Název veřejné zakázky:	**Aktivní prvky pro novou knihovnu**

Technická podmínka:	**Odůvodnění**
Tabulka mandatorních požadavků pro modulární přístupový/agregační přepínač	V tabulce uvedené níže, jsou požadovány vlastnosti, které jsou využívány v univerzitní síti WEBnet. Vlastnosti jsou požadovány velmi podrobně, neboť máme zkušenosti, že při příliš obecném požadavku vznikají problémy při integraci prvku do prostředí sítě WEBnet.

Odůvodnění požadovaných technických parametrů dodávky

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

- Modulární přístupový/agregační přepínač (1 ks) včetně instalace.
- Bezdrátový přístupový bod (1 ks).
- Záložní zdroj napájení UPS 3000VA v rackovém řešení maximální velikosti 3RU (1 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 komunikačními protokoly a systémy správy sítě.

Tabulka mandatorních požadavků pro modulární přístupový/agregační přepínač (požadován 1 ks)

Požadavek na funkcionalitu	Minimální požadavky	Odůvodnění
Základní vlastnosti		
Typ zařízení	L3 přepínač	Specifikace potřebného typu funkčnosti dle referenčního modelu ISO OSI
Formát zařízení	modulární	Zajištění ochrany investice zaručující budoucí potřebné rozšiřování
Počet slotů pro moduly rozhraní	5	Minimálně 5 slotů kvůli ochraně investice zaručující budoucí potřebné rozšiřování o nová rozhraní
Počet 10GE portů na řídícím modulu	2	Minimální potřebný počet 10GE rozhraní pro integraci do sítě ZČU
Požadovaný počet a typ 10GE transceiverů	2x 10GBASE-LR	Minimální potřebný počet 10GE vyměnitelných rozhraní typu 10GBASE-LR pro integraci do sítě ZČU
Redundantní zdroje, dosažitelný výkon každého	2500W	Požadavek zajištění vysoké dostupnosti a provozní flexibility zařízení jako celku a zároveň potřebná výkonová podpora zařízení napájených přes PoE
Podpora modulů 48x 10/100/1000 Ethernet, neblokující, 802.3af (PoE+) na všech portech současně, L2 šifrování dle 802.1AE	ano	Požadavek zajištění provozní flexibility, bezpečnosti a přepínací architektury modulu a zároveň potřebná výkonová podpora zařízení napájených přes PoE

Podpora modulů 48x 10/100/1000Base-T, neblokující, L2 šifrování dle 802.1AE	ano	Minimální potřebný počet celkových počet modulů/rozhraní 10/100/1000Base-T s napájením 802.3af PoE pro integraci do sítě ZČU
Podpora modulů 48x 10/100/1000Base-T, agregace 2:1, 802.3aft(PoE+) na 24 portech současně	ano	Požadavek zajištění provozní flexibility, bezpečnosti a přepínací architektury modulu
Požadovaný počet modulů 48x 10/100/1000Base-T, agregace 2:1, 802.3at (PoE+) na 24 portech současně	2	Minimální potřebný počet celkových počet modulů/rozhraní 10/100/1000Base-T pro integraci do sítě ZČU
Podpora modulů 48x 10/100/1000Base-T, agregace 2:1	ano	Požadavek zajištění provozní flexibility, bezpečnosti a přepínací architektury modulu a zároveň potřebná výkonová podpora zařízení napájených přes PoE
Požadovaný počet modulů 48x 10/100/1000Base-T, agregace 2:1	3	Požadavek zajištění provozní flexibility, bezpečnosti a přepínací architektury modulu
Podpora modulů s minimálně 12 porty GE/6x10GE, Jumbo rámce	ano	Požadavek zajištění provozní flexibility, bezpečnosti modulu a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Podpora modulů s 24xSFP sloty, neblokující	ano	Požadavek zajištění provozní flexibility a přepínací architektury modulu
Statické směrování IPv4, IPv6	ano	Základní požadavek na potřebný typ IP směrování používaný v síti ZČU
Podpora IPv4, IPV6 v hardware	ano	Základní požadavek na potřebnou implementaci IP směrování jako ochranu investice v prostředí vysokorychlostní sítě ZČU
Výkonnostní parametry		
Celková propustnost centrálních řídících modulů (IPv4/IPv6)	200/100 Mp/s	Základní výkonnostní požadavek na potřebnou implementaci přepínání/směrování rámců/paketů jako ochranu investice v prostředí vysokorychlostní sítě ZČU
Celková potenciální propustnost přepínacího subsystému	500 Gbit/s	Základní výkonnostní požadavek na potřebnou propustnost přepínání/směrování zařízení jako ochranu investice v prostředí vysokorychlostní sítě ZČU
Dostupná kapacita na slot	48 Gbit/s	Základní výkonnostní požadavek na potřebnou propustnost přepínání/směrování modulu jako ochranu investice v prostředí vysokorychlostní sítě ZČU
Počet záznamů ve směrovací tabulce - IPv4 unicast	64000	Základní kapacitní požadavek na potřebnou implementaci IPv4 směrování jako ochranu investice v prostředí akademické metropolitní vysokorychlostní sítě ZČU
Počet záznamů ve	32000	Základní kapacitní požadavek na potřebnou implementaci IPv6

směrovací tabulce – IPv6 unicast		směrování jako ochranu investice v prostředí akademické metropolitní vysokorychlostní sítě ZČU
Počet MAC adres	50000	Základní kapacitní požadavek na potřebnou implementaci spojové vrstvy jako ochranu investice v prostředí akademické metropolitní vysokorychlostní sítě ZČU
Protokoly fyzické vrstvy		
IEEE 802.3-2005	ano	Zajištění potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
IEEE 802.3ad	ano	Zajištění potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
IEEE 802.3ad přes více karet	ano	Zajištění potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU při současném požadavku vysoké dostupnosti a formou odolnosti vůči poruchám redundantních komponent
Podpora "jumbo rámců"	ano	Zajištění potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Protokoly spojové vrstvy		
IEEE 802.1D	ano	Zajištění potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
IEEE 802.1Q	ano	Zajištění potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Počet aktivních VLAN	4000	Zajištění potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Tunelování 802.1Q v 802.1Q	ano	Zajištění potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU pro Carrier Ethernet
IEEE 802.1X - Port Based Network Access Control	ano	Zajištění bezpečnostní politiky přístupu do sítě a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
IEEE 802.1s - multiple spanning trees	ano	Zajištění robustnosti/odolnosti vůči poruchám a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
IEEE 802.1w - Rapid Tree Spanning Protocol	ano	Zajištění robustnosti/odolnosti vůči poruchám a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
IEEE 802.1p	ano	Zajištění podpory CoS a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní	ano	Zajištění robustnosti/odolnosti vůči poruchám a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Detekce protilehlého zařízení	ano	Zajištění automatického objevování sousedních zařízení pro účely správy sítě a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Protokol pro definici šířených VLAN	ano	Zajištění škálovatelnosti a udržovatelnosti velkého počtu VLAN na velkém počtu zařízení a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Detekce jednosměrnosti optické linky	ano	Zajištění robustnosti/odolnosti vůči poruchám a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
STP root guard nebo ekvivalentní	ano	Zajištění robustnosti/odolnosti vůči poruchám a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
STP loop guard nebo ekvivalentní	ano	Zajištění robustnosti/odolnosti vůči poruchám a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní

		vysokorychlostní sítě ZČU
Možnost autorecovery po chybovém stavu	ano	Zajištění robustnosti/odolnosti vůči poruchám a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ano	Zajištění robustnosti/odolnosti vůči poruchám a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Protokol IP		
IP alias (více IP sítí na jednom rozhraní)	ano	Zajištění flexibility adresování a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
QoS (DiffServ)	ano	Zajištění podpory kvality služby/QoS dle standardu rozlišovaných služeb/DiffServ a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
DHCP relay	ano	Zajištění podpory DHCP v prostředí směrovaných podsítí a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Protokol IPv6		
Certifikace IPv6 ready logo – Phase II	ano	Zajištění minimálního profilu podporovaných IPv6 vlastností a potřebné kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Podpora IPv6 ACL	ano	Zajištění bezpečnostní síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Podpora IPv6 QoS (DiffServ)	ano	Zajištění podpory kvality služby/QoS dle standardu rozlišovaných služeb/DiffServ a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Podpora IPv6 services (DNS, Telnet, SSH, Syslog, ICMP, DHCP)	ano	Zajištění základních síťových služeb pro vzdálenou konfiguraci, management a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Podpora IPv6 MLDv2 snooping	ano	Zajištění optimalizace multimediálních síťových služeb a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Podpora IPv6 First Hop Security (IPv6 Port ACL, RA guard)	ano	Zajištění bezpečnostní síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Směrovací protokoly		
Statické směrování	ano	Zajištění základního směrování a potřebné kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Směrování multicastu		
IGMPv2	ano	Zajištění dynamického směrování pro multimediální provoz a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
IGMPv3	ano	Zajištění dynamického směrování pro multimediální provoz a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
IGMPv3 snooping	ano	Zajištění bezpečného dynamického směrování pro multimediální provoz a potřebné základní kompatibility se stávajícím prostředím akademické

		metropolitní vysokorychlostní sítě ZČU
IPv6 MLDv1 & v2 snooping	ano	Zajištění bezpečného dynamického směrování pro multimediální provoz a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Bezpečnost		
ACL pro IP	ano	Zajištění bezpečnostní síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
IPv6 ACL	ano	Zajištění bezpečnostní síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Možnost definovat povolené MAC adresy na portu	ano	Zajištění bezpečnostní síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Možnost definovat maximální počet MAC adres na portu	ano	Zajištění bezpečnostní síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	ano	Zajištění selektivní bezpečnostní síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Podpora zabezpečení a analýzy DHCP protokolu	ano	Zajištění selektivní bezpečnostní síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Podpora ochrany ARP protokolu	ano	Zajištění selektivní bezpečnostní síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Podpora ochrany podvrženého mapování IP/MAC adresy	ano	Zajištění selektivní bezpečnostní síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ano	Zajištění selektivní bezpečnostní přístupové síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)	ano	Zajištění selektivní bezpečnostní přístupové síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Vynucení IEEE 802.1x ověřování i na externím připojeném přepínači	ano	Zajištění selektivní bezpečnostní přístupové síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Ochrana centrálního	ano	Zajištění bezpečnostní síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě

procesoru (control plane) před útoky typu DoS		ZČU
Podpora klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Security Group Exchange Protocol nebo funkčně ekvivalentní).	ano	Škálovatelné flexibilní zajištění selektivní bezpečnostní přístupové síťové politiky a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Management		
CLI rozhraní	ano	Požadavek interaktivní konfigurovatelnosti zařízení z příkazové řádky lidskou obsluhou
SSHv2	ano	Zajištění bezpečnostní síťové politiky, vzdálené správy/konfigurace/monitoringu a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	Zajištění bezpečnostní síťové politiky, vzdálené správy/konfigurace/monitoringu a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
SNMPv2	ano	Zajištění vzdálené správy/konfigurace/monitoringu a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
SNMPv3	ano	Zajištění bezpečné vzdálené správy/konfigurace/monitoringu a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Konzolová linka	ano	Možnost lokálního připojení k zařízení za účelem správy/konfigurace/monitoringu
DNS klient	ano	Zajištění podpory klienta systému DNS přímo v zařízení a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
NTP klient s MD5 autentizací	ano	Zajištění bezpečné podpory synchronizace času v zařízení pomocí protokolu NTP formou klienta a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano	Zajištění bezpečného autentizovaného/autorizovaného/účtovaného vzdáleného administrátorského přístupu k zařízení pomocí protokolu RADIUS a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
TACACS+ klient	ano	Zajištění bezpečného autentizovaného/autorizovaného/účtovaného vzdáleného administrátorského přístupu k zařízení pomocí protokolu TACACS+ a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Port mirroring	ano	Zajištění možnosti odposlouchávání provozu na lokálním portu zařízení pro bezpečnostní a monitorovací účely a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Vzdálený port mirroring	ano	Zajištění možnosti odposlouchávání provozu po síti na portu vzdáleného zařízení pro bezpečnostní a monitorovací účely a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU

Syslog	ano	Zajištění možnosti logování významných lokálních událostí na zařízení po síti pro bezpečnostní a monitorovací účely a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Automatická konfigurace portu dle připojeného zařízení	ano	Zajištění pokročilých autokonfiguračních síťových služeb pro automatickou detekci připojených zařízení podle jejich typu a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Služby		
Podpora NTP	ano	Zajištění podpory synchronizace času v zařízení pomocí protokolu NTP formou serveru a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
DHCP server	ano	Zajištění podpory dynamického přidělování IP adres v zařízení pomocí protokolu DHCP formou serveru a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU

Tabulka mandatorních požadavků pro bezdrátový přístupový bod (požadován 1 ks)

Požadavek na funkcionalitu	Minimální požadavky	Odůvodnění
Základní vlastnosti		
Typ zařízení	bezdrátový přístupový bod	Specifikace potřebného typu funkčnosti zařízení
Počet portů 10/100/1000	1	Minimální počet portů zaručující možnost realizace připojení do drátové sítě
Možnost IEEE 802.3af napájení z přepínače nebo injektoru	ano	Požadavek na možnost připojení zařízení k portu aktivního prvku a využití možnosti napájet zařízení z tohoto portu
Typ antén	integrované pro obě pásma	Možnost provozování zařízení bez dalších přídavných antén
Montáž	na betonový strop	Požadovaný typ montáže pro dodání správného upevňovacího přípravku
Výkonnostní parametry		
Fyzická přenosová rychlost bezdrátové části	450 Mb/s	Základní výkonnostní požadavek bezdrátové části
Protokoly fyzické vrstvy		
IEEE 802.11a/b/g/n	ano	Zajištění potřebné základní kompatibility s bezdrátovými klienty
Podpora MIMO (Multiple Input Multiple Output)	3x3	Zajištění potřebné základní kompatibility s bezdrátovými klienty
IEEE 802.11n Maximal ratio combining (MRC)	ano	Zajištění potřebné základní kompatibility s bezdrátovými klienty
Podpora agregace rámců A-MPDU a A-MSDU	ano	Zajištění potřebné základní kompatibility s bezdrátovými klienty
Dynamický výběr volné frekvence DFS	ano	Zajištění potřebné základní kompatibility s bezdrátovým prostředím sítě ZČU
Podpora 20 MHz a 40 MHz kanálů	ano	Zajištění potřebné základní kompatibility s bezdrátovými klienty
Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k	ano	Zajištění potřebné základní kompatibility s bezdrátovými klienty

802.11a/g/n klientům (Beam Forming)		
Podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma	ano	Požadavek upřednostňování 5 GHz klientů
Hardwarová podpora spektrální analýzy (detekce zdroje rušivého signálu – interference)	ano	Zajištění pokročilých síťových služeb pro flexibilní zákaznické monitorování provozních parametrů bezdrátové sítě
Hardwarová podpora rozpoznání zdroje rušivého signálu podle signatur	ano	Zajištění pokročilých síťových služeb pro flexibilní zákaznické monitorování provozních parametrů bezdrátové sítě
Podpora výpočtu závažnosti dopadu interference na kvalitu radiového signálu bezdrátové sítě	ano	Zajištění pokročilých síťových služeb pro flexibilní zákaznické monitorování provozních parametrů bezdrátové sítě
Minimální počet inzerovaných SSID (BSSID)	8/rádiové rozhraní	Zajištění potřebné základní kompatibility s bezdrátovým prostředím sítě ZČU
Nastavitelný DTIM interval pro jednotlivé bezdrátové sítě	ano	Zajištění potřebné základní kompatibility s bezdrátovým prostředím sítě ZČU
Bezpečnost		
Certifikát s lokální platností pro nasazení PKI	ano	Zajištění bezpečného ověřování připojených bezdrátových přístupových bodů
Fyzické zabezpečení/zamknutí k okolním pevným částem	ano	Zajištění zabezpečené instalace bezdrátových přístupových bodů
Management		
CLI rozhraní	ano	Požadavek interaktivní konfigurovatelnosti zařízení z příkazové řádky lidskou obsluhou
SSHv2	ano	Zajištění bezpečnostní síťové politiky, vzdálené správy/konfigurace/monitoringu a potřebné základní kompatibility se stávajícím prostředím akademické metropolitní vysokorychlostní sítě ZČU
Konzolová linka	ano	Možnost lokálního připojení k zařízení za účelem správy/konfigurace/monitoringu
Detekce a monitorování problémů bezdrátové sítě odchytáváním provozu a jeho zasíláním do analyzátoru	ano	Zajištění pokročilých síťových služeb pro flexibilní zákaznické monitorování provozních parametrů bezdrátové sítě

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).

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

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 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. 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

[2] http://nedi.ch/
[3] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.
[4] http://www.eduroam.cz
[5] http://freeradius.org
[6] Bezdrátový řadič Cisco Wireless LAN Controller 5508 a 4404.
[7] Cisco Prime Infrastructure.
[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.

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].

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 v5. 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

[12] http://www.nagios.org/
[13] http://www.nagios.org/
[14] http://www.mikrotik.com/thedude.php
[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

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.

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.

[23] http://www.ossec.net/
[24] http://www.securityfocus.com/tools/142
[25] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.
[26] S výjimkou menšího počtu zastaralých přepínačů, které SSH nepodporují a jsou postupně podle finančních možností nahrazovány.

JUDr. Daniel Volopich
2013.08.23 08:43:39 +02'00'