Tietoturvallinen wlan-verkko terveydenhuoltoympäristössä

25.5.2018 | Pauli Riikonen

Dustin

Pauli Riikonen

- Wlan-konsultti, Dustin Finland Oy
- Kymmeniä wlan-toteutuksia kouluihin, sairaaloihin ja yksityisiin yrityksiin
- MikroPC:n/Mikrobitin avustaja vuodesta 2009

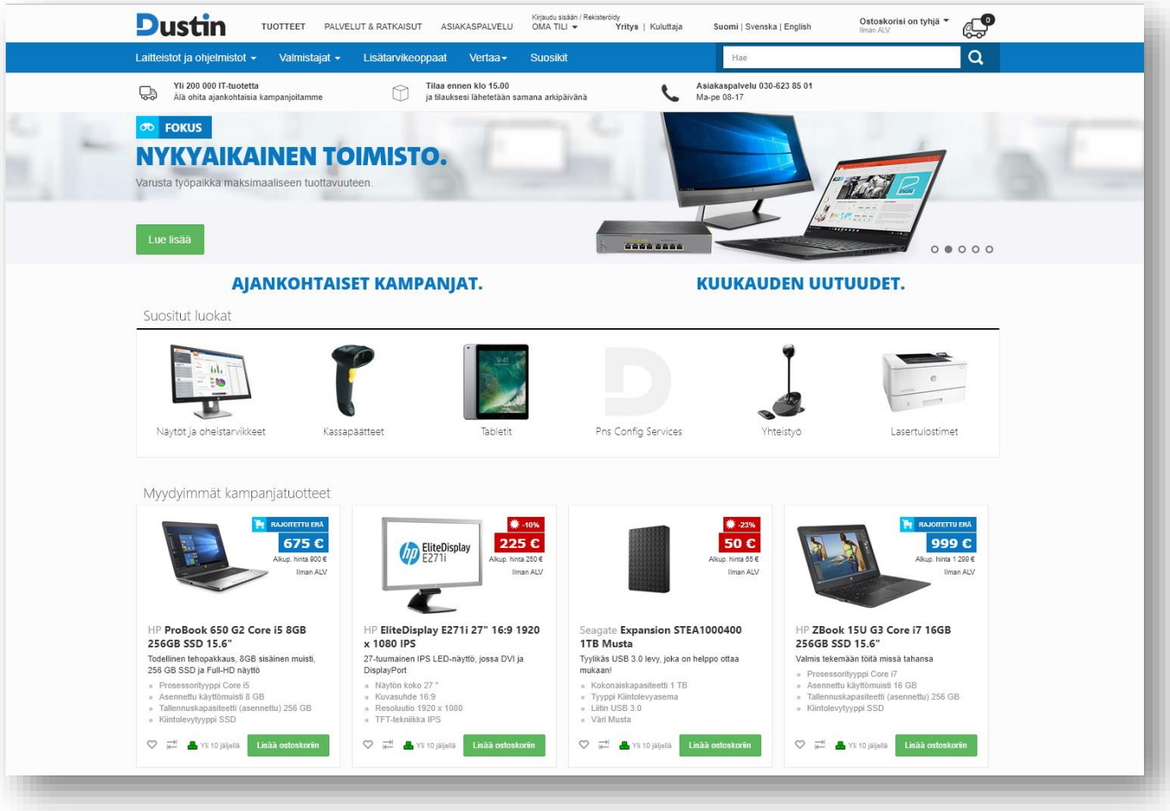
AGENDA

- Dustin lyhyesti
- Wlan-verkon vaatimukset terveydenhuoltoympäristössä
- Wlan-verkon suunnittelu
- Tietoturvallinen vierailijaverkko
- Laitevalmistajien omat suorituskykytestit

Dustin lyhyesti

Dustinista

- Perustettu vuonna 1984
- Yli 900 työntekijää Suomessa, Ruotsissa, Norjassa ja Tanskassa
- Pohjoismaiden johtavia IT-tuotteiden ja niihin liittyvien palvelujen jälleenmyyjiä
- Siirtyi Suomen markkinoille Businessforumin (2013) ja Resoluten (2015) ostojen myötä
- 20 vuoden kokemus verkkokaupasta
  - Ruotsissa dustin.se
  - Suomessa dustin.fi ja dustinhome.fi
- Liikevaihto 2016/17: n. 9,3 mrd SEK (0,9 mrd EUR)
- Yli 90 % myynnistä yrityksiltä (B2B)
- Pääkonttori ja suuri logistiikkakeskus Ruotsissa



Dustinin tarjonta

- Satoja edustettuja merkkejä

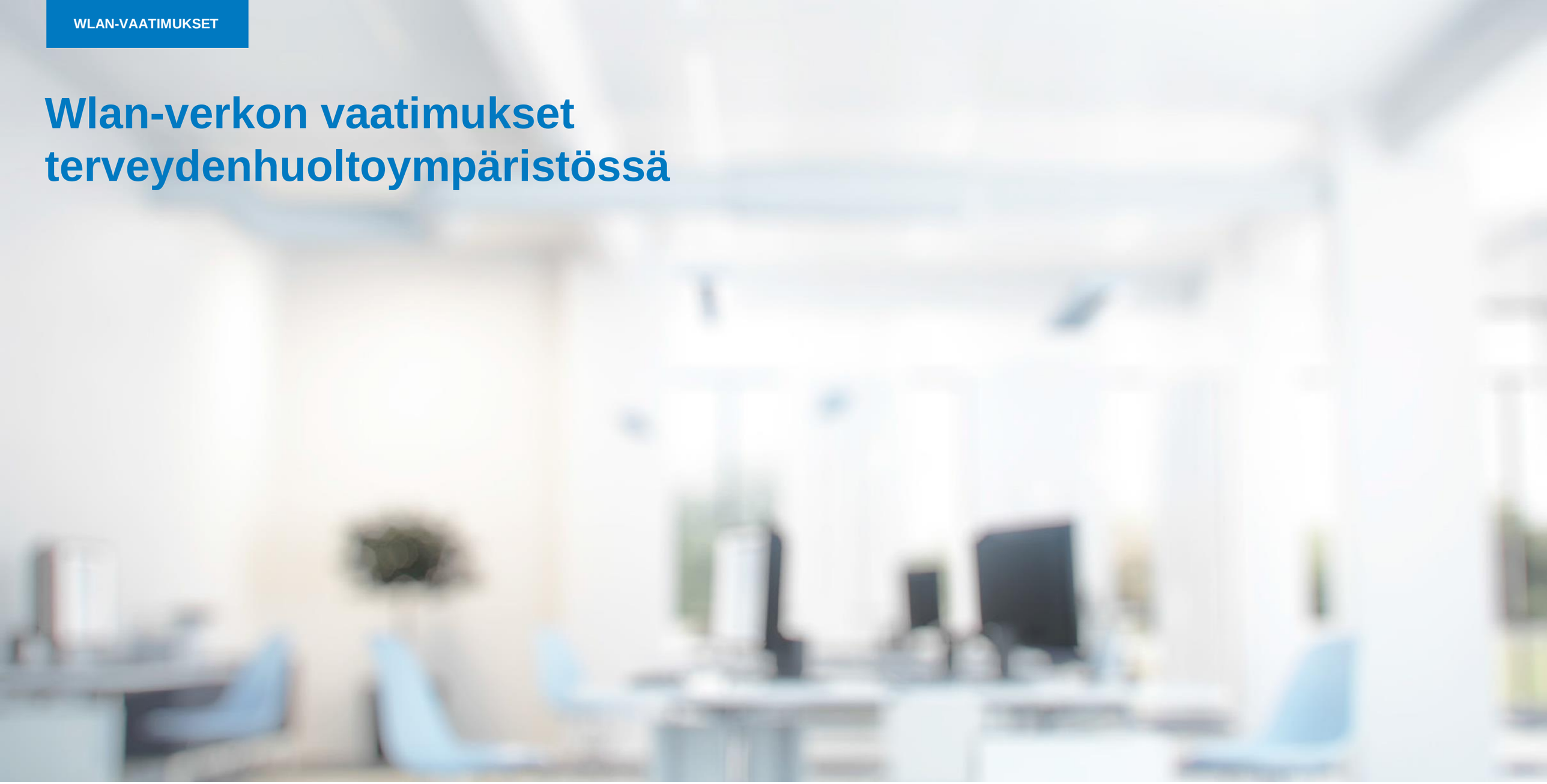
Tuotteet

- Päätelaitteet
- Ohjelmistot
- Tulostimet
- Av-laitteet
- Verkkolaitteet
- Palvelimet
- Tallennusratkaisut

Palvelut

- Konsultointi
- Asennus (sähkötyöt, verkkokaapeloinnit, av-asennukset jne.)
- Verkonvalvonta
- Langaton verkko ja tietoturva palveluna

Wlan-verkon vaatimukset terveydenhuoltoympäristössä



1. Wlan-verkon on tuettava monenlaisia päätelaitteita…

2. …mutta oltava silti mahdollisimman tietoturvallinen

- Varmennepohjainen autentikointimenetelmä (eap-tls) ylivoimaisesti turvallisin
  - Salausavain luodaan dynaamisesti autentikoinnin yhteydessä
  - Windows-työasemille varmenteiden jakelu Group policyn avulla
  - Mobiilaitteitteiden varmennejakelussa voidaan hyödyntää mobiililaitehallintaa, kuten Airwatchia tai Intunea
- Kaikki päätelaitteet eivät tue varmenteita
  - Tällöin (ja vain tällöin) vaihtoehtona staattinen wpa2-salausavain
- Lisäturvaa erillisen pääsynhallintapalvelimen, kuten Aruba Clearpassin tai Cisco ISEn avulla
  - Dhcp-profilointi, mac-osoitevääränennösten tunnistus, jälki kaikista verkossa käyneistä laitteista
- Ei omaa wlan-verkkoa jokaiselle eri laitetyypille tai palvelulle
  - Sairaalalaitteille yksi oma ssid, jossa laitteet tunnistetaan ja ohjataan tunnistuksen perusteella haluttuun aliverkkoon

3. Verkon on toimittava moitteettomasti 24/7/365

- Kliseinen totuus: Sairaalan toimimaton wlan-verkko voi maksaa ihmishenkiä
- Vikaantumisriskin huomiointi
  - Kahdennetut wlan-kontrollerit
  - Vikasietoinen tukiasemasijoittelu
  - Vikasietoiset kytkinratkaisut
- Roamauksen toimivuuden takaaminen kiertokone- ja voip-puhelinkäytössä
  - Tukiasemasijoittelu
  - Wlan-konfiguraatiot
- Liikenteen priorisointi aikakriittisille palveluille, kuten reaaliaikaiselle videokuvalle ja voip-puheluille
  - Tukiasemalta päätelaitteelle
  - Päätelaitteelta tukiasemalle

Wlan-verkon suunnittelu

Wlan-toteutuksen työvaiheet

1. Verkon vaatimusten selvittäminen
2. Tukiasemasijaintien määrittäminen
3. Tuotelistauksen laatiminen ja tuotteiden tilaus
4. Wlan-verkon käyttöönotto ja optimointi
5. Toiminnan tarkistus ja mahdolliset korjaustoimenpiteet

1. Verkon vaatimusten selvittäminen

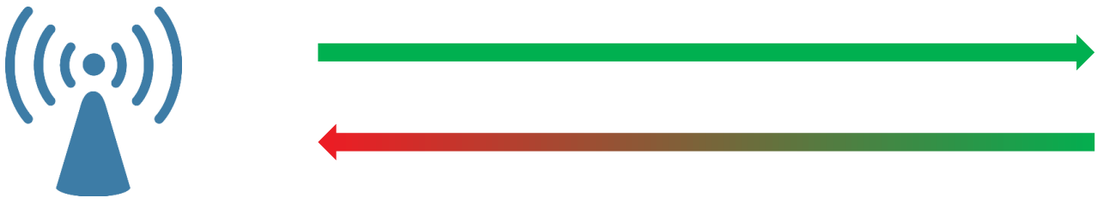
- Ilman selkeitä vaatimuksia ei ole mitään suunniteltavaa!
- Missä wlan-verkon tulee toimia?
  - Ajantasaiset pohjakuvat tarvitaan
- Mitä palveluita tarjotaan?
  - Datakäyttö
  - Voip
  - Paikannus (tukiasemamäärä kasvaa 50 % tai enemmän)
- Mitä päätelaitteita verkkoon tullaan liittämään?
  - Oleellisinta tunnistaa heikoimmin wlan-signaalia vastaanottavat ja lähettävät päätelaitteet
- Vikasietoisuuden taso?
- Alustava budjetti?

2. Tukiasemasijaintien määrittäminen

- Tukiasemasijaintien määrittäminen
  - Silmämääräisesti
  - Simulointisovelluksella
  - Paikan päällä tehtävien kuuluvuusmittausten perusteella
  - Yllä olevien yhdistelmänä
- Kuuluvuusmittausten tekemisellä vältytään astumasta pahimpiin miinoihin
  - Seinämateriaalien vaimennukset eivät välttämättä selviä pohjakuvien tai pelkän paikan päällä tehtävän katselmuksen perusteella
- Suunnittelussa huomioitava molemmat taajuusalueet

Kuuluvuusmittauksessa huomioitavia asioita

- 2,4 gigahertsin taajuusalue kantaa pidemmälle kuin 5 GHz
- Mittaustukiasemien lähetysteho pudotettava heikoimman lähetystehon omaavan päätelaitteen tasolle (kts. kuva alla)
- Mittalaitteen vastaanottoherkkyys
  - Mittalaite kalibroitava wlan-verkkoon liitettävien päätelaitteiden mukaan
  - Mittalaitteen ja esim. voip-puhelimen vastaanottoherkkyydessä voi olla yli 10 desibelin ero!



Tukiasemat
2,4 GHz: max **20** dBm (100 mW)
5 GHz: max **23 tai 30** dBm (200 tai 1000 mW)

Mobiililaitteet
2,4 GHz: max noin **16** dBm (40 mW)
5 GHz: max noin **13-14** dBm (20-25 mW)

Paikannuskelpoinen wlan-verkko

- Hoitohenkilökunnan, sairaalalaitteiden, pyörätuolien ja potilassänkyjen paikantamiseen
- Perustuu kolmiomittaukseen
  - Vähintään kolmen tukiaseman kuultava paikannustagin lähettämä signaali riittävän voimakkaasti
- Perusperiaatteena paikannettavan laitteen pysyttävä tukiasemista muodostetun kolmion sisällä (=tukiasemia tarvitaan kerroksen reunoillekin)
- Paikannustarkkuus noin 5-10m, parannettavissa huonekohtaisilla excitereilla

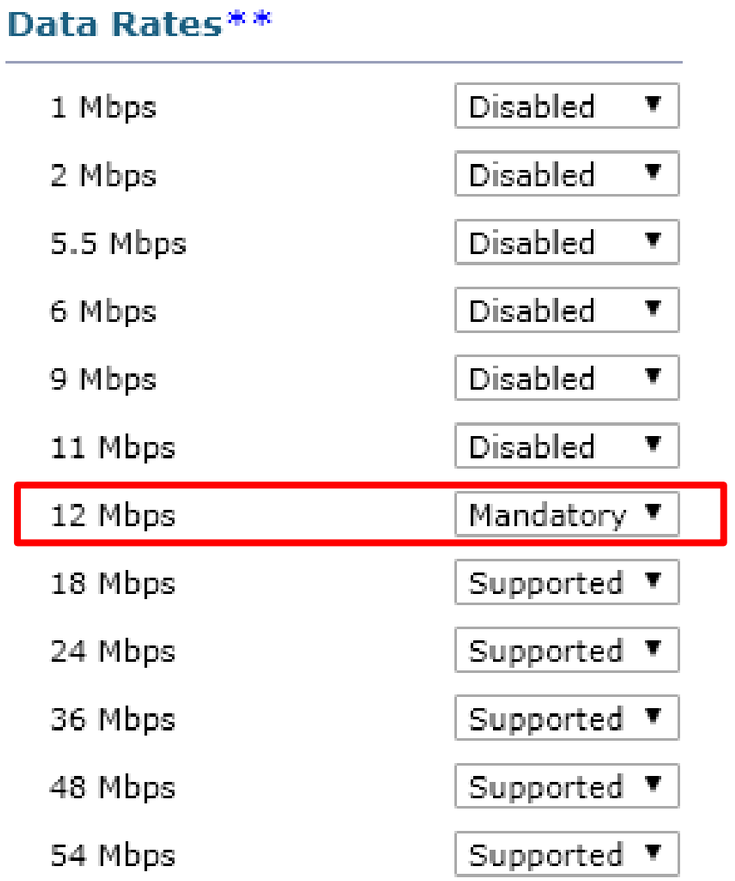
Paikannuskelpoinen wlan-verkko

Datakäyttö

Paikannus

4. Wlan-verkon käyttöönotto ja optimointi

- Roamauksen optimointi
  - Alimpien datanopeuksien kieltäminen (kts. kuva)
  - 802.11k: Liikkuvalle päätelaitteelle tarjotaan lista sopivista uusista tukiasemista kanavineen
  - 802.11r: Päätelaitteen autentikointitieto säilyy tukiasemaa vaihdettaessa. Älä käytä, jos kaikki päätelaitteet eivät tue
  - 802.11v: Päätelaitteelle voidaan lähettää suositus vaihtaa tukiasemaa
- Liikenteen priorisointi
- Pääsynhallintapalvelimen konfigurointi
- (Paikannuksen kalibrointi ja hienosäätö)



5. Toiminnan tarkistus ja mahdolliset korjaustoimenpiteet

- Riittävän signaalivahvuuden todentaminen
  - Tukiaseman signaalivahvuus päätelaitteelle
  - Päätelaitteen signaalivahvuus tukiasemalle
- Ylikuuluvuuden mittaaminen
- Roamauksen testaus kaikissa huoneissa
- Voip-puheluiden testaus kaikissa huoneissa
- (Paikannuksen testaus)

Dustin

Vierailijaverkon toteutus

Sairaalan vierailijaverkon ominaispiirteitä

- Vierailijaverkon käyttäjä on useimmiten potilas
- Wlan-verkon toimivuudella saattaa olla suora vaikutus potilaan kokonaistyytyväisyyteen, joten siihen kannattaa panostaa
  - 3G/4G ei välttämättä kuulu
- Verkkoon liittymisen tulee olla mahdollisimman helppoa:
  - Yksiselitteinen ja kuvaava ssid
  - Täysin avoin verkko tai korkeintaan käyttöehdot sisältävä portaalisivu
  - Ei monimutkaisia käyttäjänimen ja salasanan yhdistelmiä, joita kukaan ei tiedä tai muista
- Erittäin sekalainen päätelaitekanta: Miten vanhoja laitteita halutaan tukea?
  - Vähintään b-standardin laitteet kannattaa kieltää
- Kaistankäyttö suurehkoa, sillä netin suoratoistopalvelut hyvä lääke tylsyyteen
  - Torrentit ja muut epämääräiset palvelut voidaan kieltää jo tukiasemilla
  - Laitekohtainen kaistanrajoitus

Dustin

Vierailijaverkon tietoturva

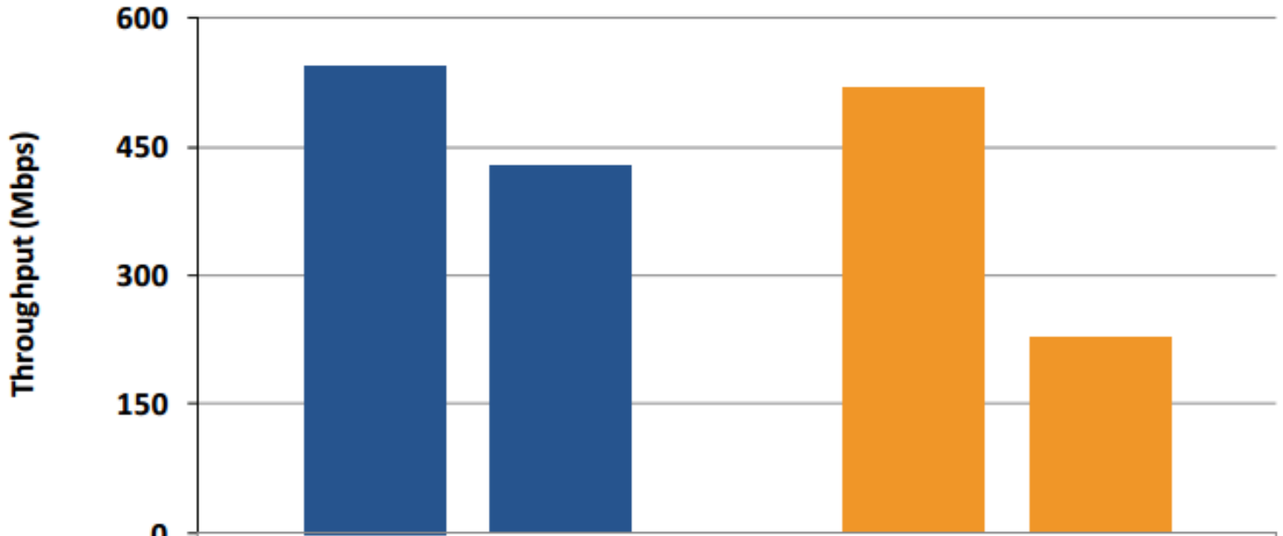
- Pääsy vain internetiin
- Ideaalitapauksessa vierailijaverkolle on oma nettiliittymänsä omalla julkisella nimipalvelulla
  - Hyökkäysrajapinta mahdollisimman pieni
  - Vierailijaverkon käyttö ei kuluta tuotantoverkon kaistaa operaattorin suuntaan
- Täysin avointa verkkoa tai web-portaalia käytettäessä liikenne päätelaitteen ja tukiaseman välillä ei ole salattu
  - Valtaosa nettipalveluista onneksi ssl-salattuja

Laitevalmistajien omat suorituskykytestit

Laitevalmistajien omat suorituskykyvertailut

- Oma tuote selviytyy mystisesti ylivoimaiseksi voittajaksi: Cisco

Figure 6: 802.11ac Throughput With and Without 802.11n 5 GHz Interference

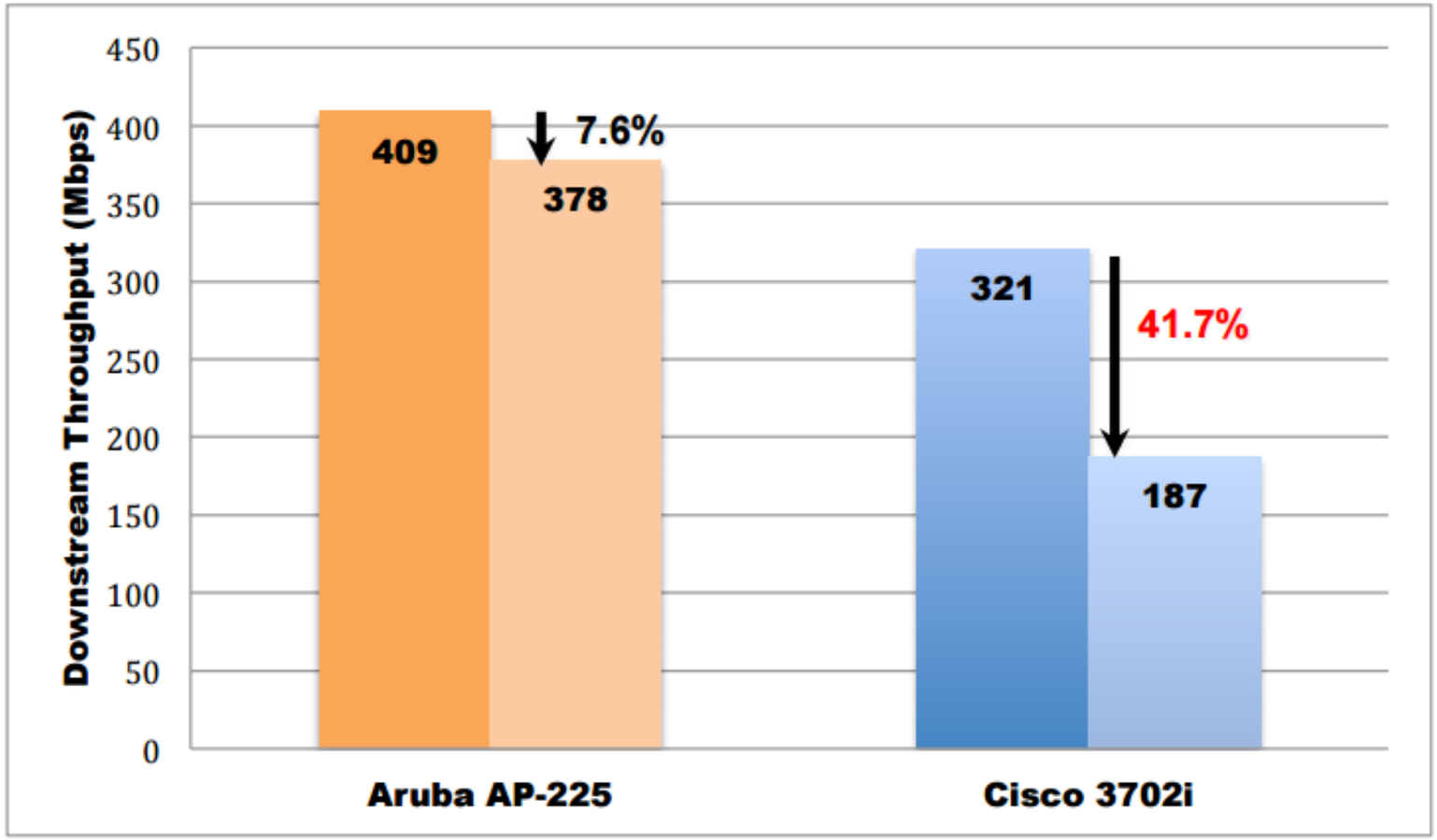


	(Cisco Aironet 3702i	Aruba AP-225
Without Interference	544	519
With Interference	428	228

Source: Miercom, November 2013

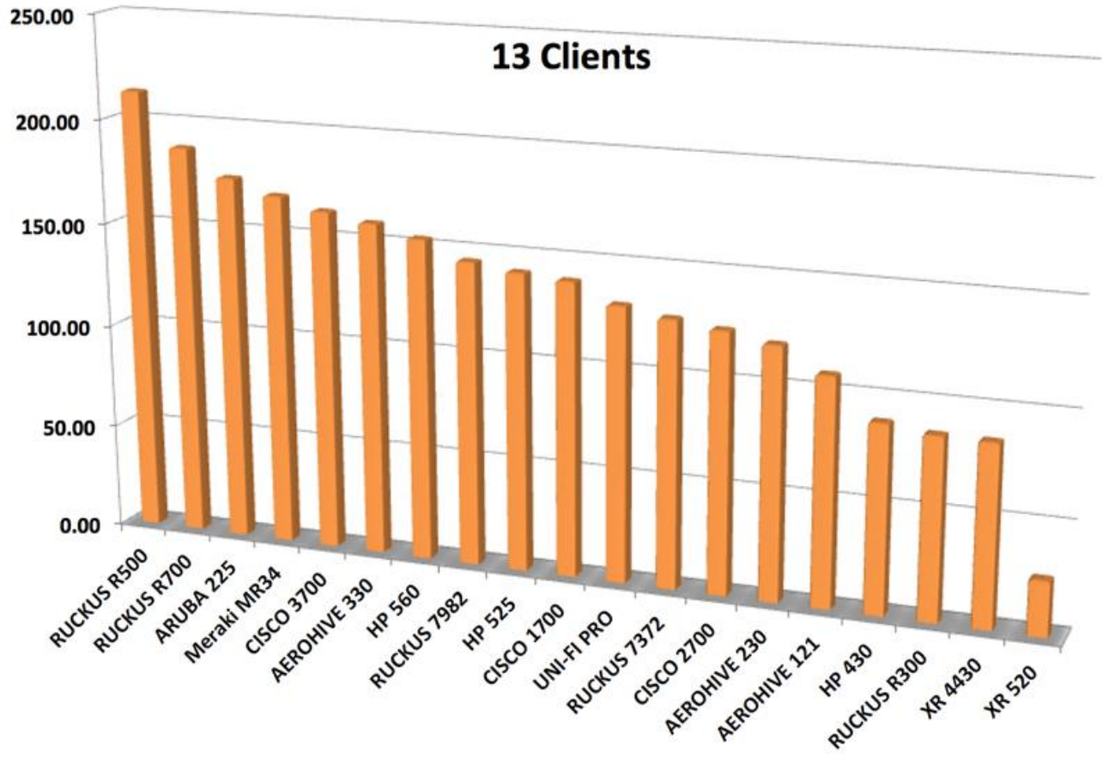
Laitevalmistajien omat suorituskykyvertailut

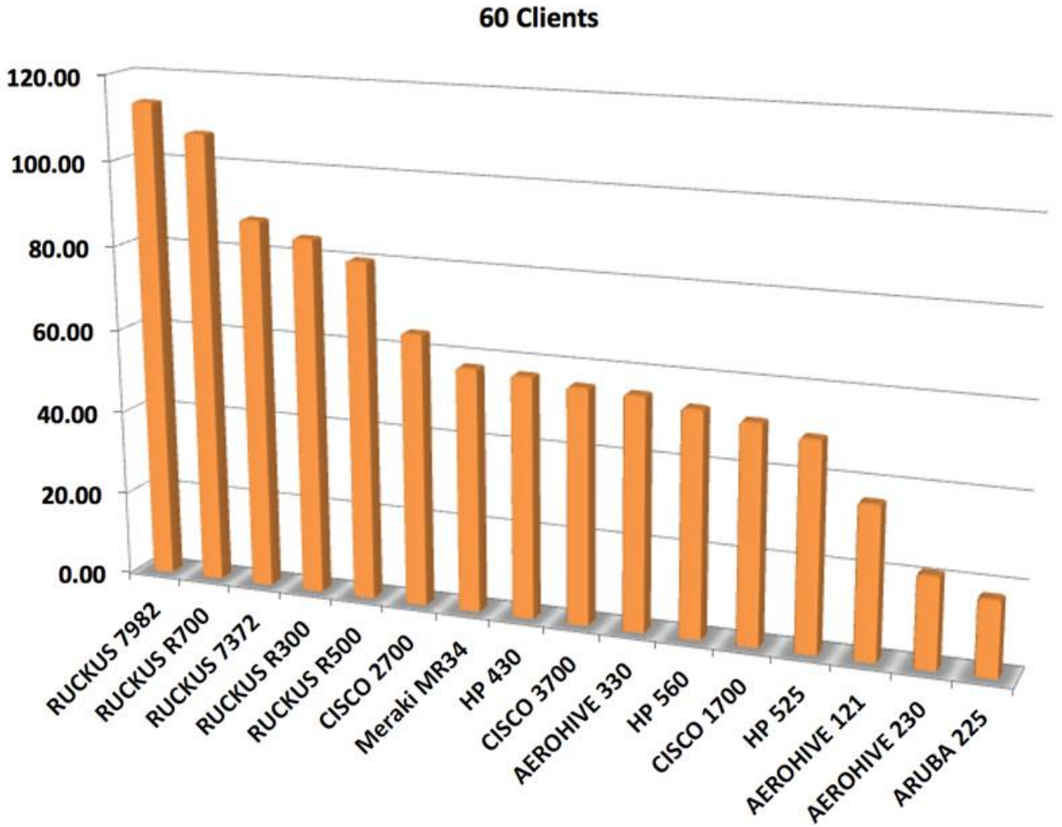
- Oma tuote selviytyy mystisesti ylivoimaiseksi voittajaksi: Aruba
- ”Once again the Aruba AP-225 clearly outperforms the Cisco 3702i.”



Laitevalmistajien omat suorituskykyvertailut

- Oma tuote selviytyy mystisesti ylivoimaiseksi voittajaksi: Ruckus





Kiitos!

Dustin

pauli.riikonen@dustin.fi