

Příloha č. x - **Standard konektivity škol**

Standard konektivity škol vychází z přílohy Ministerstva školství, mládeže a tělovýchovy dostupný zde: <https://www.edu.cz/digitalizujeme/standard-konektivity-skol/>.
Standard konektivity škol dokládá či porovnává soulad standardu s navrženými parametry vnitřní konektivity.

Bod standardu	Popis	Popis řešení
Konektivita školy k veřejnému internetu (WAN)		
1.2.1.	Šíře pásma (bandwidth) odpovídající 0,25 Mbps/žák či student nebo 0,5 Mbps/koncové uživatelské zařízení a zároveň taková šířka pásma, která neomezuje provoz zařízení a uživatelů. Šíře pásma se vztahuje na počet žáků/studentů/koncových uživatelských zařízení v budově/areálu, kde se projekt realizuje.	Do školy je v současné době přivedena konektivita s kapacitou symetrických 160 Mbps, což vyhovuje oběma navrženým kritériím.
1.2.2.	Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.	Do školy je v současné době přivedena konektivita s přidělenou veřejnou IPv4 adresou.
1.2.3.	Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení v minimální délce 3 měsíců.	Bude zajištěno nasazení UTM Firewallu včetně bezpečnostních updatů a záruky výrobce na 5 let na perimetru sítě. Požadována bude kompletní rekonfigurace stávajícího perimetru sítě s náhradou dosluhujícího firewallu Fortigate a konfigurace UTM funkcionalit (Antivir, WebFilter, Aplikační kontrola, IPS) pro zaměstnance i žáky. Dále pak Logování a monitoring NAT a logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel.
1.2.4.	Síťové zařízení podporující rate limiting, antispoofing, access listy – zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality.	Bude zajištěno nasazení UTM Firewallu včetně bezpečnostních updatů a záruky výrobce na 5 let na perimetru sítě včetně nasazení L3 funkcí a QoS pro prioritizaci provozu a zajištění průchodnosti pro všechny uživatele tak, jak vyžaduje také bod 1.2.1.
1.2.5.	Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků.	Bude zajištěno nasazení UTM Firewallu včetně bezpečnostních updatů a záruky výrobce na 5 let na perimetru sítě včetně konfigurace potřebných bezpečnostních politik pro oddělení učitelské, žákovské, IoT, management, docházkové a kamerové sítě.
1.2.6.	Zajištění šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén pro služby školy dostupné online (např. emailové služby, webové servery, studijní a ekonomické agendy atp.).	Škola poskytuje webovou službu aplikace Bakaláři, která bude migrována na nový server. Tato služba bude zabezpečena platným SSL certifikátem. Doména komenskeho288.cz již je podepsaná pomocí DNSSEC.
1.2.7.	Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem;	Na řadiči Active Directory, který bude plnit roli DNS serveru pro všechna zařízení sítě LAN bude konfigurován DNSSEC resolver.
1.2.8.	Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici.	Veškerý HW a SW bude dodán včetně záruky a podpory výrobce na min. 5 let. Součástí podpory výrobce musí být nárok na aktualizaci firmware a tzv. subscripce (bezpečnostní, antivirové, IPS, aplikační, antimalware, IP reputační databáze apod.).
1.2.9.	Poskytovatel konektivity je schopen zajistit kontaktní bod pro komunikaci, trvalý monitoring dostupnosti konektivity, realizovat blokování nežádoucí komunikace zahrnující nebo jinak omezující konektivitu a systémy školy na straně poskytovatele na základě požadavku školy.	V rámci smlouvy s poskytovatelem připojení bude rozšířena služba o trvalý monitoring dostupnosti konektivity, blokování nežádoucí komunikace zahrnující nebo jinak omezující konektivitu a systémy školy. K dispozici bude kontaktní bod pro komunikaci.
Vnitřní konektivita školy (LAN a WLAN)		
2.2.1.	Systém 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. službám. Využívání jednoho účtu více uživateli není povoleno (využívání tzv. anonymních účtů).	Bude dodán 1 ks HW serveru s montáží do datového rozvaděče, serverový operační systém s podporou pro virtualizaci a vlastní správy uživatelů. Veškerý HW bude dodán s aktuálním firmware, bude kompletně namontován a zkonfigurován pro provoz virtuální infrastruktury. V rámci virtuální infrastruktury bude nainstalován jeden řadič ActiveDirectory v aktuální verzi a s posledními „záplatami“ systému. Bude zkonfigurována a naplněna databáze ActiveDirectory pro žáky a učitele. Bude zprovozněna min. služba DNS a NTP.
2.2.2.	Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – počítačový systém.	V síti LAN bude nasazena adresářová služba na bázi Active Directory. Každý uživatel sítě bude mít svůj jedinečný uživatelský účet chráněný heslem. Pouze po přihlášení uživatele do Active Directory mu bude umožněn přístup k síťovým zdrojům. Tento přístup bude v čase logován a bude logována IP adresa stroje, ze které bylo do sítě přistoupeno.
2.2.3.	Systémy zálohování a obnovy dat serverové infrastruktury.	Bude instalován software, který umožní zálohovat serverové operační systémy, o zálohování bude podávat informaci do e-mailu. V rámci software lze zvolit, zda bude daná notifikace odeslána jen v případě neúspěchu zálohování, nebo vždy.

2.2.4.	Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů.	Na koncové stanice i počítačové servery bude instalován antivirový systém, který zajistí ochranu před aktuálními hrozbami pomocí virových definic, analýz chování i napojení na externí reputační službu výrobce software. Licence bude dodána s platností na minimálně 5 let. Zabezpečené stanice budou připojeny k centrální správě AV řešení, která umožní jejich dohled, vytváření reportů i vzdálenou aktualizaci jednotlivých verzí AV, a to včetně distribuce centrálně definovaných politik pro nastavení bezpečnostního produktu.
2.3.1.	Minimální konektivita koncových uživatelských zařízení 1000 Mbps full duplex.	Všechny projektované prvky budou osazeny porty s rychlostí alespoň 1000 Mbps full duplex a doplní současné prvky, které budou zachovány a touto rychlostí mají také všechny své porty vybavené.
2.3.2.	Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps full duplex.	Všechny projektované prvky budou osazeny porty s rychlostí alespoň 1000 Mbps full duplex a doplní současné prvky, které budou zachovány a touto rychlostí mají také všechny své porty vybavené.
2.3.3.	Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3) 12 s neblokující architekturou přepínacího subsystému (wire speed), management, podpora 802.1Q VLAN (možnost tvorby virtuálních sítí – VLAN), základní bezpečnostní prvky proti zneužití přístupu k síti [např. MAC based omezení (port-sec), 802.1X autentizace aj.].	Datová síť utvoří jeden provázaný celek se stávajícími moderními přístupovými prvky (AP a switche) a nahradí staré dosluhující vybavení v původní počítačové učebně. AP i switche budou konfigurovatelné skrze centrální management a budou disponovat podporou pro 802.1Q, 802.1X a port security. Centrální switch v novém datovém rozvaděči u serveru musí disponovat připojením pomocí 10Gbps portů stejně jako switche na páteřní lince spojující budovy školy.
2.3.4.	Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).	Strukturovaná kabeláž školy není řešena v rámci aktuálního projektu, ale již plně umožňuje využití rychlosti přípojky specifikované bodem 2.3.1., většina kabeláže je ve standardu Cat5e, zbytek v Cat6. Instalovaná optická kabeláž je jednovláknová vícevláknová linka s propustností >10 Gbps podle osazených převodníků.
2.3.5.	Páteřní rozvody mezi budovami v areálu, kde probíhá výuka nebo příprava na ni, realizovány prostřednictvím optických vláken nebo metalických kabelů. Vztahuje se na budovu/areál, kde se projekt realizuje.	Neřeší se v rámci projektu. Budovy jsou již propojeny pomocí optických vláken, viz 2.3.4.
2.4.1.	Návrh topologie Wi-Fi sítě a analýza pokrytí signálem počítačů s konzistentní Wi-Fi službou v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů.	V každé učebně, kterou je vhodné pokrýt Wi-Fi signálem je již instalována zásuvka strukturované kabeláže. Strukturovaná kabeláž je svedena do stávajících datovým rozvaděčů, kde se uvažuje umístění switchů s podporou PoE pro napájení bezdrátových AP. Bezdrátové přístupové body budou v jednotlivých učebnách připevněny na zeď pod stropem. Celkem bude instalováno nových 14 AP. Rozmístění jednotlivých AP je součástí technické zprávy.
2.4.2.	Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu.	Bezdrátová síť bude podporovat připojení pomocí zabezpečeného podnikového standardu WPA2-Enterprise s ověřováním vůči centrální adresářové službě pomocí protokolu RADIUS.
2.4.3.	Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).	Bude zajištěno nasazení UTM Firewallu včetně bezpečnostních updatů a záruky výrobce na 5 let na perimetru sítě včetně nasazení L3 funkcí pro oddělení sítí s různým určením a omezením dosahu jednotlivých zařízení v rámci školní sítě.
2.4.4.	Podpora mechanismu izolace uživatelů.	Projektované řešení bezdrátové sítě podporuje izolaci klientů.
2.4.5.	Podpora standardu IEEE 802.11ac (Wi-Fi 5) a případně novějších (Wi-Fi 6), současná funkce AP v pásmu 2,4 a 5 GHz a novějších protokolů a pásem.	Nově instalované bezdrátové prvky budou splňovat minimálně standard 802.11ax a doplní tak stávající prvky, které splňují standard 802.11ac. Prvky budou pracovat minimálně v pásmech 2.4GHz a 5GHz. Systém bude možné rozšířit o bezdrátová AP s podporou pásma 6GHz.
2.5.1.	Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele.	V síti LAN bude nasazena adresářová služba na bázi Active Directory. Každý uživatel sítě bude mít svůj jedinečný uživatelský účet chráněný heslem. Pouze po přihlášení uživatele do Active Directory mu bude umožněn přístup k síťovým zdrojům. Tento přístup bude v čase logován a bude logována IP adresa stroje, ze které bylo do sítě přistoupeno.

2.5.4.	Centralizovaná architektura správy Wi-Fi sítě (centrální řadič, centrální management, tzv. thin access pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravovanými access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení).	Bezdrátová síť je navržena jako centralizovaná s využitím funkce tzv. „virtuálního kontroleru“. Funkci virtuálního kontroleru zajišťuje software instalovaný v rámci virtualizovaného serveru. Kontroler řídí distribuci konfigurací, rozkládání zátěže, roaming, ladění kanálů, detekci rušení apod. Kontroler pro bezdrátovou síť funguje zároveň jako ovládací prvek sítě drátové.
2.5.5.	Doporučená podpora pro ověřování uživatelů oproti databázi účtů [např. pomocí protokolu IEEE 802.1X vůči centrální evidenci uživatelů (např. LDAP, MS AD) nebo pomocí Captive portalu].	Projektované aktivní prvky sítě LAN podporují protokol IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol RADIUS.
2.5.6.	Propojení aktivních prvků a důležitých systémů (např. servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.	Server a NAS budou vybaveny 10 Gbps porty, stejně jako centrální přepínače.
Další doporučené bezpečnostní prvky projektu		
3.1.4.	Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.	Dodán bude virtualizovaný server provozovaný na novém hardware, který bude monitorovat kritické prvky síťové infrastruktury, serveru, NAS a dalších prvků připojených k počítačové síti a bude o chybách a anomáliích informovat pomocí e-mailů.
3.1.8.	Podpora vzdáleného přístupu (VPN).	Bude zajištěno nasazení UTM Firewallu včetně bezpečnostních updatů a záruky výrobce na 5 let na perimetru sítě včetně nasazení SSL VPN pro přístup ke školním zdrojům pro vyjmenované skupiny uživatelů.