# Technická specifikace předmětu plnění

## KONEKTIVITA

### Popis současného stavu

Síťová konektivita školy je zcela nevyhovující, obsahuje sice datové rozvaděče, do kterých je soustředěná většina kabeláže a aktivních prvků, avšak část této kabeláže nekončí datovou zásuvkou ani v propojovacím panelu na straně datového rozvaděče, ale je ukončená konektorem a zapojena do aktivního prvku či do koncového zařízení. Datové rozvaděče nejsou řádně připojené a ukostřené, jsou připojené prodlužovacími přívody na společném okruhu s ostatními zásuvkami 230V, což způsobuje časté lokální výpadky konektivity. Aktivní prvky jsou také umístěné mimo datové rozvaděče v některých kabinetech z důvodu nedostatečného počtu datových přípojek, tímto způsobem se celá kabeláž dál větví. V několika případech je také dotažená konektivita do míst, kde je potřeba z datové zásuvky z jiné třídy či kabinetu.
Veškerá kabeláž je v kategorii Cat 5e.
Ve škole jsou dva access pointy (AP) připojené do datové zásuvky, které jsou zabezpečené heslem, avšak známým téměř celé škole. Na tyto AP se připojují jak žáci, tak učitele a je využívána jak pro výuku, tak pro různá školení pedagogů. Pokrytí WiFi signálem je velmi omezené a soustředí se pouze na dvě třídy. Kapacitně jsou tyto AP maximálně vytížené a přenosové rychlosti nejsou dostatečné pro práci s aplikacemi umístěnými na serveru školy. AP se často odpojují a je nutné je pravidelně restartovat. Díky nekvalitní konektivitě není možné naplno využívat technologie, které škola v současnosti má k dispozici nebo by ráda využívala, jako jsou například tablety, multimediální centra apod. Aktuálně škola nemá k dispozici nástroj, kterým by mohla datový tok řídit či omezovat, případně monitorovat.

Server školy plní roli doménového řadiče, DHCP a DNS serveru, jeho funkce je však díky nedostatečné konektivitě školy do značné míry degradována. Server dále plní roli souborového serveru, kterou kantoři využívají jen částečně, a to právě z důvodu nedostatečné přenosové kapacity bezdrátové sítě. To vede k tomu, že kantoři mají data uložená duplicitně jak lokálně, tak částečně na serveru. (většinou si data na server jen ručně zálohují). Samotný výkon serveru je dostačující právě pro aktuální využití, pro plánované využití serveru bude nutná jeho obměna za výkonnější.
Zálohování je prováděno integrovaným nástrojem operačního systému, bez možnosti kontroly konzistence záloh, či reportování o průběhu zálohováni. Případně nějaké další konfigurace prováděných záloh.
Server včetně zálohovací jednotky a záložního zdroje je umístěn ve třídě, volně stojící na stole pod datovým rozvaděčem. Třída je zabezpečená dvěma klíči, ale server a data jsou pak volně přístupná.

V současné době je škola připojená na metropolitní síť, která je uzavřená, ale nenaplňuje vnitřní konektivitu školy dle Standardu konektivity škol uvedenou v příloze Specifických pravidel pro žadatele a příjemce (zde).
Po realizaci projektu se tyto standardy naplní, vygenerovaným exportem potvrzení o splnění vybraných požadavků Standardu konektivity z aplikace, která je dostupná na adrese: https://www.standardkonektivity.cz/.

### Zajištění vnitřní konektivity školy a připojení k internetu – v rámci projektu

Zajištění vnitřní konektivity školy je možné rozdělit na další čtyři části, přičemž dohromady tvoří jeden celek, který splňuje specifikaci standardu konektivity škol.

a) Metalická a optická část
b) Bezdrátová část
c) Serverová část
d) Bezpečnost

**ad a)** Metalická a optická část se soustředí zejména na vybudování kvalitní strukturované kabeláže splňující standardy kategorie Cat6. Projekt počítá částečně s využitím stávajících datových rozvaděčů a také s instalacemi nových tak, aby byly efektivně rozmístěné jednotlivé datové uzly po celém areálu školy. Strukturovaná kabeláž bude ukončena datovými zásuvkami v celkovém počtu 122ks, přičemž většina datových zásuvek disponuje dvěma výstupy. Tento počet nám umožní pokrytí všech tříd, kabinetů, provozních místností i kanceláří v dostatečném počtu. Datové uzly budou vybaveny aktivními prvky sítě LAN (switch), které budou navzájem propojené a budou tvořit páteř sítě LAN. Budova

„A“ a budova “B“ bude propojená optickým kabelem. Strukturovaná kabeláž bude vedena v plastových lištách. Optický kabel bude vedený v pevné plastové trubce.

**ad b)** Bezdrátová část obsahuje 12 bezdrátových vysílačů „AP“ které pokryjí WiFi signálem převážnou část areálu školy. AP budou zapojená do jednotlivých datových uzlů potažmo do aktivních prvků sítě LAN, ze kterých budou také pomocí PoE napájeny. Všechny AP budou centrálně řízeny a plně integrovány do doménového prostředí školy, tak, aby splňovaly specifikaci standardu konektivity škol.

**ad c)** Serverová část obsahuje jak HW nového serveru, tak licence serverového operačního systému, ale hlavně migrační práce spojené s výměnou serverového prostředí. HW konfigurace je dostatečně dimenzovaná, aby byla schopna zvládnout potřebný počet virtuálních serverů a nároky na něj kladené.

**ad d)** Za samostatnou část považujeme nastavení bezpečnosti ICT prostředí školy. Pro tyto účely volíme router s pokročilými bezpečnostními funkcemi s integrací do doménového prostředí školy, doplněný o samostatný analyzátor datového provozu.

| **Konektivita školy k veřejnému internetu (WAN)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Minimální povinné parametry** | | | | | | | |
| Opatření | Stávající stav | | | Realizace v rámci projektu | | | Komentář |
| | Zajištěno | Zajištěno částečně | nezajištěno | ano | částečně | ne | |
| šíře pásma (bandwidth) odpovídající 128kbps/student nebo 512kbps/počítač nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů | | 64kbps/student | | Minimálně 128kbps/student | | | Bude prokázáno výstupem testu: www.standardkonektivity.cz |
| vlastní nebo poskytovatelem přidělené veřejné IPv4 i IPv6 adresy | | | není | 1x IPv4 plus IPv6 60bit rozsah | | | Bude prokázáno výstupem testu: www.standardkonektivity.cz |
| plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack) | | Pouze IPv4 | | IPv4 i IPv6 | | | Bude prokázáno výstupem testu: www.standardkonektivity.cz |
| validující DNSSEC resolver na straně školy | | | není | Bude zajištěno insatlaci role DNS na OS MS Windows Server | | | Bude prokázáno výstupem testu: www.standardkonektivity.cz |
| podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení | | | není | Monitorování NAT bude zajištěno pomocí nového routeru - firewallu | | | |
| logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.) | | | není | Bude zajištěno ověřením uživatelského účtu pomocí autentizace/autorizace 802.1X (Radius), | | | |
| síťové zařízení podporující rate limiting, antispoofing, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality | | | není | Bude zajištěno pomocí nového routeru - firewallu | | | |
| 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 | | | není | Bude zajištěno pomocí nového routeru - firewallu | | | |
| možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků | | | není | Bude zajištěno pomocí nového routeru - firewallu | | | |
| podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online | | | není | Podpora bude v rámci realizace projektu zajištěná | | | |
| u software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu. | | | není | Bude zajištěno pořízenou licencí garantující dostupnost aktualizací po celou dobu udržitelnosti projektu | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Nad rámec povinných parametrů** | | | | | | | |
| • symetrické připojení bez agregace a omezení (FUP) | ANO | | | | | | |
| • zapojení poskytovatele připojení v bezpečnostním projektu FENIX resp. veřejné adresy využívané školou jsou zapojeny do infrastruktury FENIX nebo ISP splňuje alespoň technické standardy definované projektem FENIX – viz http://nix.cz/cs/file/NIX_PRAVIDLA_FENIX | | | není | ISP bude splňovat technické standardy definované projektem Fenix | | | |
| **Vnitřní konektivita školy (LAN)** | | | | | | | |
| **Minimální povinné parametry** | | | | | | | |
| 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 zařízeni s kapacitou pro uchování dat po dobu minimálně 2 měsíců | | | není | Monitorování IP bude zajištěno pomocí NGFW + NETFLOW | | | |
| Povinné 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. | | Lokální přihlašování uživatelů a základní nastavení AD | | Implementace ActiveDirectory | | | |
| logování přístupu uživatelů do sítě umožňující dohledání vazeb *IP adresa – čas – uživatel* | | | není | Bude zajištěno ověřením uživatelského účtu pomocí autentizace/autorizace 802.1X (Radius), | | | |
| **Minimální povinné parametry v oblasti pevné LAN** | | | | | | | |
| • Minimální konektivita stanic a dalších koncových zařízení zařízení 100Mbit/s fullduplex | | 10/100Mbps | | 1Gbps | | | |
| • Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,…) | | Kombinace strukturované kabeláže a různě natažených kabelů ukončených konektorem | | Nová strukturovaná kabeláž a aktivní prvky. Součástí strukturované kabeláže budou předány měřící protokoly splňující standardy Cat 6 | | | |
| • Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s fullduplex | | | není | V rámci projektu budou implementovány aktivní prvky sítě LAN, NAS a servery podporují 1Gbps datové přenosy | | | |
| • Páteřní rozvody mezi budovami v areálu realizovány prostřednictvím optických, metalických vláken popř. bezdrátovými spoji v licencovaném pásmu (povolení ČTÚ) | | | nejsou | V rámci projektu bude realizován optický propoj mezi pavilony | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| • Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3) s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,… | | | nejsou | Bude zajištěno novými aktivními prvky | | | |
| **Minimální povinné parametry v případě řešení bezdrátových sítí (wi-fi)** | | | | | | | |
| Podpora mechanismu izolace klientů | | | není | V rámci projektu bude zajištěno novými aktivními prvky | | | |
| Návrh topologie wifi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou ve v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů | | | není | Pokrytí WiFi signálem školy bude zajištěno pomocí 12ks AP, umístěných tak, aby maximálně pokryly budovy školy | | | |
| Centralizovaná architektura správy wifi sítě (centrální řadič, centrální management, tzv. thin access pointy, popř. alespoň 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) | | | není | Bude zajištěno novými aktivními prvky | | | |
| Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD …) | | | není | Bude zajištěno novými aktivními prvky | | | |
| Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz | | | není | Bude zajištěno novými aktivními prvky | | | |
| Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu | | | není | Bude zajištěno novými aktivními prvky | | | |
| **Nad rámec povinných parametrů** | | | | | | | |
| Minimálně pasivní zapojení[1] do federovaného systému eduroam (www.eduroam.cz). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů. | | | není | | | X | nerelevantní |
| **Další bezpečnostní prvky (nepovinné)** | | | | | | | |
| Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů | | | není | | | X | nerelevantní |
| Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.) | | | není | | | X | nerelevantní |
| Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, blokace wifi v určitém čase) | | | není | | | X | nerelevantní |
| Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací a zpřístupnění jejich služeb) | | | není | | | X | nerelevantní |
| Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3954 nebo ekvivalent (NetFlow)) | | | není | | | X | nerelevantní |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie | | | není | | | X | nerelevantní |
| Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management) | | | není | Bude implementován monitoring | | | |
| Systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios / Icinga) | | | není | Bude implementován monitoring | | | |
| Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk) | | | není | | | X | nerelevantní |
| Nástroje pro centrální správu a audit ICT prostředků | | | není | | | X | nerelevantní |
| Systémy zálohování a obnovy dat serverové infrastruktury | | Windows Backup | | Bude realizováno pomocí zálohovacího SW umožňující zálohovat celé virtuální prostředí a vytvářet reporty o proběhlých zálohách | | | |
| Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů | | Pouze antivir pro koncové stanice a server | | Bude implementována rozšířená ochrana na úrovni routeru | | | |
| Zabezpečení přístupových protokolů (SSL/TLS) služeb (např. emailové služby, webové servery, studijní a ekonomické agendy) atp. | | | není | Škola využívá poštovní služby Google | | | |
| Podpora vzdáleného přístupu (VPN) | | | není | VPN přístup bude zajištěn pomocí NGFW a SSL klienta pro všechny členy skupiny zabezpečení kteří mají mít tuto možnost | | | |