



Příloha č. 8 – Technický popis řešení

Obsah

1. Současný stav	2
1.1. Konektivita školy k internetu	2
1.2. Strukturovaná kabeláž a síťové prvky	2
1.3. WiFi infrastruktura	2
1.4. Servery	2
1.5. Počítačové učebny	3
2. Technický popis řešení zakázky	3
2.1. Připojení k internetu	3
2.2. Centrální síťový prvek – router a firewall	3
2.3. Centrální bezpečnostní brána	4
2.4. Centrální monitoring síť	4
2.5. Centrální server pro autorizaci uživatelů	5
2.6. Obměna prvků LAN síťe a doplnění kabeláže	6
2.7. Optická síť	6
2.8. Seznam přípojných bodů LAN	7
2.9. Implementace Wifi síťe ve škole	9



1. Současný stav

1.1. Konektivita školy k internetu

Popis připojení	Výchozí stav
Operátor	CESNET - Rowanet
Rychlost připojení do internetu, technologie	Optický kabel – 100/100 Mbit/s
Přístupové zařízení do internetu, typ	Cisco Catalyst 29000
Počet žáků ve škole	357
Počet zařízení	70

1.2. Strukturovaná kabeláž a síťové prvky

Strukturovaná kabeláž v budově je realizována metalickými rozvody v kategorii 5e. Místní rozvod je realizován strukturovanou kabeláží o rychlosti minimálně 100 Mbit/s. Zásuvky nejsou v každé třídě, jsou dostupné pouze v některých třídách a PC učebnách. Kabeláž není v dobrém stavu – vyžaduje kompletní rekonstrukci.

Aktivní prvky v hlavním rozvaděči jsou:

- 2x Zyxel GS-1900-24 – serverovna (kabinety, velká učebna)
- 2x Zyxel GS-1100-24e – serverovna, ředitelna (malá učebna, kabinety)

1.3. WiFi infrastruktura

Wi-Fi síť je ve škole realizována pomocí AP TP-LINK ve třídách. AP má pouze 1 radio a není centrálně řízená. Celkem se jedná o 12 AP bodů.

1.4. Servery

Popis serverů	Výchozí stav
Typ serveru (HW, výkon, velikost úložiště)	Dell PowerEdge T20
Operační systém serveru	Windows Server 2012
Microsoft Active Directory	2012
Způsob využití serveru	Úložiště; vzdělávací programy; autorizace uživatelů
Záložní napájení	Smart UPS 750
Zálohování	Externí disk



1.5. Počítačové učebny

Popis vybavení	Výchozí stav
Počet učeben	2 učebny (24 a 20 PC)
Vybavenost WiFi	ANO
Typy HW (PC, NB, mobilní zařízení)	PC – DUAL CORE 3GHZ, 4GB RAM, 500GB
Operační systém na stanicích	20 – WIN 10; 20 – WIN 10
Další vybavení	Multimediální tabule
SW vybavení – pro výuku	Office 2003, Office 2013, Terasoft, Fraus, Nová škola, DM software – evidence, vysvědčení
Správa učebny	Není

2. Technický popis řešení zakázky

2.1. Připojení k internetu

Současné internetové připojení je dostatečné pro přístup žáků k internetu z hlediska technologie i rychlosti. Škola má 357 žáků a v plánu je mít v síti připojeno až 120 stanic. Škola tedy musí mít k dispozici připojení o rychlosti minimálně 45 Mbit synchronně s ohledem na počet žáků nebo minimálně 60 Mbit synchronně bez FUP s ohledem na počet stanic.

Dodavatel musí zajistit:

- Dodání minimálně 4 ks veřejných adres IPv4 i IPv6.
- Plnou podporu připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack).
- Připojení v bezpečnostním projektu FENIX resp. veřejné adresy využívané školou, jsou zapojeny do infrastruktury FENIX, nebo ISP splňuje alespoň technické standardy definované projektem FENIX.

2.2. Centrální síťový prvek – router a firewall

Současný centrální router bude nahrazen novým prvkem, který zvládne konektivitu až 100/100MbitMbps a všechny požadované parametry:

Parametry:

- Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)
- Podpora monitoringu a logování NAT (RFC 2663)
- Zařízení podporující rate limiting, antispoofing, ACL/xACL včetně všech licencí
- Možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků
- Podpora DNSSEC a IPv6 protokolů pro služby školy



- Neblokující architektura přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,...
- Dostupnost bezpečnostních aktualizací minimálně po dobu 5 let
- Podpora vzdáleného přístupu (VPN)

2.3. Centrální bezpečnostní brána

V rámci realizace zakázky bude pořízena centrální bezpečnostní brána, které zajistí filtrování obsahu internetu, jeho kategorizaci a také antivirovou ochranu. Brána může být i součástí centrálního routeru.

Bezpečnostní brána a Webový filtr budou určeny k detailní inspekci webového provozu v síti, statistikám, restrikcím na jednotlivé webové stránky nebo skupiny stránek a antivirové a antispamové ochraně. Jde o rozšíření zařízení Router/Firewall o možnost podrobnější kontroly a restrikce. Tento prvek bude vyžadovat pravidelné aktualizace databází od výrobce zařízení a je tedy nutné počítat s pravidelnými ročními náklady.

Parametry:

- Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirovou kontrolou stahovaného obsahu
- Zabezpečení přístupových protokolů (SSL/TLS), antivirová ochrana webových systémů
- Česká databáze webových serverů
- Statistiky přístupu uživatelů k internetovým serverům
- Dostupnost bezpečnostních aktualizací minimálně po dobu 5 let

2.4. Centrální monitoring sítě

Monitoring bude prováděn pomocí centrálního routeru, webové brány a Microsoft Active Directory. Dále bude v síti nasazeno monitorovací zařízení, které zajistí monitoring celé síťové i serverové infrastruktury a automatické hlášení v případě jakéhokoli problému.

Zařízení bude splňovat následující parametry:

- Podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení
- Podpora evidence logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)
- Monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent (např. NetFlow)
- Systém pro monitorování a sběr provozně-lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízení s kapacitou pro uchování dat po dobu minimálně 2 měsíců



- Systém pro monitorování síťových a serverových informací, informace z logů operačních systémů.
- Detekce nelegitimního provozu a síťových anomálií

2.5. Centrální server pro autorizaci uživatelů

Centrální školní server je v současné chvíli na škole dostatečný, včetně služby pro autorizaci uživatelů do sítě. Bude však doplněn druhým serverem pro zajištění redundance autorizace uživatelů a zajištění dalšího úložiště pro využití v nových učebnách.

- **Autorizace uživatelů do školní sítě a řízení jejich oprávnění k síťovým prostředkům**
K autorizaci uživatelů a zařízení do sítě bude určen Active Directory, Prostředník pro autorizaci mezi uživatelem a autorizačním serverem – Radius server – může být úplně oddělený od autorizačního serveru (může být v jiné síti), samozřejmě ale musí na autorizační server vidět; je to dobrá varianta z pohledu bezpečnosti, uživatel komunikuje s Radius serverem, ne přímo s autorizačním serverem.
- **Úložiště dokumentů a materiálů pro výuku**
Úložištěm dokumentů je obecně myšlen sdílený prostor na serveru, kde budou pro žáky a pedagogy na základě oprávnění přístupné materiály pro výuku. Může to být současně prostor, který slouží i k odevzdávání prací či osobní prostor každého uživatele.
- **E-learningový systém**
Centrální systém pro výuku a využití pro zadávání samostatných úkolů či prací.

Minimální parametry serveru:

- Minimálně 2 procesory, minimálně 6 jader
- Minimálně 32GB RAM
- Minimálně 2x 1TB HDD v RAID 10, HW RAID
- Minimálně 8 pozic pro hot-swap HDD
- Redundantní zdroj
- Hypervisor
- Serverový operační systém Windows – minimálně 4 instance
- Záložní zdroj (UPS)
- SW pro replikaci systémů a dat

Server bude splňovat minimálně následující funkcionality:

- Řešení systému správy uživatelů (Identity Management), tj. centrální databáze identit (LDAP, AD, apod.) a její využití pro autentizaci uživatelů (žáci i učitelé) za účelem bezpečného a auditovatelného přístupu k síti, resp. síťovým službám
- Úložiště dokumentů a materiálů pro výuku
- Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel
- Dostupnost bezpečnostních aktualizací minimálně po dobu 5 let
- Zálohování celé serverové infrastruktury a infrastruktury koncových stanic



2.6. Obměna prvků LAN sítě a doplnění kabeláže

V budově dojde ke kompletní rekonstrukci datové sítě, vytvoření páteřní optické sítě a výměně aktivních prvků. Jednotlivé rozvaděče budou propojeny optickým kabelem a v místě bude rozvedena strukturovaná kabeláž o rychlosti minimálně 1 Gbit/s.

Rozpis a umístění rozvaděčů a switchů:

- Rack 1 (42U) – III. patro budovy – hlavní serverovna
 - 1x12 port optický switch pro páteřní síť
 - 3x48 port switch
 - Hlavní router a FW
 - Server
 - Wifi kontroler
- Rack 2 (24U) – II. patro – Ředitelna (sklad). Bude sloužit i pro novou učebnu chemie
 - 2x48 port switch
 - Wifi kontroler
 - Server
- Rack 3 (12U) – II. patro – sborovna
 - 1x24 port switch
- Rack 4 (12U) – I. Patro – třídy I. Stupně
 - 1x48 port switch
- Rack 5 (12U) – III. patro – jazyková učebna
 - 1x48 port switch
- Rack 6 (12U) – I. Patro – tělocvična
 - 1x24 port switch

Aktivní prvky LAN sítě musí splňovat minimálně tyto parametry:

- Rychlost sítě minimálně 1 Gbit
- Webový management
- Neblokující architektura přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,...
- Podpora mechanismu izolace klientů
- Plná podpora protokolů IPv4 i IPv6 (dual-stack)
- Napájení minimálně poloviny portů (POE)
- Minimálně 2x optický SFP modul pro připojení páteřního optického kabelu
- Minimální hlučnost.
- Dostupnost bezpečnostních aktualizací minimálně po dobu 5 let

2.7. Optická síť

Optická páteř bude realizována mezi jednotlivými datovými rozvaděči
Kabely optické sítě

- R1 – R2
- R1 – R3
- R1 – R4
- R1 – R5
- R1 – R6



2.8. Seznam přípojných bodů LAN

Vedení datové sítě bude realizováno v rámci budovy z jednotlivých lokálních rozvaděčů.

I. NP

- Rozvaděč
 - R4 v učebně 112
- Učebny – dvojjásuvka u učitelského stolu
 - 109
 - 110
 - 111
 - 112
 - 113
 - 114
 - 115
 - Cvičná kuchyně B104
 - Učebna dílny B108
- Kanceláře – 2x dvojjásuvka
 - 110
 - Kabinet tělesné výchovy
- AP
 - Šatna 2x
 - Chodba u učebny 111
 - Chodba u učebny 111
 - Cvičná kuchyně B104
 - Učebna dílny B108
 - Tělocvična

II. NP

- Rozvaděč
 - R2
 - R3
- Učebny – dvojjásuvka u učitelského stolu
 - 207
 - 208
 - 209
 - 212
 - 223
 - 224
 - 225
 - 226
 - 227
 - 228
- Kanceláře – 2x dvojjásuvka
 - 202
 - 203
 - 204



- 206
- 210
- 211
- B205
- B206
- Wifi AP
 - Sborovna
 - Chodba u učebny 212
 - Chodba u učebny 224
 - Chodba u učebny 226
 - Chodba u učebny 209
 - Chodba u kabinetu 206

III. NP

- Rozvaděč
 - R1
 - R5
- Učebny – dvojjzásuvka u učitelského stolu
 - 303 – Učebna Chemie s rozvodem pro 20 žákovských PC
 - 305
 - 307 – Velká PC učebna s rozvodem pro 30 žákovských PC
 - 309 – Malá PC učebna s rozvodem pro 20 žákovských PC
 - 310
 - 317
 - 318
 - 319
 - 320
 - 321
 - 322
 - B306
 - B308
 - B309
 - B311
 - B313
 - B314
 - B315
 - B317
 - B318
 - B320
 - B322 – Jazyková učebna s rozvodem pro 24 žákovských PC
- Kanceláře – 2x dvojjzásuvka
 - 302
 - 304
 - 306
 - 308
 - 323
 - 324



- B307
- B310
- Wifi AP
 - Chodba u učebny 303
 - Chodba u učebny 305
 - Chodba u učebny 308
 - Chodba u učebny 309
 - Chodba u učebny 318
 - Chodba u učebny 320
 - Chodba u kabinetu 323
 - Chodba u učebny B306
 - Chodba u učebny B314
 - Chodba u učebny B317
 - Chodba u učebny B322

IV. NP

- Učebny – dvozásuvka u učitelského stolu
 - 401
 - 408
 - 409
 - 410
 - 411
 - 412
 - 413
- Wifi AP
 - Chodba u učebny 409
 - Chodba u učebny 411

Celkem

- Učeben - 48
- Kanceláří - 18
- AP – 26
- Speciální učebny
 - Velká PC učebna – 26 míst
 - Malá PC učebna – 24 míst
 - Učebna Chemie – 20 míst
 - Učebna jazyků – 24 míst

2.9. Implementace Wifi sítě ve škole

Pomocí Wifi prvků bude pokryta celá škola. Celkem půjde o 26 nových AP prvků. Dále bude pořízen redundantní Wifi kontroler pro řízení a správu celé sítě. K dispozici budou 3 Wifi sítě (učitelé, žáci, hosté). Jednotlivé sítě budou v oddělené VLAN.

Wifi zařízení budou muset splňovat minimálně následující parametry:



- Neblokující architektura přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,...
- Podpora mechanismu izolace klientů
- Minimální počet připojených zařízení na 1 AP – 30ks
- Centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení)
- Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD ...)
- Podpora standardu minimálně IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz
- Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu
- Minimálně pasivní zapojení do federovaného systému eduroam (www.eduroam.cz). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů
- Dostupnost bezpečnostních aktualizací minimálně po dobu 5 let