# Předmět plnění

Předmětem plnění veřejné zakázky jsou dodávky a služby pro realizaci projektu „Implementace 802.1X, modernizace a rozšíření bezdrátových služeb”, dále také jen „řešení“.

# Síť LAN

## Stávající topologie sítě

Datová síť Českého rozhlasu je tvořena třemi hlavními částmi – externí částí sítě, interní LAN a interní WAN sítí. Implementace protokolu 802.1X se týká především přístupové vrstvy. Přístupová vrstva se nachází především v centrále Českého rozhlasu, tedy v lokalitě Vinohradská, kde se nachází 39 aktivních prvků Cisco Catalyst modelů 2950G, 3550, 2960, 2960G, 3560, 3560G, 3560X, 6506(9).

Přístupová vrsta je dále přítomna na 11 mimopražských pracovištích a dále v lokalitě ČRo Regina – studio Karlín. V těchto lokalitách se nachází celkem 38 přepínačů Cisco Catalyst modelových řad 3560G a 2960.

## Obměna přístupových přepínačů

Vzhledem k plánu nasazení protokolu 802.1X je nutné provést obměnu 3 přístupových přepínačů Cisco Catalyst 2950G (1ks) a Cisco Catalyst 3550 (2ks). Zadavatel proto požaduje dodání tří kusů 48-portových L2 přepínačů. Minimálním požadavky na jejich funkcionalitu jsou uvedené v tabulce níže.

| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované funkcionality/vlastnosti** |
| --- | --- |
| **Základní vlastnosti** |  |
| Třída zařízení | L2 switch |
| Formát zařízení | fixní konfigurací, rozšiřitelný na stohování, 1RU |
| Stohovatelný bez snížení počtu ethernet portů | PODPORUJE, volitelným modulem |
| Stohování požadováno | PODPORUJE |
| Počet portů 10/100/1000 | 48 |
| Počet portů 1 Gbit/s SFP | 4x SFP |
| Možnost připojit externí redundantní zdroj | PODPORUJE |
| **Výkonnostní parametry** |  |
| Minimální propustnost přepínacího subsystému | 200 Gbit/s |
| Minimální paketový výkon přepínače | 100 milionu paketů/vteřinu |
| Rychlost stohovacího propojení | alespoň 80 Gbit/s |
| Minimální počet MAC adres | 15000 |
| **Vlastnosti stohování** |  |
| Vzájemné stohování všech modelů 10/100 s 10/100/1000 s 1Gbit/s uplinky s 10Gbit/s uplinky | PODPORUJE |
| Minimální počet přepínačů ve stohu | 8 |
| Automatická kontrola a sjednocení verze software přepínačů ve stohu | PODPORUJE |
| Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením | PODPORUJE |
| Seskupení portů (IEEE 802.3ad) mezi různými prvky stohu | PODPORUJE |
| kterýkoli prvek ve stohu může být řídícím prvkem stohu (1:N redundance) | PODPORUJE |
| **Protokoly fyzické vrstvy** |  |
| IEEE 802.3-2005 | PODPORUJE |
| IEEE 802.3ad | PODPORUJE |
| Podpora "jumbo rámců" | PODPORUJE |
| **Protokoly 2. vrstvy** |  |
| IEEE 802.1D | PODPORUJE |
| IEEE 802.1Q | PODPORUJE |
| Minimální počet aktivních VLAN | 1000 |
| IEEE 802.1X - Port Based Network Access Control | PODPORUJE |
| IEEE 802.1s - multiple spanning trees | PODPORUJE |
| IEEE 802.1w - Rapid Tree Spanning Protocol | PODPORUJE |
| IEEE 802.1p - Minimální počet vnitřních front | 4 |
| Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní | PODPORUJE |
| Detekce protilehlého zařízení (např. CDP, LLDP) | PODPORUJE |
| Detekce parametrů protilehlého zařízení (např. LLDP-MED) | PODPORUJE |
| Protokol pro definici šířených VLAN (např. VTP) | PODPORUJE |
| Detekce jednosměrnosti optické linky (např. UDLD) | PODPORUJE |
| STP root guard | PODPORUJE |
| STP loop guard | PODPORUJE |
| Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard) | PODPORUJE |
| Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech | PODPORUJE |
| **Protokol IP** |  |
| IP alias (více IP sítí na jednom rozhraní) | PODPORUJE |
| QoS | PODPORUJE |
| QoS i na stohovacím propoji | PODPORUJE |
| DHCP relay | PODPORUJE |
| **Protokol IPv6** |  |
| Certifikace IPv6 ready logo – Phase II | PODPORUJE |
| IPv6 ACL | PODPORUJE |
| IPv6 QoS | PODPORUJE |
| IPv6 services ( DNS, Telnet, SSH, Syslog, ICMP) | PODPORUJE |
| HTTP, SNMP over IPv6 | PODPORUJE |
| RADIUS, TACACS+ over IPv6 | PODPORUJE |
| IPv6 MLDv2 snooping | PODPORUJE |
| IPv6 Port ACL | PODPORUJE |
| IPv6 First Hop Security RA guard | PODPORUJE |
| IPv6 First Hop Security DHCPv6 guard | PODPORUJE |
| IPv6 First Hop Security IPv6 Binding Integrity Guard | PODPORUJE |
| **Směrovací protokoly** |  |
| statické směrování | PODPORUJE |
| **Směrování multicastu** |  |
| IGMPv2 snooping | PODPORUJE |
| IGMPv3 snooping | PODPORUJE |
| IPv6 MLDv1 & v2 snooping | PODPORUJE |
| **Bezpečnost** |  |
| ACL na rozhraní IN/OUT (včetně virtuálních - VLAN, loopback, 802.3ad) | PODPORUJE, na fyzickém rozhraní |
| ACL pro IP | PODPORUJE |
| ACL pro ethernetové rámce | PODPORUJE |
| IPv6 ACL | PODPORUJE |
| Možnost definovat povolené MAC adresy na portu | PODPORUJE |
| Možnost definovat maximální počet MAC adres na portu | PODPORUJE |
| Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy) | PODPORUJE |
| DHCP snooping | PODPORUJE |
| Dynamic ARP inspection (DAI) | PODPORUJE |
| Verifikace mapování IP-MAC (např. IP source guard) | PODPORUJE |
| IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu | PODPORUJE |
| IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači, sdílení ověření koncových stanic | PODPORUJE |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | PODPORUJE |
| Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x) | PODPORUJE |
| Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Security Group Exchange Protocol dle RFC draft-smith-kandula-sxp-01 nebo funkčně ekvivalentní). | PODPORUJE |
| Detekce parametrů připojovaného koncového zařízení a jejich sdílení s policy serverem | PODPORUJE |
| **Podpora koncových zařízení** |  |
| Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury | PODPORUJE |
| Podpora určování polohy klienta, rozšíření WiFi systému pro určování polohy klienta i v pevné LAN síti (například Network Mobility Service Protocol - NMSP) | PODPORUJE |
| EEE (IEEE 802.3az) | PODPORUJE |
| **Management** |  |
| CLI rozhraní | PODPORUJE |
| SSHv2 | PODPORUJE |
| SSHv2 over IPv6 | PODPORUJE |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | PODPORUJE |
| SNMPv2 | PODPORUJE |
| SNMPv3 | PODPORUJE |
| USB konzolová linka | PODPORUJE |
| Sériová konzolová linka | PODPORUJE |
| 10/100 management out-of-band port | PODPORUJE |
| DNS klient | PODPORUJE |
| NTP klient s MD5 autentizací | PODPORUJE |
| NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955) | PODPORUJE |
| Sběr dat pro NetFlow nebo IPFIX export z každého portu přepínače | PODPORUJE |
| Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů | PODPORUJE |
| Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb | PODPORUJE |
| RADIUS klient pro AAA (autentizace, autorizace, accounting) | PODPORUJE |
| TACACS+ klient | PODPORUJE |
| Port mirroring (SPAN) | PODPORUJE |
| Port mirroring 1 -> 1 | PODPORUJE |
| Port mirroring N -> 1 | PODPORUJE |
| Port mirroring ACL (mirroruje pouze definované toky) | PODPORUJE |
| Vzdálený port mirroring (RSPAN) | PODPORUJE |
| Syslog | PODPORUJE |
| Měření zakončení a délky metalického kabelu (TDR) | PODPORUJE |
| Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů) | PODPORUJE |
| Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute) | PODPORUJE |
| Přepínač si může automaticky zálohovat a obnovit firmware včetně konfigurace z nadřazeného směrovače nebo přepínače | PODPORUJE |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | PODPORUJE |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů | PODPORUJE |
| **Služby** |  |
| DHCP server | PODPORUJE |

1. : Minimální požadavky na přístupové přepínače.

# WiFi infrastruktura

## Stávající topologie bezdrátové sítě

Jádro bezdrátové sítě Českého rozhlasu tvoří dvojice Wireless LAN kontrolérů (dále jen WLC). Jedná se o zařízení:

* WLC 4402 s licenci pro 50 access pointů
* WLC 5508 s licenci pro 100 access pointů

ČRo dále v rámci WiFi infrastruktury dále provozuje access pointy (AP) Cisco Aironet 1142N a 1131AG, přičemž Cisco Aironet 1131AG je nahrazován již zakoupenými AP Cisco Aironet 2702.

Pro management sítě je používán nástroj Cisco Prime Infrastructure, který obsahuje 300 Lifecycle licencí.

## Obměna WiFi infrastruktury

Zadavatel požaduje dodání dvou centrálních Wireless LAN kontrolérů, které nahradí stávající jádro bezdrátové sítě.

Centrální redundantní Wireless LAN kontroléry pro řízení WLAN přístupových bodů (WLAN AP) musí mít dostatečný výkon pro centrální přepínání všech klientů bezdrátové sítě, a to především ve vztahu k obsluze nových AP podporujících 802.11ac. Musí podporovat rychlý a bezpečný roaming těchto klientů mezi WLAN AP bez potřeby opakované autentizace EAP/Radius a integrovaný centrální radio-resource management včetně spolupráce RRM mezi kontroléry v clusteru.

Centrální WLAN kontroléry musí dále podporovat šifrování řídících rámců mezi WLAN AP a kontrolérem a musí obsahovat Integrovaný IDS systém pro detekci útoků na bezdrátovou síť (wireless IDS). Požadována je také aplikační inspekce přenášeného provozu (DPI na 7. vrstvě ISO/OSI na základě aplikačních signatur), včetně rozpoznání jednotlivých aplikací, grafické zobrazení statistik a možnost řízení provozu pro rozpoznané aplikace.

Wireless LAN kontroléry musí být kompatibilní se stávajícími AP a musí obsahovat licence pro min. 125 AP. Minimální požadavky na jejich funkcionalitu jsou uvedené v tabulce níže.

| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované funkcionality/vlastnosti** |
| --- | --- |
| ***Kontrolér bezdrátové sítě – primární a redundantní zařízení*** | ***1 + 1*** |
| Minimální počet podporovaných AP | 125 |
| Možností licenčního rozšíření na 1000 registrovaných AP | PODPORUJE |
| Minimální počet 10G SFP portů per kontrolér | 2 |
| Redundantní napájecí zdroj součástí dodávky | PODPORUJE |
| Minimální propustnost pro data Gb/s | 20 Gb/s |
| Automatizované řešení rychlého roamingu uživatelů v rámci AP na jednom kontroléru i mezi 2 a více kontroléry, L2/L3, IPv4/IPv6 | PODPORUJE |
| Podpora možnosti lokálního bridgování uživatelských dat per SSID přímo na příslušném AP, platí pro IPv4 i IPv6 | PODPORUJE |
| Integrované řešení návštěvnického přístupu s možností webové autentizace (včetně nativních IPv6 klientů), bezpečné oddělení od zaměstnaneckého provozu, funkční i v módu lokálního bridgování uživatelských dat přímo na AP | PODPORUJE |
| Integrovaná správa návštěvnických účtů s možností definice jejich platnosti | PODPORUJE |
| Podpora možnosti tunelování uživatelských dat z AP až na kontrolér, možnost šifrování těchto uživatelských dat | PODPORUJE |
| Podpora 802.11e/WMM | PODPORUJE |
| Diferenciace úrovní QoS pro různé služby a skupiny uživatelů (zaměstnance a návštěvníky), možnost obousměrného omezení propustnosti per klient | PODPORUJE |
| Možnost striktní alokace vysílacího času (v procentech) per SSID, podpora funkce spravedlivého rozdělení vysílacího času mezi klienty | PODPORUJE |
| Mechanismy řízení přístupu (Call Admission Control) pro hlasový i video provoz. Konfigurovatelné parametry max. zátěže a šířky pásma. | PODPORUJE |
| Podpora Video-streamingu se spolehlivým multicastem | PODPORUJE |
| Optimalizace multicast provozu v bezdrátové síti (IGMP snooping) | PODPORUJE |
| Aplikační inspekce přenášeného provozu (DPI na 7. vrstvě ISO/OSI na základě aplikačních signatur) umožňující rozpoznání jednotlivých aplikací, grafické zobrazení statistik a možnost řízení provozu per rozpoznaná aplikace | PODPORUJE |
| Lokální profilování zařízení – per uživatel a per zařízení | PODPORUJE |
| Podpora 802.11i, respektive jeho implementací WPA a WPA2 včetně enterprise variant autentizace/šifrování | PODPORUJE |
| 802.1x/EAP autentizace: PEAP, EAP-FAST, EAP-TLS, ... | PODPORUJE |
| Možnost autentizace nových klientů k AP v módu lokálního bridgování dat pomocí 802.1x/EAP i v případě výpadku centrálního kontroléru | PODPORUJE |
| Integrovaný IDS systém pro detekci útoků na bezdrátovou síť (wireless IDS) | PODPORUJE |
| Detekce cizích AP (Rogue AP) a klientů v AdHoc režimu | PODPORUJE |
| Možnost vynuceného odpojení klientů od cizích AP | PODPORUJE |
| Možnost omezit počet klientů per SSID | PODPORUJE |
| Podpora standardu „802.11w“ pro ochranu řídících rámců na AP a klientovi | PODPORUJE |
| Podpora standardu „802.11u“ pro výběr SSID a autentizaci klienta | PODPORUJE |
| Podpora standardu „802.11k“ pro optimalizaci roamingu | PODPORUJE |
| Podpora standardu „802.11r“ pro rychlý roaming klientů mezi AP | PODPORUJE |
| Podpora standardu „802.11v“ pro optimalizaci připojení klienta | PODPORUJE |
| Automatizovaná centrální správa frekvenčního pásma, spolupráce mezi kontroléry v clusteru | PODPORUJE |
| Monitoring rádiového spektra vč. 20/40/80 MHz kanálů | PODPORUJE |
| Automatické zvýšení vysílacího výkonu okolních AP při výpadku AP („self healing“) | PODPORUJE |
| Automatické přizpůsobení se bezdrátové sítě na základě indexu kvality radiového signálu | PODPORUJE |
| Vyhodnocování kvality signálu bezdrátové sítě v reálném čase a grafické vyobrazení | PODPORUJE |
| Možnost detekce rušivých signálů (interference) a identifikace zdrojů interference na základě signatur | PODPORUJE |
| Současná funkčnost AP pro přenos dat, detekci bezpečnostních incidentů a analýzu spektra | PODPORUJE |
| Troubleshooting radiového signálu a automatické řešení problému rušivého signálu | PODPORUJE |
| Možnost členění AP do skupin | PODPORUJE |
| Konfigurace AP podle příslušnosti do skupiny | PODPORUJE |
| Možnost vytváření rádiových profilů (nastavení kanálů, rychlostí) | PODPORUJE |
| Nastavení různého rádiového profilu pro různé skupiny AP | PODPORUJE |
| Šifrovaná řídící komunikace AP-kontrolér pro IPv4 i IPv6 | PODPORUJE |
| Rychlá detekce selhání primárního kontrolérů (pod 1 sekundu) | PODPORUJE |
| Možnost redundance na úrovni kontrolérů a jejich portů | PODPORUJE |
| Výpadek aktivního kontroléru v redundantním páru nemá žádný dopad na provoz již připojených klientů (tj. bez potřeby reautentizace) | PODPORUJE |
| Centrální administrace správců s granularitou přístupových práv | PODPORUJE |
| Podpora správy přes serial CLI nebo přes IPv4 a IPv6 pomocí SSH/telnet, http a https web GUI, SNMP, aplikace pro dohled pro Android a Apple mobilní platformy | PODPORUJE |

1. : minimální požadavky - WLC

## Rozšíření nástroje Cisco Prime Infrastructure

Pro účely single point of management a správu wired a wireless sítě je v ČRo používán nástroj Cisco Prime Infrastructure. Současná používaná verze software je 2.1.

V souvislosti s modernizací a rozšířením WiFi infrastruktury požaduje Zadavatel upgrade nástroje na verzi 3.1.

Zadavatel dále požaduje rozšíření nástroje Cisco Prime Infrastructure o modul Assurance, který zabezpečí end-to-end aplikační visibilitu a kontrolu služeb.

# Cisco Identity Service Engine

## Stávající topologie autentizačních autorit

Český rozhlas provozuje v současné době dvě autentizační autority – starší Cisco ACS 5.1 a novější Cisco ISE 1.2. Autentizace, autorizace a evidence správcovských přístupů na aktivní prvky je prováděna proti systému Cisco Secure Access Control System 5.1 protokolem TACACS+. Autentizace, autorizace a evidence uživatelských přístupů do WiFi sítě a do VPN je v současné době prováděna protokolem Radius proti autentizačnímu systému Cisco Identity Services Engine 1.2.

Autentizační autorita Cisco ISE je instalována ve verzi 1.2.0.899. Použita je licence BASE-500, která umožňuje práci 500 současně přihlášených uživatelů. Autentizační autoritu tvoří dvě virtuální appliance ve vnitřním prostředí VMware vSphere, které v současné době ČRo provozuje.

V případě ČRo slouží jedna virtuální appliance jako primární Administration, PSN a Monitoring persona, druhá appliance je nastavena jako sekundární.

## Rozšíření a upgrade Cisco ISE

Zadavatel požaduje povýšení autentizační autority Cisco ISE ze stávající verze 1.2 na verzi 2.0.

Zadavatel dále požaduje rozšíření licence autority ISE na podporu 3000 současně přihlášených uživatelů.

Zadavatel požaduje rozšíření o licence na podporu protokolu TACACS+ a migraci existujících autentizačních a autorizačních pravidel ze systému ACS na Cisco ISE.

## Implementace pravidel pro LAN 802.1X

Zadavatel požaduje rozšíření stávající bezpečnostní politiky Cisco ISE o plnou implementaci ověřování 802.1X v síti LAN.

## Úprava webových portálů Cisco ISE

Zadavatel požaduje provést úpravu vzhledu webových stránek, které slouží pro přístup do vybraných WiFi sítí ČRo – sponsor portal, guest portal. Grafické podklady pro úpravu vzhledu poskytne zadavatel.

# Pilotní implementace LAN 802.1X

Zadavatel požaduje zprovoznění autentizace koncových zařízení do sítě LAN pomocí mechanismu 802.1X za pomoci stávající autentizační autority Cisco ISE. Součástí dodávky bude konfigurace autentizační autority a vytvoření konfiguračních šablon pro použité přístupové přepínače. Požadována je minimálně následující funkcionalita:

1. Autentizace koncových zařízení do sítě s pomocí mechanismu 802.1X. Ověření bude prováděno klientským certifikátem dle standardu X.509 v3 proti interní certifikační autoritě na platformě Microsoft Windows.
2. Autentizace koncových zařízení do sítě s pomocí mechanismu 802.1X. Ověření bude prováděno uživatelským jménem a heslem stanice proti stávajícímu systému Microsoft Active Directory.
3. Autentizace koncových zařízení bez 802.1X suplikanta proti interní databázi systému Cisco ISE.
4. Přiřazování koncové stanice do VLAN na základě členství ve skupině Active Directory.

Před zahájením implementace požaduje zadavatel zpracování realizačního projektu, který bude obsahovat analýzu stávajícího stavu, návrh cílového řešení a postup implementace. Implementační práce budou podmíněny akceptací projektové dokumentace zadavatelem. Projektová dokumentace bude vypracována v písemné i elektronické podobě, ve formátu MS Word/Excel, MS Visio a PDF.

V rámci implementace požaduje zadavatel zprovoznění autentizace v pilotním režimu na následujících koncových zařízeních:

* Windows 7 – nativní 802.1X suplikant (autentizace jménem a heslem stanice proti AD).
* Windows 7 – suplikant Cisco AnyConnect (autentizace jménem a heslem stanice proti AD).
* Windows 7 – nativní 802.1X suplikant (autentizace certifikátem proti AD).
* Windows 7 – suplikant Cisco AnyConnect (autentizace certifikátem proti AD).
* Windows 7 – autentizace bez suplikantu na základě MAC (MAC authentication bypass).

# Dokumentace a školení

Po dokončení implementace požaduje zadavatel dodání dokumentace konečného provedení. Dokumentace bude vypracována v písemné i elektronické podobě, ve formátu MS Word/Excel, MS Visio a PDF.

Jako součást dodávky požaduje zadavatel školení administrace HW a SW v nezbytně nutném rozsahu pro základní administraci systémů.