WLANAccessPointDevice:1

1. Prehľad a Rozsah

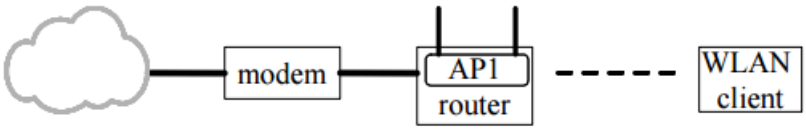
Šablóna tohto zariadenia vyhovuje UPnP Architektúre, Verzia 1.0.

Tento dokument definuje požadované koreňové zariadenie *urn:schemas-upnp-org:device:WLANAccessPointDevice*.

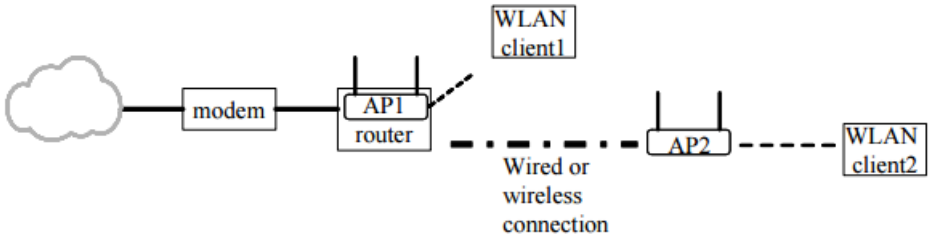
WLANAccessPointDevice zapuzdruje služby pre Access Point Device Control Protocol (DCP).

Bezdrôtový LAN (WLAN) Access Point (AP) je zariadenie ktoré implementuje IEEE 802.11 (a, b ,g) bezdrôtové štandardy, aby zabezpečil infraštruktúru siete pre domácnosť alebo malú firmu. Definícia zariadenia nezahŕňa používanie AP v „hotspot-och“ alebo v podnikových sieťach.

AP sa správa ako Ethernert-ový most (bridge), ktorý povoľuje pripojenie viacerých uzlov do LAN. Obrázok 1a ukazuje bežnú topológiu použitú pre sieť s WLAN access pointom. Obrázok 1b zobrazuje použitie AP ako spôsob na predlženie dosahu LAN. DCP pokrýva oba tieto prípady.



Obrázok 1a: WLANAccessPointDevice – bežný model použitia



Obrázok 1b: Predlženie existujúcej siete – príklad topológie

1.1. Zameranie a ciele pre DCP verziu 1.0

Výbor IGD (The Internet Gateway Device) sa zhodol zamerať na nasledujúcu množinu funkcionalít spolu so službami pre AP DCP v 1.0.

- Konfigurovanie a dopytovanie 802.11 AP parametrov.
- Samozavádzanie bezpečnosti odkazu pre WLAN-y, ktoré používajú AP, založený na 802.11. Toto zahŕňa bezpečnosť predstavenia bezdrôtového klienta a AP zariadenia. Cieľom je vytvoriť jednoduché nastavenie a konfiguráciu WLAN bezpečnosti pre 802.11 AP a spravovanie WLAN prístupovej autorizácie.

1.2. Čomu sa chceme vyhnúť v DCP verzii 1.0

Nasledujúce odrážky boli diskutované a považujú sa byť mimo rozsah tejto verzie DCP.

- Nahradenie alebo zvýšenie mechanizmu bezpečnosti odkazu poskytovanú AP
- Konfigurácia služieb pre AP v „hotspot-och“ alebo v podnikových sieťach

1.3. WLAN Bezpečnostné Požiadavky a Odporúčania

Bezpečnosť odkazu je kritická pre bezdrôtové domáce siete, pretože pripojenosť nie je obmedzená dosahom káblov alebo dostupnosťou fyzických portov. Pravdepodobnosť neúmyselných cross--linkových a zákerných drive-by útokov bude stúpať s popularitou sieti WLAN. Toto bude narúšať pohodlie užívateľa s používaním bezdrôtovej siete a bude prekážať predstaveniu nových produktových kategórií a modelov využitia. Používatelia a poskytovatelia požadujú bezpečnosť odkazu ako súčasť balíka sieti WLAN.

Alternatíva k bezpečnosti odkazu je chránenie špecifických zdrojov pomocou bezpečnostných mechanizmov zahrňujúcich vyššie (sieťová alebo aplikačná) vrstvy sieťového modelu. Avšak, nemôžeme očakávať od bežného domáceho užívateľa, že je technický zručný a schopný identifikovať všetky zraniteľné body (dáta/zariadenia) v domácej sieti a ochrániť ich individuálne s primeranými metódami.

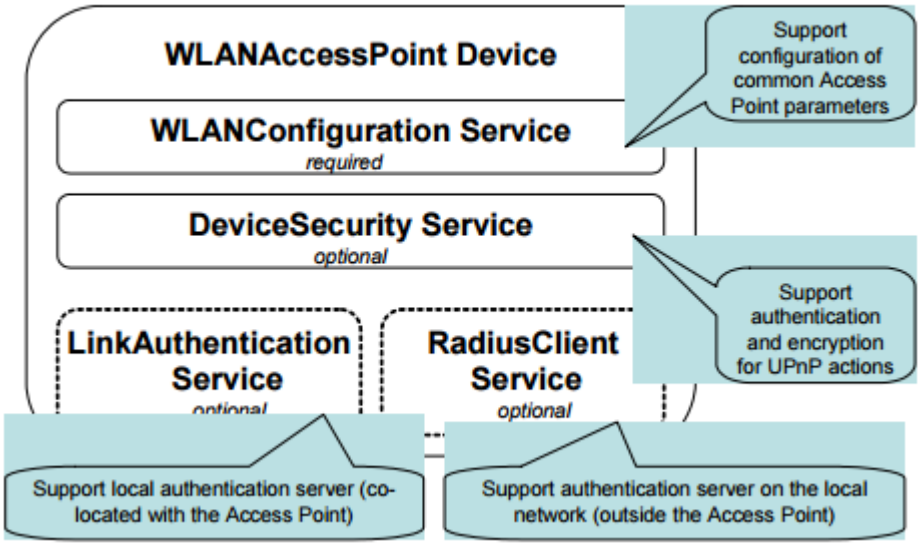
Momentálne najbežnejší spôsob, ako zabezpečiť 802.11 odkazy doma zahŕňa Wired-Equivalent Privacy (WEP), založené na šifrovaní a autentizácií. Bezpečnostné riziká spojené s WEP sú všeobecne známe. Útočník môže rozlúštiť WEP kľúč zachycovaním balíkov pomocou bezdrôtového „očuchávania balíkov“ a pomocou široko dostupných možností určiť WEP kľúč. Ak vlastník WLAN nadobudne podozrenie kompromitovania bezpečnosti, WEP kľúč na všetkých užívateľských zariadeniach a AP musí byť updatovaný, keďže rovnaký kľúč je používaný pre všetky uzly.

V rámci budovania zákazníckej dôvery a rozšírenia použitia bezdrôtových aplikácií, je dôležité, aby si domáce WLAN zariadenia osvojili bezpečnejšie mechanizmy, napríklad Wireless Protected Access (WPA), ktorý je momentálne navrhovaný do činnosti 802.11. Z dlhodobého hľadiska sa očakáva, že bezpečnostné špecifikácie spracované do kategórie 802.11i budú široko prijaté a primerané riešenie pre silné bezpečnostné mechanizmy v AP. Vylepšená bezpečnosť poskytuje autentizáciu každého užívateľa, kľúče pre každý reláciu (session), pravidelné menenie kľúčov a bezpečnejšie šifrovacie metódy, ako Advanced Encryption Standard (AES).

Jeden z hlavných problémov s používaním bezpečnosti v sieťach WLAN je proces nastavovania bezpečnostných parametrov. Súčasné mechanizmy používané pre inicializovanie bezpečnosti odkazu v AP zariadení nie sú veľmi user-friendly. Napríklad, s modelom WEP, užívateľ musí získať dlhý WEP kľúč pre AP, tak že ho najprv získa cez bezpežné/drôtové pripojenie a potom ho korektne vloží novému klientovi. Tento problém svojpomocného riešenia taktiež existuje aj s mechanizmami navrhnutými ako vylepšenie základnej bezpečnosti založenej na WEP. Vďaka tomu užívateľ zvyčajne nenastaví bezpečnosť v sieti, čo vedie k zraniteľnosti siete. Cieľom bezpečnostnej inicializácie je mechanizmus používajúci UPnP™ technológiu, navrhnutý v tomto dokumente, ktorý minimalizuje zapojenie užívateľa a predstavuje intuitívny model použitia pre užívateľov, tak aby získali úroveň bezpečnosti, ktorú AP dokáže poskytnúť.

Celkové bezpečnostné riešenie by malo chrániť užívateľa pred „man-in-the-middle“ útokmi, tým že predchádza spojeniu užívateľovho klienta s nepriateľským AP a užívateľov AP v spojení s cudzím klientom. Malo by predchádzať „session-hijack“ útokom overovaním, či všetky správy medzi AP a klientom sú autentizované. Nemalo by byť náchylné k „dictionary“ útokom, napríklad útočník rozlúšti heslo po „sniffing“ (čuchacej) výmene výzvy a odpovede z protokolu založeného na hesle.

Cieľom DCP je umožniť bezpečné WLAN riešenie s AP zariadením, ktoré implementuje požadované elementy špecifikované v DCP. Nasledujúci obrázok zobrazuje základné funkčné komponenty *WLANAccessPointDevice* zariadenia.



Obrázok 2: Funkčné komponenty *WLANAccessPointDevice* zariadenia

1.3.1 AP Konfigurácia Parametrov

WLANConfiguration služba, ktorá je povinná pre zariadenie *WLANAccessPointDevice*, poskytuje stavové premenné pre niektoré AP parametre, ktoré tím vývojárov považoval za užitočné pre konfiguráciu cez UPnP™ klienta. Poskytujú možnosť jednoduchej konfiguráciu bezpečnosti a operačných parametrov, ponúka diagnostické informácie a pomáha nastaviť funkciu prevádzača. Naviac technológia UPnP™ poskytuje aj možnosť notifikácií o udalostiach na informovanie klientov, ktorý majú záujem o stav AP. S AP, ktorý neposkytuje UPnP™ technológiu, užívatelia môžu mať prístup k niektorým parametrom cez webový prehliadač bez bezpečných mechanizmov autentizácie a kontrol prístupu. Taktiež proces konfigurácie medzi AP a klientom nie sú chránené diskrétnosťou a sú zraniteľné voči útokom.

Velmi sa odporúča AP, aby mal DCP mechanizmy na autentizáciu prístupu pre procesy UPnP™, a taktiež poskytoval diskrétnosť dát. Taktiež sa odporúča mať mechanizmus, ktorý vynechá neautentizované a neoverené prístupy k parametrom, ktoré môžu byť prístupné len bezpečným e UPnP™ procesom. Bez takejto kontroly prístupu každé klientske zariadenie v sieti LAN môže zmeniť nastavenia AP, čím ovplyvni celú sieť. Situácia je špeciálne závažná v prostredí malých podnikov. Obmedzenie povolenia zápisu v AP parametroch zníži bremeno podpory na dodávateľa vybavenia siete a poskytovateľa služieb.
Odporúča sa použiť opatrenia definované v *DeviceSecurity* službách na implementovanie kontroly

prístupu. Tím vývojárov identifikoval špecifické akcie v službách *WLANConfiguration*, *LinkAuthentication* and *RadiusClient*, ktoré sa odporučené ako bezpečné.

1.3.2 Podpora doporúčení pre každého klienta

AP môže mať prostriedky aby podporoval autentizáciu jednotlivých WLAN klientov s unikátnymi doporučeniami. Môže to podporovať bez autentizačného serveru pomocou viacerých PSK WPA kľúčov. Alebo, AP môže toto podporovať cez ukazateľ na autentizačný server ako je RADIUS server, ktorý je dostupný AP zariadeniu cez premenné, ktoré sú poskytované v *RadiusClient* službe. Alternatívne, AP môže podporovať jednotnú funkcionalitu autentizačného serveru a poskytovať to ako službu UPnP™, špecifikovanú LinkAuthentication službou. Toto je nepovinná služba, ktorá sa môže použiť s AP DCP na podporu autentizácie každého klienta s jednotným autentizačným serverom.

2. Definície Zariadenia

2.1 Typ Zariadenia

Nasledujúci typ zariadenia identifikuje zariadenie, ktoré je vyhovuje tejto šablóne:

urn:schemas-upnp-org:device:WLANAccessPointDevice:1

2.2 Model Zariadenia

Odporúča sa, aby *WLANAccessPointDevice* bolo implementované s podporou pre zabezpečenie UPnP™ opatrení. Taktiež sa odporúča, aby zabezpečenie UPnP™ opatrení bolo vytvorené pomocou služby *DeviceSecurity*, ako bolo určené UPnP™ bezpečnostným pracovným výborom. Ak implementované, služba *DeviceSecurity* musí obsahovať buď implementáciu v danom zariadení *WLANAccessPointDevice* alebo v zariadení, ktoré zahrňuje *WLANAccessPointDevice*. Tieto dva modely sú popísane nižšie.

2.2.1. Popis Požiadaviek na Zariadenie

Nasledujúca tabuľka stručne popisuje účel služieb použitých v *WLANAccessPointDevice*.

Názov Zariadenia	Popis služby
WLANConfiguration	Konfiguračné parametre spojené s WLAN odkazom, ktoré potrebujú byť spojené naprogramovaním.
DeviceSecurity	Opatrenia prebratia vlastníctva, konfigurácia kontroly prístupu, nastavanie bezpečnostných relácií a vyvolanie bezpečnostných opatrení.

2.2.1.1. *DeviceSecurity* v rámci *WLANAccessPointDevice*

Tento model je typický aplikovateľný na fyzické zariadenia, ktoré potrebujú *DeviceSecurity* funkčnosť (zahrňujúc vlastníctvo zariadenia a kontrolu prístupu), aby mohlo byť použité len zariadením

WLANAccessPointDevice. V tomto prípade produkty, ktoré vystavujú zariadenia typu *urn:schemas-upnp-org:device: WLANAccessPointDevice:1* musia implementovať minimálny počet verzií služieb, ktoré sú špecifikované tabuľkou nižšie.

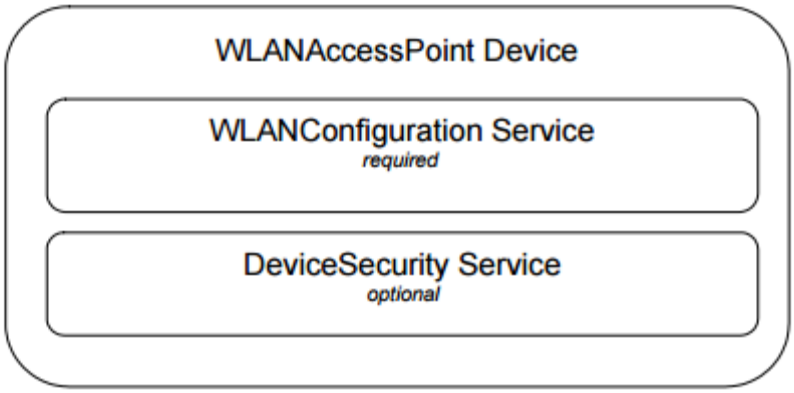
Tabuľka 1: Systémové požiadavky na samostatné zariadenie *WLANAccessPointDevice*

DeviceType	Root	Req. or Opt.[1]	ServiceType	Req. or Opt.[1]	Service ID[2]
			WLANConfiguration:1	*R*	*WLANConfiguration1*
			DeviceSecurity:1	*O*	*DeviceSecurity1*
			Non-standard services embedded by an UPnP™ device vendor go here.	*X*	*TBD*

[1] R = požadované, O = voliteľné, X = neštandardné
[2] S predponou *urn:upnp-org:serviceId:* .

Vzťahy medzi Službami

Obrázok 3 zobrazuje logickú štruktúru zariadenia a služieb definovanými tímom vývojárov pre UPnP™ technológiu umožnenú AP zariadeniam.



Obrázok 3: *DeviceSecurity* v rámci zariadenia *WLANAccessPointDevice*

Navyše služba *LinkAuthentication* (voliteľne) môže byť použitá ak AP podporuje autentizáciu každého klienta s jednotným autentizačným serverom. *LinkAuthentication, RadiusClient* a *WLANConfiguration* služby môžu byť závislé na službe *DeviceSecurity*, keďže poskytuje kontrolu prístupu opatrení definovaných v službách.

2.2.1.2 *DeviceSecurity* mimo *WLANAccessPointDevice*

Tento model je typicky aplikovateľný na fyzické zariadenia, ktoré implementujú funkcionalitu AP, ale zariadenie *WLANAccessPointDevice* smie použiť *DeviceSecurity*, ktoré je už súčasťou iného zariadenia. Príkladom tohto by mohlo byť zariadenie, kde *urn:schemas-upnp-org:device: WLANAccessPointDevice:1* je implementované v rámci zariadenia typu *urn:schemas-upnp-org:device: BasicDevice:1*. Zariadenie *BasicDevice* v tomto prípade obsahuje službu *DeviceSecurity*, ktorá môže byť použitá iným UPnP™ zariadením, napríklad IGD. Implementácia *WLANAccessPointDevice* musí obsahovať minimálny počet verzií služieb, ktoré sú špecifikované tabuľkou nižšie.

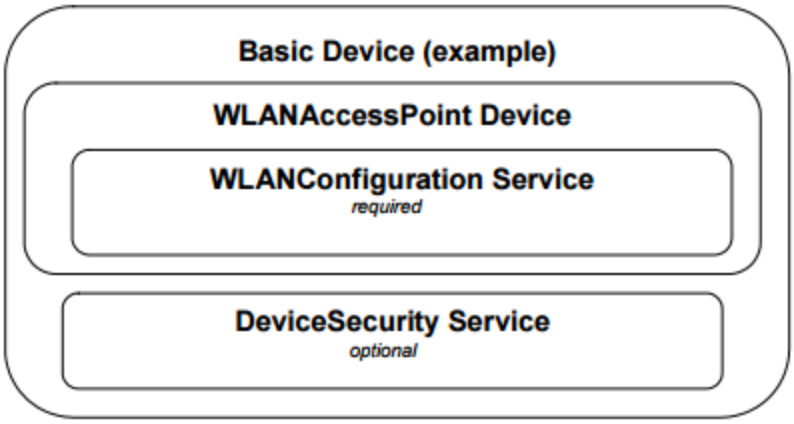
Tabuľka 2: Systémové požiadavky pre zabudované zariadnie *WLANAccessPointDevice*

DeviceType	Root	Req. or Opt.[1]	ServiceType	Req. or Opt.[1]	Service ID[2]
			WLANConfiguration:1	*R*	*WLANConfiguration1*
			Non-standard services embedded by an UPnP™ device vendor go here.	*X*	*TBD*

[1] R = požadované, O = voliteľné, X = neštandardné.
[2] S predponou *urn:upnp-org:serviceId:* .

Vzťahy medzi Službami

Obrázok 4 zobrazuje logickú štruktúru zariadenia a služieb definovanými tímom vývojárov pre UPnP™ technológiu umožnenú AP zariadeniam, ktoré môžu používať *DeviceSecurity* službu pre ostatné UPnP™ zariadenia v rámci toho istého fyzického zariadenia. Navyše voliteľná služba *LinkAuthentication* môže byť použitá ak AP podporuje autentizáciu každého klienta s jednotným autentizačným serverom. *LinkAuthentication, RadiusClient* a *WLANConfiguration* služby môžu byť závislé na službe *DeviceSecurity*, keďže poskytuje kontrolu prístupu opatrení definovaných v službách.



Obrázok 4: Príklad *DeviceSecurity* zariadenia mimo zariadenia *WLANAccessPointDevice*