



Předmět veřejné zakázky – Příloha č. 4 – Technická specifikace

Předmětem veřejné zakázky je pořízení sestavy dvou centrálních L3 přepínačů a souboru koncových aktivních síťových prvků.

Současný stav celé počítačové sítě UJEP

2x centrální L3 přepínač (Cisco Catalyst 6506-E)

180x L2 koncových přepínačů (Cisco Catalyst 2950 a 2960)

26x budov propojených optickými kabely (další 4 objekty v přípravě)

Na všech centrálních i koncových přepínačích jsou používány následující technologie

Vlan Trunking Protocol

Rapid PVST+

klient TACACS+

CDP

VTP doména přes celou síť

Agregace portů LACP pro redundantní připojení hostů virtualizačním platformem UJEP (12 hostů připojených do L3 přepínačů)

Export NetFlow dat z L3 přepínačů do kolektoru Caligare Flow Inspector a Flow monitor (CESNET)

Monitoring a sběr dat přes SNMP protokol (NetDisco a vlastní skripty)

Policy Based Routing na L3 přepínačích

Ověřování přístupu (802.1x, klient radius)

Ochrana proti neautorizovanému DHCP serveru

Ochrana proti neautorizovaným Router Advertisement zprávám

Ochrana proti podvržení MAC adresy a IP adresy na jednotlivých portech

Ochrana proti připojení neautorizovaného přepínače na port určený pro koncové zařízení

Možnost nastavení maximálního limitu broadcast rámců

Možnost filtrování provozu podle MAC adresy na jednotlivých portech

Sestava dvou centrálních L3 přepínačů

Centrální L3 přepínače

Současný stav

Ve dvou optikou propojených lokalitách máme umístěny dva samostatné L3 přepínače Cisco Catalyst C6506. Přepínače tvoří jádro sítě, provádějí směrování mezi VLANami sítě a zajišťují propojení na zařízení poskytovatele Internetu v dual-stack konfiguraci (IPv4 a IPv6). Z důvodu nedostatku veřejných IPv4 adres, zajišťuje směrovač překlad privátních adres na adresy veřejné (IP NAT), využíváme omezení počtu překladů pro jednotlivé IP adresy. Redundanci výchozí brány zajišťuje HSRP protokol. Metadata o provozu jsou exportována do dvou nezávislých netflow kolektorů. Autentizaci, autorizaci a accounting zajišťuje TACACS+ server. Používáme Rapid PVST+ protokol (IEEE 802.1w). K omezení provozu mezi VLANami používáme ACL.



Používáme automatickou aktivaci portu z chybového stavu. Dále používáme policy-based routing, agregaci portů (protokol LACP), vzdálené logování a sběr dat protokolem SNMP interně vyvinutými aplikacemi.

Lokalita 1 (PF) – Cisco Catalyst 6506 v konfiguraci

- 1 24 CEF720 24 port 1000mb SFP WS-X6724-SFP
- 2 48 CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX
- 3 48 48 port 10/100/1000mb EtherModule WS-X6148-GE-TX
- 5 5 Supervisor Engine 720 10GE (Active) VS-S720-10G
- 6 5 Supervisor Engine 720 10GE (Hot) VS-S720-10G

- 1 Centralized Forwarding Card WS-F6700-CFC
- 2 Centralized Forwarding Card WS-F6700-CFC
- 5 Policy Feature Card 3 VS-F6K-PFC3C
- 5 MSFC3 Daughterboard VS-F6K-MSFC3
- 6 Policy Feature Card 3 VS-F6K-PFC3C
- 6 MSFC3 Daughterboard VS-F6K-MSFC3

Lokalita 2 (MFC) – Cisco Catalyst 6506 v konfiguraci

- 1 48 CEF720 48 port 1000mb SFP WS-X6848-SFP
- 2 48 CEF720 48 port 10/100/1000mb Ethernet WS-X6848-GE-TX
- 3 4 WiSM 2 WLAN Service Module WS-SVC-WISM2-K9
- 5 5 Supervisor Engine 2T 10GE w/ CTS (Active) VS-SUP2T-10G
- 6 5 Supervisor Engine 2T 10GE w/ CTS (Hot) VS-SUP2T-10G

- 1 Distributed Forwarding Card WS-F6K-DFC4-A
- 2 Distributed Forwarding Card WS-F6K-DFC4-A
- 5 Policy Feature Card 4 VS-F6K-PFC4
- 5 CPU Daughterboard VS-F6K-MSFC5
- 6 Policy Feature Card 4 VS-F6K-PFC4
- 6 CPU Daughterboard VS-F6K-MSFC5

Cílový stav

Dva centrální modulární L3 přepínače propojené, nakonfigurované a chovající se jako jedno logické zařízení - virtuální šasi na úrovni L2 a L3 protokolů. Přepínače budou umístěny ve dvou lokalitách propojených optickým kabelem. Tím bude možné zajistit redundantní připojení ke dvěma POP poskytovatele internetu. Dalším cílem výměny centrálních prvků je zvýšení propustnosti jádra sítě a zvýšení počtu 10 Gbps portů. To umožní zvýšit rychlost propojů mezi jednotlivými budovami a zároveň rychlejší připojení serverů v datových centrech. Propojení centrálních boxů bude realizováno propojem alespoň 40 Gbps.

Minimální počet portů v přepínači podle lokality:

Lokalita 1 (PF)
4x 40GE QSFP+



48x 10GE SFP+
24x GE SFP
48x GE T (RJ-45)

Lokalita 2 (MFC)
4x 40GE QSFP+
48x 10GE SFP+
48x GE SFP
96x GE T (RJ-45)

U optických portů se jedná jen o sloty bez osazení optickými moduly (požadované optické moduly jsou v sekci Příslušenství)

Každý L3 přepínač musí splňovat následující minimální podmínky:

- napájení CZ standard (230V, vidlice typ E)
- redundantní interní hot-swap napájecí zdroje (dostatečně výkonné pro šasi plně obsazené moduly)
- redundantní řídicí modul (supervisor)
- 2.8 Tb/s propustnost přepínacího subsystému
- modulární 7 nebo více slotové šasi s možností montáže do 19'' racku, alespoň jeden slot neosazený pro budoucí rozšíření
- 250 aktivních VLAN
- 30000 záznamů v MAC adresní tabulce
- směrování IPv4 a IPv6 v hardware (dual-stack)
- redundance výchozí brány pro IPv4 i IPv6 (Pokud dojde k poruše primárního routeru, automaticky se aktivuje spojení k záložnímu routeru a uživatelé sítě nejsou nijak postiženi)
- IPv4 NAT v hardware
- Rapid PVST+ (IEEE 802.1w)
- MSTP (IEEE 802.1s)
- dynamické šíření VLAN (přenášení čísel a názvů virtuálních LAN mezi přepínači zařazených do jedné domény včetně zabránění odesílání zbytečných paketů (broadcast, multicast, neznámé) na přepínače, kde není žádný port v dané VLANě a ani přes něj nevede funkční cesta dál)
- TACACS+ klient pro AAA (autentizace, autorizace a accounting - ověřování správců sítě, omezení přístupu na konkrétní zařízení, omezení práv na konkrétní příkazy, záznam všech použitých příkazů, přiřazení práv podle skupiny uživatele)
- policy-based routing podle ACL
- agregace portů IEEE 802.3ad / IEEE 802.1ax přes více modulů šasi
- agregace portů IEEE 802.3ad / IEEE 802.1ax přes více šasi
- protokol LACP pro automatické sestavení agregovaných portů
- IEEE 802.1q
- detekce protilehlého zařízení (protokol linkové vrstvy ke zjišťování informací o přímo připojených zařízeních)
- podpora velkých rámců v hardware (jumbo frames)
- detekce jednosměrnosti optické linky
- konfigurovatelné HW prostředky ochrany CPU před útoky typu DoS
- hardwarová filtrace (ACL) na fyzickém i logickém L2 i L3 rozhraní pro IPv4 i IPv6
- hardwarová filtrace (ACL) dle L2, L3 i L4 informací pro IPv4 i IPv6
- vzdálené logování (syslog)



- vzdálený management a dohled SNMPv2c i SNMPv3
- export toků do alespoň dvou netflow kolektorů (monitorování síťového provozu na základě IP toků umožňující podrobný pohled do provozu sítě v reálném čase, dohledávání bezpečnostních incidentů, export dat bez agregace)
- statistiky určovány z každého paketu toku (netflow)
- sběr a export TCP příznaků pro monitorování bezpečnostních hrozeb
- zobrazení sbíraných informací o tocích přímo v přepínači
- ochrana proti neautorizovanému DHCP serveru
- ochrana proti neautorizovaným Router Advertisement zprávám
- ochrana proti podvržení MAC adresy a IP adresy na jednotlivých portech
- ochrana proti připojení neautorizovaného přepínače na port určený pro koncové zařízení
- možnost nastavení maximálního limitu broadcast rámců
- možnost filtrování provozu podle MAC adresy na jednotlivých portech
- dynamické směrování protokolů BGPv4
- dynamické směrování protokolů OSPFv2 a OSPFv3
- dynamický směrovací protokol IS-IS pro IPv4 a IPv6
- multicast směrování PIM-SM, PIM SSM
- IGMPv2 a IGMPv3
- antispoof ochrana pro IPv4 i IPv6
- plnohodnotné CLI konfigurační rozhraní přístupné přes SSHv2 protokol po IPv4 i IPv6
- import/export konfigurace zařízení v textové podobě protokoly TFTP, FTP, SCP
- omezení přístupu k managementu zařízení pomocí ACL (SSH, SNMP)
- synchronizace času NTP protokolem
- zrcadlení portu (SPAN) a vzdálené zrcadlení portu (RSPAN)
- interní nástroje pro ladění (debugging) procházejícího provozu

Součástí dodávky je konfigurace L3 přepínačů do jednoho logického zařízení, migrace konfigurace ze stávajících L3 přepínačů při zachování služeb popsaných v sekci “Současný stav”.

Součástí dodávky je bezplatné proškolení čtyř osob zadavatele v dodávané technologii. Rozsah školení: 80 hodin. Školení musí být autorizovaná výrobcem dodávané technologie. Oblast školení: routing, pokročilý switching, síťová bezpečnost, optimalizace a správa sítě. Certifikovaný školitel v českém jazyce, podklady ke školení v českém nebo anglickém jazyce. Školení musí obsahovat praktickou část (nejlépe na dodaném zařízení).

Záruka a servisní podpora

Záruka na L3 přepínače minimálně 5 let záruka NBD v místě.

Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.

Uchazeč poskytne Zadavateli po dobu trvání podpory všechny relevantní verze SW nabízené výrobcem tak, aby dodané řešení vyhovovalo zadání Zadavatele a fungovalo bez závad.

Uchazeč se zároveň zavazuje informovat Zadavatele o nových verzích SW a funkcích, které mohou rozšiřovat dodané řešení způsobem, který Zadavatel shledá ve shodě s potřebami dalšího rozvoje dodaného řešení. Uchazeč se dále zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení.

Zároveň je Uchazeč povinen zajistit Zadavateli přístup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.



Soubor koncových aktivních síťových prvků

Současný stav

Připojení uživatelů zajišťují koncové přepínače. Z části jsou to 100 Mbps přepínače s 1 Gbs uplinky (Cisco Catalyst 2950 a 2960), z části již plně gigabitové přepínače (Cisco Catalyst 2960S a 2960X). Propoje mezi budovami jsou převážně na rychlosti 1 Gbs. Autentizaci, autorizaci a accounting správců zajišťuje TACACS+ server. Používáme Rapid PVST+ protokol (IEEE 802.1w). Používáme automatickou aktivaci portu z chybového stavu. Vzdáleně logujeme na centrální syslog server. Provádíme sběr dat protokolem SNMP interně vyvinutými aplikacemi a aplikací NetDisco. Na koncových zásuvkách využíváme 802.1x ověřování uživatelů proti radius serveru. Využíváme automatické šíření jmen a čísel VLAN mezi všemi přepínači.

Cílový stav

Propojení klíčových budov rychlostí 10 Gbps a náhrada 100 Mbps přepínačů plně gigabitovými. Zachování funkcí popsaných v současném stavu (Autentizace, autorizace a accounting správců TACACS+ serverem, Rapid PVST+ protokol (IEEE 802.1w), automatická aktivace portu z chybového stavu, vzdálené logování na centrální syslog server, sběr dat protokolem SNMP (NetDisco), ověřování 802.1x uživatelů proti radius serveru, automatické šíření jmen a čísel VLAN mezi všemi přepínači).

Počet požadovaných aktivních prvků

47 ks přepínačů 48 portů 10/100/1000Base-T a 4 x slot pro optické moduly 1 Gbit (SFP)

10 ks přepínačů 24 portů 10/100/1000Base-T a 4 x slot pro optické moduly 1 Gbit (SFP)

4 ks přepínačů 24 portů 10/100/1000Base-T a 4 x slot pro optické moduly 1 Gbit (SFP), přepínač musí podporovat PoE dle IEEE 802.3af pro 24 portů současně

7 ks přepínačů 24 portů 10/100/1000Base-T a 2 x slot pro optické moduly 10 Gbit (SFP+)

12 ks přepínače 48 portů 10/100/1000Base-T a 2 x slot pro optické moduly 10 Gbit (SFP+)

Prvky musí splňovat minimální parametry:

- zařízení musí být kompatibilní se stávajícím stavem infrastruktury provozované na UJEP
- napájení CZ standard (230V, vidlice typ E)
- výška 1U a možnost montáže do 19" racku
- zařízení typu L2 přepínač
- automatická volba rychlosti portu a automatická detekce přímého/kříženého kabelu (MDIX)
- protokol LACP pro automatické sestavení agregovaných portů
- Rapid PVST+ (IEEE 802.1w)
- MSTP (IEEE 802.1s)
- dynamické šíření VLAN (přenášení čísel a názvů virtuálních LAN mezi přepínači zařazených do jedné domény včetně zabránění odesílání zbytečných paketů (broadcast,



multicast, neznámé) na přepínače, kde není žádný port v dané VLANě a ani přes něj nevede funkční cesta dál)

- autorecovery - automatická aktivace portu po návratu z chybového stavu
- storm control multicast/broadcast: HW omezení poměru unicast / multicast rámců na portu v procentech
- podpora DHCP relay
- IEEE 802.1q
- podpora velkých rámců v hardware (jumbo frames)
- měření metalického kabelu (TDR) - délka, zakončení
- detekce protilehlého zařízení (protokol linkové vrstvy ke zjišťování informací o přímo připojených zařízeních a jejich parametrech)
- detekce jednosměrnosti optické linky
- podpora minimálně 250 aktivních VLAN
- 15000 záznamů v MAC adresní tabulce
- přepínače musí být schopny stohování bez omezení stanoveného minimálního počtu portů
- možnost propojení až osmi přepínačů do stohu
- podpora seskupení portů (IEEE 802.3ad) mezi různými prvky stohu
- kterýkoliv člen stohu může být jeho řídicím prvkem
- rychlost stohovacího propojení 80 Gbit/s
- možnost připojit externí redundantní zdroj
- ochrana proti neautorizovanému DHCP serveru
- ochrana proti neautorizovaným Router Advertisement zprávám
- ochrana proti podvržení MAC adresy a IP adresy na jednotlivých portech
- ochrana proti připojení neautorizovaného přepínače na port určený pro koncové zařízení
- možnost nastavení maximálního limitu broadcast rámců
- možnost filtrování provozu podle MAC adresy na jednotlivých portech
- možnost nastavení maximálního počtu MAC adres na port
- nastavení chování portu při překročení maximálního počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy.)
- možnost nastavení pořadí postupného ověřování zařízení na portu (IEEE 802.1X, MAC, Web autentizace)
- ochrana root bridge
- plnohodnotné CLI konfigurační rozhraní přístupné přes SSHv2 protokol po IPv4 i IPv6
- omezení přístupu k managementu zařízení pomocí ACL (SSH, SNMP)
- vzdálený management a dohled SNMPv2c i SNMPv3
- NTP klient
- TACACS+ klient pro AAA (autentizace, autorizace a accounting - ověřování správců sítě, omezení přístupu na konkrétní zařízení, omezení práv na konkrétní příkazy, záznam všech použitých příkazů, přiřazení práv podle skupiny uživatele)
- IEEE 802.1x - port based network access control, ověřování pracovních stanic proti radius serveru, autentizace i autorizace více koncových zařízení na jednom portu
- zrcadlení portu (SPAN) a vzdálené zrcadlení portu (RSPAN)
- vzdálené logování (syslog)

Příslušenství

1 ks kompatibilní optický transceiver SFP+ 10Gbit, DWDM transceiver na vzdálenost 80 km na vlnové délce 1536.61 nm, ITU channel 51, spacing 50GHz

2 ks kompatibilních optických transceiverů QSFP+ 40Gbit, SM (single mode), konektor typu LC pracující se dvěma vlákny, vzdálenost použití do 2 km



38 ks kompatibilních optických transceiverů SFP+ 10Gbit, SM (single mode), konektor typu LC pracující se dvěma vlákny, vzdálenost použití do 10 km

28 ks kompatibilních optických transceiverů SFP+ 10Gbit, MM (multi mode), konektor typu LC pracující se dvěma vlákny, vzdálenost použití do 300m

6 ks kompatibilních optických transceiverů SFP 1Gbit, MM (multi mode), konektor typu LC pracující se dvěma vlákny, vzdálenost použití do 500m

2 ks Patchcord optický, SM (single mode), duplexní. Konektory E2000APC/E2000APC.

Délka 2 m

18 ks Patchcord optický, SM (single mode), duplexní. Konektory LC/E2000APC. Délka 2 m

2 ks Patchcord optický, SM (single mode), duplexní. Konektory LC/E2000APC. Délka 10 m

6 ks Patchcord optický, SM (single mode), duplexní. Konektory LC-LC. Délka 2 m

2 ks Patchcord optický, SM (single mode), duplexní. Konektory LC-LC. Délka 15 m

4 ks Patchcord optický, SM (single mode), duplexní. Konektory LC-LC. Délka 20 m

6 ks Patchcord optický, MM (multi mode), duplexní. Konektory LC-ST. Délka 2 m

3 ks Patchcord optický, MM (multi mode), duplexní. Konektory LC-LC. Délka 15 m

11 ks doplňků (moduly vybavené kabely) pro propojení 11ti (2 skupiny) L2 přepínačů (kombinace 24 a 48mi portových) do stohů, pokud je dodávaná zařízení neobsahují ve výchozí konfiguraci.

150ks UTP patchcord Cat6, délka 1m

350ks UTP patchcord Cat6, délka 2m

Záruka:

Doživotní záruka dle standardních podmínek výrobce zařízení na dodané přepínače

Záruka na příslušenství 5 let

V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.

Uchazeč poskytne Zadavateli po dobu trvání podpory všechny relevantní verze SW nabízené výrobcem tak, aby dodané řešení vyhovovalo zadání Zadavatele a fungovalo bez závad. Uchazeč se zároveň zavazuje informovat Zadavatele o nových verzích SW a funkcnostech, které mohou rozšiřovat dodané řešení způsobem, který Zadavatel shledá ve shodě s potřebami dalšího rozvoje dodaného řešení. Uchazeč se dále zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení.

Zároveň je Uchazeč povinen zajistit Zadavateli přístup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.