, ktorým väčšina škôl nedisponuje. Taktiež stúpajúce požiadavky na flexibilitu a rýchlosť nasadenia nových aplikácií či funkcionalít sú v ostrom protiklade s potrebou efektívnejšieho využívania zdrojov, respektíve vynaloženými investíciami do IT infraštruktúry.

Z toho dôvodu verejný obstarávateľ plánuje umožniť školám poskytovanie výpočtového priestoru od uchádzača/ poskytovateľa takejto služby a zdefinovať si potrebný priestor podľa aktuálnych požiadaviek, ktoré sa môžu časom veľmi dynamicky meniť.

Verejný obstarávateľ požaduje nasledovné minimálne parametre webhosting služby:

- úložný priestor – najmenej 1 GB
- webový server – Apache 2.2.x alebo IIS 7.5 a vyššie
- podpora dynamických stránok – PHP 5.6/Perl/Python alebo .NET 4.5 a vyššie
- databáza – MySQL/PgSQL/MSSQL
- podpora HTML/JavaScript/Flash
- prístup – FTP/FTP-SSL, HTTP
- vlastný názov domény druhej úrovne
- patchovanie
- štatistiky návštevnosti
- možnosť používania overených SSL certifikátov
- služba migrácie súčasných webových stránok škôl
- spravidla 200MB per škola, počet web stránok cca 2900

1.7. Spoločný dohľad EDUNET_SK, SANET, DUD

Verejný obstarávateľ požaduje spoločný dohľad sietí IKT prostriedkov na lokalitách pripojených cez EDUNET_SK, SANET a DUD. Vzhľadom na IP konektivitu všetkých 3 sietí, SNMP správy z aktívnych sieťových zariadení budú zasielané z lokalít pripojených cez SANET a DUD na dohľadové systémy Poskytovateľa EDUNET_SK.

Poskytovateľ navrhne riešenie monitoringu a požiadavku na komunikačné rozhranie sietí škôl zapojených v Národnom projekte Digitálne učivo na dosah a pripojených prostredníctvom SANET.

2. Požiadavky na jednotlivé komponenty a služby

2.1. Jednorazové služby

Zriadenie prístupu a implementácia CE na koncových lokalitách:

- vypracovanie migračného plánu pre CE zariadenia,
- vypracovanie implementačného plánu pre CE zariadenia,
- príprava podkladov (IP adresy, predpokladané počty pracovných staníc, existujúce špeciálne nastavenia, ktoré treba zachovať, ...) pre každú lokalitu na základe vstupných podkladov od zástupcu lokality a/alebo verejného obstarávateľa,
- príprava konfigurácií pre CE zariadenia na koncových lokalitách,

- fyzická inštalácia a prepojenie CE zariadení na koncových lokalitách,
- preverenie funkčnosti komunikácie z danej lokality v sieti RIRŠ po migrácii na nové riešenie,
- doprava koncových zariadení do jednotlivých lokalít.

Implementácia WiFi na koncových lokalitách:

- vypracovanie implementačného plánu pre WiFi zariadenia,
- fyzická realizácia káblového pripojenia WiFi AP s LAN resp. CE podľa typu lokality,
- doprava koncových zariadení do jednotlivých lokalít,
- vypracovanie časového harmonogramu,
- pravidelná aktualizácia harmonogramu,
- riadenie a koordinácia technických pracovníkov.

Zaškolenie pracovníka Lokality:

- predstavenie telekomunikačných zariadení implementovaných na lokalite a ich funkcia.
- zapojenie inštalovaných telekomunikačných zariadení,
- kontakty na help-desk uchádzača/ poskytovateľa,
- informovanie o službách poskytovaných na centrále EDUNET_SK,
- predstavenie autentifikačného servera pre WiFi a spôsobu autentifikácie užívateľov.

2.2. Pravidelné služby

Prevádzka a údržba:

- dohľad dostupnosti a odstraňovanie porúch konektivity všetkých koncových bodov,
- WiFi monitoring dostupnosti a kvality služieb, riešenie problémov.

Monitoring:

- implementácia koncových zariadení do monitorovacieho managementu,
- sledovanie management nástrojov jednotlivých komponentov riešenia,
- proaktívne riešenie vznikajúcich problémov,
- podmienkou vzdialenej diagnostiky je read-only SNMP prístup na CE (resp. CPE podľa navrhnutej architektúry),

- vzdialená správa LAN-switch zariadení (vykonávanie rekonfigurácií a zmien na základe jednoduchých požiadaviek škôl, ktoré nemajú vplyv na funkčnosť a architektúru riešenia) bez limitu počtu požiadaviek,
- vzdialená správa LAN-switch zariadení (vykonávanie rekonfigurácií a zmien na základe požiadaviek objednávateľa v zmysle budúcich potrieb (napr. pre lokality/školy zapojené v Národných projektoch Digitálne učivo na dosah, Elektronizácia vzdelávacieho systému regionálneho školstva, Zvyšovanie kvality vzdelávania na základných a stredných školách SR s využitím elektronického testovania),
- konfiguračný management pre tieto zariadenia,
- o vzniknutých problémoch súvisiacich s poskytovaním služieb týkajúcich sa verejného obstarávateľa, resp. lokalít bude uchádzač informovať verejného obstarávateľa minimálne raz mesačne formou reportov a adhoc formou štruktúrovaných emailov.

Monitoring služby:

- sledovanie sieťovej prevádzky,
- generovanie reportov v týždňových intervaloch,
- generovanie reportov na požiadanie,
- zmena konfigurácie na požiadanie,
- úprava a vývoj autentifikačného prostredia pre užívateľov,
- servisné práce na zariadeniach,
- aktualizácia softvérového vybavenia.

2.3. Centrálné riadenie sieťovej prevádzky

<i>Požadovaný parameter</i>
Monitorovanie sieťovej komunikačnej infraštruktúry
Riadenie sieťovej prevádzky
Minimálna priepustnosť 10Gbps
Zariadenie sa musí správať transparentne (nie detekovateľne)
Minimálny počet otvorení spojení 10 mil/s
Minimálny počet aktívnych jednosmerných spojení 25.000.000
Spĺňať požiadavky na vysokú dostupnosť
Monitorovanie musí siahať až na aplikačnú vrstvu OSI modelu, s možnosťou definovania parametrov aplikačnej vrstvy pre monitorovanie vybraných protokolov

Dokáže klasifikovať služby/aplikácie, ktoré sú na sieti používané a to aj v prípade, že sú používané neštandardne (napr. ak služba http, ktorá štandardne využíva sieťový port 80 bude používať iný port).
Funkcia monitorovania prevádzky až na úroveň užívateľa samostatne
Monitorovanie až na úroveň rozpoznanej aplikácie na základe nakonfigurovaných aplikačných parametrov
Extenzívne reportovacie vlastnosti
Možnosť prispôbiť existujúce reporty a možnosť zadať vlastné reporty
Namerané údaje musia byť dostupné aj pomocou webovej aplikácie v grafovej a tabuľkovej podobe s možnosťou jednoduchšej manipulácie
Možnosť integrácie s aplikáciami tretích strán pre spracovanie nameraných údajov
Možnosť riadenia sieťovej prevádzky pre každého užívateľa samostatne
Možnosť riadenia sieťovej prevádzky pre každú rozpoznajú aplikáciu samostatne
Riešenie musí byť spravovateľné na diaľku
Centrálny Firewall na prestupe do Internetu
Dedikované fyzické zariadenie pre projekt EDUNET_SK
Stavový firewall
Možnosť konfigurácie active/active, active/standby, clustering
Minimálna priepustnosť firewallu: • 1518-byte packet size: 120 Gbps • 512-byte packet size: 120 Gbps • 64-byte packet size: 80 Gbps
Minimálny počet kontrolovaných spojení súčasne 150 Mpps
Minimálny počet nadviazaní/zrušení spojenia 300.000
Podpora NAT, PAT, NAT Traversal
Minimálna priepustnosť pri zapnutom IPS 15Gbps
Voliteľné rozhrania typu gigabitethernet, 10Gigabitethernet, 40Gigabitethernet
Garancia filtrácie webového obsahu podľa pravidiel obstarávateľa
Vytváranie skupín na filtráciu webového obsahu podľa skupín užívateľov a času

2.4. LAN prepínač

Požadovaný parameter
Prepínač 1: 8x 10/100/1000 Base T 2x SFP Gigabit Ethernet uplink
Prepínač 2: 24x 10/100/1000 Base T 4x SFP Gigabit Ethernet uplink
Prepínač 3: 48x 10/100/1000 Base T 4x SFP Gigabit Ethernet uplink
Prepínač 1: minimálne 20 Gbps no-blocking fabric
Prepínač 2: minimálne 48 Gbps no-blocking fabric
Prepínač 3: minimálne 96 Gbps no-blocking fabric
Broadcast storm control
Podpora IGMP snooping
Počet VLAN ID: 4096
Veľkosť MAC tabuľky: minimálne 8000
802.1p
802.1Q
802.1D
802.1w
802.1ab
802.1ad
802.3 af (PoE)
802.3at (PoE+)
Podpora PoE na všetkých portoch súčasne
Podpora 802.1x
Podpora DHCP snooping

• Integrovaná two-factor autentifikácia
• Role-based administrácia
• Manažovateľné prostredníctvom spoločného Cloudového riešenia ako bezdrôtová časť navrhnutého riešenia
• integrovaný monitoring aplikácií na L7 s previazanosťou na klienta
• Detailné historické štatistiky per-port
• Detailné historické štatistiky per-klient
• DHCP a hostname fingerprinting
• SNMP v2c
• Vzdialená analýza rámcov na portoch
• Logovanie eventov, vyhľadávanie v logoch
Zariadenie musí byť vybavené sadou na montáž do štandardných 19" stojanov
Výška zariadenia v "rack units"
Uveďte výrobcu a presný typ zariadenia (zariadení), ktorých sa týkali Vaše odpovede v tabuľke.

2.5. Bezdrôtová LAN infraštruktúra s centrálnym manažmentom

<i>Požadovaný parameter</i>
Centrálny riadiaci systém pre WiFi
Cloudový riadiaci systém je out-of-band, t.j. užívateľská dátová prevádzka nie je smerovaná ani procesovaná cloudom
out-of-band komunikácia medzi Cloudom a bezdrôtovým bodom je kryptovaná v SSL tunely, minimálne na úrovni protokolu AES 256
out-of-band komunikácia slúži na konfiguráciu, prenos sieťových štatistík a update firmwaru bezdrôtových prístupových bodov
Konfigurácia ako aj real-time štatistiky sú uložené na bezdrôtovom prístupovom bode
Požadovaný počet podporovaných WiFi prístupových bodov v riešení 20.000
Požadované navýšenie počtu WiFi prístupových bodov v balíkoch po 5.000
Dostupnosť Cloudu na úrovni 99,99%
V prípade nedostupnosti Cloudu:

• Užívatelia ostávajú autentifikovaní
• Dátová komunikácia prebieha bez prerušenia
• Užívatelia môžu roamovať medzi bezdrôtovými AP
• L7 traffic shaping pravidiel ostávajú v platnosti a sú naďalej aplikované
• Firewall politiky ostávajú v platnosti a sú naďalej aplikované
• RF vlastnosti bezdrôtovej siete (napr. DFS) sú bez prerušenia
• Wireless mesh routing pracuje bez prerušenia
Implementácia nových črt a vlastností si nevyžaduje upgrade na strane klienta ale na strane Cloudu
Centrálna správa firmwaru bezdrôtových AP prostredníctvom Cloudu
Podpora mesh WiFi infraštruktúry
Všetka prevádzka medzi mesh AP je kryptovaná na úrovni minimálne AES 256
Nie je potreba žiadneho prídavného HW alebo SW na monitoring a manažment WiFi
Integrácia CAD názkresov podlaží lokalít s podporou formátov ako sú JPEG, GIF, PDF, PNG
Adaptácia na problémy súvisiace s RF pokrytím:
• Automatické vykrytie oblastí rádiových dier
• Zabudovaný spektrálny analyzátor na automatickú analýzu možných interferencií
• Zabudované site-survey nástroje slúžiace administrátorovi na real-time spektrálnu analýzu, analýzu úrovne WiFi signálu, speed testy
Bezpečnosť a traffic manažment:
• Požadované metódy autentifikácie a enkrypcie: ○ WEP ○ WPA2-PSK ○ MAC-based access control ○ WPA2-Enterprise s 802.1x autentifikáciou
• 802.1x autentifikácia s RADIUS integráciou
• Blokovanie aplikácií ako sú napríklad bitTorrenty, sociálne médiá a podobne na SSID báze
• Vytváranie whitelistov a blacklistov pre individuálnych užívateľov na SSID báze

• Limitácia šírky pásma (Traffic shaping) pre aplikácie s nízkou prioritou na SSID báze
• Podpora QoS pre kritické aplikácie
• Zabudovaná podpora pre wireless intrusion detection a prevention služby
• Systém podporuje detekciu a remediáciu proti rogue AP
• Systém podporuje detekciu a remediáciu proti DoS útokom
• Integrovaná podpora pre riadenie prístupu užívateľov do siete na základe nainštalovaných aplikácií (antivírus)
• Vytváranie skupinových bezpečnostných politík na základe užívateľa a typu zariadenia
• Zabudovaný device manažment umožňujúci školám centrálnie manažovať a kontrolovať aplikácie na školou vlastnených zariadeniach
• Integrácia s 3rd party infraštruktúrou na autentifikáciu užívateľov (AD/LDAP integrácia)
Podpora mobility:
• Požaduje sa podpora pre L2 roaming
• Požaduje sa podpora pre L3 roaming
Lokalizačné služby:
• Schopnosť trackingu zariadenia/užívateľov v jednotlivých lokalitách
• Integrácia s 3rd party tracking systémami
Monitoring a štatistiky:
• Logovanie a ukladanie eventov automaticky
• Automatické uchovávanie štatistík
• Vyhľadávanie v logoch na základe časových značiek
• Monitoring pripojených sieťových zariadení
• Štatistiky o správaní sa jednotlivých užívateľov, štatistiky podľa jednotlivých aplikácií
Cloudové riešenie musí garantovať, že riadiaca prevádzka z LAN prepínačov a WiFi prístupových bodov, užívateľské štatistiky a lokalizačné dáta nikdy neopustia územie Európskej únie
Cloudové riešenie musí garantovať možnosť „shapeingu“ dátovej prevádzky podľa SSID, skupiny užívateľov a podľa typu a obsahu dátovej prevádzky
WiFi prístupový bod
Súčasne podporované frekvenčné pásma:

• 2.412-2.484 GHz • 5.150-5.250 GHz (UNII-1) • 5.250-5.350, 5.470-5.600 GHz, 5.650-5.725 GHz (UNII-2)
Podporované WiFi štandardy
• IEEE 802.11a/b/g/n
Požaduje sa podpora 2 streamov pre 802.11n
Požaduje sa podpora pre dual-band WIPS a spektrálnu analýzu
Požaduje sa podpora Beamforming
Požaduje sa podpora pre mesh WiFi infraštruktúru
Podpora Cyclic shift diversity (CSD)
LAN uplink port
• 1x 100/1000 BaseT rozhranie
Napájanie cez Ethernet injector alebo externý napájací adaptér
Diaľkové elektrické napájanie podľa IEEE 802.3af alebo 802.3at
Integrované omni-directional antény
VLAN tagging (802.1Q)
Podpora WEP, WPA, WPA2-PSK, a WPA2-Enterprise s 802.1X
Podpora TKIP a AES kryptovania s HW akceleráciou
Guest Isolation
Podpora Wireless Quality of Service (WMM/802.11e)
Podpora DSCP (802.1p)
Layer 7 application traffic shaping a firewall
Podpora PMK and OKC credential pre Layer 2 roaming
Podpora 802.11r a 802.11k
Layer 3 roaming
Požadujeme aby WiFi prístupové body boli certifikované od Wireless Ethernet Compatibility Alliance (WECA): WiFi Certified
Zariadenie musí byť vybavené sadou na montáž
Autentifikačný server pre WiFi

Podpora minimálne dvoch rozdielnych protokolov pre autentifikáciu, autorizáciu a accounting (AAA) vrátane RADIUS
Podpora integrovanej užívateľskej databázy
Podpora integrácie s externými identity databázami Windows Active Directory a LDAP, možnosť súčasného použitia viacerých externých užívateľských databáz
Podpora autentifikačného protokolu PAP
Podpora autentifikačného protokolu MS-CHAP
Podpora autentifikačného protokolu Extensible Authentication Protocol (EAP)-MD5
Podpora autentifikačného protokolu Protected EAP (PEAP)
Podpora autentifikačného protokolu EAP-Flexible Authentication via Secure Tunneling (FAST)
Podpora modelu vytvárania politík na základe rôznych pravidiel a atribútov akými sú rôzne autentifikačné protokoly, obmedzenia plynúce z autentifikačných zariadení, obmedzenia dané časovým údajom, validácia atribútov operačných systémov a antivírusového softvérového vybavenia, prípadne iné prístupové obmedzenia

2.6. Manažment a monitoring riešenia, helpdesk a servis počas 48 mesiacov

Požadovaný parameter
Požadované softwarové updaty v cene na 4 roky
24x7x365 prístup na Helpdesk a Callcentrum
24x7x364 Monitoring a manažment riešenia
Integrácia sieťových komponentov z lokalít pripojených prostredníctvom iného operátora pod spoločný dohľadový systém
Plnenie SLA v kalendárnom kvartáli min na úrovni 90%
Komunikácia e-mailom, telefonicky a prostredníctvom webu v slovenčine
SLA Lokality - Bežná prevádzka:
Reakčná doba do 2 hodín

Zabezpečenie dočasného/náhradného riešenia 1 deň
Zmena konfigurácie prostredníctvom vzdialeného prístupu do 1 pracovného dňa
Zabezpečenie trvalého riešenia do 3 pracovných dní
<i>SLA Lokality - Kritická prevádzka:</i> <u>Dni s vysokou prioritou a požiadavkou na vysokú dostupnosť systému (napr. testovanie, maturity). Objednávateľ sa zaväzuje dodať Poskytovateľovi zoznam dní s kritickou prevádzkou najneskôr 14 kalendárnych dní vopred.</u>
Reakčná doba do 1 hodiny
Zabezpečenie dočasného/náhradného riešenia 6 hodín
Zmena konfigurácie prostredníctvom vzdialeného prístupu do 6 hodín
Zabezpečenie trvalého riešenia do 1 pracovného dňa
<i>SLA Centrála EDUNET_SK - Bežná aj kritická prevádzka</i>
Dostupnosť Centrály EDUNET_SK min. 99,9%
Reakčná doba do 1 hodiny
Zabezpečenie dočasného/náhradného riešenia do 2 hodín
Zmena konfigurácie prostredníctvom vzdialeného prístupu do 6 hodín
Zabezpečenie trvalého riešenia do 1 pracovného dňa
Iné požiadavky na zmeny do 30 dní od schválenia cenovej kalkulácie
Monitoring <i>SLA na mesačnej báze:</i>
Nepĺnenie SLA
Eskalované požiadavky
Najčastejšie typy problémov (min. 3)
Zoznam vyriešených požiadaviek
<i>Na požiadanie:</i>
Stav zariadenia
Topológia
Zoznam nedostupných zariadení

Výkonnosť
Riešené požiadavky
SNMP štatistiky
<i>Problém management:</i>
Auto-vytváranie incidentov z monitoringu
Auto-eskalácia
<i>Monitoring:</i>
Aktívnych prvkov
Korelácie udalostí
Analýza prvej príčiny
Správa konfigurácií
Správa zoznamu zariadení

3. Vytvorenie informačného systému/ komunikačného prostredia

(uvedená požiadavka vytvára komunikačné prostredie medzi verejným obstarávateľom a uchádzačom a náklady na jej zriadenie pokrýva celková cena za služby)

Uchádzač sa zaväzuje navrhnuť, vytvoriť a prevádzkovať pre verejného obstarávateľa informačný systém, v ktorom uchádzač bude pravidelne aktualizovať a zdieľať údaje a bude slúžiť najmä na:

- sledovanie plnenia časového harmonogramu projektu,
- sledovanie zapájania lokalít/ škôl do siete EDUNET_ SK (možnosť filtrovania a prezerania zoznamu zapojených škôl, plánovaných na zapojenie s termínom zapojenia),
- sledovanie historických údajov o jednotlivých lokalitách (od zapojenia do siete EDUNET, cez všetky vykonané zmeny a žiadosti o zvýšenie rýchlosti, o prekládku, o dodatočné IKT zariadenia, o služby expertov, web hosting, až po prípadné zrušenie školy, resp. odpojenie zo siete EDUNET_SK,
- kontrolu údajov pre účely verifikácie oprávnenosti faktúr (najmä filtrovanie zoznamov škôl podľa typu pripojenia a pravidelného mesačného poplatku, s možnosťou filtrovania zvoleného časového obdobia, ...),

- vytváranie exportov štatistických údajov podľa zvolených kritérií (počet zapojených škôl vo zvolenom období, počet zapojených škôl podľa krajov, podľa typu pripojenia, atď.), štatistiky a filtrované údaje bude možné vyexportovať do súboru excel.
- sledovanie stavu vybavenosti požiadaviek škôl (žiadosť o zapojenie do projektu, zvýšenie rýchlosti, prekládka, ...)
- prístup do systému Trouble Ticket Managementu, ktorým uchádzač/poskytovateľ sleduje, vyhodnocuje a odstraňuje poruchy (napr. výpadok MPLS VPN, poruchy koncových zariadení, nefunkčnosť internetového pripojenia),
- archívne úložisko všetkých vystavených a uhradených/neuhradených faktúr a vystavených objednávok,
- archívne úložisko elektronických verzií preberacích protokolov,
- archiváciu údajov o lokalitách EDUNET_SK s možnosťou pravidelnej a jednoduchšej aktualizácie (adresa školy, kontaktné údaje riaditeľ/ správca IKT v škole) – za doplňovanie aktuálnych údajov bude zodpovedný pracovník uchádzača (podklady si vyžiada, resp. mu budú zasielané verejným obstarávateľom), zodpovedný pracovník verejný obstarávateľ bude mať možnosť dané údaje len prezerať, filtrovať a exportovať (bez možnosti úpravy – tá sa bude nahlasovať štruktúrovaným e-mailom,

K informačnému systému a jeho funkcionalitám vytvorí uchádzač pre verejného obstarávateľa používateľský manuál.

4. Asistenčné služby koncových zariadení (služby PC experta, WiFi a LAN experta, administrátora serverov)

Cieľom asistenčných služieb je podporiť technickú pripravenosť a prevádzkovú bezpečnosť IKT lokality/ školy. Verejný obstarávateľ v prípade potreby zabezpečí pre lokality nasledovné služby expertov. Uchádzač na základe objednávky zabezpečí:

Služby WiFi a LAN Experta

- Naplánovanie návštevy servisného tímu v škole a dohodnutie termínu návštevy s predstaviteľom školy
- Kontrola siete a pripojenia na internet
 - kontrola ochrany siete (prístupu do siete). Najmä v prípade prístupu na internet cez viacerých poskytovateľov,
 - kontrola izolácie sieťových segmentov (učební). Najmä v prípade integrácie vlastných a dodaných zariadení,
 - kontrola správneho smerovania v sieti,
 - kontrola/aktualizácia zoznamu externých IP adries
- Preverenie funkčnosti tlače
- Poučenie správcu IKT odporúčaných prevádzkových praktikách a údržbe IKT prostredia

- Vyhotovenie protokolu o asistenčných službách

Služby PC Experta

- Kontrola konfigurácie PC s maticou podporovaných konfigurácií
 - porovnanie HW konfigurácie PC s minimálnou predpísanou konfiguráciou,
 - porovnanie inštalovaného systémového SW s predpísanou konfiguráciou,
 - porovnanie inštalovaných SW produktov s predpísanými SW produktami
- Základná diagnostika PC: testy pamäti, konfliktné zariadenia, pripojenie na internet, systémový denník, frekvencia porúch, atď
- Kontrola základných bezpečnostných nastavení
 - nainštalovaný a pravidelne aktualizovaný antivírusový program,
 - v operačnom systéme sú nainštalované všetky bezpečnostné aktualizácie,
 - heslová politika, oddelenie používateľských a administratívnych účtov, šetrič obrazovky,
 - zdieľanie v rámci siete je riadené a sú popísané pravidlá na zdieľanie súborov,
 - všetky nepotrebné sieťové služby sú zakázané na úrovni lokálneho firewall-u
- Aktualizácia SW produktov
 - aktualizácia systémového SW,
 - aktualizácia predpísaných SW produktov
- Riešenie konfliktov, nekompatibility, odstraňovanie problémov

Služby Server Administrátora

- Kontrola konfigurácie servera:
 - porovnanie HW konfigurácie servera s minimálnou podporovanou konfiguráciou,
 - porovnanie inštalovaného systémového SW s predpísanou konfiguráciou,
 - porovnanie inštalovaných aplikácií s požadovanými požiadavkami na HW zdroje servera
- Základná diagnostika servera: testy pamäti, služby servera, databázy, sledovanie aktuálnych verzií BIOS pre danú platformu (plánovanie aktualizácii na základe odporúčaní výrobcu), pripojenie na internet, systémový denník, frekvencia porúch, atď
- Kontrola základných bezpečnostných nastavení
 - nainštalovaný a pravidelne aktualizovaný antivírusový program,
 - v operačnom systéme sú nainštalované všetky bezpečnostné aktualizácie,
 - heslová politika
 - zdieľanie v rámci siete je riadené a sú popísané pravidlá na zdieľanie súborov,
- Aktualizácia SW produktov
 - aktualizácia systémového SW,
 - aktualizácia aplikačných produktov
- Riešenie konfliktov, nekompatibility, odstraňovanie problémov

Cena za asistenčné služby koncových zariadení zahŕňa:

- Náklady za výjazd do školy (Per škola)
- Náklady za vykonanie servisných činností, ktoré nezávisia od počtu PC (Per škola)
- Náklady za vykonanie servisných činností na 1 PC (Per PC)
- Hodinová sadzba za servisné činnosti, ktoré sa musia vykonať nad rámec očakávaných prác. Takéto činnosti musí vopred odsúhlasiť zákazník na základe odhadu prácnosti servisnej organizácie.