

**štítek**

## Úvod

Předmětem projektové dokumentace je výměna aktivních prvků, UPS a vybudování nové optické páteře v objektu.

UHK PALACHOVY KOLEJE, č.p. 1129 - 1135 a 1289  
ČÁSTEČNÁ REKONSTRUKCE A MODERNIZACE - I. ETAPA

Projekt je vypracován ve stupni **pro provedení stavby DPS**.

## Prostředí dle ČSN 33 2000-5-51 ED.3

Pokud není ve výkresové části uvedeno jinak, pak ve všech vnitřních prostorech je stanoveno působení vnějších vlivů:

### Vnitřní prostory

AA5, AB5, AC1, AD1, AE1, AF1, AG1, AH1, AK1, AL1, AM1, AN1, AP1, AQ1, AR1, AS1, BA4, BC1, BD1, BE1, CA1, CB1. - prostory normální.

## Podklady pro zpracování projektu

Projekt je zpracován na základě následujících podkladů:

- obhlídka objektu
- stavební půdorysy jednotlivých podlaží v elektronické podobě
- koordinační schůzky s projektanty ostatních profesí
- konzultace s generálním dodavatelem projektu
- platné ČSN v době zpracování projektové dokumentace

### Kompatibilita

Vzhledem k tomu, že se jedná o rozšíření stávajících prvků a výměnu většiny dosluhujících přístupových aktivních prvků datové sítě je nutné zachovat vzájemnou kompatibilitu se stávajícím prostředím.

### Systémová záruka

Na veškerou datovou kabeláž je požadována systémová záruka výrobce na systém strukturované kabeláže na dobu 20 roků.

### Úprava datových rozvaděčů

Ve všech datových rozvaděčích bude provedena výměna stávajících aktivních prvků a budou instalovány nové UPS. Je nutné uvažovat s případnou úpravou HW prvků datových rozvaděčů.

### UPS

Stávající UPS budou demontovány a budou nahrazeny novým záložním zdrojem UPS a budou vybaveny kartou dálkového dohledu.

### Optická páteř

Hlavní rozvaděč je umístěn v 1.PP vchod B Palachovy koleje, z tohoto rozvaděče budou do hvězdy připojeny podružné datové rozvaděče na vchodech D, E, F a vrátnici. Optická kabeláž bude instalována v ochranné mikrotrubičce, která bude vedena novou kabelovou trasou v 1.PP přes jednotlivé vchody v drátěném kabelovém žlabu 150x35 po stropem. Optická kabeláž bude ukončena v optické vaně na LC konektorech. Do rozvaděče na vrátnici bude trubička vedena vkladací lištou po povrchu.

### **Kabelové nosné systémy**

Mezi jednotlivými datovými uzly bude v prostoru v 1.PP pod stropem instalován drátěný žlab 150x35 a bude procházet přes jednotlivé vchody. Všechny prostupy železobetonová konstrukcí budou po montáži vyplněny univerzální stavební pěnou.

Trasa kabelového žlabu bude uzpůsobena dle stávajících rozvodů vody a potrubí, které jsou vedeny v souběhu s plánovanou kabelovou trasou optické páteře.

### **Kabelová trasa do vrátnice**

Kabelová trasa do vrátnice bude provedena v nových vkládacích lištách. V prostoru 1.PP je možno použít stávající kabelové trasy. Uvažuje se s vybudováním nových kabelových prostupů, případně budou upraveny stávající.

V prostoru krytého schodiště je možno provést kabelovou trasu nad stáv. podhledy (PD uvažuje o instalaci vkládací lišty na povrchu).

### **Popis stáv. stavu a požadavky na vybavení**

Metropolitní i jednotlivé lokální počítačové sítě Univerzity Hradec Králové jsou tvořeny aktivními prvky společnosti Cisco Systems a tvoří jednotný celek. Přepínače zajišťují jak L2, tak L3 komunikaci. LAN infrastruktura univerzity je virtualizována do více VLAN, což reflektuje existenci více typů uživatelů a potřebu tyto různé uživatele od sebe izolovat.

Jedním z velmi důležitých aspektů implementace VLAN je využití tzv. end-to-end konceptu, kde jsou jednotlivé VLAN roztaženy napříč celou nebo velkou částí univerzitní sítě. L2 topologie je plně řízena Cisco Per-VLAN STP protokolem, který dovolí jednak přesně reflektovat geografické potřeby každé VLAN, jednak umožňuje optimalizovat využití celkové kapacity sítě. Databáze VLAN je mezi přepínači synchronizována protokolem VTP. Dodávané zařízení musí být podporováno v současné době provozovanými management SW Cisco Prime ver. 3.1, SNMP monitoring Cacti a Icinga. Každé dodané nebo rozšiřované zařízení, které umožňuje správu provozovaným managementem, musí být vybaveno licencí pro přístup k těmto centrálním management software. Ověřování přístupu k aktivním prvkům je prováděno prostřednictvím protokolu TACACS+ oproti Cisco ACS ve verzi 5.6. Je nutné zajistit plnou kompatibilitu se všemi řídicími protokoly, které se již nyní uvnitř sítě UHK využívají, tak aby nedošlo k navýšování nákladů a zvýšení pracnosti na správu infrastruktury. Kriticky důležité je zejména zajištění stability L2 topologie. Nově dodané aktivní prvky proto musí být plně kompatibilní s Cisco Per-VLAN STP protokolem. Dále je třeba zajistit kompatibilitu s VTP protokolem. Z pohledu dalšího rozvoje univerzitní sítě je počítáno s ukončením vybraných VLAN na agregačních přepínačích budov. Kvůli bezpečnosti přitom budou různé skupiny VLAN ukončeny v různých instancích směrovací tabulky.

Personál Centra informačních technologií UHK je se stávající LAN infrastrukturou a s provozovanou technologií obeznámen/proškolen/certifikován tak, aby ji byl sám schopen spravovat a plně konfigurovat. Náklady na vybudování celouniverzitní počítačové sítě přesáhly desítky milionů Kč. Dodání aktivních prvků jiných výrobců je přípustné v případě, že součástí dodávky budou i potřebné licence pro řídicí a monitorovací SW, případně nové nástroje pro řízení a monitorování této rozsáhlé sítě, dále pak dojde k zaškolení personálu CIT UHK na stejnou úroveň jako je nynější. Proškolení by mělo být 9 osob do následující úrovně:

- Technologie LAN přepínačů - základní konfigurace přepínače, VLAN sítě, konfigurace Trunk rozhraní
- Statické a dynamické směrování (OSPF), směrování mezi různými VLAN
- Nastavení DHCP, ACL, NAT, Overloading
- Nastavení zabezpečení síťových zařízení - SSH, nastavení hesel, Port security
- Řešení problémů v datových sítích
- Podrobná metodika návrhu logické oblasti Enterprise Campus (moduly Campus Infrastructure, Network Management, Server Farm, Edge Distribution) a logické oblasti Enterprise Edge (moduly WAN, Remote Access & VPN, Internet Connectivity, ECommerce)

- Návrh síťové správy a managementu
- Návrh služeb vysoké dostupnosti (high availability)
- Návrh efektivní IP adresace (segmentace)
- Návrh škálovatelného a efektivního směrování
- Návrh datacentrových řešení v Campus síti
- Návrh bezpečnostního řešení
- Návrh hardwarové virtualizace (VSS, vPC, StackWise)
- Návrh QoS Návrh Multicast služeb Návrh VPN sítí
- Návrh bezdrátových sítí Návrh řešení IP telefonie
- Metodologie návrhu sítí
- Strukturalizace a modularizace návrhu sítí
- Návrh sítí v campusu a v datových centrech
- Design vzdáleného připojení
- IP adresace a routovací protokoly
- Security řešení pro sítě
- Identifikace síťových požadavků pro wireless
- Implementace a zprovoznění síťového designu
- Implementace řešení založeném na EIGRP
- Tunelování Q-in-Q
- Rapid spanning tree IEEE802.1w
- Multiple spanning tree IEEE802.1s
- Dodatečné spanning tree funkce (root guard, bpdu guard, loop guard, bpdu filter, UDLD)
- Private VLAN

Pro připojení pevných přípojných míst jsou na každý vhod potřeba 3 kusy 48 portových přepínačů. Všechny páteřní propojovací linky, včetně páteřních rozvodů uvnitř budov, budou optické, redundantně zapojené o rychlosti 10 Gbit/s.

Kvůli efektivnímu nakládání se síťovou kapacitou budou přepínače sloučeny do jednoho virtuálního šasi. Díky tomu bude možné obě linky mezi přístupovou a agregační vrstvou sloučit do jednoho 20Gbit/s port-channelu.

### Mandatorní požadavky pro přístupové přepínače

Přístupový přepínač – typ 1 – verze POE		
Popis parametru	Požadovaná hodnota	Parametry nabízené zboží
Výrobce zařízení	Uvedení výrobce	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	
		Splňuje požadovaný parametr ANO/NE
Typ přepínače	L2/L3 přepínač	
Formát přepínače	Stohovatelný	
Uplink porty	4x10GE SFP+	
Počet portů 10/100/1000 Base-TX	48	
PoE (IEEE 802.3af)	ANO	
PoE+ (IEEE 802.3at)	ANO	
Dostupný výkon pro PoE napájení	740W	
Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače	ANO	
Minimální propustnost přepínacího subsystému	170 Gbit/s	
Minimální paketový výkon přepínače	260 mil. paketů/s	
Stohování požadováno	ANO	
Počet dedikovaných stohovacích portů	2	
Minimální počet zařízení ve stohu	8	
Minimální kapacita sběrnice stohu	80 Gb/s	
Datový stohovací kabel požadován	ANO	
Stateful Switch Over v rámci stohu (okamžité převzetí funkce náhradním řídicím modulem)	ANO	
Možnost instalovat interní redundantní napájecí zdroj	ANO	
Interní redundantní napájecí zdroj požadován	NE	
Redundantní ventilátory	ANO	
Velikost MAC address tabulky	16000	
Min. počet IPv4 routes	1000	
Min. počet IPv6 routes	1000	
Min. počet konfigurovatelných security ACL	1000	

IEEE 802.3ad (Link Aggregation)	ANO	
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	
Minimální počet konfigurovatelných Link Aggregation Group trunků	32	
IEEE 802.1Q	ANO	
Minimální počet aktivních VLAN	1000	
IEEE 802.1x	ANO	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	
RADIUS CoA	ANO	
Podpora instance spanning-tree protokolu per VLAN	ANO	
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	
Podpora jumbo rámců (min. 9198 bytes)	ANO	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	
Směrování protokolů IPv4 a IPv6 v hardware	ANO	
OSPFv2	ANO	
OSPFv3	ANO	
ISIS	ANO, povýšením firmware	
IP Multicast (PIM SSM, PIM SM)	ANO, povýšením firmware	
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	
Reverse path check (uRPF) pro IPv4 i IPv6	ANO, povýšením firmware	
IGMPv2, IGMPv3	ANO	
IGMP snooping	ANO	
MLD snooping	ANO	
Minimální počet HW QoS front	8	
QoS classification – ACL, DSCP, CoS based	ANO	
QoS marking - DSCP, CoS	ANO	
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	
QoS Policing	ANO	
QoS-Hierarchical QoS	ANO, min. 2 úrovně	
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	
Možnost definovat povolené MAC adresy na portu	ANO	

PACL, VACL	ANO	
IEEE 802.1ae na uplink portech	ANO	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	
SSHv2	ANO	
CLI rozhraní	ANO	
SNMPv2/v3	ANO	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	
NTPv3 server	ANO	
Licence k management software	ANO	

Přístupový přepínač – typ 2 – verze bez POE		
Popis parametru	Požadovaná hodnota	Parametry nabízené zboží
Výrobce zařízení	Uvedení výrobce	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	
		<b>Splňuje požadovaný parametr ANO/NE</b>
Typ přepínače	L2/L3 přepínač	
Formát přepínače	Stohovatelný	
Uplink porty	4x10GE SFP+	
Počet portů 10/100/1000 Base-TX	48	
Minimální propustnost přepínacího subsystému	170 Gbit/s	
Minimální paketový výkon přepínače	260 mil. paketů/s	
Stohování požadováno	ANO	
Počet dedikovaných stohovacích portů	2	
Datový stohovací kabel požadován	ANO	
Minimální počet zařízení ve stohu	8	
Minimální kapacita sběrnice stohu	80 Gb/s	
Stateful Switch Over v rámci stohu (okamžité převzetí funkce náhradním řídicím modulem)	ANO	
Možnost instalovat interní redundantní napájecí zdroj	ANO	
Interní redundantní napájecí zdroj požadován	NE	
Redundantní ventilátory	ANO	
Velikost MAC address tabulky	16000	
Min. počet IPv4 routes	1000	
Min. počet IPv6 routes	1000	
Min. počet konfigurovatelných security ACL	1000	
IEEE 802.3ad (Link Aggregation)	ANO	
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	
Minimální počet konfigurovatelných Link Aggregation Group trunků	32	
IEEE 802.1Q	ANO	



Minimální počet aktivních VLAN	1000	
IEEE 802.1x	ANO	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	
RADIUS CoA	ANO	
Podpora instance spanning-tree protokolu per VLAN	ANO	
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	
Podpora jumbo rámců (min. 9198 bytes)	ANO	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	
Směrování protokolů IPv4 a IPv6 v hardware	ANO	
OSPFv2	ANO	
OSPFv3	ANO	
ISIS	ANO, povýšením firmware	
IP Multicast (PIM SSM, PIM SM)	ANO, povýšením firmware	
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	
Reverse path check (uRPF) pro IPv4 i IPv6	ANO, povýšením firmware	
IGMPv2, IGMPv3	ANO	
IGMP snooping	ANO	
MLD snooping	ANO	
Minimální počet HW QoS front	8	
QoS classification – ACL, DSCP, CoS based	ANO	
QoS marking - DSCP, CoS	ANO	
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	
QoS Policing	ANO	
QoS-Hierarchical QoS	ANO, min. 2 úrovně	
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	
Možnost definovat povolené MAC adresy na portu	ANO	
PACL, VACL	ANO	
IEEE 802.1ae na uplink portech	ANO	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	

Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloADERu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	
SSHv2	ANO	
CLI rozhraní	ANO	
SNMPv2/v3	ANO	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	
NTPv3 server	ANO	
Licence k management software	ANO	

Michal Pipek  
04/2019