Požadované parametry dodávky

Předmětem veřejné zakázky je **dodávka, konfigurace a instalace** aktivních síťových prvků dle technických podmínek uvedených níže.

- Místo dodání zařízení je budova **CIV, Univerzitní 20, Plzeň**, pokud není dále stanoveno jinak.
- Požadovaná minimální konfigurace síťových prvků je popsána v kapitole ***Další technické požadavky*****.** Konkrétní parametry konfigurace dodá zadavatel dodavateli před realizací dodávky.
- Rozmístění jednotlivých síťových prvků je popsáno v kapitole ***Požadovaná topologie síťových prvků*****.**
- Požadavky na instalaci aktivních síťových prvků jsou popsány v kapitole ***Fyzická instalace zařízení.***

Počty aktivních síťových zařízení a jejich typy

Kolej Máchova budova Máchova 20

- 1 ks páteřní přepínač/směrovač

Kolej Máchova budova Máchova 14

- 5 ks 48 portový přístupový přepínač
- 1 ks 48 portový přístupový přepínač s napájením po Ethernetu

Kolej Máchova budova Máchova 16

- 5 ks 48 portový přístupový přepínač
- 1 ks 48 portový přístupový přepínač s napájením po Ethernetu

Kolej Máchova budova Baarova 36

- 11 ks 48 portový přístupový přepínač
- 2 ks 48 portový přístupový přepínač s napájením po Ethernetu

Kolej Máchova budova Klatovská 100

- 4 ks 48 portový přístupový přepínač
- 1 ks 24 portový přístupový přepínač s napájením po Ethernetu

Kolej Borská budova Borská 53 A1

- 1 ks páteřní přepínač/směrovač
- 5 ks 48 portový přístupový přepínač
- 1 ks 48 portový přístupový přepínač s napájením po Ethernetu

Kolej Borská budova Borská 53 A2

- 4 ks 48 portový přístupový přepínač
- 1 ks 48 portový přístupový přepínač s napájením po Ethernetu

Kolej Borská budova Borská 53 A3

- 5 ks 48 portový přístupový přepínač
- 1 ks 48 portový přístupový přepínač s napájením po Ethernetu

Kolej Borská budova Borská 53 A4

- 1 ks 48 portový přístupový přepínač
- 1 ks 48 portový přístupový přepínač s napájením po Ethernetu

Kolej Bolevecká budova Bolevecká L2

- 1 ks páteřní přepínač/směrovač
- 8 ks 48 portový přístupový přepínač
- 2 ks 48 portový přístupový přepínač s napájením po Ethernetu

Kolej Bolevecká budova Bolevecká L1

- 8 ks 48 portový přístupový přepínač
- 2 ks 48 portový přístupový přepínač s napájením po Ethernetu

Výměnné moduly rozhraní přístupových přepínačů (30 ks)

Další technické požadavky

- Všechny **páteřní přepínače/směrovače** (celkem 3 ks) musí být stejného typu.
- Všechny **48 portové přístupové přepínače** (celkem 56 ks) musí být stejného typu.
- Všechny **48 portové přístupové přepínače s napájením po Ethernetu** (celkem 13 ks) musí být stejného typu**, 1 ks z toho se liší počtem portů – 24 portů** (kolej Máchova budova Klatovská 100).
- Všechny aktivní síťové prvky budou předkonfigurované v topologii dle kapitoly Požadovaná topologie síťových prvků. Parametry konfigurace (IP adresy zařízení, požadované VLAN, parametry AAA ověřování, základní směrování) dodá Zadavatel dodavateli před realizací dodávky.
- Všechny aktivní síťové prvky musí být z důvodů ochrany stávajících investic a minimalizace celkových nákladů na vlastnictví a provoz počítačové sítě zadavatele kompatibilní se všemi již používanými zařízeními, komunikačními protokoly a systémy správy sítě specifikovanými níže.
- Zadavatel požaduje fyzickou instalaci aktivních síťových zařízení včetně instalace patch kabelů v budovách **Baarova 36, Bolevecká 32 - L1 a Bolevecká 32 - L2**.

Tabulka povinných požadavků pro páteřní přepínač/směrovač (3 ks)

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**
Základní vlastnosti	
Typ zařízení	L2/L3 přepínač/směrovač
Velikost zařízení	1 RU
Redundantní AC (230 V) napájení (zařízení musí být schopno plné funkce při poruše jednoho napájecího zdroje)	ano
Minimální počet neblokovaných portů 1/10/25GE s volitelným fyzickým rozhraním typu SFP/SFP+/SFP28	24
Minimální počet uplink portů 40/100GE s volitelným fyzickým rozhraním QSFP+/QSFP28	4
Výkonnostní parametry	
Propustnost přepínacího subsystému	2 Tb/s
Paketový výkon přepínače	1 miliarda paketů/vteřinu
Počet záznamů v MAC tabulce	80000
Počet aktivních VLAN	4000
Minimální počet IPv4 záznamů ve směrovací tabulce	200000
Minimální počet IPv6 záznamů ve směrovací tabulce	200000
Min. počet oddělených (nezávislých) směrovacích tabulek	10
Protokoly spojové vrstvy	
IEEE 802.1D	ano
IEEE 802.1Q	ano
IEEE 802.1X – Port Based Network Access Control	ano
IEEE 802.1s – Multiple Spanning Tree	ano
IEEE 802.1w – Rapid Tree Spanning	ano
Per VLAN Rapid Spanning Tree (PVRST+) nebo ekvivalentní	ano
Podpora jumbo rámců minimálně 9216 B	ano
Detekce protilehlého zařízení	ano
Detekce parametrů protilehlého zařízení (CDP, LLDP nebo ekvivalentní)	ano
Protokol pro definici šířených VLAN (VTP, MVRP nebo ekvivalentní)	ano
Detekce jednosměrnosti optické linky	ano

STP root guard	ano
STP loop guard	ano
STP BPDU guard	ano
STP BPDU filter	ano
Autorecovery portu po chybovém stavu	ano
Multicast/broadcast storm control – hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ano
IEEE 802.3ad LACP (Link Aggregation Control Protocol) pro agregaci linek (LAG)	ano
Filtrování provozu v rámci VLAN (L2/VLAN ACL)	ano
Protokol IP	
IP alias (více IP sítí na jednom rozhraní)	ano
QoS – Strict Priority Queue	ano
QoS classification – ACL, DSCP, CoS based	ano
QoS marking – DSCP, CoS	ano
QoS Policing	ano
QoS-Hierarchical QoS	ano
DHCP relay	ano
Protokol IPv6	
Podpora IPv6 ACL	ano
Podpora IPv6 services (DNS, Telnet, SSH, Syslog, ICMP)	ano
Podpora IPv6 MLDv2 snooping	ano
Podpora IPv6 Port ACL	ano
Podpora IPv6 First Hop Security RA guard	ano
Podpora IPv6 First Hop Security DHCPv6 guard	ano
Podpora IPv6 First Hop Security IPv6 Binding Integrity Guard	ano
Směrování multicastu	
IGMPv2 snooping	ano
IGMPv3 snooping	ano
IPv6 MLDv1 & v2 snooping	ano
PIM SM	ano
PIM SSM	ano
PIM Bidirectional	ano
MSDP	ano
Static Multicast Routes	ano
Směrování	
L3/směrování IPv4/IPv6	ano
First Hop Redundancy Protocol pro IPv4/IPv6 (např. VRRP, VRRPv6)	ano
Konfigurace L3/směrovaných fyzických rozhraní (L3 interfaces)	ano
Konfigurace L3/směrovaných podrozhraní (L3 subinterfaces)	ano
Konfigurace L3/směrovaných loopback rozhraní	ano
Přístupový seznam pro filtrování IPv4/IPv6 vstupního/výstupního L3 datového provozu (ACL, Access Control List)	ano
Směrovací protokoly OSPFv2 a OSPFv3 pro všechna rozhraní včetně LAG/MLAG	ano
Směrovací protokol OSPFv2, OSPFv3	ano
OSPF graceful restart	ano
Směrovací protokol BGPv4 pro všechna rozhraní včetně LAG/MLAG	ano
Směrovací protokol MP-BGP IPv6 pro všechna rozhraní včetně LAG/MLAG	ano

VXLAN s BGP EVPN	ano
Graceful Insertion and Removal (GIR)	ano
Konfigurace směrovacích map (route maps)	ano
Policy Based Routing (PBR) pro IPv4/IPv6	ano
Virtualizace směrovacích tabulek pro IPv4/IPv6 (VRF)	ano
BFD pro všechna rozhraní včetně LAG/MLAG	ano
BFD v4/v6 ve VRF	ano
Reverse Path Check (uRPF)	ano
Bezpečnost	
ACL na rozhraní in/out	ano
ACL pro IP	ano
ACL pro ethernetové rámce	ano
IPv6 ACL	ano
Možnost definovat povolené MAC adresy na portu	ano
Možnost definovat maximální počet MAC adres na portu	ano
Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	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
IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu	ano
IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači, sdílení ověření koncových stanic	ano
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ano
Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)	ano
Podpora protokolů pro monitoring a export datových toků IP Flow Information Export (IPFIX), Netflow v9 dle RFC3954 nebo funkčně ekvivalentních	ano
Management	
CLI rozhraní	ano
SSHv2	ano
SSHv2 over IPv6	ano
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
SNMPv2	ano
SNMPv3	ano
Konzolová linka	ano
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ano
Streaming telemetrie prostřednictvím NETCONF/XML	ano
DNS klient	ano
NTP klient s MD5 autentizací	ano
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano
Vzdálený port mirroring (ERSPAN)	ano
Vzdálený port mirroring	ano
Syslog	ano
Měření zakončení a délky metalického kabelu (TDR)	ano
Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute)	ano

Tabulka povinných požadavků pro všechny přístupové přepínače

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti
Základní vlastnosti	
Třída zařízení	L2 přepínač
Velikost zařízení	1RU
Stohovatelný	ano, modulem
Stohování požadováno	ano
Stohování kompatibilní se všemi přístupovými přepínači požadovanými v této ZD	ano
Výkonnostní parametry	
Propustnost přepínacího subsystému	200 Gbit/s
Paketový výkon přepínače	100 milionů paketů/vteřinu
Rychlost stohovacího propojení	80 Gbit/s
Vlastnosti stohování	
Počet přepínačů ve stohu	8
Automatická kontrola a sjednocení verze software přepínačů ve stohu	ano
Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením	ano
Seskupování portů (IEEE 802.3ad) mezi různými prvky stohu	ano
Kterýkoli prvek ve stohu může být řídícím prvkem stohu (1:N redundance)	ano
Protokoly fyzické vrstvy	
IEEE 802.3-2005	ano
IEEE 802.3ad	ano
Podpora "jumbo rámců"	ano
Protokoly spojové vrstvy	
IEEE 802.1D	ano
IEEE 802.1Q	ano
Počet aktivních VLAN	4000
IEEE 802.1X – Port Based Network Access Control	ano
IEEE 802.1s – multiple spanning trees	ano
IEEE 802.1w – Rapid Tree Spanning Protocol	ano
IEEE 802.1p – počet vnitřních front	4
Per VLAN Rapid Spanning Tree (PVRST+) nebo ekvivalentní	ano
Detekce protilehlého zařízení	ano
Detekce parametrů protilehlého zařízení	ano
Protokol pro definici šířených VLAN	ano
Detekce jednosměrnosti optické linky	ano
STP root guard	ano
STP loop guard	ano
Možnost autorecovery po chybovém stavu	ano
Multicast/broadcast storm control – hardwarové omezení rámců na portu	ano
Protokol IP	
IP alias (více IP sítí na jednom rozhraní)	ano
QoS	ano
QoS i na stohovacím spoji	ano
DHCP relay	ano
Protokol IPv6	
Podpora IPv6 ACL	ano

Podpora IPv6 services (DNS, Telnet, SSH, Syslog, ICMP)	ano
Podpora IPv6 MLDv2 snooping	ano
Podpora IPv6 Port ACL	ano
Podpora IPv6 First Hop Security RA guard	ano
Podpora IPv6 First Hop Security DHCPv6 guard	ano
Podpora IPv6 First Hop Security IPv6 Binding Integrity Guard	ano
Směrování multicastu	
IGMPv2 snooping	ano
IGMPv3 snooping	ano
IPv6 MLDv1 & v2 snooping	ano
Bezpečnost	
ACL na rozhraní in/out	ano
ACL pro IP	ano
ACL pro ethernetové rámce	ano
IPv6 ACL	ano
Možnost definovat povolené MAC adresy na portu	ano
Možnost definovat maximální počet MAC adres na portu	ano
Možnost definovat různé chování při překročení počtu MAC adres na portu	ano
Podpora zabezpečení a analýzy DHCP protokolu	ano
Podpora ochrany ARP protokolu	ano
Podpora ochrany podvrženého mapování IP/MAC adresy	ano
IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu	ano
IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači	ano
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu	ano
Ověřování dle IEEE 802.1x volitelně bez omezování přístupu pro monitoring	ano
Podpora koncových zařízení	
Měření a ovládání spotřeby připojených koncových zařízení a infrastruktury	ano
Podpora IEEE 802.3az	ano
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením	ano
Management	
CLI rozhraní	ano
SSHv2	ano
SSHv2 over IPv6	ano
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
SNMPv2	ano
SNMPv3	ano
Konzolová linka	ano
DNS klient	ano
NTP klient s MD5 autentizací	ano
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano
TACACS+ klient	ano
Port mirroring	ano
Vzdálený port mirroring	ano
Syslog	ano
Měření zakončení a délky metalického kabelu (TDR)	ano
Přepínač obsahuje traceroute utilitu operující na linkové vrstvě	ano
Automatická záloha/obnova firmware včetně konfigurace z nadřazeného prvku	ano

Tabulka povinných požadavků pro 48 portový přístupový přepínač (56 ks)

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti
Délka stohovacího kabelu	50 cm
Počet RJ-45 portů 10/100/1000	48
Počet uplink portů a jejich typ	4, 1GE SFP

Tabulka povinných požadavků pro 48 portový přístupový přepínač s napájením po Ethernetu (12 ks)

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti
Redundantní AC (230 V) napájení (zařízení musí být schopno plné funkce při poruše jednoho napájecího zdroje)	ano
Délka stohovacího kabelu	100 cm
Počet RJ-45 portů 10/100/1000	48
Podpora PoE (IEEE 802.3af, 15,4 W/port)	ano
Podpora PoE+ (IEEE 802.3at, 30 W/port)	ano
Dostupný výkon pro napájení PoE portů	1000 W
Počet uplink portů a jejich typ	4, 10GE SFP+

Tabulka povinných požadavků pro 24 portový přístupový přepínač s napájením po Ethernetu (1 ks)

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti
Redundantní AC (230 V) napájení (zařízení musí být schopno plné funkce při poruše jednoho napájecího zdroje)	ano
Délka stohovacího kabelu	50 cm
Počet RJ-45 portů 10/100/1000	24
Podpora PoE (IEEE 802.3af, 15,4 W/port)	ano
Podpora PoE+ (IEEE 802.3at, 30 W/port)	ano
Dostupný výkon pro napájení PoE portů	600 W
Počet uplink portů a jejich typ	4, 10GE SFP+

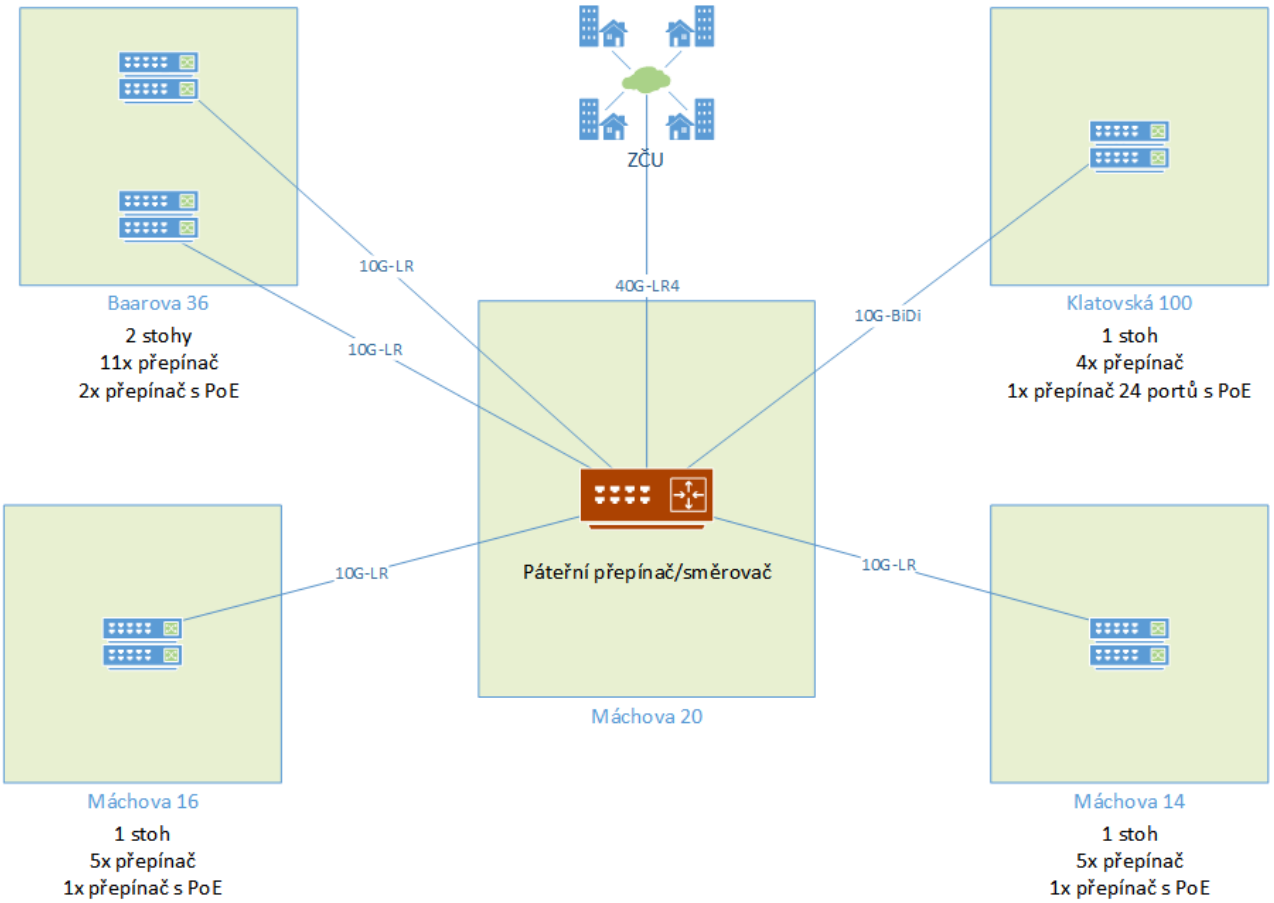
Tabulka povinných požadavků pro výměnné moduly rozhraní páteřních přepínačů/směrovačů a přístupových přepínačů (30 ks)

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti
Základní vlastnosti	
Modul 40G-LR4, rozhraní QSFP+, dosažitelná vzdálenost 20 km	8 ks
Kompatibilní s páteřními přepínači/směrovači požadovaným v této ZD	ano
Modul 10GBase-LR, rozhraní SFP+, dosažitelná vzdálenost 20 km	9 ks
Modul 10G Active Optical Fiber (AOC), rozhraní SFP+, délka 3 m	13 ks
Kompatibilní s páteřními přepínači/směrovači i s přístupovými přepínači požadovanými v této ZD	ano

Požadovaná topologie síťových prvků

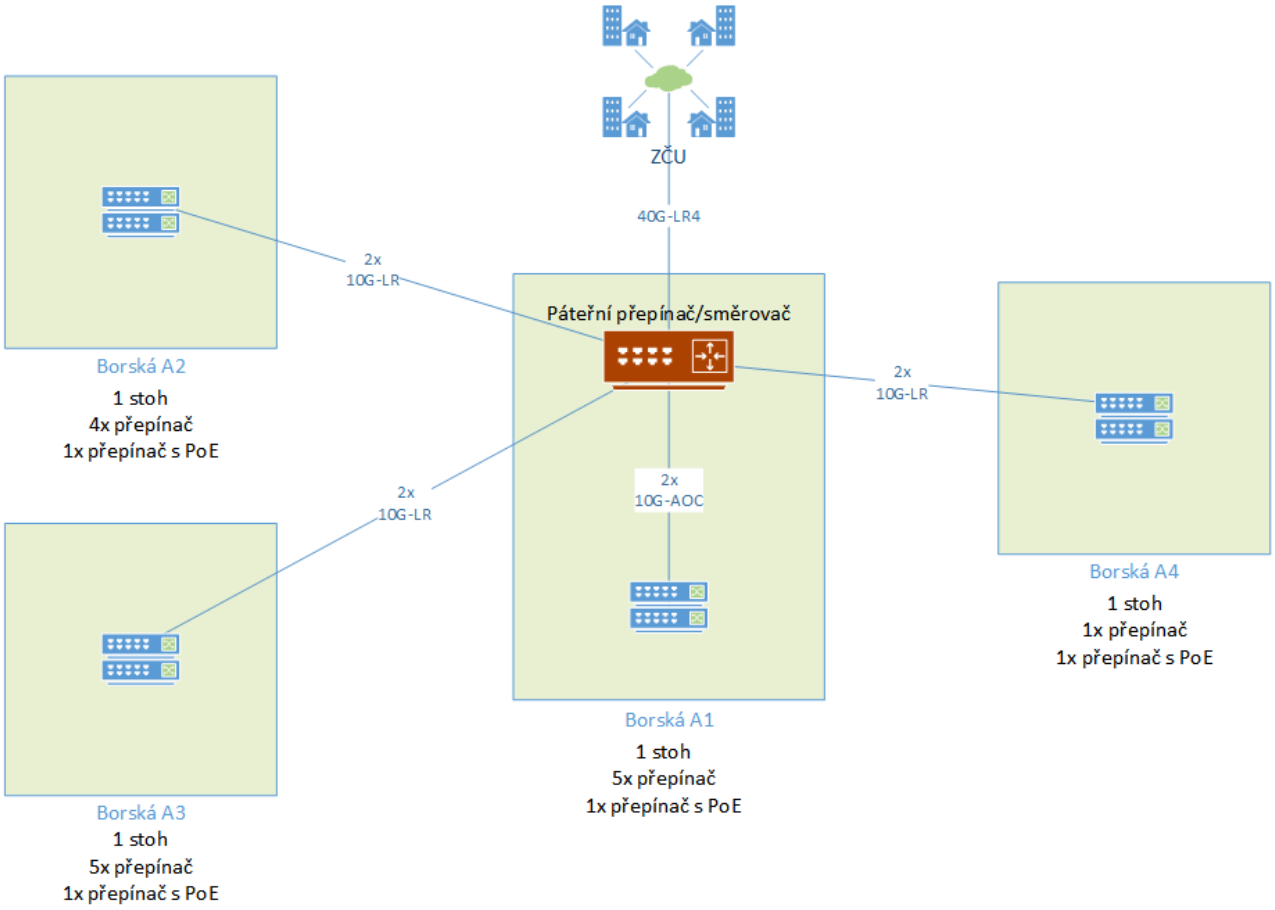
Kolej Máchova

V každé budově je jeden nebo dva stohy přístupových přepínačů připojených hvězdicovitě do páteřního přepínače/směrovače v budově Máchova 20. Každý stoh obsahuje jeden 48 portový přístupový přepínač s napájením po Ethernetu. V budově Klatovská 100 stoh obsahuje jeden 24 portový přístupový přepínač s napájením po Ethernetu. Ostatní 48 portové přístupové přepínače jsou rovnoměrně rozděleny do stohů. Některé optické výměnné moduly nejsou součástí dodávky, protože Zadavatel je již vlastní.



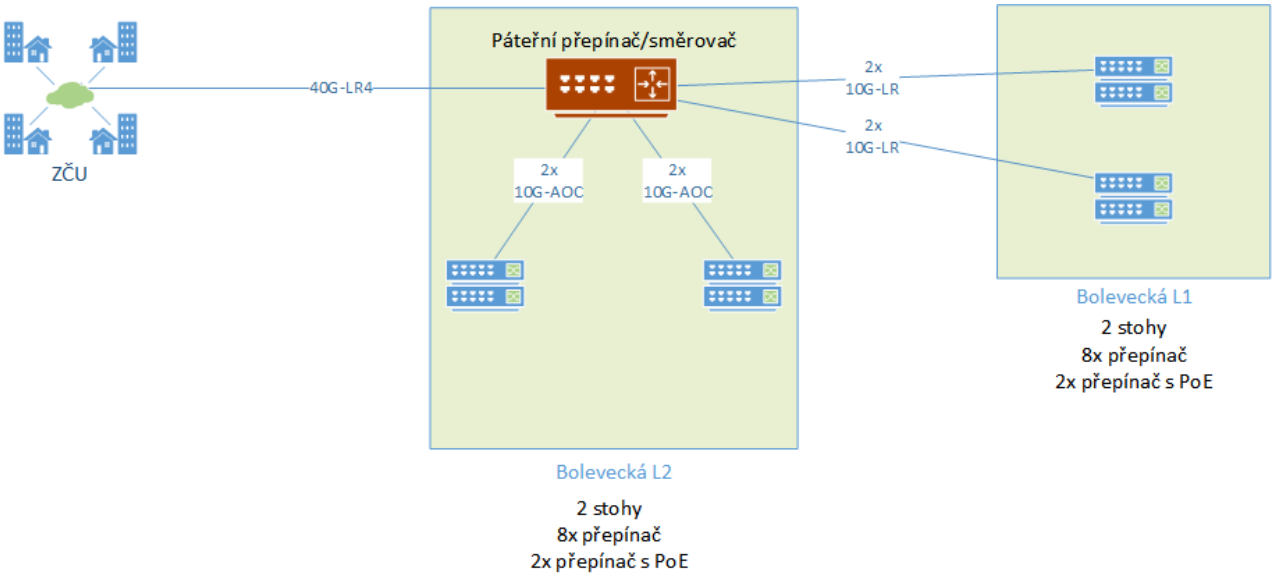
Kolej Borská

V každé budově je jeden stoh přístupových přepínačů připojených hvězdicovitě do páteřního přepínače/směrovače v budově Borská A1. Každý stoh obsahuje jeden 48 portový přístupový přepínač s napájením po Ethernetu. Některé optické výměnné moduly nejsou součástí dodávky, protože zadavatel je již vlastní.



Kolej Bolevecká

V každé budově jsou dva stohy přístupových přepínačů připojených hvězdicovitě do páteřního přepínače/směrovače v budově Bolevecká L2. Každý stoh obsahuje jeden 48 portový přístupový přepínač s napájením po Ethernetu. Ostatní přístupové přepínače jsou rovnoměrně rozděleny do stohů.



Fyzická instalace zařízení

V budovách **Baarova 36, Bolevecká 32 - L1 a Bolevecká 32 - L2** zadavatel požaduje:

1. Demontáž stávajících aktivních síťových prvků.
2. Demontáž stávajících patch kabelů.
3. Instalaci dodaných aktivních síťových prvků.
4. Instalaci nových patch kabelů.

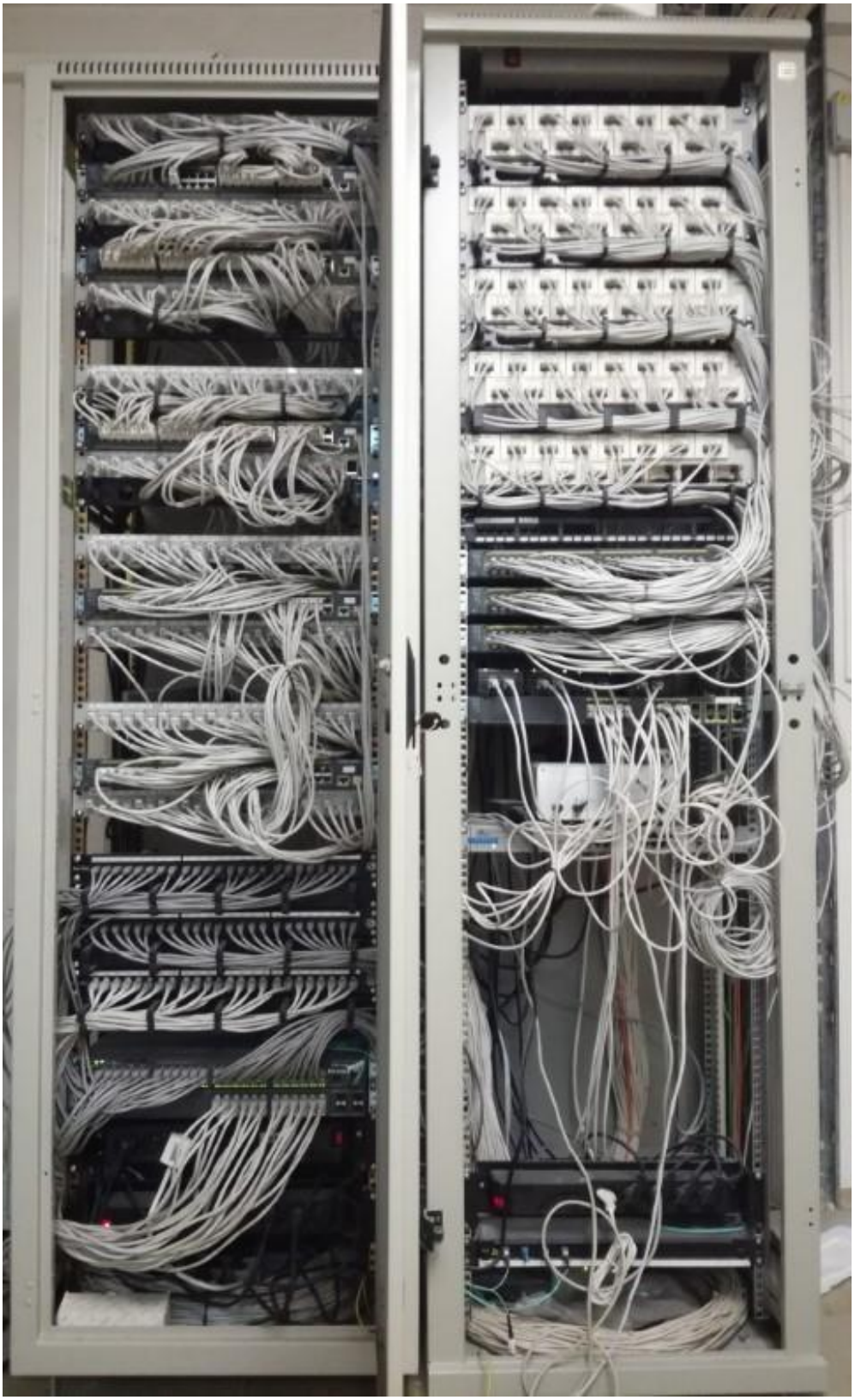
V ostatních budovách si instalaci zařízení provede sám Zadavatel.

Budova Baarova 36

V budově Baarova 36 je rozvaděč umístěn v pátém nadzemním podlaží. V místnosti jsou dva 42RU vysoké racky. V levém racku je 505 přístupových portů vyvedených na patch panely. Stávající aktivní prvky jsou umístěné v pravém racku. Nové aktivní prvky budou umístěné také v pravém racku. Lze zachovat rozestupy mezi prvky stohu, ale není to podmínkou. Lze použít stávající patch kabely, ale není to podmínkou.

Budova Bolevecká 32 - L1

V budově Bolevecká 32 - L1 je rozvaděč umístěn v pátém nadzemním podlaží. V místnosti jsou dva racky vysoké 40RU a 42RU. V levém i pravém racku je 462 přístupových portů vyvedených na patch panely, z toho 78 portů vyžaduje napájení po Ethernetu. Stávající aktivní prvky jsou umístěné v levém i pravém racku. Nové aktivní prvky budou umístěné v pravém racku dole.



Budova Bolevecká 32 - L2

V budově Bolevecká 32 - L2 je rozvaděč umístěn v pátém nadzemním podlaží. V místnosti jsou dva racky vysoké 40RU a 42RU. V levém i pravém racku je 462 přístupových portů vyvedených na patch panely, z toho 78 portů vyžaduje napájení po Ethernetu. Stávající aktivní prvky jsou umístěné v levém i pravém racku. Nové aktivní prvky budou umístěné v pravém racku dole. Je potřeba demontovat některé vyvazovací panely ve spodní části pravého racku.

Popis stávajícího prostředí počítačové sítě ZČU

Používané komunikační protokoly a podpůrné vlastnosti aktivních prvků sítě ZČU

V akademické síti ZČU WEBnet jsou v současné době používány následující komunikační protokoly a další podpůrné vlastnosti aktivních prvků, s nimiž musí být poptávaná zařízení kompatibilní:

- Podpora IEEE 802.1Q/p (minimálně 1000 VLAN, konfigurační možnosti statického omezování síření VLAN), IEEE 802.1s/w (RSTP/MSTP), IEEE 802.3ad, IGMPv2/v3, MLDv1/v2 a vlastnické L2 protokoly VTPv3, PVRSTP+, CDPv2, UDLD.
- Možnosti ochrany spanning tree protokolu vůči zneužití (filtrace BPDU rámců na jednotlivých rozhraních, kontrola přípustnosti BPDU apod.).
- Podpora agregace linek (LACP nebo PAgP).
- Podpora privátních VLAN (logická izolace jednotlivých rozhraní nebo skupin rozhraní v rámci téže VLAN).
- Podpora omezení (procentuálního poměru) broadcastového a multicastového provozu na rozhraní.
- Duální podpora IPv4 a IPv6 unicast i multicast (možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, dual-stack).
- Podpora směrovacích protokolů BGPv4, OSPFv2, OSPFv3, PIM-SMv2, RIP, statického směrování a možnosti redistribuce směrovacích informací mezi jednotlivými protokoly, rozkládání zatížení na L3 paralelních cestách, možnosti vytváření logicky oddělených instancí virtuálních směrovacích tabulek v rámci téhož L3 přepínače (podpora virtuálních směrovacích instancí).
- Podpora HSRP nebo VRRP pro zajištění redundance výchozí brány koncovým stanicím/serverům.
- Podpora GRE tunelů.
- Podpora IGMPv2, IGMPv3 a hardwarová podpora omezování zbytečného šíření multicastových rámců/paketů na rozhraní bez explicitních příjemců (IGMPv2/v3 a MLDv1/v2 snooping).
- Možnost definovat povolené MAC adresy na portu, jejich maximální počet na portu a definování různého chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy).
- Hardwarová podpora bezstavové bezpečnostní filtrace provozu podle L2/L3/L4 atributů na úrovni linkové/síťové/transportní vrstvy aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní (VLAN).
- Vzdálený management aktivních prvků (typicky pomocí protokolů Telnet, SSH, HTTP/HTPS nebo SNMPv2/v3).
- Implementace čítačů přenesených bytů/paketů pro jednotlivé relevantní entity síťových informací (typicky rozhraní, filtry apod.) přístupné přes příkazovou řádku a SNMP.
- Možnost nastavení omezení distribuce IP multicastu ve VLAN.
- Možnost ochrany proti útokům na úrovni síťové a linkové vrstvy (IP DHCP Snooping, Dynamic ARP Inspection, IP Source Guard).
- Hardwarová podpora zajištění kvality služby (QoS) podle L2/L3/L4 atributů umožňující implementaci QoS podle modelu rozlišovaných služeb (DiffServ).

Nástroje používané pro správu sítě ZČU

Pro správu sítě ZČU jsou používány následující nástroje síťového managementu, s nimiž musí být poptávaná zařízení kompatibilní.

Správa konfigurací

Zálohování konfigurací všech aktivních komunikačních prvků Cisco je prováděno centrálně automaticky pomocí systému RANCID[1] s webovou nadstavbou Subversion (pro přehledné zobrazování změn) periodicky alespoň jednou denně. Archivace (změn) historie konfigurací je udržována minimálně po dobu jednoho roku. Navíc jsou paralelně zálohovány konfigurace (a jejich přehledných sumárních změny) všech aktivních komunikačních prvků Cisco pomocí systému NeDi[2] periodicky alespoň jednou denně. Archivace (změn) historie konfigurací je opět v systému NeDi udržována minimálně po dobu jednoho roku.

Pro hromadné konfigurace skupin zařízení se využívají systémy Netmanager[3], umožňující paralelní vykonávání příkazů, a NeDi.

Inventarizace síťových zařízení

Pro inventarizaci veškerých síťových zařízení (typicky aktivních komunikačních prvků a koncových zařízení jako jsou uživatelská PC, notebooky, servery a síťové tiskárny) se využívají dva druhy nástrojů:

- registrační systém Sauron[4] v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet[5] v prostředí kolejní sítě (včetně funkce řízení přístupu oprávněných uživatelů do sítě na základě konfigurace kolejních DHCP/DNS serverů a pravidel na centrálním kolejním firewallu)
- on-line systémy Netdisco[6] a NeDi, které na základě periodicky získávaných informací z aktivních komunikačních prvků pomocí protokolů SNMP a CDP poskytují informace o zařízeních připojených do sítě (např. počty, typy a verze OS aktivních prvků, informace o topologii sítě, VLAN, IP podsítích, bezdrátových SSID, mapování MAC adres na IP adresy, připojení MAC/IP adres za konkrétními fyzickými porty jednotlivých přepínačů, informace o SMB atd.) s možností pokročilého vyhledávání (např. nalezení fyzického připojení zařízení s danou IP/MAC adresou, nalezení duplicitních MAC/IP adres apod.), včetně uchovávání stavové historie.

Monitorování provozu

Provozní trendy

Pro sledování non-stop dostupnosti na úrovni služeb se používá systém Nagios[7], který je současně také využíván pro monitorování dostupnosti všech aktivních komunikačních prvků a služebních/management serverů, včetně konfigurace automatického upozorňování/eskalace e-mailem při detekci problémové/chybové situace.

Pro sledování non-stop dostupnosti na úrovni služeb pro systém VoIP ZČU se používá systém Nagios[8], který je využíván pro monitorování dostupnosti všech aktivních komunikačních prvků a služebních/management serverů systému VoIP ZČU, včetně konfigurace automatického upozorňování/eskalace e-mailem při detekci problémové/chybové situace.

---

[1] http://www.shrubbery.net/rancid/

[2] http://nedi.ch/

[3] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

[4] http://sauron.jyu.fi/

[5] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

[6] http://www.netdisco.org/

[7] http://www.nagios.org/

[8] http://www.nagios.org/

Pro non-stop historii sledování základních L2 provozních charakteristik aktivních komunikačních prvků všech prostředí pomocí SNMP[9] (typicky zatížení CPU, obsazení operační paměti, stav napájecích zdrojů, teplota, počet BGP prefixů a stavové informace jednotlivých portů/rozhraní jako počet přenesených bytů/rámců/paketů, chybovost portů/rozhraní atd.) se používá optimální konfigurace dvojice nástrojů Cricket[10] a Torrus[11] pracujících nad RRD databázemi.
Pro sledování provozu na úrovni L3/L4 datových toků se využívá technologie NetFlow v9. NetFlow informace exportované ze směrovačů, linuxových firewallů (kolejní extranet) a specializované FlowMon[12] sondy (kolejní intranet) se zpracovávají jednak nevzorkované pomocí produkčního IPv4 software Caligare Flow Inspector/CFI[13] a jednak vzorkované 1:10 pomocí testovacího IPv4/IPv6 software FTAS[14].
Pro monitorování historie latence/jitteru/ztrátovosti paketů (typicky VoIP subsystému) se používá aktivní nástroj Smokeping[15].
Pro monitorování problémových provozních stavů se používá standardní mechanismus zpracování nevyžádaných deníkových zpráv generovaných aktivními prvky na bázi protokolu Syslog a SNMP trap, přičemž se navíc využívá i nadstavba Zenoss Core[16] pro inteligentní korelaci trapů.
Bezpečnostní monitorování
Pro monitorování síťové bezpečnosti se jednak využívají standardní nástroje Syslog a SNMP trapy, které mohou být ještě dále inteligentně předzpracovány/filtrovány, korelovány a reportovány SIEM systémem zpracování Syslog hlášení z aktivních prvků OSSEC[17] a pro SNMP trapy systémem Zenoss Core.
Přehled o anomáliích na úrovni automatické detekce podezřelých IPv4 datových toků podle analýzy NetFlow dat poskytuje software Caligare Flow Inspector/CFI.
Automatický přehled o (změnách) mapování aktivních MAC adres na IP adresy pro všechna zařízení připojená do vybraných/důležitých podsítí zajišťuje software ARPwatch[18].
Vynucování bezpečnostní síťové přístupové politiky umožňující centralizované systémové zablokování přístupu problémových uživatelů do sítě či síťových služeb (blacklist) zejména na úrovni L2 VACL nebo L3 ACL případně ještě s kombinací vypnutí daného portu na přístupovém prvku (typicky nejblíže místu svého vzniku podle typu komunikačního prvku) je řízeno pomocí nástroje NetSpy[19]. Tento vlastní nástroj také poskytuje další potřebné podpůrné administrátorské funkce, jako např. automatickou detekci neregistrovaných zařízení, vyhledání různých konfliktních síťových stavů, management VLAN/IP podsítí atd.
Vzdálený administrátorský přístup ke všem aktivním síťovým prvkům je zajištěn pouze[20] pomocí SSH protokolu s autentizací/autorizací protokolem TACACS+ z předdefinovaných povolených bezpečných podsítí/IP adres. Management rozhraní L2 přepínačů je umístěno ve vyhrazené IP podsíti chráněné firewallem. Pro L3 přepínače/směrovače je konfigurována ochrana Control Plane Policing/CoPP, pokud tuto vlastnost podporují. AAA auditní informace o administrátorských přístupech ke konfigurovaným zařízením je k dispozici na TACACS+ serverech CIV ZČU.

Požadavky na instalaci zařízení

Dodavatel dodrží při instalaci zařízení pokyny Zadavatele. Informace týkající se požadované minimální konfigurace zařízení budou obsahovat (zadavatel tyto informace předá dodavateli až před vlastní realizací dodávky):

- IP adresy zařízení,
- Konfiguraci virtuálních sítí VLAN,
- Parametry AAA ověřování přístupu k zařízení,
- Základní směrování páteřních přepínačů/směrovačů.

[9]Konfigurace aktivních prvků pouze v režimu pro čtení s povolenými IP adresami management stanic dle ACL.
[10]http://cricket.sourceforge.net/
[11]http://torrus.org/
[12]http://www.invea.cz/produkty-sluzby/flowmon/flowmon-sondy
[13]http://www.caligare.com/
[14]http://www.cesnet.cz/doc/techzpravy/2004/ftas-arch/,
http://www.cesnet.cz/doc/techzpravy/2006/ftas-interface/,
http://www.cesnet.cz/akce/2009/zazemi-pro-cert-csirt/p/sledovani-provozu.pdf

[15]http://oss.oetiker.ch/smokeping/
[16]http://www.zenoss.com/solution/network-monitoring
[17]http://www.ossec.net/
[18]http://www.securityfocus.com/tools/142
[19]Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.
[20]S výjimkou menšího počtu zastaralých přepínačů, které SSH nepodporují a jsou postupně podle finančních možností nahrazovány.