

***Projektová dokumentace***

***„Vybudování JCE IB SOŠ INFORMATIKY A SPOJŮ A SOU  
KOLÍN - zpracování projektové dokumentace“***

***TECHNOLOGICKÁ ČÁST JCE IB***

***D.1.4.9. Technologie a řešení JCE IB***

***D.1.4.9.04. ŘÍZENÍ PŘÍSTUPU DO LAN A WLAN VČETNĚ  
SEGMENTACE - ŠKOLA***

**Zpracoval:**

Petr Lacina

## 4 ŘÍZENÍ PŘÍSTUPU DO LAN A WLAN VČETNĚ SEGMENTACE - ŠKOLA

### 4.1 ŘEŠENÍ PŘÍSTUPU ZAŘÍZENÍ A UŽIVATELŮ DO LAN A WLAN VČETNĚ SEGMENTACE

Součástí navrženého řešení řízení přístupu zařízení a uživatelů (autentizace a autorizace) je konfigurace aktivních prvků, kontrolérů a autentizačního a autorizačního serveru (dále jen AA server) minimálně v rozsahu v této kapitole uvedené. AA server je součástí návrhu celého řešení a bude nakonfigurován a zalicencován v redundantním zapojení (HA režim). Oba tyto servery budou nainstalovány do navrženého virtuálního v prostředí ŠKOLY.

Systém řízení přístupu uživatelů do LAN a WLAN bude realizován prostřednictvím jednotné správy uživatelských účtů (jednotná identita), autentizací uživatelů při přístupu k jednotlivým zdrojům poč. sítě pomocí několika zásadních komponent a to:

- konfigurovatelné aktivní prvky, se zásadní vlastností, a to podporou protokolu IEEE 802.1x jako standardu pro kontrolu přístupu do LAN založenou na portu akt. prvku,
- autentizační a autorizační server (specializovaný server RADIUS), který síťovým autentizačním protokolem Kerberos umožňuje bezpečně prokázat identitu uživatele nebo zařízení,
- databáze uživatelů (přihlašovacího jména a hesla) uložená v LDAP (Lightweight Directory Access Protocol), který v tomto řešení reprezentuje Active Directory (dále jen „AD“),
- důvěryhodná zařízení s OS Win, která budou naimportovány v LDAP.

Autentizace uživatelů, při přístupu k jednotlivým službám, bude řešena přes LDAP. Při přihlašování libovolného uživatele je kontaktován AA server napojený na LDAP.

Aktivní prvky disponují konfigurací, která omezuje přístup do sítě pomocí protokolu 802.1x napojeného na AA server a LDAP. V tomto případě je použita databáze uživatelů uložené v AD (Active Directory). Všechny porty, které jsou určeny pro uživatele, jsou zabezpečené a všechny porty jsou stejně nakonfigurované. Switch na portu ověřuje, zda připojené zařízení může do poč. sítě. Uživatel své zařízení může připojit kamkoliv do ethernetové zásuvky a vždy se ověří a je mu přidělena správná VLAN.

#### 4.1.1 Lokální počítačová síť – drátová (LAN)

V LAN bude minimálně nakonfigurován a vynucován následující princip ověřování zařízení. Switch připojované zařízení ověří, zda JE či NENÍ v AD přítomen objekt tohoto zařízení s příslušnými vlastnostmi. Pokud objekt ověřovaného zařízení existuje v AD, tak switch na portu povolí komunikaci a nastaví na něm příslušnou konfiguraci, která je poslána z AA serveru. Tato konfigurace se pro každý typ zařízení liší a je mu přidělena na základě splněných kritérií dle typu zařízení:

*Doménový počítač (typicky zařízení s OS WIN)*

- počítač MUSÍ být v doméně (AD),
- počítač v AD je zařazen v příslušné OU (organizační jednotka),
- počítači je přidělena VLAN kde se dostane do interní sítě a má přístup na servery,

#### *Soukromé zařízení*

- uživatel musí mít v AD účet,
- účet v AD je zařazen v příslušné OU (učitel/student),
- na zařízení bude nastartovaná služba Wired AutoConfig service (i v ČJ Windows) - je nutné zapnout automatické spuštění služby,
- na síťové kartě bude nastaveno ověřování PEAP/MSChapV2,
- zařízení je přidělena VLAN učitel nebo VLAN student.

#### *Tiskárny, tabule, scannery apod. (školní zařízení, které neumí 802.1x a nepotřebují přístup na internet)*

- každé zařízení bude v AD v OU = Zařízení,
- účet pro zařízení v AD bude ve tvaru: Jméno: MAC\_zařízení, Heslo: MAC\_zařízení,
- tyto zařízení budou mít přidělenou uživatelskou VLAN, ale budou mít omezení v podobě Access Listů (nemohou do internetu, jsou povoleny jen služby pro tisk, DNS, DHCP,...).

Pokud nebude v AD nalezen objekt příslušného zařízení, tak se zařízení neověří a je mu zakázáno připojení do poč. sítě. Uživatelé, kteří se chtějí připojit do lokální poč. sítě nebo do internetu, musí mít účet v AD.

#### 4.1.2 Lokální počítačová síť – bezdrátová (WLAN)

Bezdrátová síť využívá stejný způsob ověřování jako LAN pouze s tím rozdílem, že se uživatel nepřipojuje do ethernetového portu („datové zásuvky“), ale připojuje se prostřednictvím přístupových bodů a ověření probíhá prostřednictvím kontroléru. Bezpečnost je jednotná pro LAN tak WLAN tzn. způsob autentifikace je pro učitele, studenty a notebooky, kteří jsou v AD totožný (viz výše).

*V bezdrátové síti budou nakonfigurována tato jména bezdrátových sítí (SSID):*

- JMENO\_SKOLY – SSID používají učitelé, studenti a notebooky, kteří jsou v AD,
- JMENO\_SKOLY\_Hoste – bude vytvořeno pro hosty školy.

Součástí cenové kalkulace je kompletní nasazení segmentace počítačové sítě prostřednictvím VLAN, nasazení nového IP plánu a ověřování všech zařízení prostřednictvím AA serveru. AA servery v počtu 2ks budou nasazený v HA režimu.

Licence AA serveru, pro minimálně 1200 identit, bude funkční, včetně podpory, 5 let od nainstalování tohoto SW. Po uplynutí této doby je nutné dokoupit předplatné (subscription) min. na další rok. Při nezakoupení této podpory AA server přestane být funkční tzn. žádné zařízení se nepřipojí do LAN a WLAN.

## 4.2 SPECIFIKACE MINIMÁLNÍCH POŽADAVKŮ TECHNICKÉHO ŘEŠENÍ

### 4.2.1 AA server – 2ks pro minimálně 1200 identit

- On-premise appliance, nepřipouští se cloud řešení
- Licence pro alespoň 1200 současně připojených zařízení
- Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení, čas připojení apod.)
- Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo řídicími moduly, VPN branami) poskytuje ochranu před neoprávněným přístupem k pevné LAN síti, bezdrátové wifi síti (metodou 802.1x) a pro VPN přístup
- Poskytuje AAA funkce (viz níže)
- S příslušnou licencí podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control)
- Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování kapacity
- Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace
- Je dostupné ve formě Appliance (hardware i software podporovaný jedním výrobcem)
- Je dostupné ve formě Virtuálního stroje na platformách ESX/ESXi, KVM nebo Hyper-V
- RADIUS pro autentizaci, autorizaci, zaznamenávání
- proxy funkce pro externí RADIUS
- PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, TEAP, EAP-FAST
- S příslušnou licencí podpora TACACS+ pro administraci zařízení
- Ověření uživatelů heslem nebo certifikátem
- Ověření MAC adresou připojovaného zařízení
- Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle:
  - o stavu a typu koncového zařízení (viz níže),
  - o uživatele (role, skupiny),
  - o místa připojení,
  - o historie připojení
- Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě
- Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě
- Využívání Change of Authorization (CoA, RFC 3576) pro změny vynucovaných politik „za běhu“
- Řízení autentizace a založení důvěryhodné infrastruktury mezi jednotlivými prvky sítě, pro bezpečný a šifrovaný transport dat
- Zaznamenávání aktivity uživatelů a zařízení připojených k síti
- Dotazovací systém, korelace záznamů, centralizované výkazy
- Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů)
- Vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i WiFi
- Oprávnění pro hosty přidělována správcem přístupu přes portál pro snadné vytváření dočasných účtů
- Samoobslužný portál pro hosty
- Ověření hostů přes HTTP a HTTPS

- S příslušnou licencí automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se síťovou infrastrukturou
- Předdefinované profily pro běžná mobilní zařízení (zařízení s OS Android, SymbianOS, Apple, Blackberry, HTC)
- Předdefinované profily pro síťová zařízení NAD od různých výrobců
- Podpora pro IPv6 koncová zařízení
- S příslušnou licencí podpora BYOD:
  - o Onboarding (registrace, provisioning, nastavení klientských zařízení)
  - o Onboarding/provisioning proces formou samoobsluhu
  - o Specifické politiky pro BYOD zařízení
  - o Možnost nastavení limitu BYOD zařízení pro jednoho uživatele
  - o Interní CA, pro vydávání certifikátů BYOD zařízením
  - o Interní CA lze řetězit jako subordinate pod firemní CA
- Možnost autentizace oproti více AD domén, i když nejsou v trust režimu
- Aktivace šifrování MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují)
- Podpora Multi-Domain integrace s AD
- Podpora SXP (Exchange Protocol) dle IETF
- Centralizovaná správa
- Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému
- Zjednodušení správy vytváření skupin uživatelů, koncových a síťových zařízení
- Grafické rozhraní pro definici pravidel přístupu k síti
- Grafické rozhraní pro monitorování, definici výkazů, řešení problémů
- Diagnostika problémů (systémová, údaje o chybách přihlašování, TCP dump, packet capture)
- Zaznamenávání událostí na externí syslog server
- Podpora SNMPv3
- NTP pro synchronizaci času
- SMTP pro zasílání zpráv a výstrah přes e-mail
- Centralizované nasazení s podporou vysoké dostupnosti v režimu Active-Active (minimálně 2 servery)
- Appliance podporuje ochranu dat a záznamů