

De secure Wi-Fi vero quae sunt...

Biztonságos Wi-Fi pediglen létezik...

(Könyves Kálmán után szabadon)

Tartalomjegyzék

Tartalomjegyzék	2
Igazi vékony AP (thin AP) architektúra	3
Teljes titkosítás, biztonságos hálózat	3
Felhasználó-centrikus hálózat: a felhasználó mozog, a hálózat követi	3
Konfiguráció nélküli kihelyezés és OS/firmware menedzsment	4
Valós idejű monitorozás és kliens-szabályozás	4
A legmagasabb fokú biztonsági szolgáltatások	5
Biztonság kienstől a kontrollerig	5
Wireless titkosítás	5
Integrált tűzfal wireless-wired és wireless-wireless irányban	5
Integrált wireless IPS/IDS	6
Rogue AP felismerés és kizárás	6
Rádiófrekvenciás IPS (RFprotect)	6
Integrált vagy külső Network Access Control	6
Integrált végponti biztonság (client integrity)	6
VPN koncentrátor	7
Egymásba ágyazott autentikációs eljárások	7
Helymeghatározás, location tracking	7
Egyszerű és integrált menedzselhetőség	7
Automatikus rádiófrekvencia-menedzsment (ARM)	7
Szolgáltatásközpontúság	8
Nagysűrűségű telepítés	8
Kültéri és beltéri MESH hálózat	8
Autentikáció	9
Ultra Fast Roaming < 10 ms	9
Vendég hálózatok, Guest Access, Captive Portal	9
RF traffic shaping	10
Sávszélesség-menedzsment, QoS	10
Remote AP	10
(nem csak) Kisirodai funkciók - tűzfal és VPN koncentrátor	11
Teljes redundancia (master-master/aktív-passzív)	11
Részleges redundancia (master-local)	11
Helymeghatározás, location tracking	11
VoIP támogatás és application/voice-aware-ing	11
Wi-Fi video megfigyelés (Video Surveillance)	12
RF tervezés	12
Performancia - a kábeles hálózat kiváltása	12
Teljesítmény	12
PoE 802.11n-re is	13

Igazi vékony AP (thin AP) architektúra

Míg a hagyományos wireless architektúrákban a felhasználók kapcsolatait az Access Pointok fogadják és terminálják, addig az Aruba **valóban vékony AP eszközöket használ**, amelyek 802.11/Ethernet média konverterként működnek, és a wireless csomagokat Ethernetté alakítva továbbítják a központi controllernek. Az **adatkapcsolat így megszakítás nélkül közvetlenül épül ki a controller és a Wi-Fi kliensek között**, és ez a technológia nem csak a hálózat kialakítását és menedzsmentjét teszi egyszerűbbé, de olyan szolgáltatásokat tesz lehetővé, amelyek más eszközökkel nem - vagy csak plusz megoldások bevonásával - valósíthatók meg.

Teljes titkosítás, biztonságos hálózat

A vékony AP média konverterek GRE/IPSEC tunnelben, megszakításmentesen továbbítják az adatokat a controllernek, így **nincs egyetlen pontja sem a hálózatnak, ahol az adatok titkosítatlanul haladnának keresztül**. Az adatok tehát még a kábeles szakaszon (AP és controller között) is titkosításra kerülnek, ezért az adatforgalom lehallgatása ezen a szakaszon sem lehetséges.

Az Aruba AP eszközök a bootolási folyamatuk során töltik le a kontrollerről operációs rendszerüket és konfigurációjukat, ezért eltulajdonításuk vagy kompromittálódásuk esetén sem férhet hozzá támadó konfigurációs adatokhoz, titkosítókulcsokhoz vagy az operációs rendszerhez.

A Wi-Fi kapcsolat titkosításához használt kulcsok a kapcsolatot termináló controllerben kerülnek eltárolásra, tehát **egy WPA-TKIP titkosítás esetén a felhasználó adatcsomagjait a controller bontja ki, illetve titkosítja be**. Egy AP egységet érő támadás esetén a támadó legfeljebb magát az eszközt szerezheti meg, de titkosító kulcsokhoz vagy más olyan adathoz, amellyel beleavatkozhat a kommunikációba, nem férhet hozzá.

Felhasználó-centrikus hálózat: a felhasználó mozog, a hálózat követi

Az Aruba vékony AP architektúra lehetővé teszi, hogy a felhasználó bármerre mozogjon egy épületben vagy az épületek között, bárhol csatlakozhat a hálózathoz, minden esetben pontosan ugyanazokat a szolgáltatásokat éri el, mint a saját asztalánál. Ha egy vidéki irodában csatlakozik a vállalat Wi-Fi hálózatához, ugyanazokkal a hálózati erőforrásokkal tud dolgozni, mintha csak a központi irodában dolgozna.

A hagyományos Wi-Fi hálózatoknál az AP eszközök hálózati portjához minden olyan VLAN-t ki kell adni, amelyet a felhasználók el szeretnének érni, hiszen a felhasználók kapcsolatát a hagyományos, „kövér” AP eszközök terminálják és adják tovább egy esetleges controllernek.

Az Aruba esetében a wireless controller a vállalat központi switch-éhez van csatlakoztatva, egy olyan portra, amelyen megjelenik az összes Wi-Fi-re valaha

kiadandó VLAN. A vékony AP eszközök fali portjára csak egyetlen olyan hálózati szegmenst kell kiadni, amelyen keresztül az Access Point csatlakozni tud a kontrollerhez. A felhasználóhoz kiadandó VLAN a GRE/IPSEC csatornában halad, és csak az a felhasználó látja, akinek szántuk.

A felhasználó csatlakozásakor a hálózati erőforrások elérhetőségét nem az szabja meg, hogy a fali portokon milyen VLAN-ok vannak konfigurálva, hanem hogy a felhasználónak van-e joga elérni a hálózati erőforrásokat. Ha van joga, akkor eléri az adott VLAN-okat a saját irodájából, de eléri akkor is, ha átmegy egy másik épületbe, vagy akár egy vidéki irodából is.

Konfiguráció nélküli kihelyezés és OS/firmware menedzsment

A vékony AP architektúra lehetővé teszi, hogy akár maga a felhasználó csatlakoztasson AP-t a hálózathoz. Az AP képes megkeresni a kontrollerét (DHCP-vel vagy saját discovery protocol-lal), letölteni az operációs rendszerét, így az üzemeltetőnek már csak azt kell megadnia, hogy az eszköz melyik AP csoportba tartozik. A **provisioning** folyamata nem vesz többet igénybe, mint **10-15 másodperc**, és az eszköz külön konfigurálás nélkül beillesztődött a vállalati Wi-Fi hálózatba.

Nincs szükség eszközönkénti frissítésre vagy szoftver-cserére, mert az operációs rendszer a kontrolleren tárolódik. Ha a kontrolleren frissítés történik, az AP eszközök a következő bootolási folyamatban már az operációs rendszer új verzióját töltik le.

Az AP-k PKI-technológiával azonosítják magukat a kontrollerük számára, ám ez a felhasználó és az üzemeltető előtt rejtett marad, automatikusan történik.

Valós idejű monitorozás és kliens-szabályozás

A kontroller integrált menedzsmentfelületén valós időben nyomon követhető mind a rádiófrekvenciás környezet, mind a Wi-Fi kliensek pontos állapota. A felhasználók kapcsolata a kontrollerben végződik, ezért a kontroller valós időben, késleltetés nélkül, pontosan tudja, hogy a kliens milyen átviteli sebességet ér el adott pillanatban, milyen zavaró tényezők csökkentik az átvitelt, és pontos adatokkal (heat map, data rate, bandwidth, autentikáció, felhasználói adatok, stb.) rendelkezik a kapcsolat jellemzőiről.

Az állapotjellemzők ismerete teszi lehetővé, hogy a kontroller szabályozni tudja a csatlakozott kliensek rádiófrekvenciás jellemzőit (adáserősség, roaming, csatornaváltás, stb.). Az Aruba az egyetlen vállalati wireless megoldás, amely akár csatornaváltással együtt képes biztosítani, hogy a kliens akár 10 ms-on belül, újra-authentikálás és kapcsolatbontás nélkül egy másik AP eszközhöz csatlakozzon (Ultra Fast Roaming). A rendszer képes a kliensek adáserősségét szabályozni, csökkentve a kliensek által okozott rádiófrekvenciás zajokat, vagy megakadályozni, hogy egy-egy erősebb chipsettel rendelkező kártya elnyomja a gyengébb klienseket.

A legmagasabb fokú biztonsági szolgáltatások

Biztonság kienstől a kontrollerig

A vékony AP média konverterek GRE/IPSEC tunnelben továbbítják az adatokat a kontrollernek, tehát nincs egyetlen pontja sem a hálózatnak, ahol az adatok titkosítatlanul haladnának keresztül. Az adatok az AP és a kontroller közötti kábeles szakaszon is megszakítás nélkül, titkosítva haladnak, ezért az adatforgalom lehallgatása ezen a szakaszon még akkor sem lehetséges, ha az esetleges támadó beékelődik az adatfolyamba (Man-in-the-middle támadás).

Wireless titkosítás

Az Aruba támogatja a szabványos azonosítási/titkosítási eljárásokat (OPEN, WEP, WPA/PSK, WPA/TIKIP, WPA2/TIKIP/AES, MAC, stb.), sőt, az integrált VPN-koncentrátor segítségével a biztonság egészen IPSEC/PPTP/L2TP szintig fokozható, míg az xSec szoftvermodul segítségével OSI Layer2 szinten hozható létre titkosítás.

Integrált tűzfal wireless-wired és wireless-wireless irányban

A Wi-Fi megjelenésével a vállalati hálózatok 3 dimenzióssá válnak, és a korábbi határvédelmi megoldások nem képesek a Wi-Fi kliensek megfelelő kezelésére; nem tudják biztosítani, hogy a felhasználók sem a hálózatot, sem pedig egymást ne támadhassák, vagy ne fertőzzék.

Az Aruba az egyetlen vállalati wireless megoldás, amely rendelkezik integrált tűzfalal (FIPS 140-2 level 2, ICSA, CC-EAL2), amely wireless-wired és wireless-wireless irányban is véd, ezért például az amerikai kormányzati és nemzetbiztonsági szerveknél, vagy katonai környezetben csak Aruba Wi-Fi megoldások használhatóak.

Az integrált tűzfal szerepkör-alapú (*role based*), nem csak szolgáltatásokban, forrásokban és célokban gondolkodik. A felhasználóhoz szerepkör rendelhető (pl.: vendég, dolgozó) és a szerepkör határozza meg a felhasználóra érvényes tűzfal policy csomagokat, valamint hogy a szerepkörbe tartozó felhasználó milyen VLAN-ok felé kommunikálhat. Ez a szerepkör a felhasználót akkor is követi, ha vándorol, és a vándorlás során például új IP-címet kap.

Lehetőség van az autentikációs szerverekben (RADIUS, LDAP, AD, TACACS) meghatározni, hogy az adott felhasználónak milyen hálózatokat van jogosultsága igénybe venni, csatlakozáskor melyik VLAN-ba kerüljön, vagy milyen autentikációval csatlakozhat a hálózathoz (*Server Derived Rules*).

Külön elérések oszthatóak ki, ha valaki Captive Portalon, WPA-val, WPA2-vel csatlakozik a hálózathoz, vagy megadható, hogy bizonyos helyekről csatlakozva csak csökkentett jogosultságokkal és elérésekkel rendelkezzen a felhasználó.

A szerepkörök és policy csomagok csatlakozáskor és az autentikációkor külön-külön rendelhetőek a felhasználóhoz, tehát a felhasználó más-más jogosultsággal rendelkezhet az autentikáció előtt és után. Bizonyos események bekövetkezésekor

(támadások, sávszélesség-pazarlás, jogosulatlan hozzáférési kísérletek, stb.) a tűzfal dinamikusan új szerepkörbe kényszerítheti a felhasználót, jogosultságokat/korlátozásokat oszthat a felhasználónak, üzemeltetői beavatkozás nélkül elhárítva a problémát.

Integrált wireless IPS/IDS

Az Aruba kontroller integrált wIPS rendszere századmásodpercek alatt felismeri, majd akár méterre pontosan lokalizálja a támadásokat, felismeri a támadások vagy a leggyakoribb letapogatások szignatúráit (AirJack, NetStumbler, Kismet, stb.). A rádiófrekvenciás környezet védelméről szenzor-üzemmódú (AirMonitor vagy RFprotect) Access Pointok gondoskodnak, amelyek folyamatosan figyelik és értelmezik a hálózat működését, környezetét és szükség esetén beavatkoznak.

Rogue AP felismerés és kizárás

A szenzor-üzemmódú Access Pointok felismerik a hálózathoz csatlakoztatott idegen és veszélyes eszközöket (Rogue AP-k) vagy ad-hoc pontokat és bridgeket, automatikusan képesek rádiófrekvenciás ellentámadással lezárni a hálózati biztonságban keletkezett réseket, és ha a saját felhasználói idegen eszközökre csatlakoztak, utasítani őket a leválásra és a biztonságos hálózathoz való visszacsatlakozásra.

Rádiófrekvenciás IPS (RFprotect)

Az önálló RFprotect alkalmazás nem csak Aruba hálózathoz illeszthető, de bármely más vállalati wireless rendszerhez csatlakoztatható. Segítségével a teljes rádiófrekvenciás környezet monitorozható, és komplex IPS megoldásként működik. Felismeri a támadásokat és a szándékos zavarásokat, átvizsgálja a hálózatot és megszünteti a sebezhetőséget. Komplex, környezetre, felhasználókra, adatforgalomra, veszélyforrásokra fókuszáló PCI, HIPAA, DoD 8100.2, GLBA riportolást tesz lehetővé.

Integrált vagy külső Network Access Control

Az Aruba saját NAC megoldásával biztosítható a csatlakozó eszközök vizsgálata és engedélyezése, viselkedés-alapú hozzáférés korlátozás, valamint a teljes kommunikáció vizsgálata és szűrése. Az Aruba bármely más NAC eszközhöz illeszthető és együttműködik a legelterjedtebb Cisco NAC-cal és a Mirage Networks eszközeivel, amelyek a legbiztonságosabb NAC megoldások.

Integrált végponti biztonság (client integrity)

A kapcsolódó kliensek vizsgálatával megelőzhető a fertőző gépek csatlakozása. Az Aruba *client integrity* megoldása a csatlakozás után megvizsgálja a klienseket, és ha biztonsági szoftverek nem felelnek meg a vállalat által definiált elvárásoknak, korlátozza a hálózati hozzáférést, vagy kizárja a gépet a hálózatból. Képes ellenőrizni a telepített tűzfal, anti-vírus, anti-spyware alkalmazásokat, megvizsgálni az utolsó ellenőrzések eredményét vagy a telepített szoftverek állapotát.

VPN koncentrátor

Az Aruba kontroller VPN koncentrátoraként is működik, és terminálni tudja a leggyakoribb VPN klienseket (*Cisco, xAuth, Juniper, IPSEC, PPTP, L2TP*). Használatával nem csak megspórolható a külön VPN eszköz használata, de a wireless hálózat biztonsága egészen a VPN szintig fokozható. Az Aruba kontroller akár egy-egy adott, vagy akár az összes hálózati szegmensben és VLAN-ban képes működni és fogadni a kapcsolatokat. Szegmensenként külön-külön konfigurálhatóak az address poolok, és szabályozhatóak a kapcsolat biztonsági paraméterei.

Egymásba ágyazott autentikációs eljárások

Lehetőség van az autentikációs és titkosítási eljárások egymásba ágyazására. Létrehozható akár olyan SSID, amely WEP, majd Captive Portal alapú, végül VPN autentikációt vár el. Az autentikációs szinteken más-más jogosultsággal rendelkezhet a felhasználó, míg végül a teljes hálózati elérést csak a VPN csatlakozással kapja meg.

Helymeghatározás, location tracking

Az integrált rádiófrekvenciás tervezőfelületen nem csak a hálózat tervezhető meg, de lehetőséget nyílik a vállalati Wi-Fi hálózat térképalapú nyomonkövetésére. A külső, platformfüggetlen **AirWave** menedzsment segítségével a térképeken felügyelhetőek a rádiós környezet állapotai, sáv szélességek, terjedés, zavaró jelenségek, illetve akár percre pontosan nyomon követhetőek a kliens-mozgások.

Egyszerű és integrált menedzselhetőség

Az Aruba Wi-Fi hálózat villámgyorsan és egyszerűen integrálható bármely vezetékes hálózatba, álljon az egy gyártótól származó routerekből és switchekből vagy legyen akár inhomogén.

Az Aruba hálózatokhoz nincs szükség külön menedzsment-alkalmazás vásárlására. A wireless kontroller tartalmazza a menedzsment-felületet, amelyen keresztül minden konfiguráció elvégezhető.

A menedzsment-felületen keresztül lehetőség van a rádiófrekvenciás tervezésre (*RF Planning*), a hálózat kialakítására és folyamatos nyomon követésére, AP eszközök konfigurálására, AP csoportok létrehozására, új SSID-k kialakítására vagy akár a felhasználók monitorozására. A kontroller természetesen menedzselhető parancssoros felületen (*CLI*) keresztül is. A *CLI* használatát megkönnyíti, hogy a webes felület megmutatja az aktuális változtatás parancssori verzióját.

Automatikus rádiófrekvencia-menedzsment (ARM)

A Wi-Fi hálózatok soha nem statikusak, elég csak egy ajtót kinyitni, vagy elég, ha a közelben valaki ugyanazonokon a csatornákon üzemel be egy idegen rádiós eszközt, amelyek a vállalaton belül is használatban vannak, és azonnal megváltozik a hullámterjedés vagy interferencia keletkezhet.

Az *Adaptive Radio Management* transzparensen, automatikusan és gyorsan (tipikusan századmásodpercek alatt) biztosítja az interferenciamentes csatornahasználatot és a kliensek rádiófrekvenciás forgalmának szabályozhatóságát. Nemcsak megkeresi a szabad csatornákat az Access Pointok számára, de az adáserősségük automatikus szabályozásával még nagysűrűségű rádiós környezetben is interferenciamentes kapcsolatot biztosít. Szükség esetén csatornaváltásra kényszeríti az eszközöket, egészen addig, amíg a rádiós környezet nem biztosítja a megfelelő minőségű átvitelt és terjedést.

A kliensek rádiófrekvenciás forgalmát úgy képes irányítani, hogy kiküszöböli a kevert hálózatokban fellépő problémákat (802.11b kliens 802.11g hálózatban, erős chipsetek rádió-sávszélesség használata, kliensek közötti interferencia, kétrádiós csatlakozási problémák, stb.).

Szolgáltatásközpontúság

Nagysűrűségű telepítés

Olyan helységeken és területeken, ahol a felhasználók száma miatt szükség van sok AP használatára (tárgyalók, konferenciatermek, egyetemi előadók és aulák) az Aruba dinamikus rádiófrekvencia- és sávszélesség-menedzsment szolgáltatása biztosítani tudja a folyamatos és jó minőségű kapcsolatot.

Az SAP AG központi éttermében több száz Aruba AP eszköz interferencia- és kapacitásprobléma nélkül szolgálja ki a -csúcsidőben- 1500 felhasználó akár 3000 Wi-Fi eszközét.

A világ egy helyen lévő legnagyobb méretű Wi-Fi hálózatában, az Ohio State University campusában 10.000 Aruba AP eszköz fogadja egyidőben csaknem 50.000 felhasználó csatlakozását.

Kültéri és beltéri MESH hálózat

A MESH topológia nagyon megnöveli a vállalati wireless hálózat flexibilitását. A MESH alapját olyan AP eszközök képezik, amelyek hagyományosan, Ethernet kapcsolattal csatlakoznak a kábeles hálózathoz (*MESH Portal*), és amelyekre rádiós linken (*MESH Link*) keresztül más, Ethernet nélküli AP eszközök (*MESH Point*) csatlakozhatnak.

A kiépítés alkalmazható műemléki vagy ipari környezetben és minden olyan helyen, ahol nincs lehetőség a fizikai kábelezésre, vagy zsúfolt előadóknak, konferenciákon ahol gyorsan kell a Wi-Fi hálózat kapacitását megnövelni.

Az Aruba MESH hálózat **bármely Aruba AP-vel kialakítható**, nem szükséges külön drága MESH-képes AP-ket vásárolni.

Autentikáció

Az Aruba kontroller támogatja a legtöbb autentikációs szervert, képes *Active Directory*, *LDAP*, *RADIUS*, *TACACS* és más szervereken keresztül autentikáltatni a felhasználókat.

Rendelkezik saját, belső autentikációs szerverrel, a vendég felhasználókat egy recepciós is könnyedén felveheti egy csökkentett jogú felületen (*Guest Provisioning*) keresztül, akár percre pontosan megadva a lejárati idejét, vagy a felhasználó jogosultságait.

Az Aruba képes az autentikációs szerverek paramétereivel együttműködni (pl. *RADIUS* paraméterek), így a felhasználók jogosultságai beállíthatóak magában az autentikációs szerverben.

Például, ha a felhasználó tagja a Wi-Fi Active Directory csoportnak, bejelentkezhet a vállalati Wi-Fi hálózatba, vagy RADIUS esetén számos paraméterrel befolyásolható az autentikáció során hozzárendelt jogosultság.

Ultra Fast Roaming < 10 ms

Az Aruba az egyetlen vállalati wireless megoldás, amely képes csatornaváltással és újraautentikációval együtt 10 ms-on belül átirányítani a klienst egy másik AP egységre. Az Ultra Fast Roaming biztosítja, hogy a felhasználók szabadon mozoghassanak az épületben, anélkül hogy a kapcsolatuk megszakadna, vagy a szolgáltatás minősége romlana.

A 10 ms-on belüli roaming teszi lehetővé, hogy a Wi-Fi VoIP telefonok, vagy akár a SIP-képes mobilkészülékek, streaming média eszközök a GSM-rendszerhez hasonlóan vonalszakadás vagy hangminőség-romlás nélkül képesek egyik AP egységről a másikra csatlakozni.

Vendég hálózatok, Guest Access, Captive Portal

Az Aruba kontrolleren keresztül egyszerűen és **plusz rendszerek bevonása nélkül**, nagy biztonsággal alakíthatóak ki a vendég hálózatok. A vendég felhasználókat a beépített *Guest Provisioning* felületen egy recepciós is könnyedén létrehozhatja, pontosan beállítva a hozzáférések lejárati idejét. A felületen keresztül a vállalat arculatának megfelelő kártyákat lehet kinyomtatni, amelyek tartalmazzák a felhasználói azonosítót, jelszót és a hozzáférés érvényességi idejét.

A vendég felhasználók *Captive Portal* felületen autentikálhatnak a Wi-Fi hálózatba, és adatforgalmukat a beépített tűzfal (akár több vendég VLAN-ba is besorolhatóak) teljesen elválasztja a vállalati forgalomtól. **Több Captive Portal felület is kialakítható, melyek több külön SSID-hez is hozzárendelhetők, mindez a vállalat saját designjában.**

RF traffic shaping

A kevert Wi-Fi hálózatokban (a,b,g,n kliensek, dual-rádiós környezet) számos rádiófrekvenciás probléma merülhet fel, amelyekre a vállalati Wi-Fi hálózatnak reagálnia kell.

Ha több Wi-Fi szabvány van jelen a hálózatban, a leggyengébb kliensek lecsökkentik a hálózat átviteli teljesítményét. Egy .b kliens megjelenése az 54Mbit-es .g hálózat átviteli teljesítményét 11Mbit-re csökkentheti.

A különböző Wi-Fi kártyák chipsetjei különböző teljesítményre képesek. Egy erős teljesítményű kártya (Pl. XSpan alapú Atheros, Intel) a teljes rádiófrekvenciás sáv szélességet le tudja foglalni, így a gyengébb teljesítményű kártyák nem tudnak szóhoz jutni.

Dual-rádiós (2.4 és 5Ghz együtt) környezetben performancia-problémát okoz, ha az 5Ghz képes eszköz 2.4Ghz-en akar csatlakozni.

Az Aruba automatikus rádió-menedzsment szolgáltatásai biztosítják a folyamatos, nagysebességű kapcsolatot, szabályozzák a kliensek adáserősségét és kikényszerítik a megfelelő rádiós csatlakozást.

Sávszélesség-menedzsment, QoS

Az Aruba integrált tűzfalának QoS szolgáltatása megvalósítja az SSID-k közötti sávszélesség szabályozást (pl. vendég SSID 20%, dolgozói SSID 80%), vagy akár létrehozhatóak az egyes SSID-ken belül, szerepkörökhöz rendelt QoS szabályok (vendég szerepkör: feltöltés 128K, letöltés 512). Megadható, hogy a korlátozás felhasználónként legyen érvényes (egy felhasználó maximális letöltési sebessége 128K, feltöltési sebessége 64K), vagy a tűzfal szabályrendszerében is létrehozhatóak az egyes szolgáltatások prioritásai (high/low, TOS paraméterek).

Remote AP

A Remote AP funkció segítségével a vállalati wireless hálózat teljesen mobillá válik. A felhasználók hazavihetik az AP eszközöket, amelyeket csatlakoztathatnak az otthoni ADSL/broadband routereikhez. A Remote AP-k IPSEC VPN kapcsolatot építenek ki az Interneten keresztül a kontrollerrel, és a felhasználó otthonából, távoli konferenciák helyszínéről vagy akár külföldön egy hotelszobából - mintha a dolgozó a saját íróasztala mögött ülne - biztonságosan elérheti a vállalati Wi-Fi hálózatot, pontosan ugyanolyan módon, mintha a benti íróasztalánál ülne.

Az IPSEC VPN kapcsolat biztosítja, hogy a kommunikáció nem lehallgatható, míg „a felhasználó mozog, a hálózat követi” elv lehetővé teszi, hogy a felhasználó saját, megszokott jogosultságait használva ugyanazokat az erőforrásokat érje el távolról, mint az irodán belül.

Bizonyos AP eszközök képesek USB HSDPA modemekkel együttműködni, és 3G-n keresztül csatlakozni a központi kontrollerhez. Ebben az esetben nincs szükség vezeték internet-kapcsolatra sem.

A Remote AP funkció ideális, ha távoli kirodákat kell a központi irodával összekapcsolni. Nincs szükség külön VPN koncentrátorok és kliensek vagy tűzfalak konfigurálására, a Remote AP eszköz csatlakozik a kontrolleréhez, és a távoli irodában megjelenik a vállalati Wi-Fi hálózat.

Az intelligens vékony Access Pointok képesek eldönteni az érkező adatforgalomról, hogy valóban szükséges-e a forgalmat a kontroller felé irányítani, vagy egy másik átjárót használva érje el a célállomást. Ez a funkció lehetővé teszi, hogy az Internet felé irányuló adatforgalom ne haladjon keresztül a kontrolleren, jelentősen meggyorsítva a kommunikációt.

Ha a felhasználó egy belső szervert akar elérni, a Remote AP a forgalmat a kontroller felé irányítja, míg egy weboldal megtekintését a direkt Internet kijárat felé küldi, így nem a kontrolleren keresztül tölti le az oldal tartalmát.

(nem csak) Kirodai funkciók - tűzfal és VPN koncentrátor

Kisebb irodákban kiváltható az ADSL/broadband router, mert az Aruba kontroller képes ADSL kapcsolatokat létrehozni. Akár több ADSL kapcsolatot is tud kezelni, egyszerűen létrehozható egy másodlagos vonal, amely back up vonalként is működhet

Nincs szükség külön tűzfalra, mert a kontroller integrált tűzfala nem csak wireless, de wired irányban is véd.

Nincs szükség VPN koncentrátor vagy alkalmazás bevezetésére, mert a kontroller integrált VPN koncentrátora fogadhatja a kliensek VPN kapcsolatait vagy akár Site to Site kapcsolatok is kiépíthetőek.

Teljes redundancia (master-master/aktív-passzív)

A master-master architektúrában 2 azonos kapacitású kontroller kerül telepítésre, amelyek egymás aktív-passzív párjai. Az aktív eszköz leállásakor automatikusan a passzív kontroller veszi át az AP eszközök és kliensek fogadását.

Részleges redundancia (master-local)

Részleges redundancia esetén a központi kontroller nagyobb kapacitású, mint a távoli irodák helyi (local) kontrollerei. Ha a helyi kontroller leáll, a távoli iroda AP eszközei és kliensei automatikusan átcsatlakoznak a központi kontrollerre.

Helymeghatározás, location tracking

A helymeghatározás nem csak a rádiófrekvenciás problémák vagy támadások helyének beazonosítására használható, de alkalmas arra, hogy az üzemeltető nyomon kövesse a felhasználók mozgását, vagy használható RFID tag-ekkel ellátott eszközök, berendezések vagy személyek helyének meghatározására is.

VoIP támogatás és application/voice-aware-ing

Az Aruba felismeri a hálózaton keresztülhaladó VoIP csomagokat, teljes protokoll és minőség-támogatást nyújtva a VoIP szolgáltatásoknak. Felismeri az egyes VoIP

protokollokat (SIP, H323, SCCP, SVP, SRC, Vocera, NOE), codeceket, ellenőrzi a hívások minőségét (Call Admission Control), képes sáv szélességet allokálni, vagy hívásokat hangminőség-romlás nélkül, 10 ms-on belül átterhelni szabad kapacitással rendelkező Access Pointokra. Teljes VoIP statisztika készíthető a menedzsment-felületen, pontosan láthatóvá válik a vállalat VoIP forgalma, minőségi statisztikái és paraméterei.

Wi-Fi video megfigyelés (Video Surveillance)

Az Aruba teljes támogatást nyújt a streaming média és videojelek továbbítására (akár nem WMM képes eszközöknek is), amelyek a biztonságos Wi-Fi csatornán keresztül jutnak el a tároló és feldolgozó rendszerekig. Az application-aware és QoS funkcióknak köszönhetően a kapcsolat folyamatos és mindig jó minőségű. A kamerák képesek akár MESH hálózaton keresztül csatlakozni a központhoz, így nem szükséges végpontokat kiépíteni a megfigyelőrendszerhez.

RF tervezés

A rádiófrekvenciás tervezés segítségével átfedés- és hézagmentes hálózat építhető ki, kiküszöbölhetőek az interferencia- vagy terjedési és átviteli problémák. **Az Aruba az egyetlen vállalati wireless megoldás, amely integrált tervező felületet tartalmaz,** és az elkészült tervrajz alapján biztosítani tudja az eszközök automatikus kihelyezését. Kültéri tervezéshez az Aruba speciális, Google Earth-integrált, 3D-s tervezőszoftvert biztosít, amelyből az adatokat át lehet tölteni a kontrollerbe.

Performancia - a kábeles hálózat kiváltása

Teljesítmény

Míg a korábbi szabványok esetében az elérhető sebesség maximuma 54Mbit volt, addig a 802.11 n szabvány megjelenésével a Wi-Fi elméleti kapacitási maximuma 300Mbit lett, amely a valós adatkapcsolatot és a tipikus gyártókat tekintve közel sem éri el a 100Mbit-et.

Az Aruba 802.11 n szabványú, 3x3 MIMO-val rendelkező, második generációs chipsetet tartalmazó Access Pointjai jelenleg (laborkörülmények között) akár 187 Mbit-es sebességre is képesek (valós adatkapcsolat, letöltési sebesség), és **egy átlagos irodai környezetben is elérhető a 130-140Mbit-es sebesség sok felhasználó esetén is.**

Az Aruba teljesítménye alkalmassá teszi a wireless hálózatot, hogy ne csak másodlagos hozzáférési pontot jelentsen, de akár kiváltsa a hagyományos kábeles architektúrát is.

A Microsoft világméretű Aruba Wi-Fi hálózatában jelenleg 13.000 Access Point szolgál ki 80.000 felhasználót. A Microsoft már egyáltalán nem épít ki kábeles hálózatot a munkahelyekhez.

A teljesítményt javítja továbbá az Adaptive Radio Management összes olyan funkciója, mely sok felhasználó egyidejű csatlakozása esetén a

frekvenciatartomány és z egyes AP-k kihasználását optimalizálja még vegyes felhasználói eszközök esetén is.

PoE 802.11n-re is

Az Aruba 802.11n AP-i 13,5W fogyasztással szabványos PoE-switchekkel meghajthatók, nincs szükség külön tápra vagy nem szabványos injektorra a használatukhoz.