

## **1.7 Počítačové vybavení**

### **1.7.1 Všeobecné údaje**

**Název stavby:**

**Objekt:** Základní škola Zachar, Kroměříž

**Název PS:** Slaboproud – SLP

**Místo stavby:**

**Zpracovatel projektu:** Zdeněk Indra

### **1.7.2 Výchozí podklady**

Pro zpracování této zprávy bylo použito následujících podkladů:

- Ing. Zona Jan - projekce
- Standard konektivity škol
- Současný stav počítačového vybavení

**Základní normy:**

#### ***Všeobecné***

Vyhláška č. 268/2011 Sb., kterou se mění vyhláška č. 23/2008 Sb., o technických podmínkách požární ochrany staveb

Vyhláška č. 221/2014 Sb., kterou se mění vyhláška č. 246/2001 Sb., o stanovení podmínek požární

bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci)

ČSN 34 2300, změna Z1, 09/2014 - Předpisy pro vnitřní rozvody sdělovacích vedení

ČSN 73 0804, změna Z2 02/2015 - Požární bezpečnost staveb – Výrobní objekty

ČSN 73 0848, 04/2009 - Požární bezpečnost staveb – Kabelové rozvody

ČSN 33 4000, změna 09/1990 - Požadavky na odolnost sdělovacích zařízení proti přepětí a nadproudu

#### ***STRUKTUROVANÁ KABELÁŽ***

ČSN EN 50173-1 ed.3, 04/2012 - Informační technologie - Univerzální kabelážní systémy – Část 1:

Všeobecné požadavky

ČSN EN 50173-2, 05/2008 - Informační technologie - Univerzální kabelážní systémy – Část 2:

Kancelářské prostory

ČSN EN 50174-1 ed.2, 05/2010 - Informační technologie - Instalace kabelových rozvodů – Část 1:

Specifikace a zabezpečení kvality

ČSN EN 50174-2 ed.2, 05/2010 - Informační technologie - Instalace kabelových rozvodů – Část 2:

Projektová příprava a výstavba v budovách

### **1.7.3 ZÁKLADNÍ TECHNICKÉ ÚDAJE**

#### **Napěťové soustavy:**

- Silová soustava – síťové napájení 230V/50Hz: 1 NPE AC 230 V / TN-S

#### **Ochrana před úrazem elektrickým proudem dle ČSN EN 61140:**

- základní ochrana, ochrana při poruše

#### **Ochranná opatření dle ČSN 332000-4-41 ed. 2**

- Ochrana před dotykem neživých částí elektrického zařízení dle čl. 413:
- Silové rozvody 230V/50Hz: samočinným odpojením od zdroje, dvojítá, nebo zesílená izolace
- Sdělovací rozvody: malým napětím SELV
- Ochrana před dotykem živých částí elektrického zařízení dle čl. 412:
- je dána jejich konstrukčním uspořádáním a je řešena některou z těchto ochranných opatření: polohou, zábranou, krytem nebo přepážkami, izolací živých částí, doplňkovou izolací a doplňkovou ochranou proudovým chráničem.

#### **Vnější vlivy dle ČSN 33 2000-3, 332000-5-51**

- Prostředí: protokol o vnějších vlivech nebyl v době zpracování této projektové dokumentace k dispozici. Dle získaných podkladů a dle charakteru objektu, by mělo být zařízení, včetně rozvodů, umístěno v prostorech s prostředím normálním.

### **1.7.4 TECHNICKÁ ZPRÁVA - Strukturovaná kabeláž – SK**

#### **1. Popis řešení**

V objektu bude instalován páteřní a horizontální rozvod strukturované kabeláže (SK) UTP cat. 5e. V místnosti Informatiky bude osazena 1 skříň (rack) hlavního datového rozvaděče DR1. V učebně Informatiky bude 20 pracovišť žáků se stolními PC a 10 pracovišť žáků vybavenými nově notebooky, jedno pracoviště učitele se stolním PC celkově 30 pracovišť pro žáky. V učebně Chemie je 10 pracovišť žáků vybavené notebooky 1 pracoviště učitele se stolním PC. Učebna chemie je osazena interaktivní tabulí.

Hlavní datový rozvaděč bude propojen s podružnými rozvaděči páteřními propoji – vždy 4x metalickým kabelem UTP 4x2x0,5 cat. 5e., 1x optickým kabelem 24 vláken, SM, 9/125μm, OS1. Tyto páteřní propoje budou ukončeny na metalických, resp. optických, (patch) panelech. Venkovní přípojky případných operátorů (poskytovatelé internetových a TV služeb) nejsou v rámci projektu SLP řešeny.

V rámci dodávky SK v objektu budou v jednotlivých učebnách osazeny zásuvky, resp. připraveny vývody SK pro napojení zařízení (počítačů) do sítě LAN. Zásuvky budou řešeny

jako jednoportové a dvouportové do zdi, nebo na omítku, budou ukončeny konektorem RJ45. Počet a rozmístění zásuvek je patrný z výkresové dokumentace.

Horizontální rozvody strukturované kabeláže budou vedeny od zásuvek a vývodů do příslušných datových rozvaděčů, kde budou ukončeny na propojovacích (patch) panelech. Silové zásuvky určené pro připojení aktivních prvků jsou opatřeny přepětovou ochranou.

V místnosti Informatiky je umístěn centrální datový rozvaděč s připojením WAN. Dále je zde umístěn File server a server s AD. Odtud jsou data již distribuována do ostatních datových rozvaděčů v objektu školy prostřednictvím optických a metalických páteřních rozvodů. Datové rozvaděče jsou osazeny přepínači 10/100/1000 Mb/s s parametry dle výše uvedených požadavků.

V rámci projektu je navrženo osazení přístupových bodů (access point) bezdrátové WiFi sítě SK. Přístupové body budou rozmístěny tak, aby kompletně a co nejlépe pokryly všechny prostory daného patra objektu. Počet a rozmístění přístupových bodů bude optimalizováno v rámci realizace po dokončení stavebních prací a po měření signálu v objektu pomocí SW. Přístupové body budou řízeny a spravovány pomocí síťového kontroléru integrovaného do centrálního řídicího prvku.

Správa uživatelů je řešena prostřednictvím serveru SR1 s AD (active directory). Zařízení je dimenzováno pro správu všech uživatelů v přistupujících do LAN – tj 600 členů.

## **2. Provedení**

Veškeré metalické rozvody (horizontální i páteřní) budou provedeny kabely UTP 4x2x0,5, cat. 5e. Optické páteřní rozvody budou provedeny univerzálním optickým kabelem 24 vl., SM, 9/125 µm, OS1.

Kabely budou vedeny jednak v páteřních kovových drátěných žlabech osazených pod podlahou a v podlaze, a jednak v trubkách zasekaných do zdi, nebo v ohebných trubkách popřípadě žlabech v nábytku. V technických prostorech bude kabeláž vedena v tuhých trubkách po povrchu. Veškeré kabelové prostupy požárně dělicími konstrukcemi mezi jednotlivými požárními úseky budou dle ČSN 73 0848, 04/2009 – Požární bezpečnost staveb – Kabelové rozvody, kap. 5.2.8. utěsněny požárními ucpávkami.

## **3. Aktivní prvky –AP**

Z důvodu zabezpečení standardu konektivity škol je navrženo osazení prvky s možností plného managementu. Na rozhraní WAN/ LAN je osazen řídicí prvek zajišťující následující funkce:

- podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)
- síťové zařízení podporující rate limiting, antispoofing, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality
- 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
- možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků
- podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online

- Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3 s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,...
- 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
- Povinné řešení systému správy uživatelů (Identity Management), tj. centrální databáze identit (LDAP, AD, apod.) a její využití pro autentizaci uživatelů (žáci i učitelé) za účelem bezpečného a auditovatelného přístupu k síti, resp. síťovým službám.
- logování přístupu uživatelů do sítě umožňující dohledání vazeb *IP adresa – čas – uživatel*

Aktivní prvky (switche) zajišťující vnitřní konektivitu umožňují následující funkce:

- Minimální konektivita stanic a dalších koncových zařízení 100Mbit/s full duplex
- Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s full duplex
- Pátevní rozvody mezi budovami v areálu realizovány prostřednictvím optických nebo metalických vláken
- Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3 s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,...

Bezdrátové komponenty splňují následující parametry:

- Podpora mechanismu izolace klientů
- 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
- 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
- Minimálně pasivní zapojení do federovaného systému eduroam. Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů.
- Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu

V LAN jsou navržena další zařízení vyhovující následujícím bezpečnostním požadavkům:

- Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů

- Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.)
- Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, bloky wifi v určitém čase)
- Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací a zpřístupnění jejich služeb)
- Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3954 nebo ekvivalent (NetFlow))
- Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie
- Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management)
- Systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios / Icinga)
- Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk)
- Nástroje pro centrální správu a audit ICT prostředků
- Systémy zálohování a obnovy dat serverové infrastruktury
- Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů
- Zabezpečení přístupových protokolů (SSL/TLS) služeb (např. emailové služby, webové servery, studijní a ekonomické agendy) atp.
- Podpora vzdáleného přístupu (VPN)

### **Zásady bezpečnosti a ochrany zdraví při práci na staveništi a ochrany zdraví podle jiných právních předpisů**

Při montáži budou dodržovány v době realizace platné zákony, vyhlášky, prováděcí předpisy, ČSN a technologické předpisy, především: Zákon č. 262/2006 Sb. zákoník práce, NVč.591/2006 Sb.

O bližších minimálních požadavcích na bezpečnost práce a ochranu zdraví při práci na staveništích, NV č. 494/2001Sb. o evidenci a hlášení pracovních úrazů, z.č.309/2006 Sb. o BOZP, NV č. 362/2005 Sb. o bližších požadavcích na bezpečnost práce a ochranu zdraví při práci na pracovištích s nebezpečím pádu z výšky nebo do hloubky.

Přesný postup prací stanoví zhotovitel.

Technologické postupy a opatření se musí vždy přizpůsobit aktuální situaci na místě montáže.

Montáž bude prováděna za provozu, je potřeba vyžádat součinnost bezpečnostního technika investora stavby.

Na realizaci se bude podílet více než jeden zhotovitel, je tedy dle z. č. 309/2006 Sb. potřeba koordinátor BOZP.