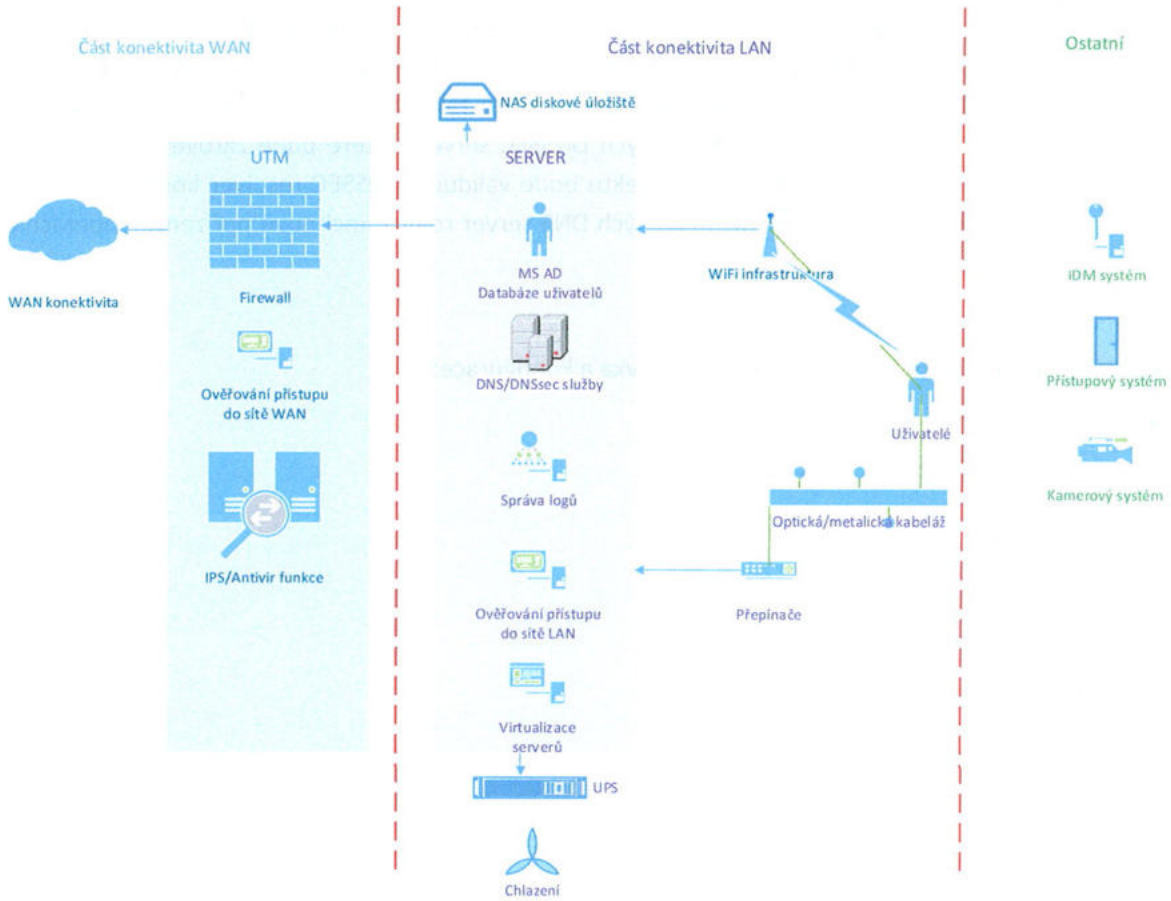
Základní škola Frýdlant nad Ostravicí, náměstí T. G. Masaryka 1260, příspěvková organizace

Následující dokument obsahuje seznam minimálních technických, funkčních požadovaných parametrů pro splnění standardu konektivity školy.

Hlavní aktivity projektu jsou rozděleny do třech základních částí:

- konektivita WAN,
- konektivita LAN a
- ostatní části

Jejich vzájemnou návaznost ilustruje následující obrázek:



Konektivita školy k veřejnému internetu (WAN)

Připojení k Internetu

V rámci projektu musí být realizována konektivita min. symetrických **90 Mbps** s poskytovatelem přidělenými veřejnými IPv4 i IPv6 adresami. IPv4 adresy budou konfigurovány na externím rozhraní firewallu, naproti tomu IPv6 adresy budou použity ve vnitřní síti formou koexistence (dual-stack) obou verzí IP protokolů. Pro směrování IPv6 prefixu může být mezi firewallem školy a koncovým směrovačem poskytovatele využito link-local adres nebo jiného přiděleného nebo domluveného prefixu.

DNSEC

DNSEC je bezpečnostním rozšířením překladu doménových názvů za pomoci digitálních podpisů DNS zóny a v ní vnořených záznamů. Díky tomuto rozšíření nelze podvrhnout, nebo jinak upravit, odpověď DNS serveru. DNSSEC dále vylučuje většinu známých praktik zneužití regulérních DNS serverů k útokům na třetí cíle. Významně tak zvyšuje bezpečnost a garantuje autenticitu odpovědí. Pro plné nasazení DNSSEC budou v rámci projektu realizována opatření ve dvou oblastech:

- **Externí zóna** - škola používá svou doménu zsfrydlantno.cz registrovanou v ACTIVE 24, s.r.o., pod jejímiž DNS záznamy jsou publikovány služby, na jmenných (NS) serverech externího registrátora, nikoliv na vlastním NS serveru. V rámci projektu budou ve spolupráci s registrátorem domény doplněny podpisy DNSSEC k používaným zónám a zároveň budou doplněny záznamy pro služby publikované skrz IPv6 adresy, viz výše. Pokud současný registrátor neumožní doplnění podpisů DNSSEC, bude zóna převedena k jinému registrátorovi.
- **Vnitřní validující 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 odpovědí na DNS dotazy vnitřních zařízení. 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.

Vnitřní konektivita školy (LAN)

V rámci této části projektu bude realizována dodávka a konfigurace:

- Firewall
- Server se SW a s příslušenstvím
- Log manager
- NAS pro zálohování
- Zapracování ICT do řádu školy
- LAN přepínače
- WiFI AP s centrálním řízením
- Monitorování IP datových toků

Firewall

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/Passive 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**).

Požadované HW parametry:

- Počet síťových rozhraní min. 24x GB, z toho min. 6x SFP, min. 2x 10GE SFP+
- Počet portů pro DMZ min. 1
- Podpora LACP 802.3ad na min. 4 portech
- Dva, redundandní, napájecí zdroje

Výkonnostní parametry:

- Výkonnost FW nezávislá na velikosti paketu
- Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 64 B- min 10 Gbps
- Propustnost FW paketů za sekundu - min. 15 Mbps
- Latence firewallu (64 B UDP paket) - max 5 mikro sec
- Počet naráz otevřených spojení - min 1,5 Mil.
- Počet nových spojení za sekundu - min. 55000
- Propustnost IPSEC VPN (512 B paket) - min. 11 Gbps
- Propustnost SSL VPN min 750 Mbps
- Propustnost IPS - min 2,5 Gbps
- Propustnost AV - min. 1,5 Gbps
- Podpora virtualizace (min 10 virtuálních kontextů)
- Podpora funkce bezdrátový kontrolér - 32 AP

Funkce:

- Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, VRRP, synchronizace stavové tabulky mezi nódy v clusteru
- Režim fungování L2 – transparentní režim, L3 – NAT/Router
- Podopora 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 konfiugrace, internet browsing konfigurace, podpora vice tunelů – redundantní VPN,
- podpora IPv6,
- podpora dynamických routovací protokolů - OSPF), PPTP, L2TP, GRE

Firewall:

- Možnost nastavovat firewall politiku na základě geografických údajů
- Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru
- Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora healt check funkcí, podpora SSL offload
- Podpora centrální NATovácí tabulky

Filtrační funkce:

- Možnost výběru mezi file based režimem (buffer) nebo flow based (inspekce on-the-fly)
- Antivirus pro vybrané protokoly, možnost volby různých databází, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd)
- Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty
    - Intrusion Protection System – detekce útoků založena na signaturové části a na anomálním filtru, možnost vytvářet vlastní signatury.
- Web Filter – založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne

- Application Control – detekce, monitoring, povolení či zakázání vice než 2000 síťových aplikací na základě signatury dané aplikace, nikoliv dle portu
    - Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,...)
    - DoS Policy prevence proti základním útokům typu DoS, syn proxy

Ověřování uživatelů:

- LDAP, Active Directory, FortiNet Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu,
- Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – Token pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů
- Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.

Dynamické routování:

- RIP, BGP, OSPF, IS-IS
- Policy routing
- Traffic Shaping, QoS s podporou DSCP markování a ToS
- Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu
- WAN optimalizace (optimalizace vybraných protokolů, byte chaching), Web Cache, Explicitní Proxy, Reverzní proxy, WCCP

Reporty:

- Integrované logování a reporting

Server - HW, SW, implementační práce

V rámci projektu bude pořízen a nasazen server se SW a dalším příslušenstvím, na kterém bude nasazen serverový OS. Na tomto serveru budou nakonfigurovány služby a funkce, které jsou povinné (viz. dokunment P1 SP_Parametry Konektivity)

Parametry serveru – 1 ks

- 64-bit architektura, 1x procesor - kmitočet minimálně 2,1GHz/8Core, rozšiřitelné na dva CPU
- velikost RAM min 96 GB
- kmitočet RAM min. 2933 MHz
- pokročilá kontrola chyb a oprava paměti (ECC) a memory mirroringu
- rozšiřitelnost až na minimálně 8x 2,5" HDD ve výšce max 1U
- server osazen řadičem disků o velikosti zálohované cache min. 2GB s podporou min. Raid1, Raid5
- server osazen min. 2ks SSD s velikostí min 960GB a 6ks disků SAS min. 2,4TB
- konektor pro interní USB klíč a SD kartu na základní desce serveru
- možnost rozšíření až na 3x PCIe 3.0 slot
- minimálně 4x 1Gb ethernet portů, min. 2x 10Gb port SFP+
- redundantní hot-swap chlazeni a napájení
- redundantní napájení, za chodu vyměnitelné zdroje min. 800W s účinností min. 94%
- 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 management SW, který musí podporovat technologii Remote KVM, možnost zapínat a vypínat server, virtuálně připojovat lokální média
- Certifikát potvrzující možnost nasazení nabízené virtualizačních řešení
- HW pro instalaci do 19" skříně
- Záruka na 5let se zahájením opravy následující pracovní den v místě instalace, garantovaná výrobcem HW

Licence serverového operačního systému

Požadujeme dodávku serverové licence (aktuálně nejnovější dodávaná verze) pro výše popsaný server, která umožní provozovat ve virtuálním prostředí 6 virtuálních serverů.
Požadované vlastnosti serverového operačního systému

- Možnost adresářové služby kompatibilní s X.509
- Adresářová služba umožňuje obsahovat objekty typu uživatel, skupina, počítač a další
- Autentizace protokoly Kerberos V5, NTLMv2, NTLM
- Centrálně řízené politiky uživatelů a počítačů
- Možnost funkcí DNS, DHCP, WINS. Služba DNS poskytuje mechanismus multimaster replikace
- Možnost sdílení souborů a nastavování práv na objekty adresářové služby
- Sdílení souborů pomocí protokolu CIFS
- Distribuovaný souborový systém a delta replikace
- Možnost sdílení tiskáren a nastavování práv na objekty adresářové služby
- Možnost grafického uživatelského rozhraní v češtině

Implementační práce

V rámci instalace serveru budou provedeny následující práce:

- Zahoření nového serveru; firmware update
- 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, migrace na novou verzi včetně potřebných služeb DNS, DHCP
- Propagace nových komponent v síti.
- instalace tiskáren

Příslušenství k serveru

Součástí dodávky serveru bude kromě potřebných propojovacích LAN a napájecích kabelů také:

- serverový 19" RACK (uzamykatelná skříň pro umístění HW), který zajistí bezpečné uložení serveru, perforace správné větrání i zamezení neoprávněné manipulaci se serverem a dalším HW
  - výška max. 27U
  - rozměr 600x1000

- perforované přední i zadní dveře osazené zámky
- pevná police a sada šroubů pro instalaci prvků

- záložní napájecí zdroj UPS 2200VA, v 19" provedení, která zajistí chod serveru při výpadku napájení a následné korektní vypnutí systémů před vyčerpáním kapacity baterií.
  - Provedení do racku, max. 2U, včetně montážního materiálu (kolejnic)
  - Jmenovité napětí 230 V, jednofázová na vstupu i výstupu
  - Vstupní napětí nastavitelné min. v rozsahu 150V-294V
  - Výkon (VA/W): 2200/1980
  - Technologie: Line- interactive
  - Doba běhu na baterie min. 10 min při 50% zátěži
  - Vestavěný úplný systémový autotest, možnost automatického plánovaného provádění
  - Výstupy: Min. 8 zásuvky IEC C13
  - LAN karta pro management a komunikaci se serverem

Log Management (Syslog)

Součástí dodávky řešení je i nástroj pro sběr a uchování textových logů. Tento musí umožnit příjem všech druhů zpráv, min. protokoly SNMP (traps) a SYSLOG. Syslog bude rovněž užit pro export NAT tabulky firewallu pro případné dohledání komunikace k vnitřnímu zařízení. Jeho zdroji dále budou události systému Windows serverů (tzv. EventLog), kde musí být schopen přejímat min. bezpečnostního charakteru (EventLog Security a EventLog System). Ze síťových zařízení bude dostávat a musí být schopen přijaté zprávy automaticky rozdělovat pro budoucí vyhledávání min. do kategorií čas, datum, hostname, IP. Musí umožnit včasné a automatické notifikace min. jako email.

- 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.

NAS

Pro uchování a zálohy logů a provozních informací bude v rámci projektu pořízeno síťové (NAS) úložiště. Sítové úložiště NAS bude z důvodu fyzické bezpečnosti záloh a dat umístěno mimo místnost se servery. Jako možné se jeví umístění NAS v centrálním rozvaděči v prostorách hovorny, popř. jiném distribučním rozvaděči, nejlépe v takovém, kde není očekáván velký pohyb osob. Podmínkou bude rovněž uzamčení rozvaděče.

Prostoru na úložišti NAS může být paralelně využito i k jiným účelům, jako například pro zálohování serverů a jejich dat. NAS úložiště běžně automatizaci záloh nenabízí. Zálohování bude proto prováděno nativními nástroji operačních systémů, které jsou pro ten účel dostatečné a povedou k úspoře finančních prostředků za nástroje třetích stran.

Samotné síťové úložiště bude rovněž zálohováno na k němu připojení externí disk, který zajistí dodržení pravidla 3 záloh, 3 míst, díky čemuž by neměla nastat situace faktické ztráty provozních, či jiných, dat.

Požadované parametry

- 4-jádrový procesor s podporou AES-NI.
- Paměť DDR4 s kapacitou 6 GB, rozšířitelná až na 18 GB
- min. prostor pro 4x HotSwap HDD 3.5"/2.5" SATA III/II x 2 s možností rozšíření na dvojnásobek
- Osazeny minimálně 4xHDD každý s kapacitou 8TB
- Minimálně 2x USB 3.0 porty
- Minimálně 2x LAN port 10Gbit v provedení SFP+.
- 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
- Podpora práce v HA clusteru
- Provedení pro umístění do 19" skříně

Příslušenství k NAS

- záložní napájecí zdroj UPS 1500VA, v 19" provedení, která zajistí chod serveru při výpadku napájení a následné korektní vypnutí systémů před vyčerpáním kapacity baterií.
    - Provedení do racku, max. 2U, včetně montážního materiálu (kolejnic)
    - Jmenovité napětí 230 V, jednofázová na vstupu i výstupu
    - Vstupní napětí nastavitelné min. v rozsahu 150V-294V
    - Výkon (VA/W): 1500/1350
    - Technologie: Line- interactive
    - Doba běhu na baterie min. 10 min při 50% zátěži
    - Vestavěný úplný systémový autotest, možnost automatického plánovaného provádění
    - Výstupy: Min. 8 zásuvky IEC C13
    - LAN karta pro management a komunikaci se serverem

Zapracování 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.

Integrace s prostředím školy + support prostředí

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.

Podpora

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

LAN přepínače

Součástí projektu bude kompletní výměna LAN přístupových přepínačů. Na dodané přepínače budou při/přepojena všechna stávající zařízení vč. serverů.

Vhodnou segmentací sítě (pomocí vlan) bude skokově navýšena bezpečnost na úkor velikosti stávající broadcastové domény. Nové přepínače budou schopné simultánně odbavovat provoz drátové i bezdrátové sítě a budou vhodné pro připojení nových serverů. Veškeré směrování IP provozu vč. interního se bude odehrávat výše v části WAN (na firewallu).

Přepínače LAN budou stejné řady jednoho výrobce

Bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1X.

Pro hosty a externí uživatele bude zřízena samostatná VLAN (Guest VLAN), která bude komunikačně (min. L3 pravidla, ACL) oddělena od ostatních vnitřních sítí školy. Veškerá komunikace z této VLAN bude podrobena kontrole za pomoci UTM nástrojů (min. AV, IPS, kategorizace obsahu) a bude mít přiřazen přísnější (hlubší kontrola) profil odlišný od profilů pro učitele a žáky. Ověřování přístupu do této VLAN bude zajištěno pomocí tzv. captive portálu – webové autorizace. Captive portál bude zajištěn firewallem případně jiným samostatným řešením nebo prvkem, ale vždy s důrazem na bezpečné oddělení uživatelského provozu od zbytku vnitřních sítí.

Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě se směrováním provozu mezi VLAN na úrovni firewallu s řádně nastavenými ACL a filtry (AV apod.).

Přístupové přepínače

- 1x 8 portů 1G, PoE+, 2x SFP+ Switch
- 2x 24 portů 1G, 4x SFP+ Switch
- 3x 24 portů 1G, PoE+, 4x SFP+ Switch
- 4x 48 portů 1G, 4x SFP+ Switch

Požadované parametry

- Třída zařízení L3 switch
- Formát zařízení do racku
- Velikost zařízení max. 1U
- Počet 1Gbit/s metalických portů

- Model A0 - 8x10/100/1000Mbit RJ45
- Modely A1 a A2: 24x10/100/1000Mbit RJ45
- Modely B1: 48x10/100/1000Mbit RJ45

- Počet optických portů s volitelným fyzickým rozhraním
  - Model A0: 2x SFP/SFP+ 1G/10G port nezávislé
  - Model A1, A2, B1: 4x SFP/SFP+ 1G/10G port nezávislé
- 10Gbit opt. interface zpětně kompatibilní se 1000Mbit/s transceivery
- Všechny ethernet porty jsou dostupné zepředu
- Primární napájecí zdroj - interní AC
- Podpora PoE+ dle standardu 802.3at
  - Modely A1 a B1: ne
  - Modely A0, A2: ano
- Dostupný výkon pro PoE+ napájení
  - Model A0: 125W
  - Model A2: 370W
- Podpora Energy Efficient Ethernet (802.3az)
- Celková propustnost přepínače
  - Model A0: 55 Gbps
  - Modely A1 a A2: 128 Gbps
  - Model B1: 176 Gbps
- Celkový paketový výkon přepínače
  - Model A0: 41 Mpps
  - Modely A1 a A2: 95 Mpps
  - Model B1: 112 Mpps
- Podpora stohování přepínačů
  - Stoh podporuje distribuované přepínaní paketů
  - Kterýkoli prvek ve stohu může být řídícím prvkem (1:N redundance)
  - Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)
  - Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)
  - Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF
  - Stohování mezi vzdálenými lokalitami až 10 km
- Základní funkce a protokoly
  - Podpora "jumbo rámců" včetně velikosti 9220 Byte

- Podpora linkové agregace IEEE 802.1AX
- Konfigurovatelné rozkládání LACP zátěže podle L3 a L4
- Počet LACP skupin/linek ve skupině min. 60/8
- Počet záznamů v tabulce MAC adres min. 32 000
- Protokol pro definici šířených VLAN - MVRP
- Podpora VLAN podle IEEE 802.1Q, 2000 aktivních VLAN
- Zařazování do VLAN podle protokolu 802.1v
- Zařazování do VLAN podle MAC adresy bez nutnosti externího řízení (Radius)
- Podpora Private VLAN
- IEEE 802.1s - Multiple Spanning Tree
- STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
- Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
- Detekce jednosměrnosti optické linky (např. UDLD)
- Tunelování 802.1Q v 802.1Q
- DHCP server
- DHCP relay pro IPv4 a IPv6 včetně option 82 a 79
- NTP pro IPv4 a IPv6 včetně MD5 autentizace
- Statické směrování IPv4 a IPv6
- Počet záznamů ve směrovací tabulce min. 10 000
- Dynamické směrování RIPv2 a RIPng
- Dynamické směrování OSPFv2 a OSPFv3
- Hardware podpora IPv4 a IPv6 ACL
- ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN
- DHCP snooping pro IPv4 a IPv6
- HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na % rychlosti portu a množství paketů za vteřinu
- ICMPv4 a ICMPv6 rate-limiting per port
- Podpora ověřování 802.1X včetně více uživatelů per-port
- RADIUS MAC autentizace, probíhající před 802.1x pro případy, že koncové zařízení není softwarově vybaveno pro 802.1x autentizaci
- Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675
- Podpora 802.1X Guest VLAN
- ověřování 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)
- Port security - omezení počtu MAC adres na port, statické MAC, možnost definování akcí při překročení

- Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení

- Management
  - CLI formou RJ45 serial konsole port
  - USB konzolový port
  - Konfigurace zařízení v člověku čitelné textové formě
  - Podpora managementu přes IPv4 i IPv6
  - SSHv2 a a SFTP
  - Podpora SNMPv2c a SNMPv3
  - RMON
  - Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
  - Lokálně vynucené RBAC na úrovni přepínače
  - Dualní flash image
  - TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
  - Podpora oddělených čítačů paketů pro IPv4 a IPv6 provoz
  - Podpora RADIUS včetně RADIUS CoA (RFC3576)
  - Aktivní monitoring dostupnosti RADIUSu přednastaveným jménem a heslem
  - Podpora TACACS+
  - Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)
  - Analýza síťového provozu sFlow podle RFC 3176
  - Port mirroring, alespoň 4 různé obousměrné session
  - SPAN, RSPAN
  - Zrcadlení provozu na základě filtrů: Mac-adressa, VLAN, ACL (traffic mirroring)
  - Podpora IP SLA pro měření zpoždění provozu VoIP
  - Podpora OpenFlow verze 1.3
  - Podpora Zero Touch Provisioning (ZTP)
  - REST API pro automatizaci nastavení, včetně popory CLI a batch CLI příkazů
  - Podpora Chromecast Gateway
  - Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty. (Apple Bonjour Gateway)
  - Podpora service insertion včetně technologie VXLAN
  - Automatická konfigurace portu podle připojeného zařízení
  - Podpora Cloud based management
- Plná záruka na HW v délce 60měsíců s výměnou následující pracovní den garantovaná výrobcem zařízení
- SW aktualizace po dobu 5 let

- Součástí dodávky budou všechny potřebné síťové kabely a transceivery

Wifi - Advanced AP

V rámci projektu bude vybudované nové centrálně řízené WiFi, které bude obsahovat 32 ks AP.

Architektura WiFi bude založena na centralizovaném řešení. Jedním místem správy bude centrální kontrolér (řadič). Požadovány jsou nové, aktuální typy přístupových bodů (802.11ac) stejného typu náležící do daného systému. Systém musí být schopen detekovat (a min. reakčně vizualizovat) wifi a non-wifi rušení, provádět automatický i dynamický výběr frekvenčního kanálu (DFS), zajišťovat spravedlivé rozdělení přístupu k mediu (airtime-fairness) i případnou distribuci klientů mezi vlastními AP (dynamicky nebo dle nastavené hodnoty). Roaming klientů mezi AP a band-stearing (nucený přesun klienta do 5G spektra) jsou nutností. Pořízené AP budou podporovat WiFi6, WPA2, PoE+, multi SSID a ACL pro filtrování provozu.

Uchazeč na základě svého vlastního technického šetření může určit vhodnější rozmístění

Součástí dodávky AP bude i jejich připojení do LAN, v případě potřeby včetně přivedení UTP k místu instalace AP.

Síť AP, musí zajistit konzistentní WiFi službu především v učebnách.

Napájení AP bude zajištěno pomocí standardu 802.3at z LAN přepínačů, jak je uvedeno v předchozí kapitole.

Řízení přístupu do sítě WiFi bude zajištěno implementací technologie 802.1X. Ověřování a autorizace uživatelů a zařízení bude probíhat protokolem Radius vůči vybudované adresářové službě a případným dalším systémům – např. EDUROAM.

Požadované parametry WIFi AP

- 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 802.11ax, současná funkce AP v pásmu 2,4 a 5 GHz
- přenosová rychlost min. 1,2 Gbps na 5Ghz a 390 Mbps na 2,4Ghz
- Podpora WPA2, podpora multi-user MIMO (MU-MIMO)
- standardizované PoE napájení
- multi SSID - min. 10x
- ACL pro filtrování provozu
- Rychlá instalace i rozšíření sítě, škálovatelnost
- RF optimalizace sítě
- Vynikající zabezpečení sítě PCI DSS certifikace
- Automatický QoS pro hlas a video, certifikace pro MS Lync
- Vysoká dostupnost
- Integrovaný Firewall, integrované IPS/IDS

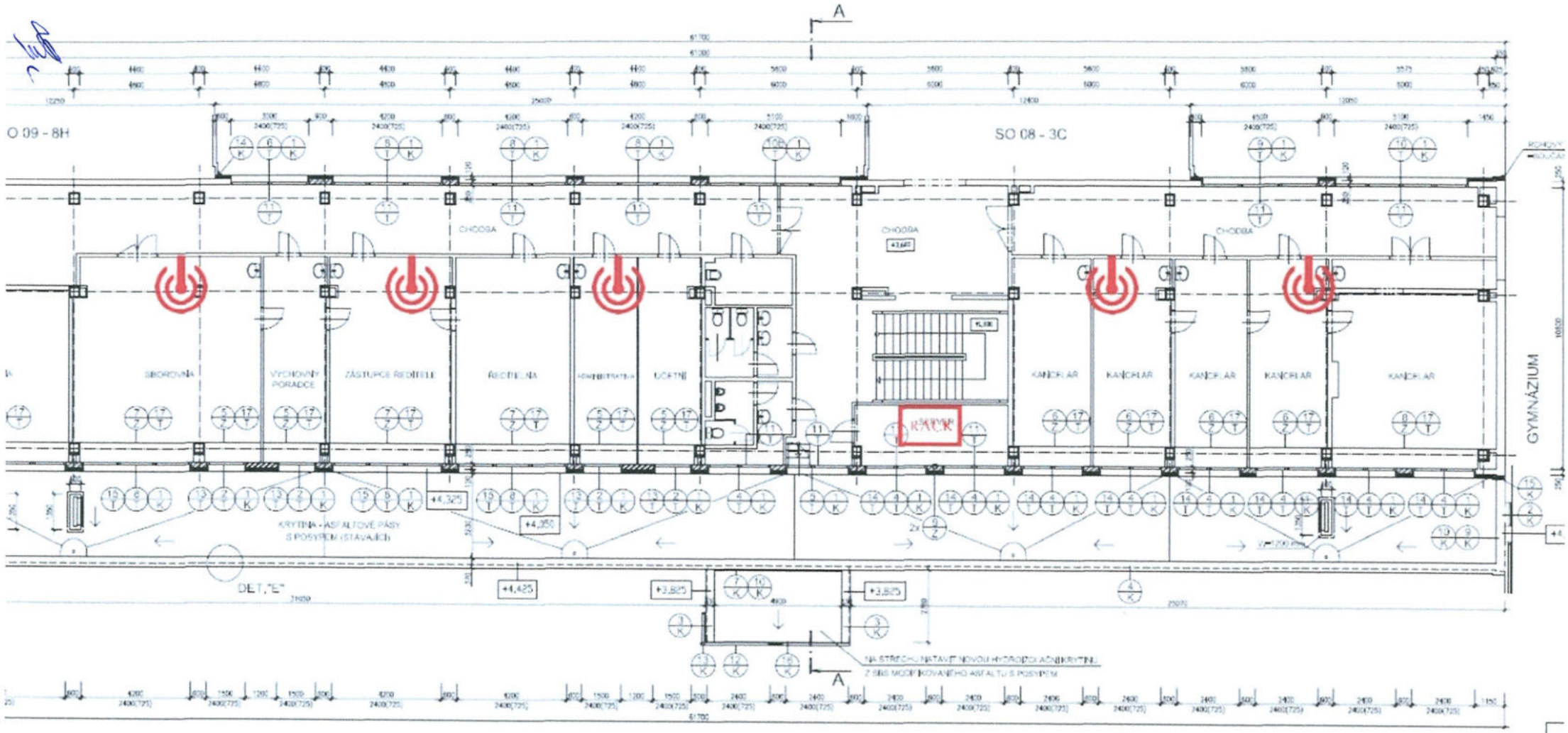
NetFlow

Součástí řešení bude i 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.

Požadované parametry, vlastnosti

- ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie NetFlow (nutná podpora NetFlow v5 a NetFlow v9), zařízení o velikosti max. 1U
- sledují komunikaci na počítačové síti a vytvářejí NetFlow/IPFIX statistiky
- musí obsahovat vestavěný kolektor pro sběr, vizualizaci a analýzu NetFlow/IPFIX dat
    - Detailně monitorovat síťový provoz v reálném čase i umožnit získat přehled o síťové aktivitě v rámci specifikovaného časového období v minulosti (min. 60 dnů).
    - nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích, nesmí docházet k ovlivňování chování sítě
    - specializovaná dedikovaná zařízení (sondy) pro vytváření detailních statistik IP toků o dění na síti, standardizovaný protokol pro výměnu dat o IP tocích (NetFlow v5, v9)
    - dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů
    - plná zákaznická podpora v českém jazyce
- detekce aplikací dle standardu NBAR2, monitorování a analýza HTTP provozu a VoIP statistik
- snadná instalace do stávající síťové infrastruktury
- pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, případně v kombinaci se SPAN porty)
- jeden administrativní port 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat
- zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS
- správa uživatelů a přístupových práv na zařízení
- možnost nastavení rychlosti monitorované linky 10/100/1000Mb/s na metalických rozhraních
- vestavěný kolektor pro dočasné ukládání NetFlow statistik (zajištění redundance), který zahrnuje uživatelsky definovaný dashboard, automatickou tvorbu reportů, detekci aktivních zařízení a detailní analytické možnosti
- časová synchronizace zařízení proti centrálnímu zdroji času na síti
- jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky
- možnost přístupu a konfigurace zařízení prostřednictvím sériové linky (RS-232)
- použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména
- podpora autentizace vůči LDAP (Active Directory).
- pasivní odposlech dat ze sítě pomocí specializovaných zařízení (TAPů) či SPAN portů

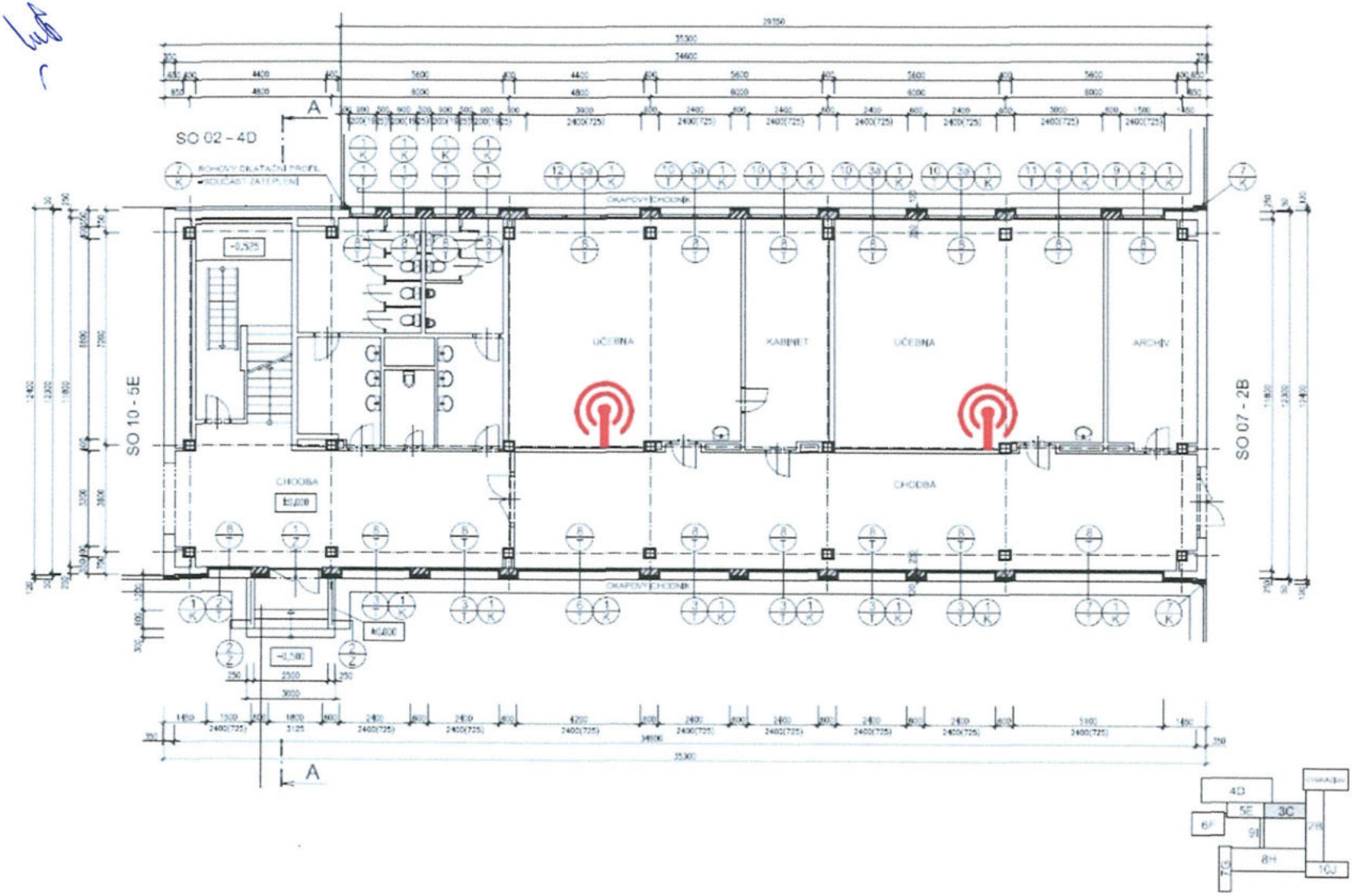
- podpora protokolů pro výměnu dat – programové vybavení sondy musí umožnit vytváření NetFlow dat ve formátech verzi 5 a 9
- zpracování datového provozu IPv4 a IPv6, VLAN, MPLS, GRE a jejich reportování na kolektor
- uživatelsky definovatelné šablony pro protokoly NetFlow v9 a případně IPFIX
- podpora monitorování MAC adres
- detekce aplikací dle standardu NBAR2
- monitorování a analýza HTTP provozu - včetně položek typu URL, hostname
- monitorování VoIP statistik
- dlouhodobé a stabilní zpracování na všech měřících rozhraních
- podpora pro nastavení časů u aktivní a neaktivní expirace toků
- podpora vzorkování na úrovni paketů
- podpora vzorkování na úrovni toků
- podpora simultánního exportu NetFlow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na sondě)
- podpora filtrování dat na sondě na základě IP prefixů a VLAN (pro různé cíle exportu různé statistiky)
- podpora vyplňování AS na základě vestavěného či dodaného seznamu
- podpora filtrování a export datových toků na základě AS
- počty a rychlosti/typy rozhraní – 2x 1GbE, metalika
- podpora 1 Gigabit Ethernetu
- současné měření síťového provozu na minimálně dvou gigabitových rozhraních současně pomocí jednoho zařízení
- Služba podpory, která bude zahrnovat všechny updaty i upgrady, přístup k webovému zákaznickému centru, podporu telefonem a emailem v českém jazyce v pracovní době (8x5), vzdálenou podporu přes SSH, konzultace síťového a bezpečnostního technika a NBD (Next-Bussines-Day) on-site hardwarovou záruku.



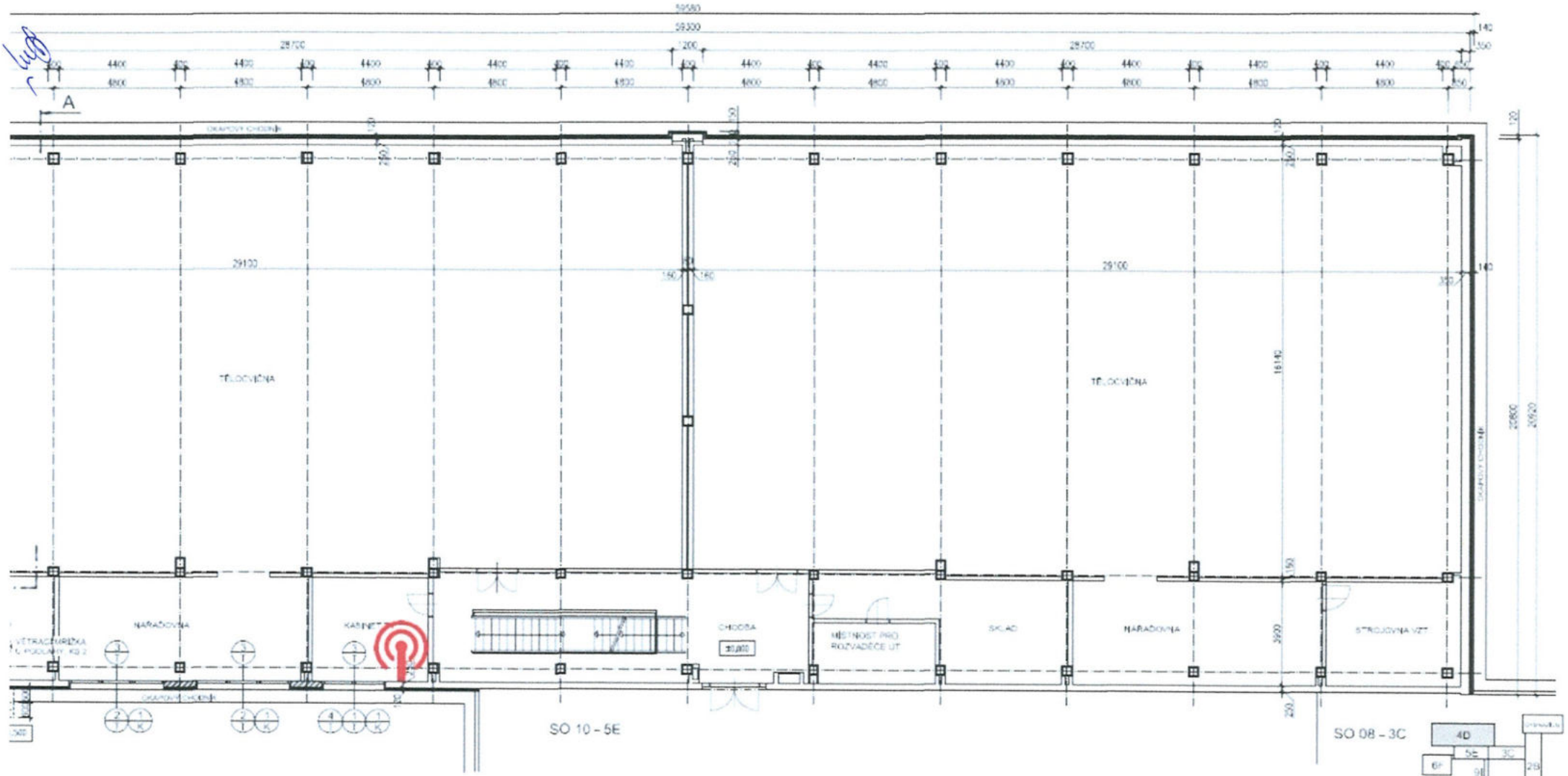
STAVEBNÍ ÚPRAVY Z
T.G.MASARYKA
FRÝDLANT NAD

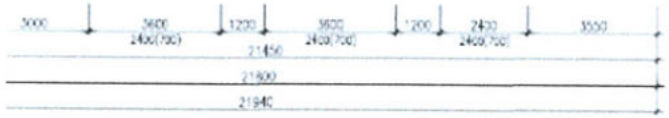
SO 07 STAVEBNÍ ÚPR
- VSTUP, ŠATNY,

PŮDORYS



Stavba:	STAVEBNÍ ÚPRAVY ZAKLADNÍ ŠKOLY T.G.MASARYKA č.p. 1260, FRÝDLANT NAD OSTRAVICÍ	Číslo zakázky: 104/11	Stupeň: DPS
Objekt:	SO 08 STAVEBNÍ ÚPRAVY OBJEKTU 3C - KLUBY ZŠ	Datum: leden/2013	Formát: 4x A4
Obsah: Architektonické a stavebně technické řešení	PŮDORYS 1NP	Měřítko: 1:100	Číslo přílohy: F.1.4.-2.'



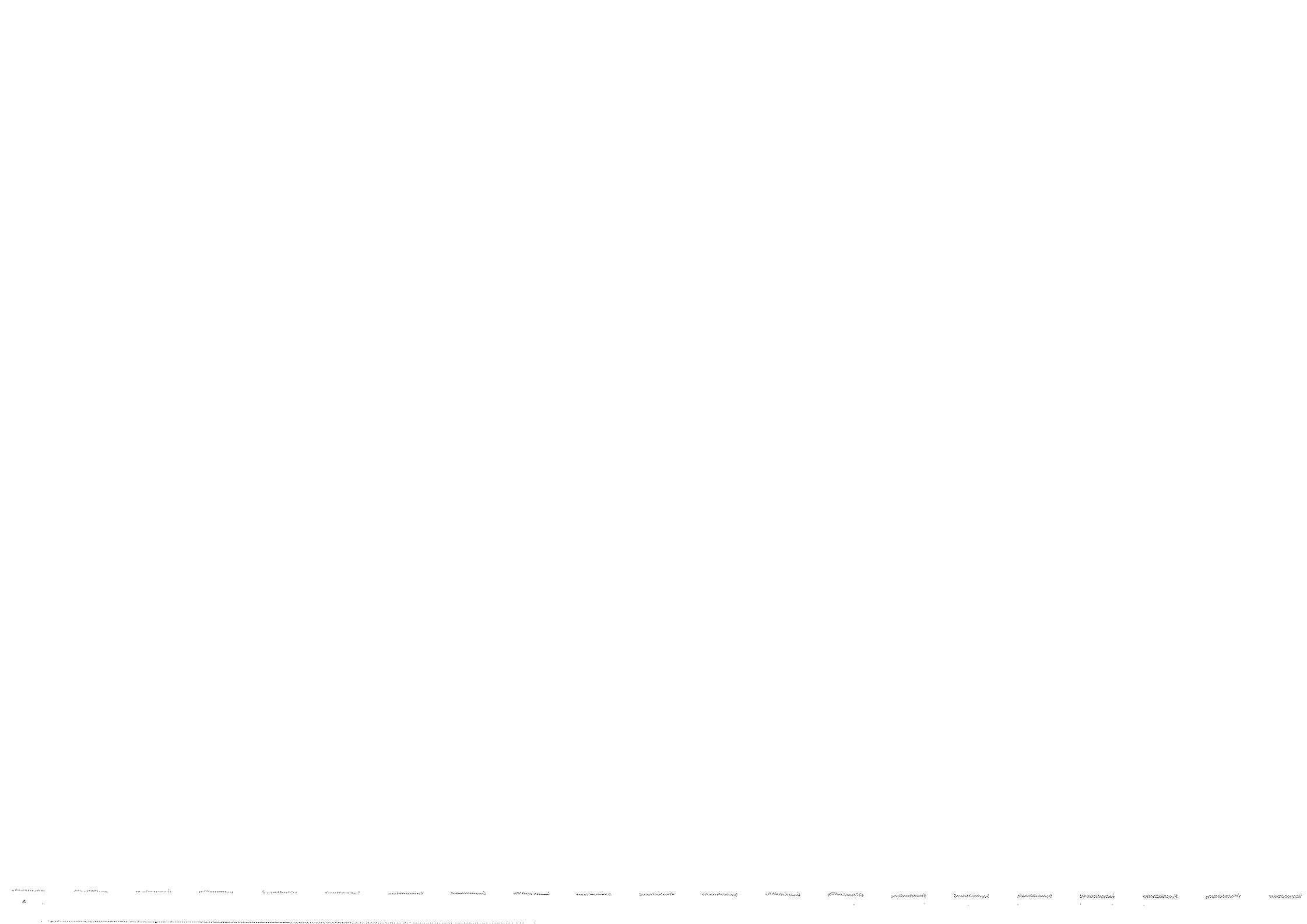


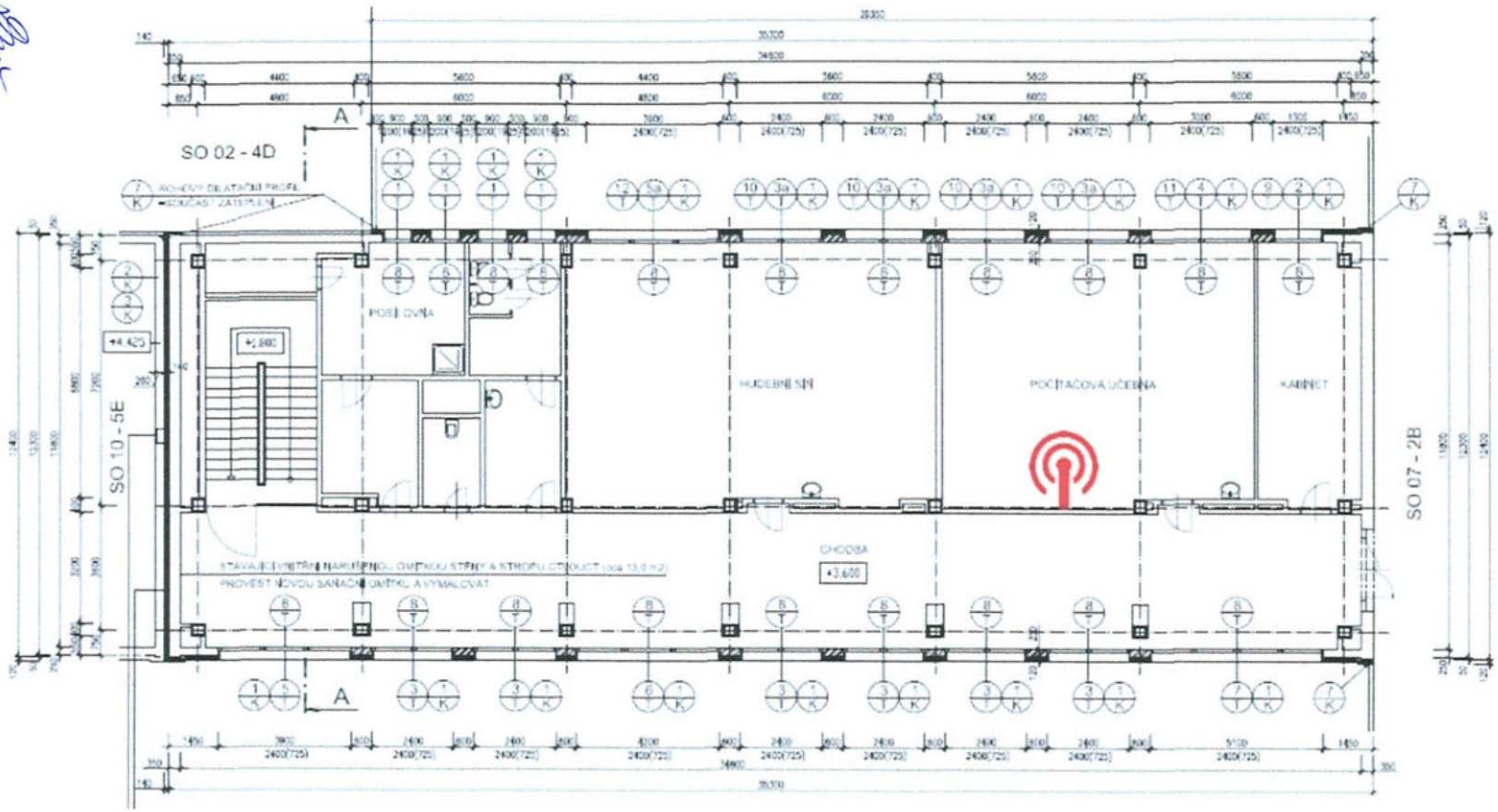
STAVEBNÍ ÚPRAVY Z
T.G.MASARYKA
FRYDLANT NAD

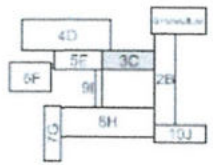
SO 02 STAVEBNÍ ÚPR
- TĚLOCV

Architektonické a stavebně technické

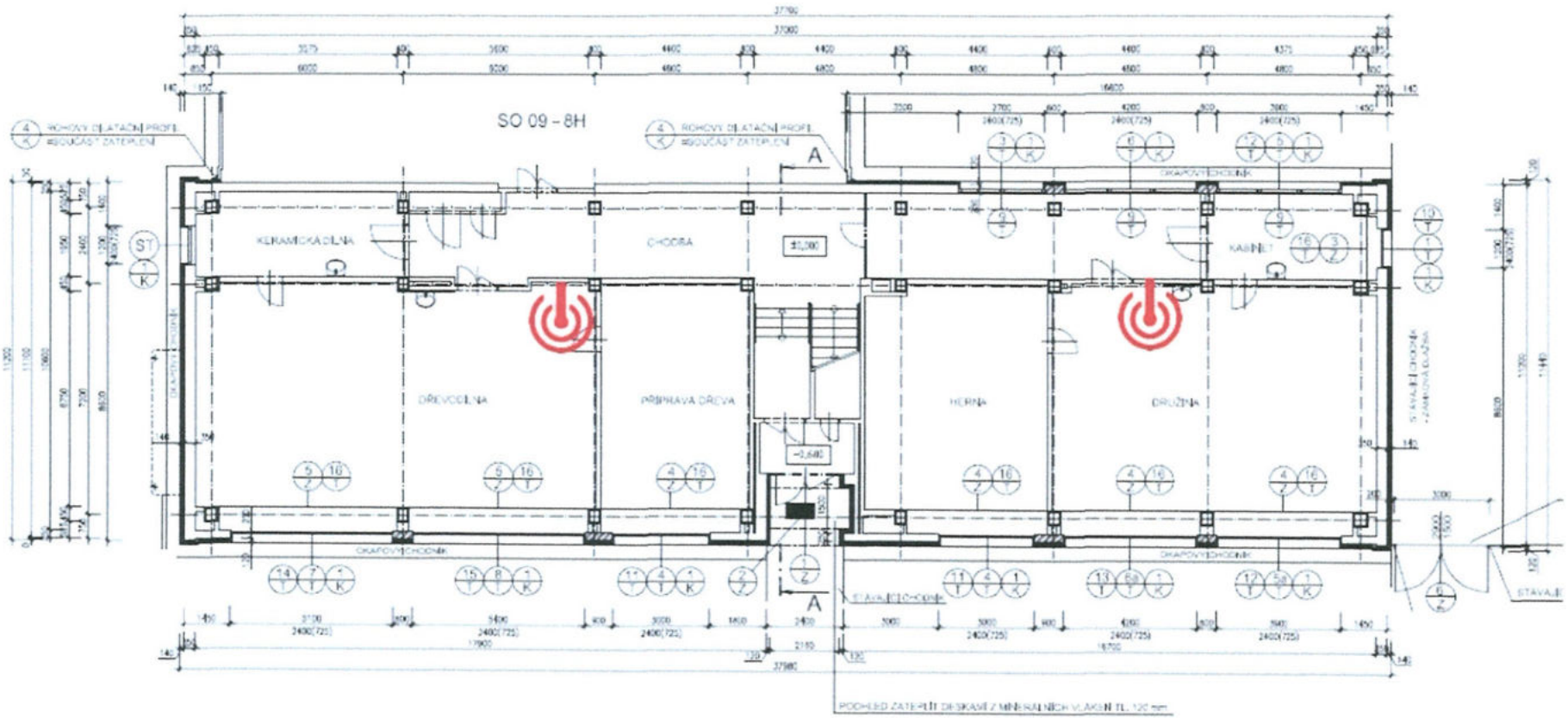
PŮDORYS

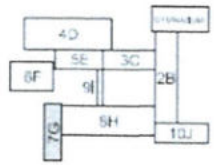




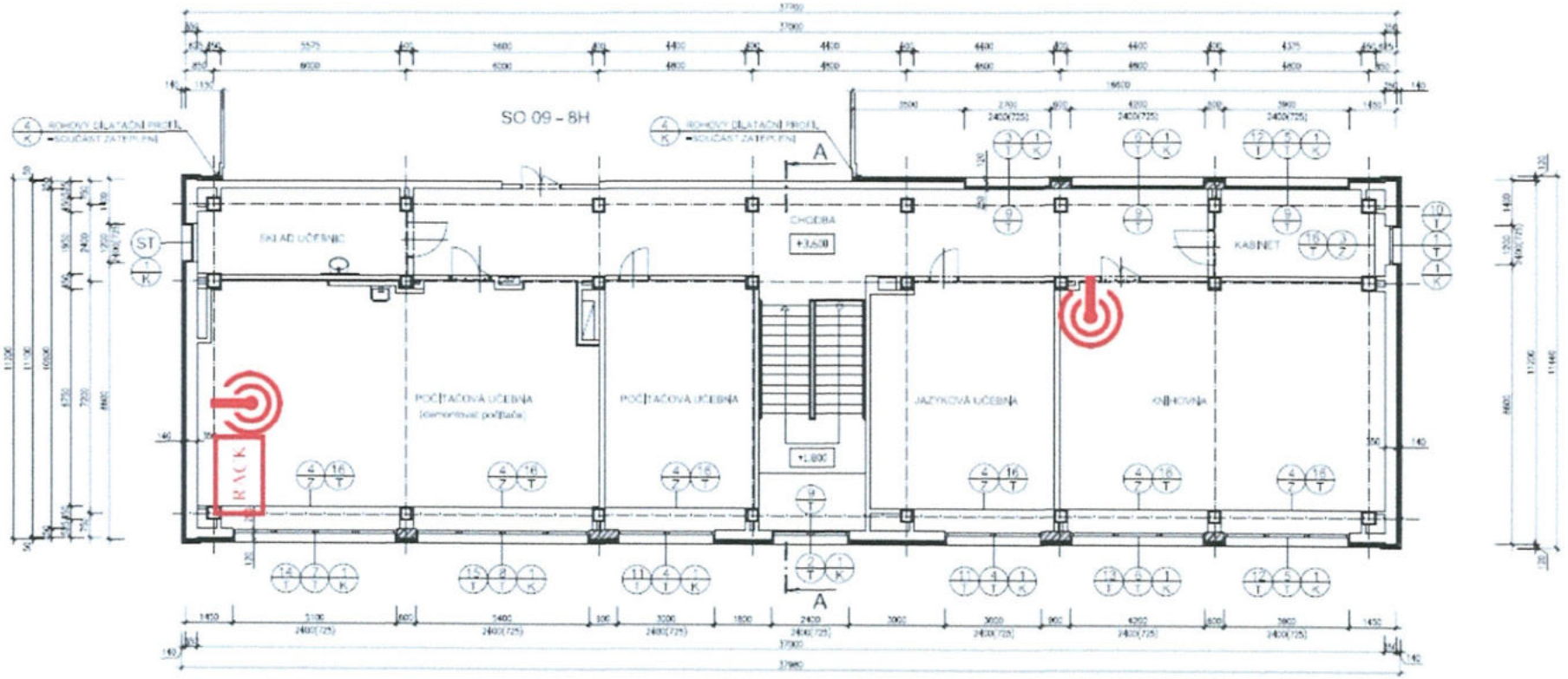


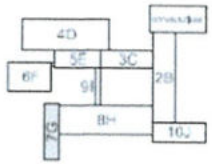
Stavba: STAVEBNÍ ÚPRAVY ZÁKLADNÍ ŠKOLY T.G.MASARYKA č.p. 1260, FRÝDLANT NAD OSTRAVICÍ		Číslo zakázky: 104/11	Stupeň: DPS
Objekt: SO 08 STAVEBNÍ ÚPRAVY OBJEKTU 3C - KLUBY ZŠ		Datum: leden/2013	Formát: 4x A4
Obsah: Architektonicko-stavební technická řešení: PŮDORYS 2NP		Měřítko: 1:100	Číslo přílohy: F.1.4.-3.



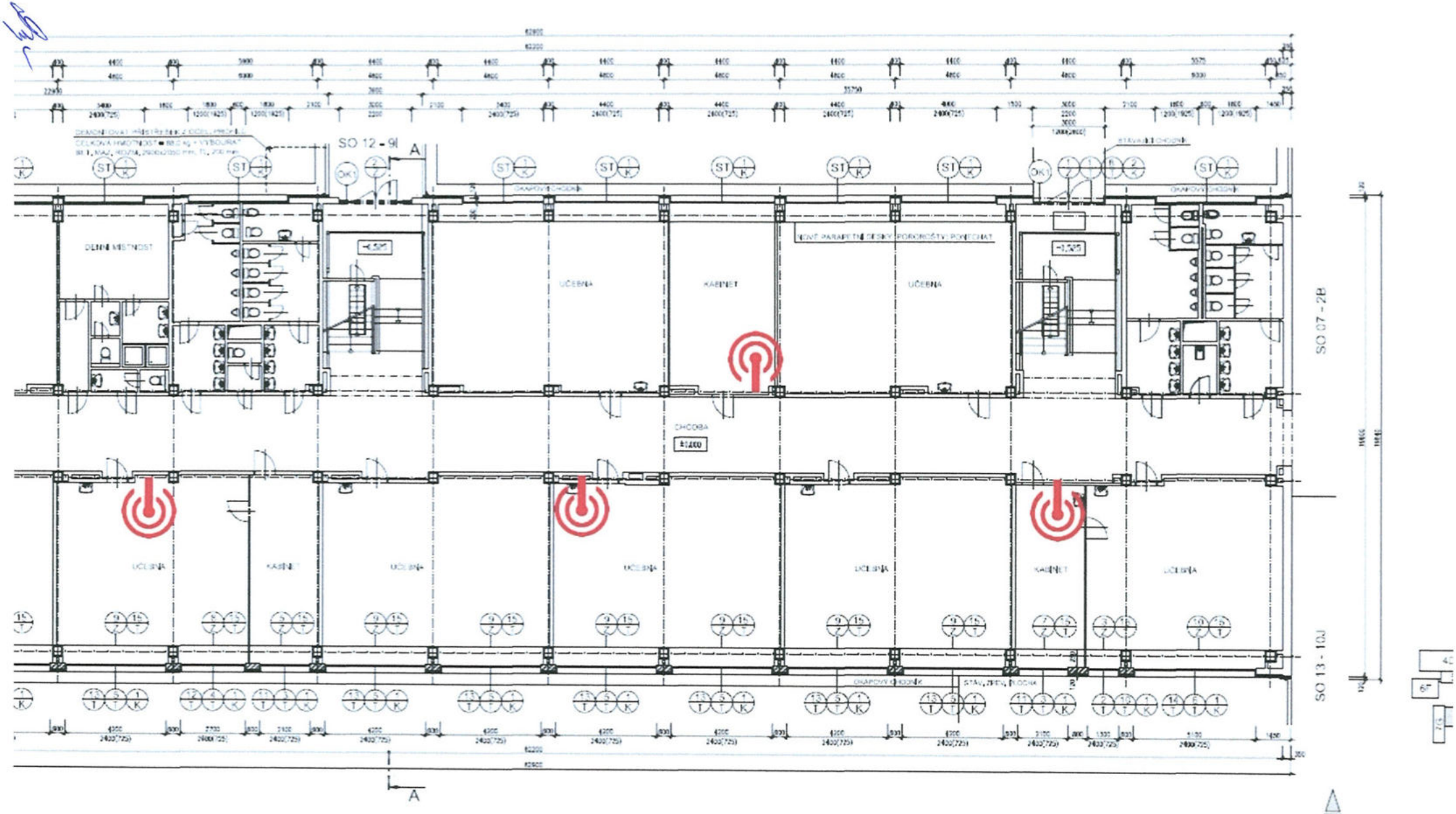


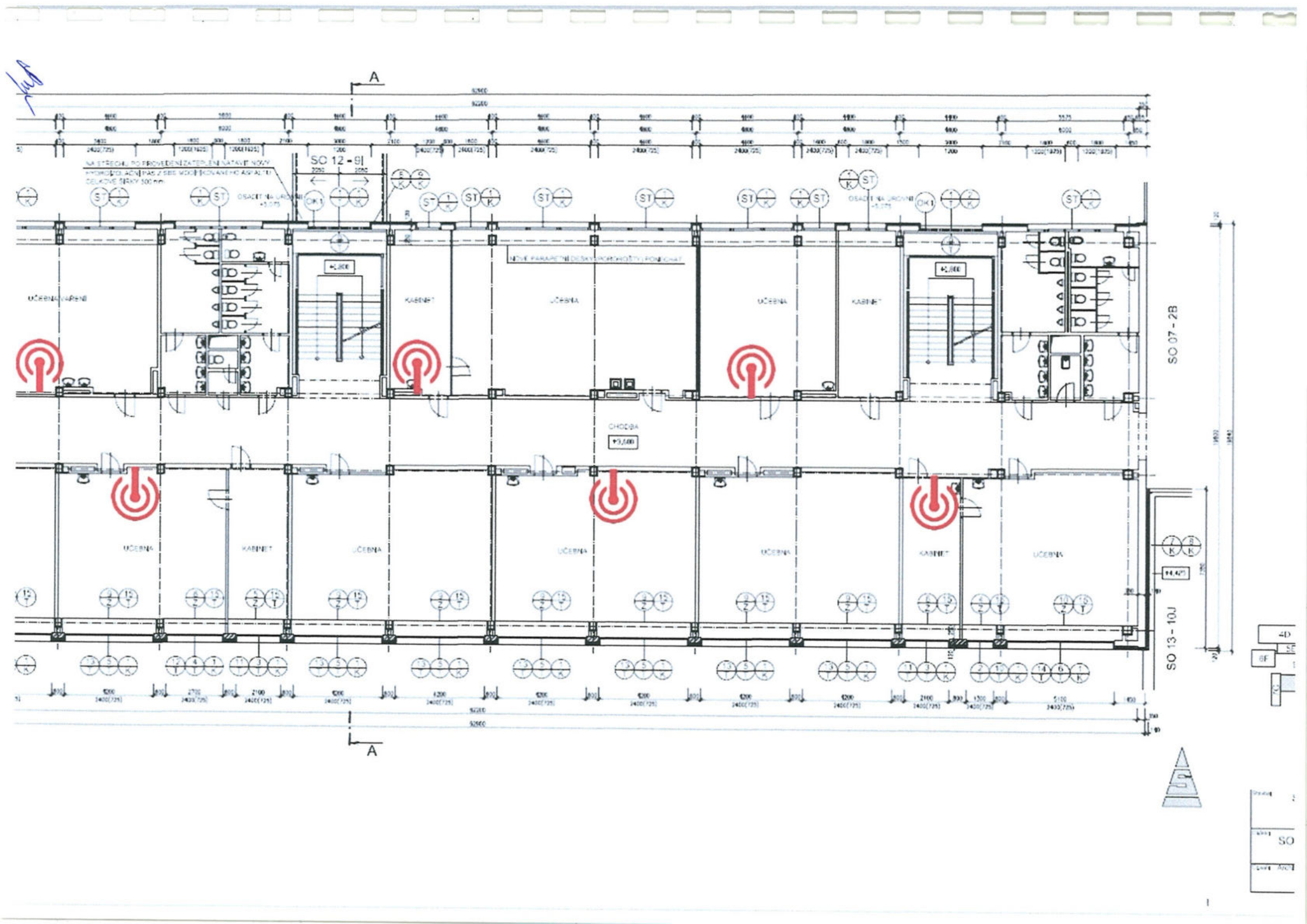
Stavba: STAVEBNÍ ÚPRAVY ZÁKLADNÍ ŠKOLY T.G.MASARYKA č.p. 1260 FRÝDLANT NAD OSTRAVICÍ		Číslo zakázky: 104/11	Stupeň: DPS
Část: SO 11 STAVEBNÍ ÚPRAVY OBJEKTU 7G - ŠKOLNÍ DÍLNY A DRUŽINA		Datum: leden/2013	Formát: A1
Obsah: Architektonicko a stavebně technické řešení: PŮDORYS 1NP		Měřítko: 1:100	Číslo přílohy: F.1.7.-2.

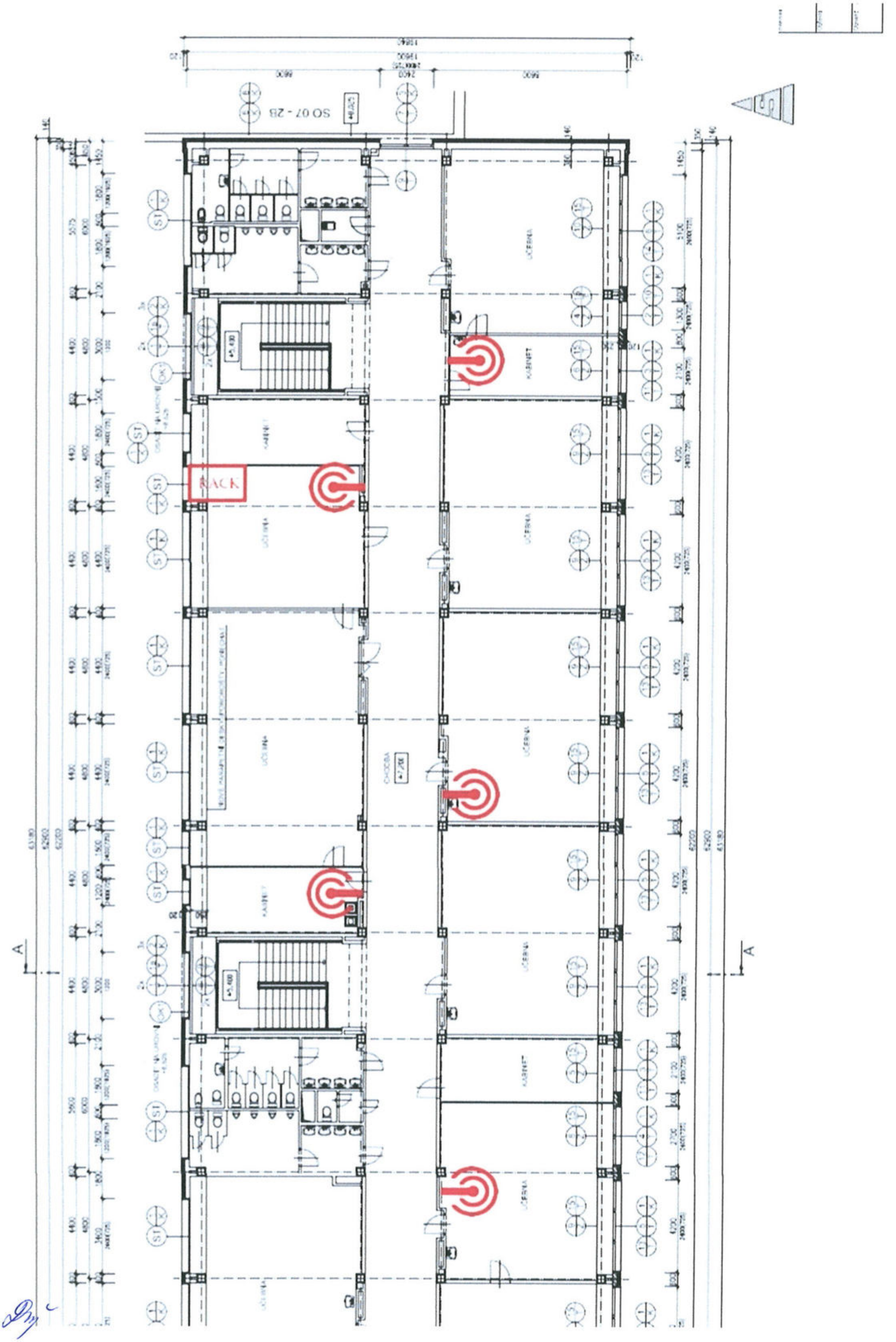


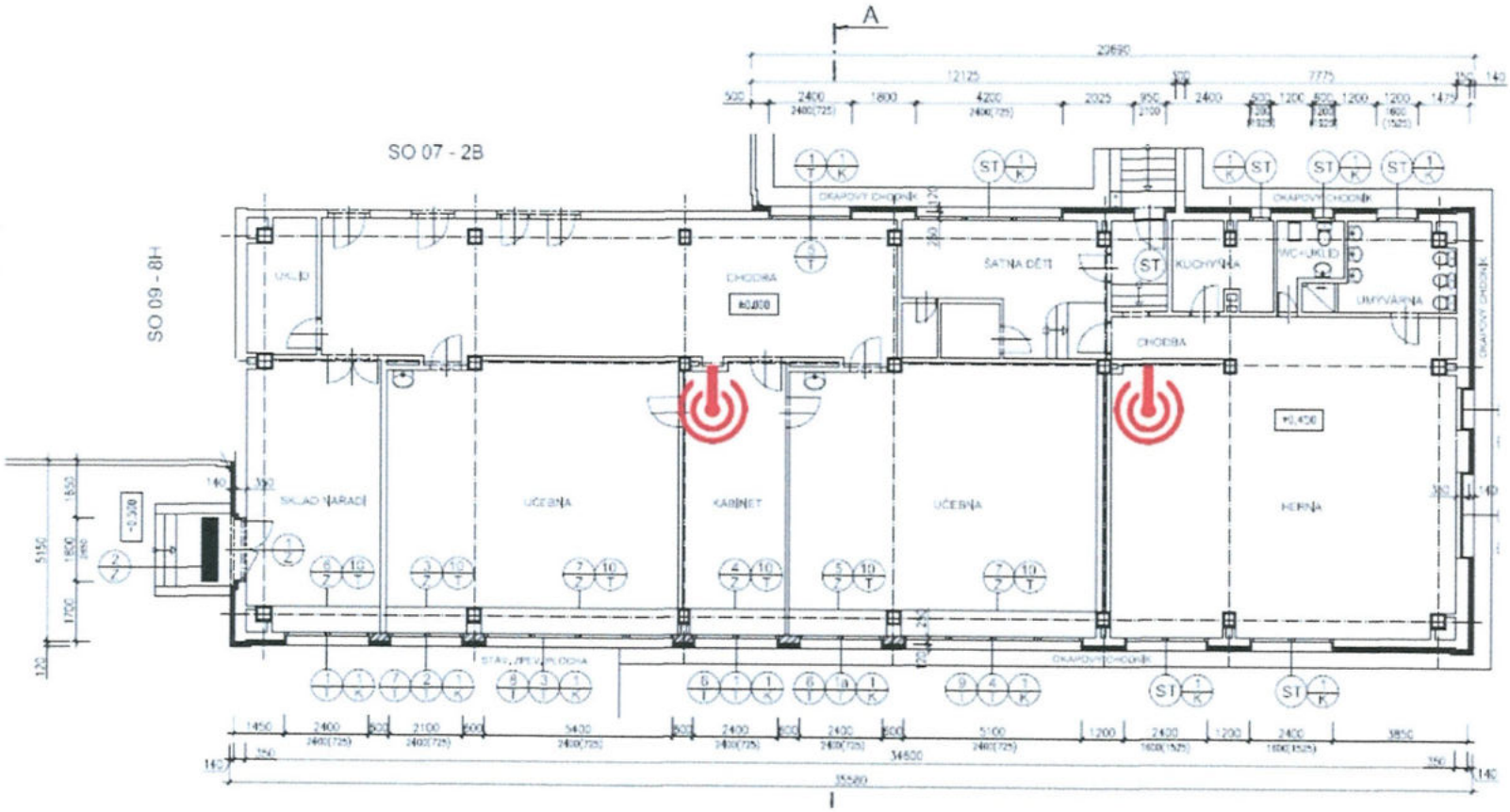


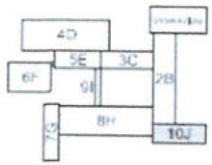
Stavba: STAVEBNÍ ÚPRAVY ZÁKLADNÍ ŠKOLY T.G.MASARYKA č.p. 1260, FRÝDLANT NAD OSTRAVICÍ		Číslo zakázky: 104/11	Stupeň: DPS
Objekt: SO 11 STAVEBNÍ ÚPRAVY OBJEKTU 7G - ŠKOLNÍ DÍLNY A DRUŽINA		Datum: leden/2013	Formát: 4x A4
Obsah: Architektonické a stavebně technické řešení	PŮDORYS 2NP	Měřítko: 1:100	Číslo přílohy: F.1.7.-3.


SO 12 - 9I
SO 07 - 2B
SO 13 - 10J
DENNÍ MÍSTNOST
UČEBNA
KABINET
UČEBNA
UČEBNA
KABINET
UČEBNA
UČEBNA
KABINET
UČEBNA
CHODBA
A
A


A
SO 12 - 9I
SO 07 - 2B
SO 13 - 10J
OSAZENÍ NA ÚROVNI +3,075
NOVÉ PARAPETNÍ DESKY POKRYTÉ PONTICHAT
UČEBNA
KABINET
CHODBA
+3,600
+4,800
+4,425
A


RACK





Stavba: STAVEBNÍ ÚPRAVY ZÁKLADNÍ ŠKOLY T.G.MASARYKA č.p. 1260, FRÝDLANT NAD OSTRAVICÍ		Číslo zakázky: 104/11	Stupeň: DPS
Objekt: SO 13 STAVEBNÍ ÚPRAVY OBJEKTU 10J - 1.ROČNÍK. MATEŘSKÁ ŠKOLKA		Datum: leden/2013	Formát: 4x A4
Část: Architektonické a stavebně technické řešení	PŮDORYS 1NP	Měřítko: 1:100	Číslo výkresu: F.1.9.-2.