



EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program



MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR

MARKETINGOVÝ PRŮZKUM KONEKTIVITY ŠKOL – ZŠ Skálova

Program:

Integrovaný regionální operační program (IROP)

Prioritní osa:

2 Zkvalitnění veřejných služeb a podmínek života pro obyvatele regionů

Specifický cíl:

2.4 Zvýšení kvality a dostupnosti infrastruktury pro vzdělávání a celoživotní učení

Investor průzkumu:

Město Turnov

Antonína Dvořáka 335, Turnov

Zpracovatel:

AutoCont CZ a.s., Hornopolní 3322/34, 702 00 Ostrava - Moravská Ostrava



1 ÚČEL ZPRACOVÁNÍ MARKETINGOVÉHO PRŮZKUMU

Tento marketingový průzkum je zpracován jako podklad pro tvorbu studií proveditelnosti k žádosti o podporu z Integrovaného regionálního operačního programu na projekt „Modernizace učeben a konektivity tří základních škol v Turnově“. Žádost je podávána v rámci 46. kola výzvy IROP, prioritní osy 2, specifického cíle 2.4.

Informace z marketingového průzkumu budou především použity jako vstupy pro vypracování finančních částí studií proveditelnosti.

Studie proveditelnosti jsou zpracovány, aby:

- popsaly záměr vybudování konektivity školy tak, aby odpovídala jednak současným kvalitativním i bezpečnostním standardům, dále pak aby byla v souladu s přílohou Specifických pravidel pro žadatele č. 9 Standard konektivity škol
- prokázaly, že pro samotné projekty byly vybrány ekonomicky nejvýhodnější varianty,
- prokázaly udržitelnost projektu a schopnosti jeho financování po ukončení finanční podpory ze strukturálních fondů
- prokázaly reálnost plánovaných rozpočtů
- prokázaly opodstatněnosti jednotlivých způsobilých výdajů co do druhu a velikosti.

2 ROZSAH MARKETINGOVÉHO PRŮZKUMU

Dokument popisuje průzkum na základní škole.

Základní škola Turnov, Skálova 600, příspěvková organizace

Skálova 600

Turnov 511 01

ředitel Mgr. Michal Loukota

IČ: 00854794

IZO: 102454027

REDIZO: 600099369

Investor bude podávat žádost o dotaci na modernizaci několika základních škol a pro každou z nich vzniká samostatný marketingový průzkum konektivity. Tento pak bude podkladem pro zpracování studie proveditelnosti k žádosti o dotaci. V rámci snahy získat v průzkumu co nejvíce relevantní údaje a reálnou odezvu z trhu, je průzkum zvolen tak, aby zatížil dotazovaný komerční sektor co nejmenším počtem dotazů a získal tak informace pro všechny subjekty.

Následující tabulka identifikuje množství v jednotlivých oblastech řešení jednotlivě po školách. Za každou oblast je pak množství zprůměrováno a hodnota průměru je pak použita ve vzorovém kalkulačním formuláři, který je přílohou průzkumu a je požadováno jeho vyplnění od jeho účastníků.

3 SEZNAM POŽADAVKŮ VÝZVY

Požadavek	Povinný/Volitelný	Splněno čím	Poznámka
WAN			
<ul style="list-style-type: none"> šíře pásma (bandwidth) odpovídající 128kbps/student^[1] nebo 512kbps/počítač^[2] nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů^[3] 	Povinný	ISP	
<ul style="list-style-type: none"> symetrické připojení bez agregace a omezení (FUP) 	Povinný	ISP	
<ul style="list-style-type: none"> vlastní nebo poskytovatelem přidělené veřejné IPv4 i IPv6 adresy 	Povinný	ISP	
<ul style="list-style-type: none"> plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack) 	Povinný	ISP	
<ul style="list-style-type: none"> validující DNSSEC resolver na straně školy 	Povinný	DNSSEC resolver	virtuální appliance/služba serveru
<ul style="list-style-type: none"> podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení 	Povinný	UTM	
<ul style="list-style-type: none"> logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.) 	Povinný	UTM/LAN a její přístupová vrstva .1x	
<ul style="list-style-type: none"> sítové zařízení podporující rate limiting, antispoofing, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality 	Povinný	UTM	
<ul style="list-style-type: none"> 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 	Povinný	UTM	
<ul style="list-style-type: none"> možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků 	Povinný	UTM	
<ul style="list-style-type: none"> podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online 	Povinný	ISP/registrátor domény/ hostingu	
<ul style="list-style-type: none"> zapojení poskytovatele připojení v bezpečnostním projektu FENIX resp. veřejné adresy využívané školou jsou zapojeny do infrastruktury FENIX^[4] nebo ISP splňuje alespoň technické standardy definované projektem FENIX – viz. http://nix.cz/cs/file/NIX_PRAVIDLA_FENIX 	Povinný	ISP	
<ul style="list-style-type: none"> u software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu. 	Povinný	obecné	Tyká se všech SW
LAN			

· 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	Povinný	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. sítovým službám.	Povinný	SRV+MS AD	
· logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel	Povinný	SRV+MS AD	
V oblasti pevné LAN musí projekt splňovat následující minimální parametry:			
· Minimální konektivita stanic a dalších koncových zařízení zařízení 100Mbit/s fullduplex	Povinný		
· Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,...)	Povinný		
· Minimální konektivita serverů, aktivních sítových prvků, bezpečnostních zařízení, NAS 1Gbit/s fullduplex	Povinný		
· Páteřní rozvody mezi budovami v areálu realizovaný prostřednictvím optických nebo metalických vláken	Povinný		
Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3)[1] s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,...	Povinný		
V případě řešení bezdrátových sítí (wifi) pak musí projekt naplňovat následující minimální parametry:			
· Podpora mechanismu izolace klientů	Povinný		
· 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	Povinný		
· 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)	Povinný		

· Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD ...)	Povinný		
· Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz	Povinný		
· Minimálně pasivní zapojení ^[2] do federovaného systému eduroam (www.eduroam.cz). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů.	Povinný		
· Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu	Povinný		

4 OBSAH MARKETINGOVÉHO PRŮZKUMU

V rámci průzkumu jsou poptávány prvky a jejich instalace a implementace v následujících oblastech:

WAN konektivita
UTM řešení
Server
OS Serveru
Terminálové licence
DNSSEC resolver
Log Management (Syslog)
NAS
Externí HDD - USB
UPS
Zapojení do Eduroam
Zapracování ICT do rádu školy
Integrace s prostředím školy+support prostředí
LAN konektivita
Přepínač - 48 port
Přepínač - 8 port
Wifi - Basic AP
NetFlow
Racková skříň
Vybavení učeben
Stolní počítače

Dále pak jejich provozní náklady po dobu udržitelnosti projektu, tedy 5let.

Konkrétní technologické požadavky na jednotlivé oblasti poptávky jsou definovány v následující kapitole.

5 PODROBNÝ POPIS POPTÁVANÝCH OBLASTÍ

5.1 UTM řešení

V rámci projektu bude pořízen a nasazen firewall jako bezpečná brána připojující celou organizaci k Internetu resp. ke konektivitě poskytovatele s využitím technologie **NAT dle RFC 2663**. Firewall bude zajišťovat oddělení vnitřního a vnějšího provozu na základě tzv. zón a mezi nimi postavených komunikačních pravidel (**ACL/xACL**), tzv. politiky.

Bude muset plně podporovat dual-stack (IPv4 a IPv6 provoz), měl by umožnit budoucí rozšíření do vysoké dostupnosti (tzv. HA) min. v režimu min. Active/Pasive a vybaven bude (vč. potřebné sady licencí) tzv. next-gen funkcemi vč. komplexní sady pro unified-threat-management (UTM). Bezpečný firewall muset být schopen blokovat nejčastější útoky typu odepření služby (DoS) a také účinně blokovat podvržení adresy (**spoofing**).

Firewall umožní zosobnění vlastních studentů a zaměstnanců organizace s aktivním napojením na účty v doméně adresářové služby, tak aby byla na firewallu neustále k dispozici aktuální vazba uživatel-IP adresa, případně zdrojový rozsah portů. Politika firewallu a její jednotlivé role budou umožňovat pohodlnou práci s AD účty i skupinami namísto IP adres a to ve všech úrovních, tedy vč. kategorizace a filtrace provozu. Role politiky musejí být schopné pracovat s těmito objekty – IP/subnet, uživatel/skupina, typ zařízení/operační systém.

Pro splnění požadavku Standardu konektivity škol na logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.) bude napojení firewallu na adresářovou službu realizováno formou instalace softwarového agenta na doménové kontroléry. Agent zpravidla nejen vyčítá statické informace o skupinách a účtech v LDAP adresáři, ale periodicky čerpá informace o aktuálně přihlášených uživatelských účtech ze security-events logu samotných doménových řadičů (AD DC) a neustále ověruje trvalost vazby IP-uživatel.

Firewall bude schopen zajistit omezení šířky pásma (tzv. **rate limiting**) pro ty druhý komunikací a protokolů zvolených ve vybraných komunikačních pravidlech politiky firewallu, třeba že jen pro vybrané skupiny vnitřních uživatelů. Firewall tedy musí umožnit rychlostní omezení určených komunikací, ale zároveň by měl být schopen některé jiné druhy komunikace naopak prioritizovat na úkor jiných.

- **Kontrola webového provozu** nešifrovaného i šifrovaného (protokoly **http** a **https**) je mandatorním požadavkem Standardu konektivity škol a firewall ji musí umožňovat spolu s další UTM funkcionalitou. Uvažovaný firewall umožní provádět shodně inspekci šifrovaných (SSL) spojení vybraných protokolů i jejich nešifrovaných verzí – minimálně protokoly HTTPS, SMTPS, POP3S, IMAPS, FTPS a inspekce na jejich výchozích portech. Pokud bude předkládán certifikát firewallem, musí být platný a důvěryhodný min. ve vnitřní síti.

- **Kategorizace a selekce obsahu** bude odlišná v závislosti na uživatelské skupině – požadované budou minimálně dva profily – **žák (student) a učitel**. V obou případech bude kategorizace a selekce prováděna na základě kategorií automaticky aktualizovaných v rámci aktualizace UTM. Veškerá varování uživatele v souvislosti s kontrolou obsahu musí být v českém jazyce a formou zobrazené náhradní webové stránky (např. s upozorněním na pravidla využívání ICT a vysvětlení důvodu blokování). K dispozici musí být možnost přesměrování uživatele na původní požadovanou stránku po stanovené době. V případě chybné blokace musí mít uživatel možnost požádat pohodlnou formou o uvolnění, resp. změnu kategorie stránky. Kategorizace a selekce obsahu bude prováděna i pro šifrovanou (**https, SSL**) verzi http protokolu.
- **Identifikace útoků a IPS** bude dalším bezpečnostním prvkem pořízeného next-gen firewallu. Ochrana proti průniku (IPS) pracuje podobně jako antivirus na základě definic připravených výrobcem. Definice mají výrobcem nastavenu zároveň i defaultní akci, jak s identifikovaným vzorcem komunikace naložit (min. blokace, monitorování, reset). Ve většině případů jsou výchozí akce plně vyhovující a lze se spolehnout na výrobce, resp. jeho bezpečnostní laboratoře, že v definicích použité výchozí akce jsou pravidelně revidovány stejně jako jejich další rozšiřování o nově identifikované hrozby vč. jejich případné blokace. Zařazením profilů IPS do vybraných v komunikačních pravidlech firewallu bude zajištěna **automatická blokace identifikovaného útoku** bez nutnosti zásahu správce. Firewallem zaznamenané útoky nebo jim podobné nežádoucí komunikace se mohou dále odrazit v rekonfiguraci pravidel firewallu popřípadě ve filtračních (ACL) pravidlech na páteřním L3 přepínači, to však již bude vyžadovat manuální zásah. Rekonfigurace pravidel lze snadno provádět v intuitivním grafickém rozhraní zařízení.
- **Antivirová kontrola**, prováděná firewallem, musí umožnit konfiguraci minimálně dvou úrovní hloubky kontroly/rychlosti a vytvoření tzv. profilů, které bude možno dle potřeby uplatnit v jednotlivých komunikačních pravidlech firewallu, dle druhu a povahy konkrétního pravidla. Antivirová kontrola bude aplikována i na šifrovaná spojení (**https, SSL**). Infikované soubory musí být možno odstranit či zablokovat.
- **Vzdálený přístup** formou zabezpečeného tunelu skrze internet bude sloužit především zaměstnancům k jejich práci z místa mimo školu a dodavatelům IT služeb. Zaměstnanci by neměli být omezováni technologicky, firewall musí umožnit vytvoření tunelu zabezpečeného protokolem SSL nejlépe na výchozím portu tcp/443 a musí být k dispozici multiplatformní klientská aplikace nebo lépe, nativní (reverse proxy) přístup skrze webový portál firewallu a jeho aplikace (SMB, RDP, SSH, HTTPS apod.). Konfigurace VPN musí být provedena tak, aby bylo možné bezpečně ověřovat uživatelské účty v adresářové službě a autorizovat je pro přístup na základě členství ve skupině adresářové služby. K tomuto účelu může být využit standardní RADIUS protokol nebo zabezpečený LDAP. Obojí může být konfigurováno jako role interního serveru, ovšem s důrazem na redundanci. Ověřování musí být konfigurováno proti dvěma nezávislým serverům, nehledě na použitý protokol. K zabezpečení SSL komunikace (VPN) musí být pořízen a na firewallu instalován a konfigurován certifikát (nejlépe typu wildcard) vystavený některou veřejnou a důvěryhodnou certifikační autoritou (root CA), tak aby byl na straně uživatele považován za validní a platný. Certifikát výrobce nebo vystavený

pomocí interní CA organizace nemůže být považován za dostatečný pro tento účel. Certifikát bude též použit pro zabezpečení publikovaných služeb školy (např. webového portálu školského informačního systému).

Bezpečné publikace bude zajištěno funkcionality tzv. reverzní proxy firewallu společně s inspekcí provozu – přístupu k těmto službám.

UTM řešení

Počet síťových rozhraní copper, RJ45 10/100/1000 - min 16x
Podpora LACP 802.3ad na min. 4 portech
Počet SFP: 2 x GbE SFP
Výkonnost FW nezávislá na velikosti paketu
Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 2.8 Gbps
Propustnost FW paketů za sekundu - min. 4 Mpps
Latence firewallu (64 B UDP paket) - max 3 mikro sec
Počet naráz otevřených spojení - min 2 M
Počet nových spojení za sekundu - min. 70 k
Propustnost IPSEC VPN (512 B paket) - min. 1.1 Gbps
Propustnost SSL VPN min 400 Mbps
Propustnost IPS - min 1.7 Gbps
Propustnost AV - min. 330 Mbps
Podpora virtuallizace (min 10 virtuálních kontextů)
Podpora funkce bezdrátový kontrolér - 128 AP
Režim vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky mezi nody v clusteru
Režim fungování L2 – transparentní režim, L3 – NAT/Router
Podpora multicast, vytváření politiky pro multicast routování
Podpora VPN: SSL (portálový režim, tunelový režim), IPSEC (IKE, manual key, certifikát, gateway to gateway, hub and spoke, dial up konfigurace, internet browsing konfigurace, podpora více tunelů – redundantní VPN, možnost VPN v L2 – transparentním režimu, podpora IPv6, podpora dynamických routovacích protokolů - OSPF, PPTP, L2TP, GRE

5.2 Server

Server

Rackové provedení včetně ližin do racku
64-bit architektura, 2x procesor - kmitočet minimálně 2,6GHz/4Core/8MB Cache, velikost RAM min 96 GB
kmitočet RAM min. 2400 MHz
pokročilá kontrola chyb a oprava paměti (ECC) a memory mirroringu
rozšiřitelnost až na minimálně 8 HDD ve výšce max 4U.
osazen řadičem disků o velikosti zálohované cache min. 2GB s podporou min. Raid1, Raid5
osazen min. 2ks HDD systémových s rozhraním SAS a velikostí min 300 GB, 15 K RPM a min. 4ks HDD SAS a velikostí min 1,2TB 10K RPM
konektor pro interní USB klíč či SD kartu na základní desce serveru osazenou min 2x 8GB mediem
možnost rozšíření až na 3x PCIe 3.0 slot
minimálně 6x 1Gb ethernet portů, možnost rozšíření o 2x 10Gb port
redundantní hot-swap chlazení a napájení

redundantní napájení, za chodu vyměnitelné zdroje min. 490W
USB nebo SD paměťové médium pro instalaci a provozování virtualizačního hypervizoru
predikce chyby na všech kritických komponentech - Procesory, RAM, HDD, zdroje,
ventilátory
samostatný LAN port pro management s možností o rozšíření o licenci pro management
SW, který musí podporovat technologii Remote KVM, možnost zapínat a vypínat server,
virtuálně připojovat lokální média
Certifikát potvrzující možnost nasazení nabízené virtualizačních řešení
Záruka 5 let následující pracovní den na místě instalace

5.3 OS Serveru

Pro potřeby školy je vyžadován MS Server 2019 pořízený v licenčním plánu EDU. Serverové licence budou provozovány na v vhodném Hypervizoru – doporučen VmWare VMWare vSphere 6 Essentials. Pro všechny role a budoucí rozvoj je požadováno min 8 licencí pro virtuální stroje.

5.4 Terminálové licence

Pro potřeby škol je vyžadován RDS CAL typu „Device“ - WinRmtDsktpSrvcsCAL 2019 pořízený v licenčním plánu EDU. Budou využívány pro vzdálený přístup vyučujících.

5.5 Klientské licence

Školy nejsou členy žádného licenčního programu pro školství, je tedy nutné zalicencovat všechny uživatele kteří budou využívat systémovou infrastrukturu. Kontrola a logování je prováděno oproti ActiveDirectory (AD), tedy je třeba aby databáze žáků, učitelů a dalších uživatelů infrastruktury byla kompletně zavedena a zalicencována. Pro školu ZŠ Skálova je stanoven počet klientských licencí na 630 ks, počet zařízení pak na 130 ks.

5.6 DNSSEC

DNSSEC resolver

Řešení musí zajistit bezpečný překlad DNS jmen na IP pro veškerá uvnitř připojená zařízení a to, vzhledem k vyžadovanému dual-stacku, shodně pro obě verze IP protokolu. Bezpečným překladem se rozumí DNS server(y) uvnitř organizace, který bude schopen ověřovat za pomoci DNSSEC podpisy dotazovaných zón resp. hash podpisy jednotlivých záznamů jako odpověď na DNS dotazy vnitřních zařízení. Podstatné je, že musí být zajištěny překlady i pro dosud nepodepsané externí domény, zóny. DNSSEC kontroly (tzv. validace) budou probíhat výhradně na DNS resolveru, tak aby nebyla nutná jakákoliv úprava konfigurace vnitřních klientů. Validující DNSSEC resolver bude konfigurován tak, aby se sám dotazoval výhradně tzv. ROOT serverů nebo důvěryhodných DNSSEC serverů, které bude zároveň používat jako tzv. Trust Anchors. V rámci projektu bude validující DNSSEC resolver konfigurován jako funkční rozšíření nově instalovaných DNS server rolí v rámci nově pořízených operačních systémů.

5.7 Log Management (Syslog)

Log Management (Syslog)

Příjem zpráv minimálně protokoly SNMP (traps) a SYSLOG.
Schopnost přejímat události systému Windows serverů (tzv. EventLog),
min. bezpečnostního charakteru (EventLog Security a EventLog System)
Schopnost přijaté zprávy automaticky rozdělovat pro budoucí vyhledávání min. do
kategorií čas, datum, hostname, IP
Včasné a automatické notifikace min. jako email.

5.8 NAS

NAS + 2x TB HDD

CPU minimálně DualCore 1,4Ghz
RAM minimálně 1GB DDR3
min. prostor pro 4x HotSwap HDD 3.5"/2.5" SATA III/II x 2
Osazeny minimálně 2xHDD každý s kapacitou 4TB
Minimálně 2x USB 3.0 porty
Minimálně 1x LAN port v provedení 100/1000 Base-T.
Podporované síťové protokoly: CIFS, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet,
SSH, SNMP
Adresářové služby: Integrace s MS AD a LDAP
Řízení přístupu pomocí ACL
Podporované typy RAID: JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10

5.9 Externí HDD

USB externí HDD

kapacita: 4 TB
rozhraní USB 3.0 (5Gb/s; možno připojit na stávající USB 2.0)
nevýžaduje napájecí zdroj (s výjimkou některých starších notebooků s USB 1.1)

5.10 UPS

UPS

Provedení do racku, max. 2U, včetně montážního materiálu (kolejnic)
Jmenovité napětí 230 V, jednofázová na vstupu i výstupu
Výkon (VA/W): 1980W / 2200 VA
Technologie: Line- interactive
Doba běhu na baterie min. 10 min při 50% zátěži
Vestavěný úplný systémový autotest, možnost automatického plánovaného provádění
Výstupy: Min. 4 zásuvky IEC C13 s měřením spotřeby
Síťové (LAN) rozhraní s konektorem RJ45 a monitoringem okolního prostředí (teplota).
Podpora pro Windows server v aktuální verzi a hypervizor VmWare

5.11 Zapojení do EDUROAM

Zapojení do Eduroam

Federovaný systém EDUROAM (www.eduroam.cz) umožňuje přistupovat k sítím subjektů zapojených v systému a prostřednictvím těchto sítí k dalším službám, typicky k Internetu. Federace umožňuje ověření uživatele v libovolné zapojené síti (v České republice i zahraničí) pomocí uživatelské jediné (domácí) identity. Technickým správcem systému EDUROAM je společnost Cesnet.

V rámci projektu bude konfigurováno připojení zajišťující přístup (wifi SSID) do EDUROAM pouze pasivním způsobem – externím studentům a pracovníkům, jejichž mateřská organizace je zapojena do federovaného systému Eduroam, bude umožněno, na základě pozitivního ověření jejich identity, neblokovaný přístup k síti Internet skrze prostředky a konektivitu školy. Vlastní uživatelé budou k síti Internet přistupovat stejnou nebo jinou cestou (např. jiným ssid). Zprostředkování ověřování identit a žádostí o přístup pomocí protokolu radius bude zajišťovat lokální Network Policy Server (NPS - standardní role Windows serveru), který bude dotaz na ověření externího uživatele, dle uvedeného realm rozlišení, směrovat na národní autentizační servery správce této federace Eduroam. Jelikož NPS (ver. 2012) nedisponeje šifrovaným komunikačním radius protokolem – RadSec, bude nutné veškerou komunikaci mezi lokálním radius serverem a národním autentizačním serverem(ry) šifrovat jinou technikou. Správce federace umožňuje variantně použití šifrovaného spojení na bázi IPSec tunelu zajištěného certifikátem. Certifikát by měl být tzv. veřejně důvěryhodný, případně jiný po dohodě s protistranou, viz:
<http://www.eduroam.cz/cs/spravce/pripojovani/ipsec/uvod>. Tunel může být zakončen až na NPS serveru. Přiřazení vlan ID pro účely Eduroam bude manuálně konfigurované na zařízeních pro přístup, vzhledem k omezením NPS serveru v tomto módu práce. Variantně lze také uvažovat o použití RadSec Proxy. Současně s konfigurací budou realizovány další netechnické požadavky pro provoz EDUROAM – např. vytvoření informační webové stránky, zajištění technického kontaktu apod. Technickým kontaktem může být i dodavatelská organizace mající ke škole doložitelný vztah – dodavatel.

5.12 Integrace s prostředím školy a support prostředí

Integrace s prostředím školy+support prostředí

Aktuálně je na škole heterogenní prostředí – provozovány jsou systémy MS server, na dodaném HW v rámci Internetu do škol+ na operačních systémech Windows 2008. Některé elektronické systémy (pošta) využívají cloudových služeb Cílem projektu je i konsolidace dat a možnost vyřazená zastaralých serverových systémů.

V rámci projektu bude zajištěna příprava veškerého dodávaného hardware, do níž mimo jiné spadá kompletace a aktualizace (firmware) veškerých komponent. Součástí integrace je nutné zároveň uvažovat nutné montážní práce a oživení hardware v určených prostorách školy v momentě jeho dodání a spolu s tím návazné práce s připojením systémů k síti.

V rámci instalace serveru budou provedeny následující práce:

Instalace a konfigurace operačního systému samotné virtualizace – hypervizoru.

Instalace a konfigurace operačních systémů virtualizovaných serverů.

Instalace a konfigurace jednotlivých serverových rolí.

Integrace s MS AD doménou organizace.

Propagace nových komponent v síti.

Po dodavateli bude vyžadováno, aby zajistil expertní podporu veškerých dodávaných komponent svého řešení, shodně pro hardware i software a po dobu trvání doby udržitelnosti projektu.

Podpora bude zahrnovat:

- reakci na nahlášené incidenty
- řešení nahlášených chybových stavů dodaného řešení
- řešení závad na dodaných zařízeních
- měsíční reporting o provedených krocích a plnění SLA

5.13 Zpracování ICT do řádu školy

Zpracování ICT do řádu školy

Pro zajištění bezpečnosti provozu, optimálního využívání ICT prostředků budou v rámci projektu zpracovány Zásady využívání ICT a přístupu k síti a budou zařazeny do souboru vnitřních předpisů školy

5.14 Přepínač – 48 portů

Přepínač - 48 portů

L2 přepínač

fixní konfigurace, 1RU

48x 100/1000 RJ45 PoE+

2xSFP nezávislé

Wirespeed (neblokující) na všech portech

Podpora "jumbo rámců" do velikosti 9k

Energeticky efektivní ethernet dle 802.3az

Podpora PoE+ dle standardu 802.3at
IEEE 802.3ad
Podpora rozkládání zátěže na LACP dle L2,L3
Minimální počet linek v jedné LACP skupině: 4
GARP VLAN registration protokol
IEEE 802.1Q
Minimální počet aktivních VLAN: 256
Minimální počet záznamů v MAC adres tabulce: 16000
Podpora MAC based VLAN
IEEE 802.1s - Multiple spanning tree
IEEE 802.1w - Rapid spanning Tree
IEEE 802.1p - Minimální počet front : 4
LLDP a LLDP-MED
DHCP klient
SFlow dle RFC3716
IGMP v2 a v3
MLD v1 a v2
BPDU guard
Root guard
Podpora ochrany proti zahlcení (broadcast/multicast/unicast storm control) nastavitelná na procentuální rychlosť portu a množství paketů za vteřinu
Podpora ověřování 802.1X
Podpora zařazování do VLAN na základě 802.1X ověření
Podpora mac-based ověřování
Sériová nebo USB konzolová linka
CLI
SSHv2
SNMP
RMON
Dual flash image
Podpora Radius
Podpora TACACS+
Podpora zrcadlení portů (SPAN)
NTP klient
Podpora managementu přes IPv4 i IPv6
Plná záruka na HW v délce 60měsíců s výměnou následující pracovní den garantovaná výrobcem zařízení
SW aktualizace po dobu 5 let

5.15 Přepínač – 24 portů

Přepínač - 24 port

L2 přepínač
fixní konfigurace, 1RU
8x 100/1000 RJ45 PoE+
2x Combo 1000Base-T/ SFP
Wirespeed (neblokující) na všech portech
Podpora "jumbo rámců" do velikosti 9k
Energeticky efektivní ethernet dle 802.3az
Podpora PoE+ dle standardu 802.3at

IEEE 802.3ad

Podpora rozkládání zátěže na LACP dle L2,L3

Minimální počet linek v jedné LACP skupině: 4

GARP VLAN registration protokol

IEEE 802.1Q

Minimální počet aktivních VLAN: 256

Minimální počet záznamů v MAC adres tabulce: 16000

Podpora MAC based VLAN

IEEE 802.1s - Multiple spanning tree

IEEE 802.1w - Rapid spanning Tree

IEEE 802.1p - Minimální počet front : 4

LLDP a LLDP-MED

DHCP klient

SFlow dle RFC3716

IGMP v2 a v3

MLD v1 a v2

BPDU guard

Root guard

Podpora ochrany proti zahlcení (broadcast/multicast/unicast storm control) nastavitelná na procentuální rychlosť portu a množství paketů za vteřinu

Podpora ověřování 802.1X

Podpora zařazování do VLAN na základě 802.1X ověření

Podpora mac-based ověřování

Sériová nebo USB konzolová linka

CLI

SSHv2

SNMP

RMON

Dual flash image

Podpora Radius

Podpora TACACS+

Podpora zrcadlení portů (SPAN)

NTP klient

Podpora managementu přes IPv4 i IPv6

Plná záruka na HW v délce 60měsíců s výměnou následující pracovní den garantovaná výrobcem zařízení

SW aktualizace po dobu 5 let

5.16 WIFI

Wifi

Ve škole bude zřízená nová, bezpečná WiFi infrastruktura s centrálním řízením, tak aby signál pokryl veškeré provozní prostory školy.

Podpora mechanismu izolace klientů

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)

Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD ...)

Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz

Podpora WPA2

standardizované PoE napájení

multi SSID - min. 4x

ACL pro filtrování provozu

5.17 NetFlow

NetFlow

Detailně monitorovat síťový provoz v reálném čase i umožnit získat přehled o síťové aktivitě v rámci specifikovaného časového období v minulosti (min. 60 dnů).

Získat přesné informace o veškeré síťové aktivitě – např. kdo (IP, hostname) komunikoval s kým (IP, hostname), kdy, kolik se přeneslo dat, pomocí které služby atd.

Umožní předcházet výpadkům a zahlcením sítě (vyhledání anomalií síťového provozu).

Zvýší bezpečnost síťového provozu, umožní odhalení vnějších i vnitřních útoků.

Sledovat aktivity uživatelů (IP, hostname) i aplikací (služeb), dohlížet nad využitím linek do Internetu.

Pomůže určit kritická místa sítě a optimalizovat její infrastrukturu (lepší plánování kapacit sítě, sledování trendů).

Architektura postavená na protokolech NetFlow/sFlow/IPFix

Grafické uživatelské rozhraní s možností filtrování a tvorby zájmových profilů, dle preference uživatele.

Forma virtuální appliance s podporou min. VMWare a MS HyperV

5.18 Racková skříň

Racková skříň

Pro bezpečnou instalaci nové techniky bude zřízena v místnosti kde jsou v současné době instalovány servery nová racková skříň se záložním zdrojem (UPS). A možností rozšíření zakončení kabeláže

Stojanový rozvaděč 42U (š)800x(h)1000

19' police A4 perforovaná 1U/650mm,max.80kg

Vent. horní(spodní) 4x ventilátor 220V/60W

19" Patch panel 3x 48 portů x RJ45 CAT6 UTP

19' vyvazovací panel 1U, háček velký 2x

Spotřební materiál včetně patch cordů

Současný rack pro síťový rozvod bude svěšen a použit pro případný rozvod LAN ve vhodném místě (učebna výpočetní techniky). Bližší viz obrazová dokumentace v příloze.

5.19 Stolní počítače

Stolní počítače

Pro běh plánovaných učeben (2 učebny) je třeba zajistit odpovídající učitelské počítače (2 ks) a žákovské počítače (2x 17ks)

Minimální doporučení konfigurace pro učitele (2 ks) : provedení MicroTower s min. 300W zdrojem s účinnosti 92%, výkon CPU min. 7200 bodů dle nezávislého testu benchmark.net, pevný disk s kapacitou min. 200 GB v provedení SSD, operační paměť min 8GB DDR3 DVD-RW optická mechanika, Gbit síťová karta, min. 1x digitální výstup DVI/DP/HDMI a 1x video výstup VGA, klávesnici a myš stejného výrobce, operační systém s podporu AD (domény), minimálně 3 roky záruky v místě instalace. Vhodný záložní zdroj s výkonem min 700VA, 2x monitor s viditelnou úhlopříčkou minimálně 27" s LED podsvícením formátem 16:9 a rozlišením 1920x1080 bodů. Vstupy DVI a VGA – 3 roky záruky v místě instalace

Minimální doporučená konfigurace žákovského PC (2x 17ks): provedení minitower s min. 150W zdrojem s účinnosti 85%, výkon CPU min. 3140 bodů dle nezávislého testu benchmark.net, pevný disk s kapacitou min 128 GB v provedení SSD, operační paměť min 4GB DDR3, DVD-RW optická mechanika, 1x Gbit síťová karta, min. 1x video výstup VGA a 1x DP, klávesnici a myš stejného výrobce, operační systém s podporu AD (ActiveDirectory). Min záruka 3 roky na místě instalace. Monitor s viditelnou úhlopříčkou min 20" LED podsvícením a formátem 16:9, rozlišení min 1600x900. Video vstup DVI a VGA – záruka 3 roky.

Všechny počítač budou vybaveny předinstalovaným softwarem včetně dodávky příslušných licencí - operační systém a školní trvalá licence MS Office.

5.20 Datová konektivita

Datová konektivita

Současné datové přípojky do Internetové sítě jsou ve správě lokální firmy a dle šetření není problém tyto navýšit na standardy vyžadované výzvou. Není očekávána vstupní investice pro navýšení, pouze při navýšení kapacity spojení dojde k (mírnému) zvýšení provozních nákladů na linky – bližší informace o cenách dodá poskytovatel datových služeb.

6 KALKULACE POPTÁVANÉHO ŘEŠENÍ

Při návštěvě školy a dle místního šetření je kalkulace rozdělena na investiční fázi, kdy je do ceny HW a SW kalkulován také náklad na jeho instalaci, implementaci a dopravu a na druhou část, která se týká provozních nároků po dobu udržitelnosti projektu. V kalkulaci vycházíme z předpokladu že současné datové rozvody splňují základní kritéria pro provoz Cat 5e sítí a neuvažujeme v ceně s náklady na přímé náklady úprav či rozšíření těchto rozvodů. Předpokládáme že v případě nutnosti budou provedeny úpravy vlastní investicí malého rozsahu.

7 PŘÍLOHY

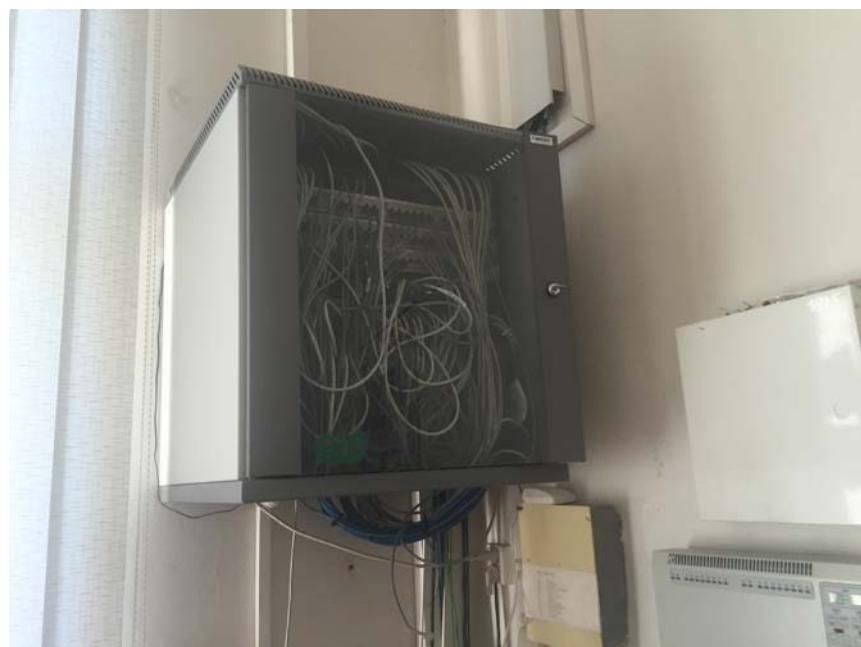
Fotodokumentace místa umístění racků

Základní orientační plánek školy

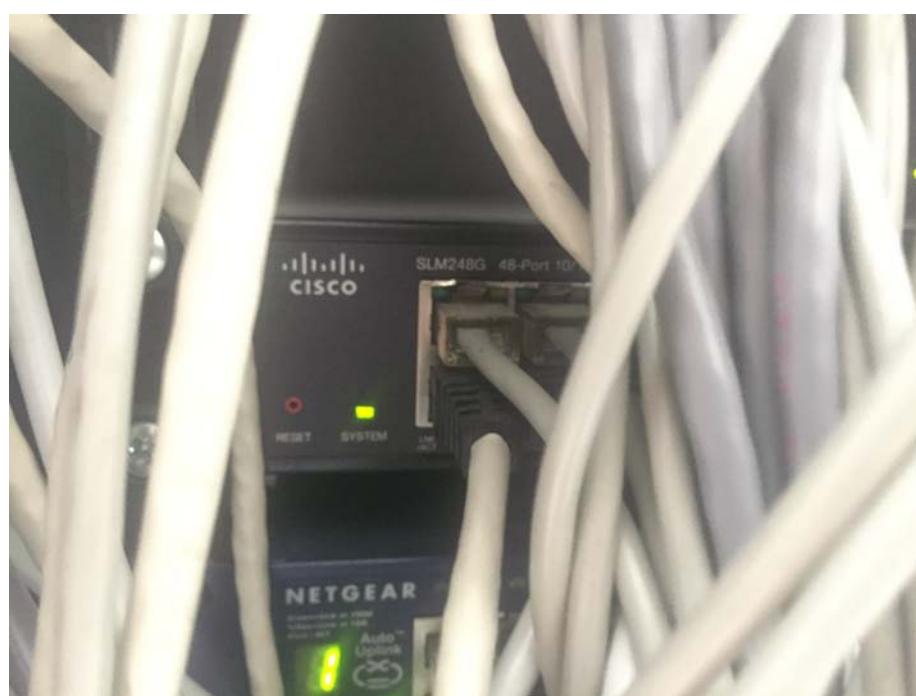
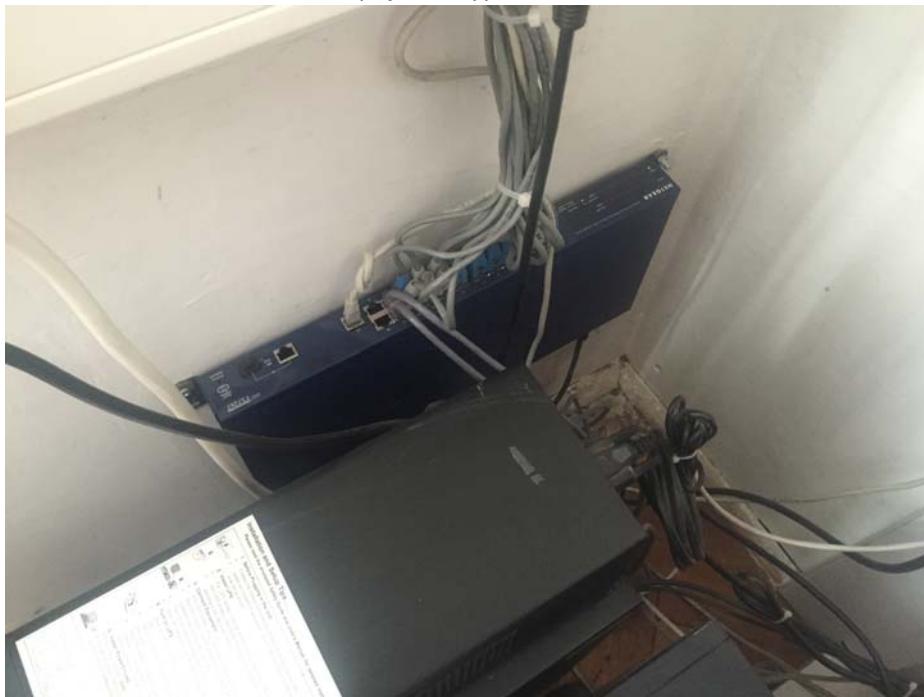
Obr 1. – budoucí umístění racku



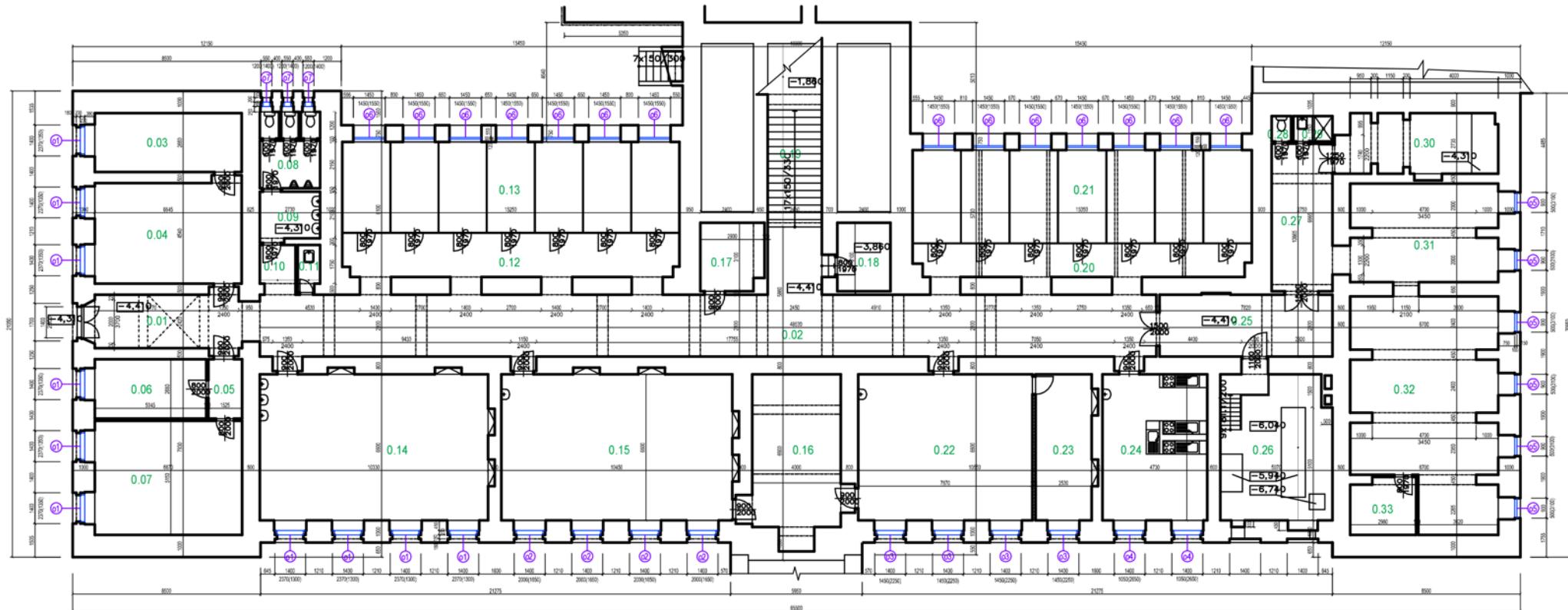
Obr 2 – detail současného racku



Obr 3, 4 - Zapojení a typ aktuálních switchů



PŮDORYS 1.PODZEMNÍHO PODLAŽÍ



LEGENDA MÍSTNOSTÍ - 1. PODZEMNÍ PODLAŽÍ

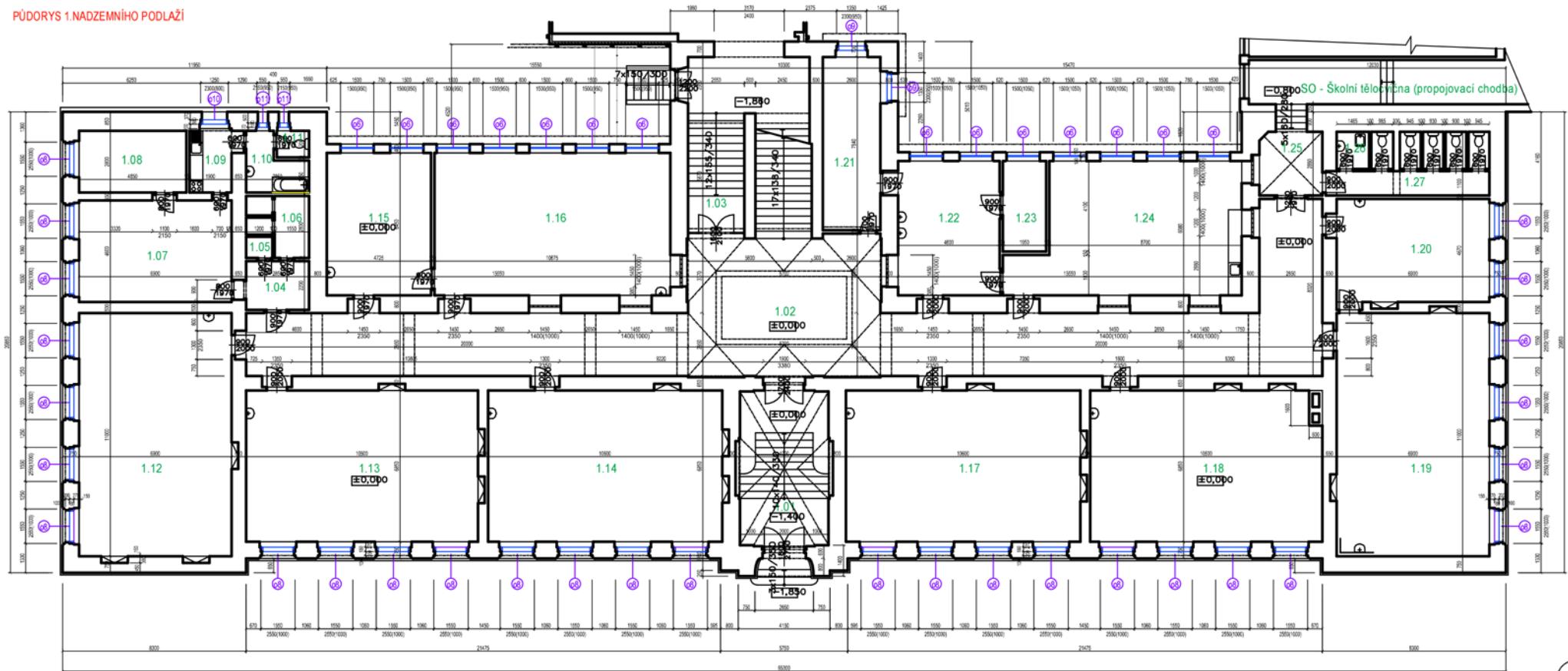
SO - Školní budova

č.m	Název místnosti	Plocha	Poznámka
0.01	VSTUPNÉ ZÁVĚŘ	17,44 m ²	
0.02	HLAVNÉ CHODBA	25,90 m ²	
0.03	SKLAD UČEBNÍ	17,48 m ²	
0.04	SKLAD UČEBNÍ II	20,64 m ²	
0.05	CHODBA	4,08 m ²	
0.06	DENNÍ MÍSTNOST UČILEDNÝ	13,92 m ²	
0.07	UČEBNA	34,35 m ²	
0.08	WC - MUŽ	0,13 m ²	
0.09	UNIFÓRMA	0,95 m ²	
0.10	CHODBA	3,52 m ²	
0.11	OKULÁDOVÁ KOMORA	2,08 m ²	
0.12	CHODBA ŠÁDEN - ZÁPAD	34,23 m ²	
0.13	SÁDNY - ZÁPAD	62,88 m ²	
0.14	UČEBNA KERAMIKY	66,16 m ²	
0.15	HERNA	68,57 m ²	
0.16	SKLAD C.O.	31,18 m ²	

č.m	Název místnosti	Plocha	Poznámka
0.17	KERAMICKÁpec	8,89 m ²	
0.18	SKLAD ČISTÝCH PROSTOROV	7,44 m ²	
0.19	SCHODSY (VAKUUM)	14,65 m ²	
0.20	CHODBA ŠÁDEN - VÝCHOД	25,78 m ²	
0.21	SÁDNY - VÝCHOД	84,83 m ²	
0.22	UČEBNA ČISTÝ JAZÝК	51,94 m ²	
0.23	KABINET ČISTÝ JAZÝК	16,70 m ²	
0.24	TECHNICKÁ MÍSTNOST	31,22 m ²	
0.25	KANCELÁŘ KOTELNÝ	21,90 m ²	
0.26	KOTELNA	32,71 m ²	
0.27	CHODBA	18,33 m ²	
0.28	WC KOTELNÝ	1,02 m ²	
0.29	OKULÁDOVÁ MÍSTNOST	2,03 m ²	
0.30	SKLAD I	19,02 m ²	
0.31	SKLAD II	29,96 m ²	
0.32	SKLAD III	62,38 m ²	
0.33	VODOVODNÍ PŘÍPOJKA	7,44 m ²	



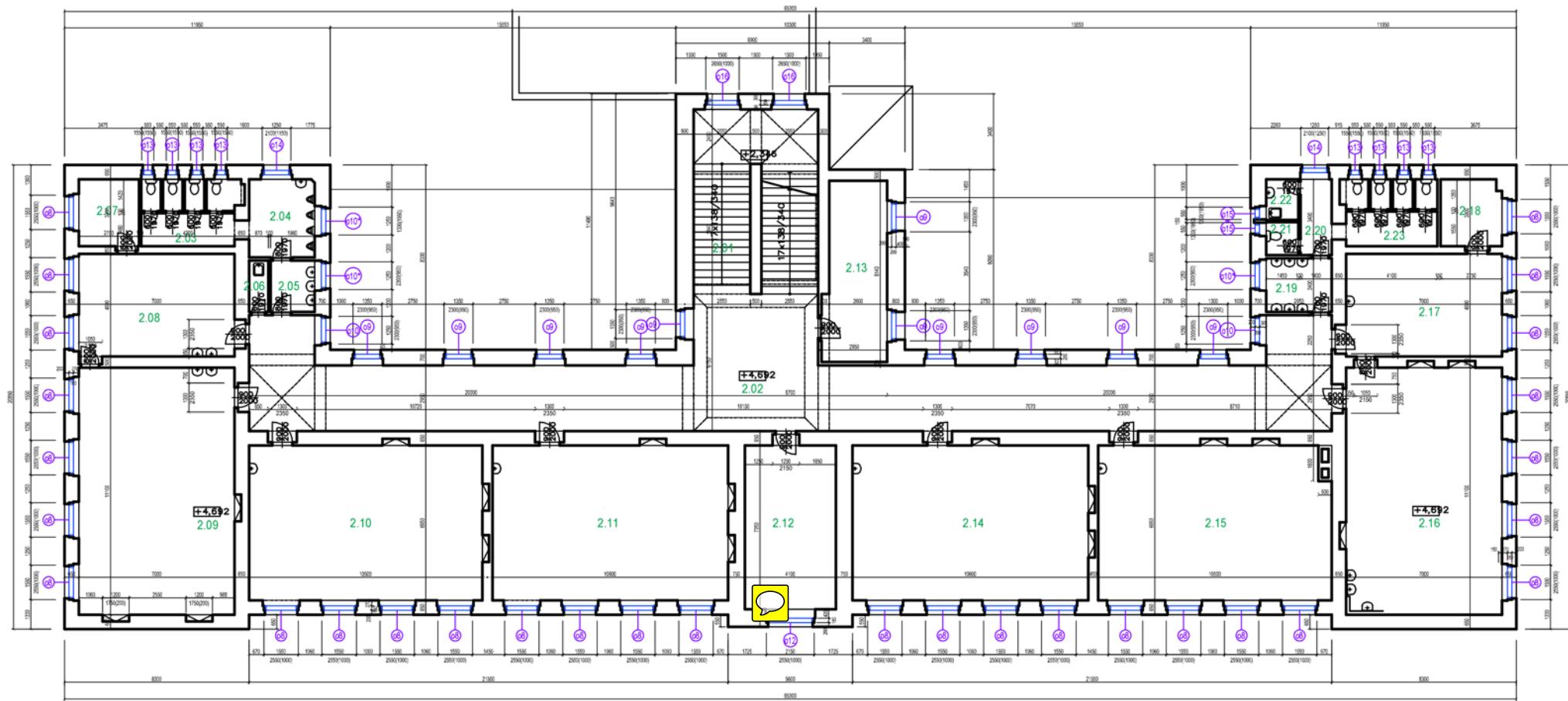
PŮDORYS 1.NADZEMNÍHO PODLAŽÍ



LEGENDA MÍSTNOSTÍ - 1. NADZEMNÍ PODLAŽÍ
SO - Školní budova

C.m	Název místnosti	Plocha	Poznámka	C.m	Název místnosti	Plocha	Poznámka
1.01	VSTUPNÍ ZÁVĚŘ	28,54 m ²		1.15	KABINET HUDEBNÉ VÝCHOVY	30,48 m ²	
1.02	HLAVNÍ CHODBA	192,59 m ²		1.16	UČEBNA HUDEBNÉ VÝCHOVY	68,85 m ²	
1.03	SCHODNÍK	31,39 m ²		1.17	KMENOVA UČEBNA	72,81 m ²	
1.04	BYT - ZÁVĚŘ	8,77 m ²		1.18	KMENOVA UČEBNA	70,97 m ²	
1.05	BYT - KOMORA	1,14 m ²		1.19	UČEBNA DĚJEPISU	75,90 m ²	
1.06	BYT - TECHNICKÁ MÍSTNOST	6,44 m ²		1.20	KABINET DĚJEPISU A ČESK.	47,9886 m ²	
1.07	BYT - POKOJ	32,19 m ²		1.21	REDAKCE	20,39 m ²	
1.08	BYT - KUCHYNĚ	13,59 m ²		1.22	KAMOĽÁK I	28,74 m ²	
1.09	BYT - Koupelna	8,87 m ²		1.23	KAMOĽÁK II	8,00 m ²	
1.10	BYT - WC	0,82 m ²		1.24	SKROVNÍKA	56,74 m ²	
1.11	BYT - WC	1,74 m ²		1.25	CHODBA	8,13 m ²	
1.12	KMENOVA UČEBNA	75,90 m ²		1.26	OKLADOVÁ KOMORA	2,48 m ²	
1.13	KMENOVA UČEBNA	71,83 m ²		1.27	ZENY	18,30 m ²	
1.14	KMENOVA UČEBNA	72,81 m ²					

PŮDORYS 2.NADZEMNÍHO PODLAŽÍ



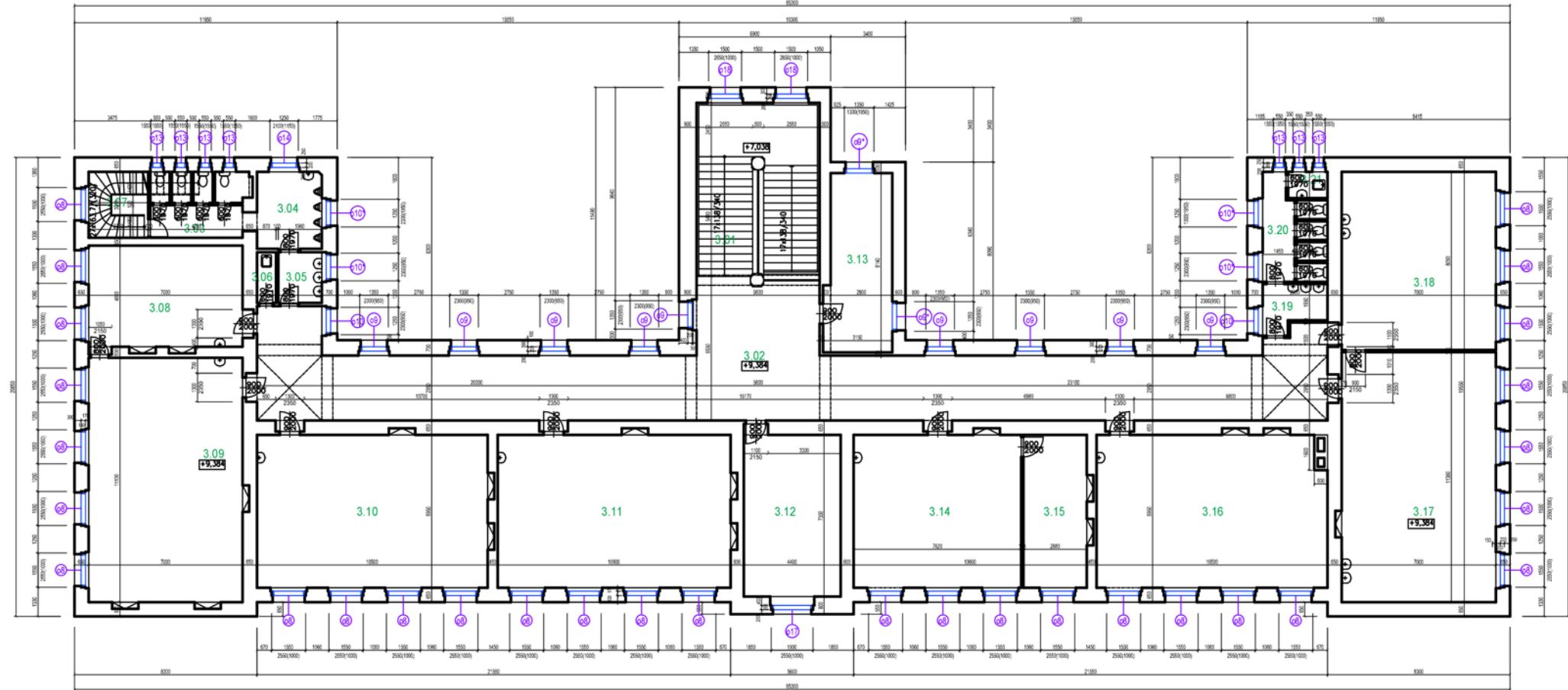
LEGENDA MÍSTNOSTÍ - 2. NADZEMNÍ PODLAŽÍ
SO - Školní budova

<i>č.m.</i>	<i>Název místnosti</i>	<i>Plocha</i>	<i>Poznámka</i>
2.01	SCHODÍSTE	43,90 m ²	
2.02	HLAVNÍ CHODBA	178,76 m ²	
2.03	WC - MUŽ KABINKY	13,04 m ²	
2.04	WC - MUŽ PISÁRKY	10,31 m ²	
2.05	WC - MUŽ UČIVÁRNA	4,55 m ²	
2.06	OKLADOVÁ KOMORA	2,00 m ²	
2.07	SKLADEK CHEMIE	8,50 m ²	
2.08	KABINET CHEMIE	33,22 m ²	
2.09	UČIVNA CHEMIE	77,70 m ²	
2.10	KMEKOVA UČIVNA	72,98 m ²	
2.11	KMEKOVA UČIVNA	73,87 m ²	

<i>č.m.</i>	<i>Název místnosti</i>	<i>Plocha</i>	<i>Poznámka</i>
2.12	UČIVNA INTERNETU	30,74 m ²	
2.13	KHNOVNA	22,23 m ²	
2.14	KMEKOVA UČIVNA	73,47 m ²	
2.15	UČIVNA LITERATURY	72,02 m ²	
2.16	UČIVNA VÝTVARNE VÝCHOVY	78,07 m ²	
2.17	KABINET VÝTVARNE VÝCHOVY	32,00 m ²	
2.18	SKLADEK VÝTVARNE VÝCHOVY	8,54 m ²	
2.19	WC - ŽENY UČIVÁRNA	7,08 m ²	
2.20	WC - ŽENY CHODBA	4,76 m ²	
2.21	WC - LÝTKY	2,14 m ²	
2.22	OKLADOVÁ KOMORA	2,45 m ²	
2.23	WC - ŽENY KABINKY	12,32 m ²	



PŮDORYS 3.NADZEMNÍHO PODLAŽÍ

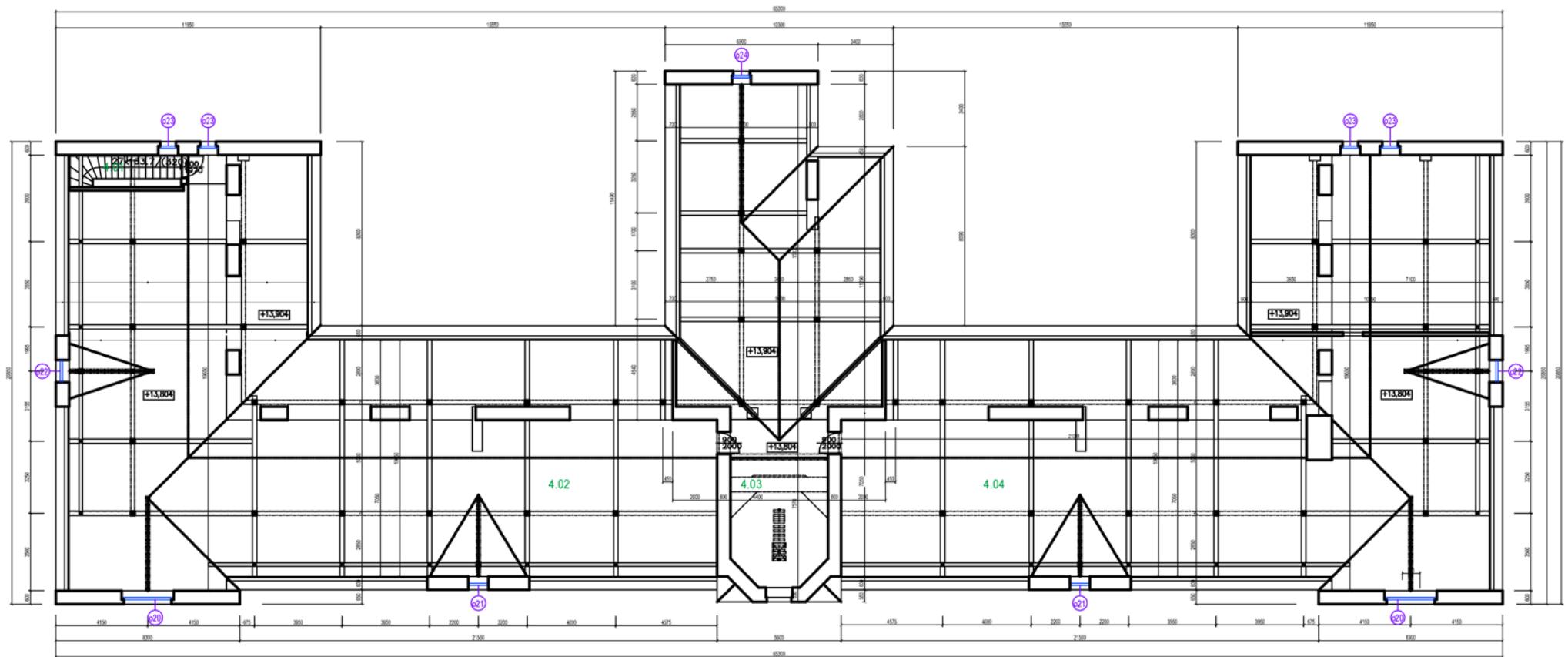


LEGENDA MÍSTNOSTÍ - 3. NADZEMNÍ PODLAŽÍ
SO - Škôlní budova

č.m.	Název místnosti	Plocha	Poznámka
3.01	SCHODNÍČEK	28,81 m ²	
3.02	HLAVNÉ CHODBY	178,44 m ²	
3.03	WC - MUŽ KARIKÁKY	13,04 m ²	
3.04	WC - MUŽ PRÍRODARY	10,31 m ²	
3.05	WC - MUŽ UMYVÁRNA	4,85 m ²	
3.06	OKLADOVÁ KOMORA	2,00 m ²	
3.07	SCHODNÍČEK	8,10 m ²	
3.08	KABINET PŘEDKOPSIU A MATEM.	903,22 m ²	
3.09	UČEBNA PŘEDKOPSIU	77,70 m ²	
3.10	UČEBNA UMYVÁRNA	72,98 m ²	

č.m.	Název místnosti	Plocha	Poznámka
3.11	KAMENOVA UČEBNA	73,67 m ²	
3.12	UČEBNA INTERNETU	32,89 m ²	
3.13	KABINET ZEMĚpisu	23,96 m ²	
3.14	UČEBNA ZEMĚpisu	52,96 m ²	
3.15	SKLAD UČEBNÝ ZEMĚPISU	20,02 m ²	
3.16	UČEBNA MATEMATIKY	72,02 m ²	
3.17	UČEBNA FYZIKY	79,92 m ²	
3.18	KABINET FYZIKY	58,43 m ²	
3.19	WC - ŽENY UMYVÁRNA	8,47 m ²	
3.20	WC - ŽENY CHODBA	11,78 m ²	
3.21	OKLADOVÁ KOMORA	2,13 m ²	

4.NADZEMNÍ PODLAŽÍ - PŮDNI PROSTORY



LEGENDA MÍSTNOSTÍ - 4. NADZEMNÍ PODLAŽÍ
SO - Školní budova

číslo	číslo místnosti	plocha	pozdnávka
4.01	SCHODIŠTE	7,35 m ²	
4.02	PODKNOV - ZÁPADNÍ ČÁST	394,43 m ²	
4.03	PODKNOV - STŘEDNÍ ČÁST	158,67 m ²	
4.04	PODKNOV - VÝHODNÉ ČÁSTI	398,89 m ²	