

Popis a technická specifikace kompletního vybavení pro síťovou infrastrukturu školy (dodávka v rámci projektu z IROPu s názvem „Škola pro 4. průmyslovou revoluci“) reg. číslo: CZ.06.2.67/0.0/0.0/16_050/0002521		
Druh zařízení	specifikace	počet jednotek
tyto parametry musí produkt splňovat		
Zařízení pro Vnitřní konektivitu školy a Další bezpečnostní prvky dle Specifických pravidel pro žadatele a příjemce, Příloha 11 – Standard konektivity škol		
<p>Dále uvedená a popívaná technická řešení budou využita k dokončení a modernizaci stávající školní infrastruktury MAN s ohledem na rozvoj IT a požadavky na rychlost a bezpečnost provozované infrastruktury. Samotná konektivita školy do internetu řešena není, bude využito stávající připojení. Stávající řešení již kapacitně nestačí současným nárokům na moderní výuku a pokrytí potřeb žáků a vyučujících v oblasti IT konektivity. Všechna dodávaná zařízení musí být nová a určená pro český trh. Dodavatel před podpisem kupní smlouvy na vyžádání doloží tuto skutečnost potvrzením přímo od výrobce. Součástí nabídky bude seznam certifikovaných pracovníků dodavatele včetně kopií jejich certifikátů.</p>		
Server pro zálohování	<ul style="list-style-type: none"> • provedení do racku • osazení dvěma procesory každý s 8 jádry a celkovým výkonem dle benchmarku SPEC CPU2006 Result – CINT2006 Rates min. 716 bodů a CFP2006 Rates min. 611 bodů • HDD 13x 900 GB, SAS, 2.5-in, 10K Hard Drive (Hot-plug) • RAM 160 GB pracující na maximální možné frekvenci, možnost rozšíření až na 1,5TB, 24 DIMM slotů • hardwarový diskový RAIDController pro RAID 0,1,1+0,5,6,60 s 1 GB cache paměti • dva Hot-plug, redundantní zdroje napájení (1+1) minimálně 550W a certifikací Platinum • Prediktivní analýza chyby na všech kritických komponentech - procesory, HDD, RAM, ventilátory, zdroje • Redundantní, za běhu měnitelné chlazení • plná vzdálená správa serveru 100 % kompatibilní s již zadavatelem používaným rozhraním u všech šesti serverů (v současné době je zadavatelem provozován např. server P/N 5463K3G) a s dedikovanou síťovou kartou • OS: MS Windows Server, licenci dodá škola • Záruka 5 let s garancí opravy NBD u zákazníka • Požadované práce: <ul style="list-style-type: none"> ○ Oživení a zahoření serveru. ○ Instalace a konfigurace virtualizace (zadavatel dodá licence VMware). ○ Instalace a konfigurace Windows server (tento OS je požadován z důvodu kompatibility se stávajícím programovým vybavením školy a licence má zadavatel již zakoupené). ○ Instalace a konfigurace zálohovacího SW (zadavatel bude mít licence na VeeamBackup) ○ Zaškolení základní obsluhy dodané technologie v rozsahu 6 hodin 	1
NAS pro zálohu mimo budovu se serverem	<ul style="list-style-type: none"> • Procesor čtyřjádrový • AES 256-bitové šifrování dat • Velikost operační paměti min. 8 GB s možností rozšíření na 16 GB • Počet slotů pro HDD min. 8 s možností rozšíření na 18 • Maximální kapacita 80TB, při rozšíření až 180TB • Porty min. 4x USB 3.0 • LAN min. 4x GbE s možností agregace a možností rozšíření o 10Gb LAN kartu • Podpora min. RAID0,1, 5, 6, 10 • Podporované protokoly min. CIFS, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN • Rychlost čtení až 1165 MB/s • OS kompatibilní se sítí školy v nejnovější verzi a možností využití starší verze • Aplikace - min. databázový server, download server, FTP server 	1

Popis a technická specifikace kompletního vybavení pro síťovou infrastrukturu školy (dodávka v rámci projektu z IROPu s názvem „Škola pro 4. průmyslovou revoluci“) reg. číslo: CZ.06.2.67/0.0/0.0/16_050/0002521		
Druh zařízení	specifikace	počet jednotek
tyto parametry musí produkt splňovat		
	<ul style="list-style-type: none"> • Spotřeba do 61,5W • Součástí NAS – 8ks HDD <ul style="list-style-type: none"> • Úložná kapacita jednoho disku min. 4 TB • rozhraní min. SATA III • rozměr 3,5" • umožňuje provoz v režimu 24/7 • kompatibilní s dodávaným NAS • Záruka 5 let i na HDD • Požadované práce - Oživení a konfigurace zálohování. 	
Zabezpečení datové sítě MAN	<p>Specifikace zabezpečení</p> <ul style="list-style-type: none"> • Předmětem je řešení klastru firewallů typu UTM (UnifiedThreat Management). Podpora, záruka a licence na dodaný HW – vše na 5 let. • Pokud se firewall skládá z více modulů, musí jít o moduly jednoho výrobce a tyto moduly musí být integrovány do jednoho celku s jednou, centrální správou. Součástí dodávky musí být veškeré potřebné programové vybavení, tj. všechny licence potřebné pro instalaci a provoz, pro neomezený počet uživatelů. • Funkce centrální správy, logování a reportování je přípustné řešit jako virtuální appliance, všechny ostatní služby musí být poskytovány zařízením typu hardware appliance. Řešení musí mít funkcionalitu vysoké dostupnosti (active-passive) pro všechny prvky poskytující funkce uvedené v bodu 2, s výjimkou logování a rozšířeného reportování, a to bez dalších licenčních nákladů (přípustné jsou pouze náklady na hardware). <p>Požadované funkce</p> <ul style="list-style-type: none"> • Paketový filtr a základní funkce • Stavové filtrování paketů • Překlady komunikace (příchozí i odchozí) • Možnost použití více internetů v režimu active-backup nebo balancing (dynamické routování). • Montáž do standardních 19" skříní (rack). • 100% administrace pouze přes webové rozhraní (bez nutnosti použít textové rozhraní typu TELNET/ SSH konzole) • Propojení a využívání ActiveDirectory • Podpora bezagentového přihlášení uživatelů (8. vrstva) • DHCP server a DNS forwarder pro konkrétní síť • Možnost automatické zálohy UTM a v případě potřeby kompletní obnovy konfigurace nahráním ze zálohy • Logování a rozšířený reporting (vč. statistik uživatelských aktivit) • Vlastní API rozhraní pro propojení s dalšími interními nástroji • Podpora routování BGP a OSPF • Proaktivní ochrana perimetru • IDS/IPS • Blokování C&C komunikace • Možnost specifikace výjimek • Identifikování kompromitovaného systému na základě C&C komunikace • Aplikační kontrola (blokování konkrétních aplikací z pravidelně aktualizovaného seznamu výrobce) • Logování • VPN – vzdálené přístupy • IPSEC – propojení vzdálených lokalit • SSL VPN – připojení vzdálených PC • SSL VPN - Odlišný certifikát / uživatel • SSL VPN - Uživatelský portál pro stažení VPN klienta 	1

Popis a technická specifikace kompletního vybavení pro síťovou infrastrukturu školy (dodávka v rámci projektu z IROPu s názvem „Škola pro 4. průmyslovou revoluci“) reg. číslo: CZ.06.2.67/0.0/0.0/16_050/0002521		
Druh zařízení	specifikace	počet jednotek
tyto parametry musí produkt splňovat		
	<ul style="list-style-type: none"> • SSL VPN - Dostupná instalace vč. konfigurace (bez nutnosti další konfigurace na koncových počítačích) • Zobrazení aktuálně připojených uživatelů v GUI • Licenčně neomezený počet VPN tunelů, připojených uživatelů a přenosu dat • Neomezený počet SSL VPN klientů v ceně • Logování <p>Reverzní proxy pro ochranu interních webových serverů a aplikací</p> <ul style="list-style-type: none"> • Ochrana skenováním antimalware motorem • Filtrování http a https komunikace • Ochrana proti trojským koním • Ochrana proti podvržení cookies (podepisování) • Možnost monitorovat nebo blokovat (odmítnout) komunikaci • Podpora reverzních formulářů přihlášení navázaných na ActiveDirectory • Blokování komunikace na základě reputační služby výrobce • Možnost specifikace výjimek • Logování <p>Ochrana emailové komunikace (SMTP)</p> <ul style="list-style-type: none"> • Ochrana skenováním antimalware motorem • Ochrana proti spamům / phishing emailům • Skenování příloh emailů vč. archivů • Skenování odchozího i příchozího provozu • Blokování komunikace na základě reputační služby výrobce • Ochrana proti DoS útokům • Nastavitelná a vynutitelná TLS komunikace pro konkrétní SMTP servery • Šifrování odchozích emailů (nastavitelné a volitelné) • Kontrola emailové fronty na UTM • Karanténa uložená na UTM • Logování a prohledávání logů min. na úrovni: Odesílatel, Příjemce, Předmět, Datum • Stejně logování a prohledání i pro uživatele pomocí GUI „uživatelského portálu“ (jen pro emaily konkrétního uživatele) • Možnost specifikace výjimek • Logování <p>Ochrana přístupů na internet</p> <ul style="list-style-type: none"> • Ochrana skenováním antimalware motorem • URL filtrování (min. 80+ kategorií) • Filtrování HTTP, HTTPS a FTP • Možnost specifikovat povolené porty • Možnost specifikace porty proxy • Propojení s ActiveDirectory • Možnost definovat výjimky • Pravidla platí pouze ve specifikovaný čas během dne • Pravidla lze specifikovat na skupinu/uživatele z ActiveDirectory • Logování <p>Možnost rozšíření o správu WiFi</p> <ul style="list-style-type: none"> • Řešení musí být rozšiřitelné o správu wifi zařízení (vše od stejného výrobce) a nesmí k tomu vyžadovat žádnou další licenci. <p>Minimální technické požadavky (deklarované výrobcem)</p> <ul style="list-style-type: none"> • Firewall: 32 Gbps • IPS propustnost: 8 Gbps • VPN (AES) propustnost: 3 Gbps • Propustnost Web proxy s aktivním AV: 5,5 Gbps 	

Popis a technická specifikace kompletního vybavení pro síťovou infrastrukturu školy (dodávka v rámci projektu z IROPu s názvem „Škola pro 4. průmyslovou revoluci“) reg. číslo: CZ.06.2.67/0.0/0.0/16_050/0002521		
Druh zařízení	specifikace	počet jednotek
tyto parametry musí produkt splňovat		
	<ul style="list-style-type: none"> • Souběžná spojení: 17 milióny • Nová spojení za sekundu: 200 tisíc • Požadované práce: <ul style="list-style-type: none"> ○ Oživení a základní konfigurace GW (práce provede certifikovaný pracovník na dodaný typ zařízení). ○ Zprovoznění HA ○ Konfigurace Firewall ○ Konfigurace Network Protection (IDS/IPS, SSL IPSex) ○ Konfigurace Web Protection (scan, antimalware, filtrování URL, reporting) ○ Konfigurace webserver protection (WAF, OWA) ○ Konfigurace email protection (Cloudprotection) ○ Zaškolení základní obsluhy dodané technologie v rozsahu 6 hodin, zadavatel požaduje možnost zdarma upravit konfiguraci po předání systému do provozu v rozsahu 50 hodin – v období následujících 6 měsíců. ○ Provedení bezpečnostního auditu nastavení nezávislou certifikovanou společností. 	
WiFi síť	<ul style="list-style-type: none"> • AP musí podporovat standardy 802.11a/b/g/n/ac wave 2 a být schopno obsluhovat WiFi pásma na frekvenci 2,4 a 5GHz souběžně • AP musí podporovat minimálně 20, 40 a 80MHz široké kanály • Rádiové čipy musí podporovat technologii MIMO a MU-MIMO s podporou minimálně 2 prostorových streamů • napájení AP musí být umožněno adaptérem DC12V, 1A a napájením po ethernetu dle standardu 802.3af • podpora WPA2 Personal/Enterprise autentizace s AES/CCMP enkrypcí • AP musí dále podporovat standardy WMM, WMM-PS, 802.11d, 802.11h a 802.11e • Podpora až 27 BSSID na jeden přístupový bod • Propustnost WLAN rozhraní (L1): 867 Mbps (5GHz) a 300 Mbps (2.4GHz) • AP musí podporovat Beamforming založený na anténním systému - tj. být schopno upravovat celkovou charakteristiku vyzařování antény v reálném čase a schopno cílit povolený vyzařovací výkon do místa, kde se nachází koncové zařízení • anténní systém AP musí být schopen vytvořit minimálně 128 různých anténních charakteristik vyzařování • AP musí být schopno aktivně potlačovat rádiové rušení ve WiFi pásmu pomocí změn charakteristiky antény v reálném čase • AP musí být schopno současně provozovat prostorový multiplex a systém beamformingu • Anténní systém AP musí být schopen pracovat současně ve vertikální a horizontální polarizaci a být schopná se dynamicky přizpůsobovat polarizaci koncového zařízení (včetně pohybujících se zařízení), tj. systém PD-MRC • Anténní systém musí mít zisk alespoň 3dBi fyzického zisku pro každý prostorový stream a musí být schopen potlačit rušení alespoň o 10dB • Minimální citlivost rádia musí být alespoň -100dBm • AP by mělo být schopno poskytnout hodnoty parametrů RTT a T-DoA za účelem možného budoucího nasazení pro lokalizační účely • AP musí podporovat systém DFS v 5GHz pásmu • AP musí šifrovat řídicí data v komunikaci s kontrolérem • AP musí být schopno komunikovat s kontrolérem i po L3 • Minimálně 2x10/100/1000 Ethernet port, podpora PoE 802.3af/at na jednom z portů • Podpora mapování definovaných VLAN tagů na jednotlivé WLAN profily 	25 AP

Popis a technická specifikace kompletního vybavení pro síťovou infrastrukturu školy (dodávka v rámci projektu z IROPu s názvem „Škola pro 4. průmyslovou revoluci“) reg. číslo: CZ.06.2.67/0.0/0.0/16_050/0002521		
Druh zařízení	specifikace	počet jednotek
tyto parametry musí produkt splňovat		
	<ul style="list-style-type: none"> • Možnost spektrální analýzy na každém rádiu • Pracovní teplota 0-50°C • AP musí být schopno volit vysílací kanál na základě scanu na pozadí, prediktivně na základě reálné kapacity každého kanálu, kombinací obou technologií a manuálně • AP musí podporovat BandSteering klientů, kteří jsou schopni vysílat na 5GHz pásmech • Bezpečnost: WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i, 802.1x • AP musí podporovat systém bezešvého roamingu klientů mezi jednotlivými rádii a AP a to i včetně propagace standardů 802.11k a 802.11r • AP musí podporovat systém AirtimeFairness (férové rozdělení a ochrana média před monopolizací staršími a pomalejšími klienty - 802.11b/g/a) • AP musí podporovat inteligentní systém bezdrátového MESH propojení mezi AP v případě nemožnosti rozvedení konektivity pomocí kabeláže • AP musí mít fyzickou ochranu proti zcizení z montážního kitu • Montážní kit pro instalaci na strop/zed'/kazetový podhled musí být součástí balení • Podpora unikátních PSK klíčů v rámci SSID • Mapování přístupových práv/prioritizace/rychlosti/VLAN dle přiděleného unikátního PSK klíče • Mapování unikátní PSK klíčů či doménových uživatelských účtů na definovanou roli uživatele a s ní související VLAN tag a další práva • AP musí být schopno konvertovat multicastové vysílání do unicastového a řádně jej prioritizovat • Podpora QoS prioritizace, rozpoznávání markovaného traffiqu dle ToS, samo markovat provoz, řadit jej do fronty v rámci domény AP a řádně jej prioritizovat dle definované politiky (802.1p) • AP musí být schopno rozpoznávat typy klientských zařízení za účelem rozřazování v rámci definované BYOD politiky • AP musí podporovat a být schopné propagovat službu BonjourGateway • L2 izolace klientů • Možnost vypnutí LED diod • Vzdálené zachytávání paketů • AP musí být schopno pracovat samostatně jako router s podporou NAT a DHCP, samo může být kontrolérem pro omezenou skupinu dalších AP, začleněno pod HW kontrolér, začleněno pod cloud kontrolér 	
HW kontrolér pro AP	<ul style="list-style-type: none"> • kontrolér musí být dodán jako samostatné HW zařízení určené pouze pro provoz Wi-Fi sítě. • kapacita řízení až 75 AP (je požadováno licenční pokrytí a podpora až pro 25 AP na do min. 5 let) • licenční inkrement po 1 AP • kontrolér nesmí být implicitně cestou pro uživatelská data generovaná na přístupových bodech, vše se musí forwardovat lokálně z AP na nejbližší výchozí bránu • kontrolér musí podporovat i režim tunelování provozu jednotlivých WLAN na sebe, kapacita musí být minimálně 200Mb/s • kontrolér musí podporovat režim vysoké dostupnosti (HA režim), alespoň v režimu active-passive (1+1 box) • při HA režimu musí být cluster kontrolérů dostupný pod jednou management IP adresou • kontrolér musí podporovat mapování VLAN tagů na jednotlivé WLAN profily (802.1q) • AP a kontrolér musí být schopný vzájemné komunikace, i když budou v jiné 	1

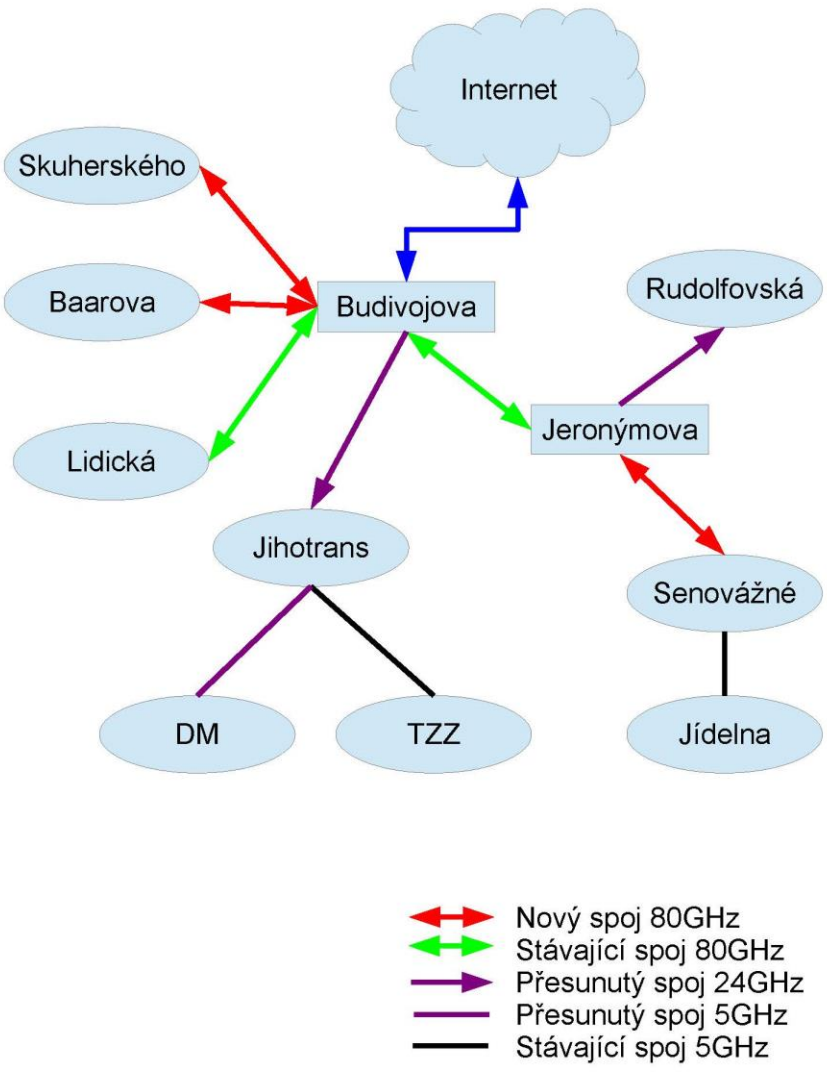
Popis a technická specifikace kompletního vybavení pro síťovou infrastrukturu školy (dodávka v rámci projektu z IROPu s názvem „Škola pro 4. průmyslovou revoluci“) reg. číslo: CZ.06.2.67/0.0/0.0/16_050/0002521		
Druh zařízení	specifikace	počet jednotek
tyto parametry musí produkt splňovat		
	<p>IP síti či VLAN</p> <ul style="list-style-type: none"> • kontrolér musí podporovat integraci jak vnitřních tak venkovních AP stejného výrobce • kontrolér prostřednictvím AP musí umět skenovat rádiové prostředí na cizí, potenciálně škodlivé, přístupové body (tzv. rogue AP), umět je klasifikovat (výrobce, detaily vysílání), zobrazit jejich přibližnou polohu na mapě podlaží, automaticky tento stav logovat a reportovat jej administrátorovi • AP síť poblíž nepřátelskému AP (rogue AP) musí umět vysílat deautentizační rámce s podvrženou zdrojovou MAC na klienty, kteří jsou již asociováni na nepřátelské AP vysílající např. na stejném SSID (SSID spoofing) • kontrolér musí nabídnout základní integrovaný captive portál pro odbavování hostovského přístupu • kontrolér musí nabídnout jednoduchý webový portál umožňující personálu generování přístupových účtů hostům včetně správy uživatelů a možnosti hromadného generování • kontrolér a celý systém musí podporovat funkce Walled Garden, HTTP(s) Get, HTTP(s) redirect, WISPr, RADIUS Proxy a SocialLogin za účelem integrace externího portálového řešení a být kompatibilní s následujícími komerčními řešeními LinkiFi, SociF, Maxifi, PurpleWiFi, Cloud4Wi • kontrolér musí podporovat autentizaci dle 802.1x s externími databázemi (např. AD, RADIUS, LDAP) či mít lokální databázi uživatelských účtů • kontrolér musí podporovat a umět řídit "Role Based Access Control" tj. možnost definovat jednotlivé typy uživatelských profilů (VLAN, práva pro přístup, šířka pásma, prioritizace) a tyto vytvořené politiky musí automaticky vynucovat na přihlašovaných klientech po jejich ověření • systém musí podporovat generování privátních WPA/WPA2-PSK klíčů pro každého uživatele i ve stejném SSID • systém musí být schopen párovat uživatelský účet (např. z RADIUS) na privátní PSK klíč a eliminovat tím nutnost nasazení 802.1x • systém musí automaticky rozpoznávat operační systém název a typ koncových zařízení za účelem zařazení jich do správné předem definované politiky • systém musí podporovat automatické generování skriptů pro přidání zabezpečeného WLAN profilu do konkrétního typu koncového zařízení • systém musí umět spolupracovat se systémy indoorwifi lokalizace • management systému musí být dostupný přes zabezpečený HTTPS webový přístup či SSH • kontrolér musí podporovat SNMPv3 a přeposílání detailních logů na externí Syslog server • je požadovaná podpora na dobu min. 5 let • Požadované práce: <ul style="list-style-type: none"> ○ Proměření umístění a instalace a konfigurace AP. ○ Montáž a konfigurace řídicího kontroléru (práce provede certifikovaný pracovník na dodaný typ zařízení). ○ Konfigurace SSID a přístupových oprávnění ○ Konfigurace black, white listů ○ Zpracování závěrečného protokolu měření pokrytí signálu včetně zakreslení do půdorysů budov. ○ Zaškolení základní obsluhy dodané technologie v rozsahu 6 hodin, zadavatel požaduje možnost zdarma upravit konfiguraci po předání systému do provozu v rozsahu 20 hodin – v období následujících 6 měsíců. 	

Popis a technická specifikace kompletního vybavení pro síťovou infrastrukturu školy (dodávka v rámci projektu z IROPu s názvem „Škola pro 4. průmyslovou revoluci“) reg. číslo: CZ.06.2.67/0.0/0.0/16_050/0002521		
Druh zařízení	specifikace	počet jednotek
tyto parametry musí produkt splňovat		
Spoj pro propojení budov školy v MAN typ A	<ul style="list-style-type: none"> • Režim komunikace: full duplex, min.1 150Mbit/s pro každý směr současně • MTU: min. 10240 byte • Napájení: 48 V, ochrana proti přepětí podle normy ČSN 334010 • Latence: < 12μs • Dostupnost: 99,99 % • Rozhraní: 2x Ethernet 1 GB • Anténa: 0,35 m • Vzdálenost antén: min. 2,1 km • Další požadavky: <ul style="list-style-type: none"> • Možnost rozšíření o optické rozhraní. • Oddělené na dva samostatné datové toky. • Jednotný síťový dohled 100% kompatibilní s již používanou technologií, služební kanál, SNMP (referenční zařízení Alcoma AL80LP) • Všechny dostupné protokoly bez omezení, VLAN. • Možnost šifrování datového provozu. • QoS, FEC, Interleaving • Integrovaný L2 switch. • Venkovní použití. • Dodávka včetně zdroje. • Záruka: min. 60 měsíců s garantovanou opravou do 4 hodin 	2
Spoj pro propojení budov školy v MAN typ B	<ul style="list-style-type: none"> • Režim komunikace: full duplex, min.1 150Mbit/s pro každý směr současně • MTU: min. 10 240 byte • Napájení: 48 V, ochrana proti přepětí podle normy ČSN 334010 • Latence: < 12μs • Dostupnost: 99,99 % • Rozhraní: 2x Ethernet 1 GB • Anténa: 0,65 m • Minimální vzdálenost antén: min. 3,5 km • Další požadavky: <ul style="list-style-type: none"> • Možnost rozšíření o optické rozhraní. • Oddělené na dva samostatné datové toky. • Jednotný síťový dohled 100% kompatibilní s již používanou technologií, služební kanál, SNMP (referenční zařízení Alcoma AL80HP) • Všechny dostupné protokoly bez omezení, VLAN. • Možnost šifrování datového provozu. • Integrovaný L2 switch. • QoS, FEC, Interleaving • Venkovní použití. • Dodávka včetně zdroje. • Záruka: min. 60 měsíců s garantovanou opravou do 4 hodin 	1
Požadované práce pro spoje	<ul style="list-style-type: none"> • Odstrojení původních spojů ze stožárů (dodavatel si zajistí potřebná povolení pro manipulaci na stožárech včetně prokázání příslušného oprávnění pro práci ve výškách u min. dvou pracovníků dodavatele – dodavatel doloží formou čestného prohlášení). • Instalace, konfigurace a zprovoznění nových spojů (práce provede certifikovaný pracovník na dodaný typ zařízení). U jednoho spoje bude nutné vybudovat retranslační bod a zajistit jeho provoz na dobu min. pěti let. • Přemístění, instalace a zprovoznění původních tří spojů na nové lokace. • Provedení domíření spojů. • Informace o všech připojených místech sítě je součástí přílohy. 	

Popis a technická specifikace kompletního vybavení pro síťovou infrastrukturu školy

(dodávka v rámci projektu z IROPu s názvem „Škola pro 4. průmyslovou revoluci“)

reg. číslo: CZ.06.2.67/0.0/0.0/16_050/0002521

Druh zařízení	specifikace	počet jednotek
tyto parametry musí produkt splňovat		
<p>Schéma nového zapojení sítě</p>  <p>Legend:</p> <ul style="list-style-type: none"> ↔ Nový spoj 80GHz ↔ Stávající spoj 80GHz → Přesunutý spoj 24GHz — Přesunutý spoj 5GHz — Stávající spoj 5GHz 		

Bc. Jan Šindelář, ředitel školy