Zkušební provoz wifi sítě na SPŠ a VOŠ Písek

3.1.2011 byl zahájen zkušební provoz wifi sítě, který potrvá cca jeden měsíc, během kterého by měly být odstraněny veškeré chyby, a případně doladěna konfigurace.

K dispozici jsou následující SSID:

spsvos-wifi – pro žáky a učitele SPŠ a VOŠ (přístup ke školní síti a internetu), pro studenty BIVŠ (pouze internet)

spsvos-wep – pro všechny, kterým HW neumožňuje připojit se k síti se zabezpečením WPA2 (pouze v nutných případech bez jiných možností), nutná registrace fyzické adresy bezdrátového rozhraní

spsvos-host – pro návštěvníky SPŠ a VOŠ, je nutné získat jméno a heslo (v Houstonu), síť bez zabezpečení, pouze internet. Po přihlášení k síti a prvním spuštění internetového prohlížeče se zadá získané jméno a heslo.

plánujeme přidat SSID:

spsvos-pristroje – síť pro učební pomůcky s bezdrátovým rozhraním, zabezpečení WEP, bude nutná registrace fyzické adresy rozhraní a síť bude dostupná pouze v některých částech budovy.

spsvos-eduroam – roamingové prostředí mezi evropskými výzkumnými a vzdělávacími institucemi. Uživatel má jediný účet (ve své domovské síti) a tento účet jej opravňuje k použití bezdrátové sítě kteréhokoliv člena projektu. Zatím ve fázi jednání. Více viz. <u>www.eduroam.cz</u>.

Z technického hlediska se jedná o řídící jednotku a 24ks přípojných bodů (AP) HP/3COM. AP pracují ve standartech :

Standard	Pásmo [GHz]	Maximální rychlost [Mbit/s]
IEEE 802.11a	5	54
IEEE 802.11b	2,4	11
IEEE 802.11g	2,4	54
IEEE 802.11n	2,4 nebo 5	600

AP jsou rozmístěna: 5ks na 2. patře, 5ks na 1. patře, 4ks v přízemí, 4ks v suterénu, 3ks v 1. patře přistavby a 3ks v dílnách.

Nastaveni windows XP

U systému s SP2 je nutné nainstalovat WPA2 aktualizaci z

O:\Free\=Aktualizace=\Windows\WXP\wpa2_pro_xp_sp2\WindowsXP-KB893357-v2-x86-CSY.exe

nebo instalovat SP3. Případně nejnovější ovladače bezdrátové karty.

V ovládacích panelech – síťová připojení – vlastnosti bezdrátového připojení – záložka bezdrátové sítě – přidat:

- nastavte SSID na spsvos-wifi
- ověření v síti WPA2
- šifrování AES

– Bezdrátové připojení k síti - vlastnosti 🛛 😨 🔀	Vlastnosti bezdrátové sítě 🔹 🕜
Obecné Bezdrátové sítě Upřesnit	Přidružení Ověřování Připojení
✓ Konfigurovat nastavení bezdrátové sítě pomocí systému Windows	Síťový <u>n</u> ázev (SSID): spsvos-wifi
– Sítě k dispozici	🔲 Připojit, i když tato síť nevysílá
Chcete-li se připojit, odpojit nebo získat další informace o	Klíč bezdrátové sítě
bezdrátových sítích v dosahu, klepněte na následující tlačítko.	Tato síť vyžaduje klíč pro následující položky:
Zobrazit bezdrátové sítě	<u>D</u> věření v síti: ₩PA2
Upřednostňované sítě: Automaticky připojit k sítím, které isou k dispozici, v uvedeném	Šifrování <u>d</u> at: AES
pořadí:	Síťový klíč:
Nahoru	Potvrzeni siłového klíče:
Dolů	
	Inde <u>x</u> klíče (rozšířené): 1 👌
Přidat Odebrat Vlastnosti	☑ Kjič je poskytován automaticky
	J.
Dalši informace o <u>konfiguraci bezdrátové sítě</u>	Toto je síť mezi počítači (ad hoc); nejsou použity bezdrátové přístupové body
	Producting a bit of the

Na záložce ověřování:

- typ protokolu EAP: protokol PEAP (Protected EAP)
- odškrtněnte Ověřit jako počítač v případě, že informace o počítači jsou k dispozici
- ve vlastnostech protokolu PEAP ZMĚNA viz. důležité na poslední stránce
- vyberte metodu ověřování Zabezpečené heslo EAP-MSCHAPv2

Vlastnosti bezdrátové sítě	? 🛛	Vlastnosti protokolu Protected EAP	? 🛛
Přidružení Ověřování Připojení Vybráním této možnosti zajistite ové sítím Ethernet. Vybráním této síti ověření IEEE Povolit v této síti ověření IEEE Jyp protokolu EAP: Protokol PEA Ověřít jako počítač v případě, že počítači nejsou k dispozici Ověřít jako hosta v případě, že	iřený přístup k bezdrátovým 802.1x P (Protected EAP) Vlastnosti ie informace o počítači jsou k informace o uživateli nebo o	Pro připojení: Důvěřít certifikát serveru Připojit k těmto serverům: Důvěřyhodné kořenové certifikační úřady: AddTrust External CA Root CA 1 Certiposte Classe A Personne Certiposte Classe A Personne Certiposte Serveur Certiposte Serveur Certiposte Serveur Certipiste - Autoridade Certificadora - AC2 Certisign - Autoridade Certificadora - AC4 Certisign	
	OK Storno	Vyberte metodu ověřování: Zabezpečené heslo (EAP-MSCHAP v2) Povolit rychlé obnovení připojení Povolit kontroly pomocí součástí Quarantine Odpojit, nenabízí-li server metodu kryptovazeb TLV OK Sto	rovat) prno

V konfiguraci EAP-MSCHAPv2: viz. obrázek.

Vlastnosti protokolu EAP MSCHAPv2 🛛 🔀		
	👘 Bezdrátové připojení k	síti 🔀
Pro připojení:	Klepnutím zde vyberete certifiká k síti.spsvos-wifi	t a další pověření pro připojení
Automaticky použít přihlašovací jméno, heslo a případně doménu systému Windows		s < <mark>)</mark> €
	Zadejte pověření	
OK Storno	20	50
Po potvrzení všech nastavení se objeví bublina		7
(vpravo), po jejímž odkliknutí vás systém požádá		
o zadání jména, hesla a domény. Viz obrázek.	Uživatelské jméno:	
	Heslo:	

Přihlašovací

doména:

SPS-PI

OK

Uložit uživatelské jméno a heslo pro budoucí použití

Storno

Windows Vista a windows 7

|--|

Jak ch	cete síť přidat?
	<u>R</u> učně vytvořit síťový profil
	Pomocí této možnosti vytvoříte nový profil sítě nebo vyhledáte existující síť a uložíte její profil do počítače. Musíte znát název sítě (SSID) a klíč zabezpečení (pokud je nastaven).
A	<u>V</u> ytvořit síť mezi počítači
~	Umožňuje vytvořit dočasnou síť pro sdílení souborů nebo připojení k Internetu.

- SSID spsvos-wifi
- typ zabezpečení
- typ šifrování AES

Náz <u>e</u> v sítě:	spsvos-wifi	
<u>T</u> yp zabezpečení:	WPA2-podnikové 👻	
Typ ši <u>f</u> rování:	AES 🔻	
<u>K</u> líč zabezpečení:	Skrýt znaky	
Vytvořit připojer	ií automaticky	
🛄 <u>P</u> řipojit, i když sí	ť právě nevysílá	
Upozornění: Pol	cud vyberete tuto možnost, může být ohroženo zabezpečení vašich o	sobních

Vyberte změnit nastavení připojení

🕞 📲 Ručně připojit k bezdrátové síti	
Byla úspěšně přidána síť spsvos-wifi.	
Změnit nastavení připojení Otevře vlastnosti připojení a umožňuje je změnit.	
	Zavřít

- na záložce připojení beze změn
- na záložce zabezpečení metoda ověřování v síti vyberte Protected EAP

psvos-wifi – vlastnosti bezdrátové sítě	spsvos-wifi – vlastnosti bezdrátové sítě
Připojení Zabezpečení	Připojení Zabezpečení
Název: spsvos-wifi SSID: spsvos-wifi Typ sítě: Přístupový bod Dostupnost sítě: Pro všechny uživatele	Typ zabezpečení: WPA2-podnikové
Přípojit automaticky, pokud je tato siť v dosahu	Z <u>v</u> olte metodu ověřování v síti:
Pripojit k preferovanejsi siti, pokud je k dispozici	Microsoft: Protokol PEAP (Protected EAF 👻 Nastavení
	Zapamatovat pověření pro toto připojení pro každé přihlášení
	Upřesnit nastavení
OK Storno	OK Storno

- nastavení protokolu PEAP ZMĚNA viz. důležité na poslední stránce
- nastavte metodu ověřování na Zabezpečené heslo EAP-MSCHAPv2
- v konfiguraci MSCHAPv2 odškrtněte Automaticky použít mé uživatelské jméno a heslo...

o připojení:		
Ověřit certi <u>f</u> ikát ser	veru	
	ຕະເວລາໃຫາ	
	iverum,	
-		
Důvěryhodné kořenov	vé certifikační autority:	44
AddTrust Externa	al CA Root	*
CA SPS a VOS Pis	ek	
📄 certifikat petr		=
certifikat petr		1
Class 3 Public Prin	nary Certification Authority	
CIL Hormos		
Equifax Secure Co	ertificate Authority	•
Equifax Secure Co Nezobrazovat výz	ertificate Authority III vu k ověření nových serverů ne	+ ebo
Equifax Secure Cr Equifax Secure Cr A Equifax Secure Cr Equifax	ertificate Authority III Vu k ověření nových serverů ne rtifikačních autorit ání: P-MSCHAP v2) ení připojení NAP (Network Access Protection	bo (Konfigurovat)
Equifax Secure Cr Equifax Secure Cr A Equifax Secure Cr Equifax	ertificate Authority III Vu k ověření nových serverů ne rtifikačních autorit ání: P-MSCHAP v2) ení připojení NAP (Network Access Protectio erver metodu kryptovazeb TLV	bo Konfigurovat
Equifax Secure Ca Equifax Secure Ca Equifax Secure Ca A Nezobrazovat výz důvěryhodných ce berte metodu ověřová abezpečené heslo (EA Povolit rychlé obnove) Vynutit architekturu I) Odpojit, nenabízí-li se Povolit osobní údaje jdentity	ertificate Authority III vu k ověření nových serverů ne rtifikačních autorit ání: P-MSCHAP v2) ení připojení NAP (Network Access Protectio erver metodu kryptovazeb TLV	<pre>bo Konfigurovat n)</pre>

Dra ničenio			
rio pripoje			
Autor	naticky použít me	é uživatelské jmé	no a heslo
Star and a	ménu pokud evis	stuie) pro pribláše	enik
	mu Windown	scale) pro primos	
systé	mu Windows		
systé	mu Windows		

- změňte režim ověřování na Ověření uživatele a můžete uložit pověření – viz. obrázek

	Zadejte režim ověřování: Ověření uživatele Odstranit pověření pro všechny uživatele	věř <u>e</u> ní
Ověření uživatele Uložit pověřerí Odstranit pověření pro všechny uživatele Povolit pro tuto gíť jednotné přihlašování @ Provádět bezprostředně před přihlášením uživatele Provádět inned po přihlášení uživatele Maximální zpošdění (sekundy): 10 Umožnit zobrazení dalších dialogových oken při jednotném přihlašování	Ověření uživatele Uložit po Odstranit pověření pro všechny uživatele	věř <u>e</u> ní
Odstranit pověření pro všechny uživatele Povolit pro tuto giť jednotné přihlašování Provádět bezprostředně před přihlášením uživatele Provádět ihned po přihlášení uživatele Maximální zpoždění (sekundy): 10 Umožnit zobrazení dalších dialogových oken při jednotném přihlašování	Odstranit pověření pro všechny uživatele	
Povolit pro tuto giť jednotné přihlašování Provádět bezprostředně před přihlášením uživatele Provádět ihned po přihlášení uživatele Maximální zpoždění (sekundy): 10 Umožnit zobrazení dalších dialogových oken při jednotném přihlašování		
 Provádět bezprostředně před přihlášením uživatele Provádět ihned po přihlášení uživatele Maximální zpoždění (sekundy): 10 Umožnit zobrazení dalších dialogových oken při jednotném přihlašování 	Povolit pro tuto sit jednotne prihlasovani	
 Provádět ihned po přihlášení uživatele Maximální zpoždění (sekundy): 10 Umožnit zobrazení dalších dialogových oken při jednotném příhlašování 	Provádět bezprostředně před přihlášením uživate	ele
Maximální zpoždění (sekundy): Umožnit zobrazení dalších dialogových oken při jednotném přihlašování	Provádět ihned po přihlášení uživatele	
Umožnit zobrazení dalších dialogových oken při jednotném přihlašování	Maximālni zpoždĕni (sekundy): 10	*
	Umožnit zobrazení dalších dialogových oken při jednotném přihlašování	
Tato síť používá samostatné virtuální sítě LAN pro ověřování počítačů a uživatelů	Tato síť používá samostatné virtuální sítě LAN pro ověřování počítačů a uživatelů	0

e, bude se mo a účelem <mark>sta</mark> h	oci počítač př lování aktuali	ipojit k sít zací).	i, když nebudet
a ücelem stah	iovani aktuali	zacı).	
PI\user			
		1	
) (
	-		-35
	Pī∖user ••	PI\user	PI\user

 po potvrzení všech nastavení se objeví bublina, kde zadáte vaše přihlašovací jméno a heslo ve tvaru viz. obrázek níže. (jestliže již máte pověření uloženo, bude tento krok přeskočen)



Ověřován	í sítě	
Zadejte pové	ření uživatele	
	SDC DD.uses	
	SPS-PI\user	

Obecné nastavení (např. mobilní telefony, psp, apod.):

zabezpečení WPA2(šifrování AES), ověřování IEEE 802.1x, typ protokolu EAP : Protected EAP, metoda ověřování : zabezpečené heslo EAP-MSCHAPv2, uživatelské jméno ve tvaru SPS-PI\uzivatel a vaše heslo

Pro Unix systémy: zatím jsem neměl možnost testovat, neměl by být problém s

wpa_supplicant (http://en.wikipedia.org/wiki/Wpa_supplicant)

xsupplicant (<u>http://en.wikipedia.org/wiki/Xsupplicant</u>)

příklad viz.: http://www.fit.vutbr.cz/CVT/auth/.cs#linux

Důležité

Pro větší bezpečnost : pro systémy windows

- nainstalujte si certifikační autoritu CA SPS a VOS Pisek (jako důvěryhodnou CA)
- ve vlastnostech bezdrátové sítě zabezpečení metoda ověřování sítě PEAP nastavení zaškrtněte Ověřit certifikát serveru a Připojit k těmto serverům a vyplňte petr.spspi.cz;hermes.sps-pi.cz a zaškrtněte certifikační autoritu CA SPS a VOS Pisek

D.	na serverim
170	petr.sps-pi.cz;hermes.sps-pi.cz
Důs	· ěrvhodné kořenové certifikační úřadv:
	AddTrust External CA Root CA SPS a VOS Pisek certifikat petr class 3 Public Primary Certification Authority CP Invest CU-Hermes Vezobrazovat výzvu k ověření nových serverů nebo důvěryhodných certifikačních úřadů
berl	e metodu ověřování:
sue	
	volit rychle obnoveni pripojeni

ole	Hodnota	
Distribuční místa seznamu o	[1]Distribuční místo CRL: Náze	
Identifikátor kliče úřadu	ID kliče=85 73 79 c1 67 a8 98	
j Identifikátor kliče předmětu zavy doktornou se předmětu	84 59 37 cb 60 f9 b1 3f 06 24	
2 akiauni Uniezeni 1 2 840 113533 7 65 0	30 05 15 04 56 37 26 31 02 02	
91.2.040.110000.7.00.0 Použití klíče	Digitální podpis. Zakódování klí	
Algoritmus miniatury	shal	
Miniatura	3d f6 b2 0d 91 a0 48 c0 5f 6c	-
-		
f6 b2 0d 91 a0 48 c0 5f 6c f3 7	0 38 3d 61 0d fa b9 52 3c	
16 b2 0d 91 a0 48 c0 51 6c 13 7	0 38 3d 61 0d fa b9 52 3c	
16 b2 0d 91 a0 48 c0 51 6c 13 7	0 38 3d 61 0d fa b9 52 3c	
- 16 b2 0d 91 a0 48 c0 51 6c 13 7	0 38 3d 61 0d fa b9 52 3c	
16 b2 0d 91 a0 48 c0 5f 8c f3 7	0 38 3d 61 0d fa b9 52 3c	
f6 b2 0d 91 a0 48 c0 5f 8c f3 7	0 38 3d 61 0d fa b9 52 3c	

Pro připojení bude nutné zadat vaše jméno a heslo a potvrdit certifikát .

Vystavitel musí být CA SPS a VOS Pisek

V záložce *podrobnosti* u certifikátu, je vhodné zkontrolovat tzv. *Miniaturu* certifikátu, zda je shodná s miniaturou:

df db cb 86 c8 4f af 02 b9 d8 cc 14 17 8c 4b 54 58 b3 64 66

Pokud se tato miniatura bude lišit s vámi nainstalovanou certifikační autoritou, jedná se s největší pravděpodobností o podvrženou certifikační autoritu. Tuto podezřelou autoritu doporučujeme okamžitě odstranit.