Požadované technické parametry dodávky

Předmětem dodávky jsou aktivní síťové prvky dle technických podmínek uvedených níže:

- Modulární přístupový/agregační přepínač (2 ks),
- Nemodulární přístupový stohovatelný gigabitový přepínač (1 ks),
- Bezdrátový přístupový bod (13 ks).

Všechny poptávané síťové prvky musí být z důvodů ochrany stávajících investic a minimalizace celkových nákladů na vlastnictví a provoz počítačové sítě ZČU kompatibilní se všemi již používanými zařízeními, komunikačními protokoly a systémy správy sítě. Ze stejného důvodu musí být poptávané stohovatelné prvky stohovatelné i s prvky již používanými v síti ZČU.

Tabulka mandatorních požadavků pro modulární přístupový/agregační přepínač (požadovány 2 ks)

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	L3 přepínač	
Formát zařízení	modulární	
Počet slotů pro moduly rozhraní	5	
Počet 10GE portů na řídícím modulu	2	
Požadovaný počet a typ 10GE transceiverů	2x 10GBase-LR, SFP+ 2x 10GBase-SR, SFP+	
Redundantní zdroje, dosažitelný výkon každého	4000W	
Podpora modulů 48x 10/100/1000 Ethernet, neblokující, 802.3at (PoE+) na všech portech současně, L2 šifrování dle 802.1AE, IEEE 802.3az	ano	
Požadovaný počet modulů 48x 10/100/1000Base-T, neblokující, 802.3at (PoE+) na všech portech současně, L2 šifrování dle 802.1AE, IEEE 802.3az	3	
Podpora modulů 48x 10/100/1000Base-T, neblokující, L2 šifrování dle 802.1AE, IEEE 802.3az	ano	
Požadovaný počet modulů 48x 10/100/1000Base-T, neblokující, L2 šifrování dle 802.1AE, IEEE 802.3az	2	
Podpora modulů 48x 10/100/1000Base-T, agregace 2:1, 802.3af (PoE+) na 24 portech současně	ano	
Podpora modulů 48x 10/100/1000Base-T, agregace 2:1	ano	
Podpora modulů s minimálně 12 porty GE/6x10GE, Jumbo rámce	ano	
Podpora modulů s 24xSFP sloty, neblokující	ano	
Podpora Non-Stop Forwarding	ano	
Podpora upgrade software za provozu	ano	
Podpora virtualizace – možnost sloučit alespoň dvě fyzická šasi do jednoho logického celku – virtuálního	ano nebo povýšením software	

šasi		
Statické směrování IPv4, IPv6	ano	
Dynamické směrování IPv4, IPv6	ano	
Podpora IPv4, IPV6 v hardware	ano	
Výkonnostní parametry		
Celková propustnost centrálních řídících modulů (IPv4/IPv6)	200/100 milionů paketů/vteřinu	
Celková potenciální propustnost přepínacího subsystému	500 Gbit/s	
Dostupná kapacita na slot	48 Gbit/s	
Počet záznamů ve směrovací tabulce - IPv4 unicast	64000	
Počet záznamů ve směrovací tabulce – IPv6 unicast	32000	
Počet MAC adres	50000	
Protokoly fyzické vrstvy		
IEEE 802.3-2005	ano	
IEEE 802.3ad	ano	
IEEE 802.3ad přes více karet	ano	
Podpora "jumbo rámců"	ano	
Protokoly spojové vrstvy		
IEEE 802.1D	ano	
IEEE 802.1Q	ano	
Počet aktivních VLAN	4000	
Tunelování 802.1Q v 802.1Q	ano	
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	ano	
Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní	ano	
Detekce protilehlého zařízení	ano	
Protokol pro definici šířených VLAN	ano	
Detekce jednosměrnosti optické linky	ano	
STP root guard nebo ekvivalentní	ano	
STP loop guard nebo ekvivalentní	ano	
Možnost autorecovery po chybovém stavu	ano	
Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ano	
Protokol IP		
IP alias (více IP sítí na jednom rozhraní)	ano	
QoS (DiffServ)	ano	
DHCP relay	ano	
Router redundancy protokol (např. VRRP, HSRP)	ano	
Protokol IPv6		
Certifikace IPv6 ready logo – Phase II	ano	
Router redundancy protokol pro IPv6	ano	
Podpora IPv6 ACL	ano	

Podpora IPv6 QoS (DiffServ)	ano	
Podpora IPv6 services (DNS, Telnet, SSH, Syslog, ICMP, DHCP)	ano	
Podpora IPv6 Multicast (MLDv1 & v2)	ano	
Podpora IPv6 Multicast (PIM SSM)	ano	
Podpora IPv6 Multicast (PIM SM)	ano	
Podpora IPv6 MLDv2 snooping	ano	
Podpora IPv6 First Hop Security (IPv6 Port ACL, RA guard, DHCPv6 guard, Destination guard)	ano	
Podpora IPv6 Tunneling: ISATAP Tunnel	ano	
Směrovací protokoly		
OSPF	ano	
OSPF s MD5 a NSSA	ano	
RIPv2	ano	
Statické směrování	ano	
Směrování multicastu		
PIM (dense i sparse mód)	ano	
Source-Specific Multicast (SSM)	ano	
IGMPv2	ano	
IGMPv3	ano	
IGMPv3 snooping	ano	
IPv6 MLDv1 & v2 snooping	ano	
Bezpečnost		
Podpora reverse path check (uRPF)	ano	
ACL pro IP	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	
Podpora zabezpečení a analýzy DHCP protokolu	ano	
Podpora ochrany ARP protokolu	ano	
Podpora ochrany podvrženého mapování IP/MAC adresy	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	
Vynucení IEEE 802.1x ověřování i na externím připojeném přepínači	ano	
Ochrana centrálního procesoru (control plane) před útoky typu DoS	ano	
Podpora klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Security Group Exchange Protocol nebo	ano	

funkčně ekvivalentní).		
Podpora koncových zařízení		
Podpora PoE (IEEE 802.3af)	ano	
Podpora PoE+ (IEEE 802.3at, 30W/port)	ano	
Podpora PoE (60W/port)	ano	
Automatické i manuální ovládání PoE výkonu portu	ano	
Měření a ovládání spotřeby energie připojených koncových zařízení	ano	
Integrovaný nástroj na profilování připojovaných koncových zařízení	ano	
Management		
CLI rozhraní	ano	
SSHv2	ano	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	
SNMPv2	ano	
SNMPv3	ano	
Konzolová linka	ano	
Interpretace uživatelských CLI a Tcl skriptů a jejich aktivace asynchronní událostí v systému zařízení	ano	
DNS klient	ano	
NTP klient s MD5 autentizací	ano	
IPFIX RFC 3917, RFC 3955	ano	
Detailní flexibilní definice "flow" dle L2/L3/L4 parametrů	ano	
Export statistik "flow" selektivně na více kolektorů	ano	
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano	
TACACS+ klient	ano	
Port mirroring	ano	
Vzdálený port mirroring	ano	
Syslog	ano	
Nástroje pro měření odezev v síti (například IP SLA nebo ekvivalentní)	ano	
Nástroje pro pasivní monitorování i aktivní testování odezev provozovaných aplikací (např. IP SLA Video Operation, performance monitor nebo ekvivalentní)	ano	
Možnost v software přepínače integrovat další aplikace (například WireShark, profilování koncových zařízení,…)	ano	
Automatická konfigurace portu dle připojeného zařízení	ano	
Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)	ano	
Služby		
Podpora NTP	ano	
DHCP server	ano	

Tabulka mandatorních požadavků pro nemodulární přístupový stohovatelný gigabitový přepínač (požadovány 1 ks)

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Třída zařízení	L2 přepínač	
Formát zařízení	fixní konfigurace, rozšiřitelný na stohování, 1RU	
Stohovatelný	ano, volitelným modulem	
Stohování požadováno	ne	
Počet portů 10/100/1000	48	
Počet uplink portů 1GE a jejich typ	4x SFP	
Možnost připojit externí redundantní zdroj	Ano	
Požadovaný počet a typ 10GE transceiverů	1x 10GBase-CU (5 m)	
Výkonnostní parametry		
Propustnost přepínacího subsystému	170 Gbit/s	
Paketový výkon přepínače	75 milionů paketů/vteřinu	
Rychlost stohovacího propojení	80 Gbit/s	
Vlastnosti stohování		
Vzájemné stohování všech modelů stejné řady s 1GE/10GE uplinky	ano	
Stohování kompatibilní se stávajícími stohovatelnými přepínači	ano	
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	1000	
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	ano	

ekvivalentní		
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 poměru unicast/multicast rámců na portu v procentech	ano	
Protokol IP		
IP alias (více IP sítí na jednom rozhraní)	ano	
QoS	ano	
QoS i na stohovacím propoji	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 (včetně virtuálních - VLAN, loopback, 802.1ad)	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	
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	ano	

přepínači, sdílení ověření koncových stanic		
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 koncových zařízení		
Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury	ano	
Podpora IEEE (IEEE 802.3az)	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 (Layer 2 traceroute)	ano	
Přepínač si může automaticky zazálohovat a obnovit firmware včetně konfigurace z nadřazeného směrovače	ano	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ano	
Služby		
DHCP server	ano	

Tabulka mandatorních požadavků pro bezdrátový přístupový bod (požadováno 13 ks)

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Typ zařízení	bezdrátový přístupový bod	
Rádiové rozhraní pro pásmo 2,4 GHz	ano	
Rádiové rozhraní pro pásmo 5 GHz	ano	

Počet portů 10/100/1000	1	
Možnost IEEE 802.3af napájení z přepínače nebo injektoru	ano	
Typ antén	integrované pro obě pásma	
Montáž	na betonový strop	
Podpora stávajících centralizovaných řadičů bezdrátové sítě	ano	
Podpora centralizovaného řadiče poptávaného v této ZD	ano	
Výkonnostní parametry		
Fyzická přenosová rychlost bezdrátové části	450 Mb/s	
Protokoly fyzické vrstvy		
IEEE 802.11a/b/g/n	ano	
Podpora MIMO (Multiple Input Multiple Output)	3x4:3	
IEEE 802.11n Maximal ratio combining (MRC)	ano	
Podpora agregace rámců A-MPDU a A-MSDU	ano	
Dynamický výběr volné frekvence DFS	ano	
Podpora 20 MHz a 40 MHz kanálů	ano	
Optimalizace fáze vysílaného bezdrátového signálu směrem k 802.11a/g/n klientům (Beam Forming)	ano	
Podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma	ano	
Hardwarová podpora spektrální analýzy (detekce zdroje rušivého signálu – interferencí)	ano	
Hardwarová podpora rozpoznání zdroje rušivého signálu podle signatur	ano	
Podpora výpočtu závažnosti dopadu interference na kvalitu radiového signálu bezdrátové sítě	ano	
Minimální počet inzerovaných SSID (BSSID)	8/rádiové rozhraní	
Nastavitelný DTIM interval pro jednotlivé bezdrátové sítě	ano	
Bezpečnost		
Certifikát s lokální platností pro nasazení PKI	ano	
Fyzické zabezpečení/zamknutí k okolním pevným částem	ano	
Management		
CLI rozhraní	ano	
SSHv2	ano	
Konzolová linka	ano	
Detekce a monitorování problémů bezdrátové sítě odchytáváním provozu a jeho zasíláním do analyzátoru (například Wireshark)	ano	

Požadavky na záruku a servis dodávky:

Všechny dodané síťové prvky (Zařízení) musí být z důvodů ochrany stávajících investic a minimalizace celkových nákladů na vlastnictví a provoz počítačové sítě ZČU kompatibilní se všemi již používanými komunikačními protokoly a systémy správy sítě.

Požadovaná záruční doba na dodaná Zařízení činí 60 měsíců.

Další požadované související plnění:

- dodávka Zboží do místa plnění
- technická dokumentace (v elektronické podobě, čeština, angličtina);
- Uchazeč poskytne Zadavateli po dobu trvání záruky všechny relevantní verze operačního software nabízené výrobcem tak, aby dodané řešení fungovalo bez závad. Dodavatel se současně zavazuje informovat Zadavatele o nových softwarových verzích a funkčnostech, které mohou rozšiřovat dodané řešení. Dodavatel se zavazuje získat potřebné softwarové produkty legálním způsobem za podmínek stanovených výrobcem zařízení.
- Uchazeč zajistí Zadavateli přístup k dokumentaci výrobce zařízení a znalostní bázi, pokud ji výrobce v rámci své podpory koncovým uživatelům poskytuje.
- veškeré zákonem vyžadované dokumenty potřebné pro provoz nabízených zařízení na území České republiky (prohlášení o shodě apod.);
- Uchazeč je povinen zajistit dostupnost nových originálních náhradních dílů od výrobce pro dodané řešení za podmínek specifikovaných Zadavatelem v režimu 8h x 5d x NBD (počet hodin dostupnosti servisu uchazeče x počet dní v týdnu dostupnosti servisu dodavatele x doba pro doručení náhradního dílu Zadavateli do místa plnění).
- Výše specifikovanou záruční lhůtu, servis a dostupnost náhradních dílů Zadavatel požaduje po dobu 60 měsíců.

Struktura technické části nabídky

Technická část nabídky musí obsahovat:

- Podrobný popis technických a funkčních parametrů nabízeného řešení, z něhož bude jasně patrné splnění jednotlivých položek technických a funkčních požadavků technického zadání.
- Podrobný popis servisních a záručních podmínek, z něhož bude jasně patrné splnění jednotlivých položek servisních a záručních požadavků zadání.
- Podrobnou položkovou specifikaci nabízených zařízení (např. typů šasi, jednotlivých modulů, operačního software, napájecích zdrojů apod.).

Popis 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 je prováděno centrálně automaticky pomocí systému RANCID[1] s webovou nadstavbou Subversion (pro přehledné zobrazování změn). Archivace (změn) historie konfigurací je udržována minimálně po dobu jednoho roku. Navíc jsou paralelně zálohovány konfigurace (a jejich přehled sumárních změn) všech aktivních komunikačních prvků pomocí systému NeDi[2].

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

Správa bezdrátové sítě

Na ZČU je provozována bezdrátová síť eduroam[4], která podporuje IP mobilitu a roaming uživatelů v rámci české sítě národního výzkumu a vzdělávání. Kromě toho je provozována síť zcu-mobile, která mobilitu a roaming nepodporuje. Pro její provoz byl vyvinut vlastní systém

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

2 http://nedi.ch/

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

4 http://www.eduroam.cz

založený na open-source řešení. Obě řešení jsou navázána na AAA infrastrukturu založenou na ověřovacím serveru freeRADIUS[5]. Pro správu a konfiguraci bezdrátových přístupových bodů je využíváno centralizované řešení. Jako centrální prvky jsou použity dva bezdrátové řadiče[6] pracující v režimu active/active, které jsou schopny současně spravovat až 200 AP. K udržení konzistentní konfigurace obou bezdrátových řadičů je používán specializovaný software[7].

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[8] v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet[9] 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[10] 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.[11]) 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[12], 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[13], 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.

Pro sledování non-stop dostupnosti všech aktivních komunikačních prvků včetně IP telefonů se používá systém Mikrotik The Dude[14].

---

5 http://freeradius.org

6 Bezdrátový řadič Cisco Wireless LAN Controller (WLC) 5508 pro 100 AP a Cisco WLC 4404 pro 100 AP.

7 Cisco Prime Infrastructure verze 1.3 pro 200 AP.

8 http://sauron.jyu.fi/

9 Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

10 http://www.netdisco.org/

11 Z bezpečnostních důvodů se však záměrně nevyužívají integrované služby manipulace se stavy portů přepínačů vyžadující SNMP přístup pro zápis.

12 http://www.nagios.org/

13 http://www.nagios.org/

14 http://www.mikrotik.com/thedude.php

Pro non-stop historii sledování základních L2 provozních charakteristik aktivních komunikačních prvků všech prostředí pomocí SNMP [15] (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[16] a Torrus[17] 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 [18] sondy (kolejní intranet) se zpracovávají jednak nevzorkované pomocí produkčního IPv4 software Caligare Flow Inspector/CFI[19] a jednak vzorkované 1:10 pomocí testovacího IPv4/IPv6 software FTAS[20].
Pro monitorování historie latence/jitteru/ztrátovosti paketů (typicky VoIP subsystému) se používá aktivní nástroj Smokeping[21].
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[22] 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[23] 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[24].
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[25]. 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.

---

15 Konfigurace aktivních prvků pouze v režimu pro čtení s povolenými IP adresami management stanic dle ACL.
16 http://cricket.sourceforge.net/
17 http://torrus.org/
18 http://www.invea.cz/produkty-sluzby/flowmon/flowmon-sondy
19 http://www.caligare.com/
20 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
21 http://oss.oetiker.ch/smokeping/
22 http://www.zenoss.com/solution/network-monitoring
23 http://www.ossec.net/
24 http://www.securityfocus.com/tools/142
25 Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

Vzdálený administrátorský přístup ke všem aktivním síťovým prvkům je zajištěn pouze[26] 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.

[26] S výjimkou menšího počtu zastaralých přepínačů, které SSH nepodporují a jsou postupně podle finančních možností nahrazovány.