

Funet-ohjeistusdokumentti: Langattomat vierailijaverkot

Tunniste	Funet-ohjeistusdokumentti
Päiväys	6.11.2017
Otsikko	Langattoman vierailijaverkon toteutus kampuksille
Työryhmä	
Laatijat	FUNET
Vastuutaho	wenche.backman-kamila@csc.fi
Tyyppi	ohjeistus

Lataa PDF:

[Vierailijaverkon-toteutus-kampuksille-ohjeistus.pdf](#)



Vierailijaverkon-toteutus-kampuksille-ohjeistus.pdf

Tiivistelmä

Työtä ja opiskelua tehdään entistä useammin muualla kuin omalla työpisteellä tai tietokonehuoneessa, joten langattomien verkkojen merkitys on korostunut. Yliopistojen, ammattikorkeakoulujen ja tutkimuslaitosten vierailijoille onkin syytä taata toimiva, helppokäyttöinen ja tietoturvallinen ratkaisu verkkoon pääsemiseksi, jotta vierailijoiden työskentely tai opiskelu myös vierailtaessa on helppoa ja sujuvaa.

WLAN-tekniikalla toteutetulle vierailijaverkolle on neljä erilaista toteutustapaa. Niiden hyvät ja huonot puolet sekä kustannusarvio on esitetty taulukossa 1. Täysin avoin WLAN-verkko on kaikkien käytettävissä verkon kuuluvuusalueella. Web-autentikointiin perustuvaan verkkoon tarvitaan etukäteen luotu käyttäjätunnus ja salasana, jotka syötetään verkkosivulle verkkoon liittymisen jälkeen. Henkilökohtainen jaettu avain on menetelmä, jossa syötetään liittymisen yhteydessä etukäteen luotu avain, jota käytetään autentikointiin ja kryptaukseen. Käytettäessä 802.1x autentikointia ja WPA2/AES-salausta, käyttäjät tunnistetaan ennen kuin liikennöinti on mahdollista. Liikenne on kryptattua ja kryptausavainta vaihdetaan usein. Liittyminen verkkoon tapahtuu suplikantin avulla.

Taulukko 1. Eri tekniikoilla toteutetut WLAN-vierailijaverkot, niiden hyvät ja huonot puolet sekä kustannusarvio.

Tekniikka	Hyvät puolet	Huonot puolet	Kustannukset
Avoin verkko	Helppokäyttöinen Vierailijatunnuksia ei tarvitse luoda	Ei voida mitenkään määritellä kuka saa käyttää verkkoa Salaamaton yhteys, verkon tietoturva huono (tietoturva käyttäjän vastuulla)	Ei erityisiä investointi- tai operointikustannuksia (halpa)
Web-autentikointiin perustuva verkko	Helppokäyttöinen ja toimintavarma Osittainen mahdollisuus määritellä kuka saa käyttää verkkoa	Salaamaton yhteys, verkon tietoturva huono (tietoturva käyttäjän vastuulla) On määriteltävä prosessi, jolla luodaan vierailijatunnuksia yksittäiselle vierailijalle ja tapahtumille.	Vaatii RADIUS-palvelimen, sisäänkirjautumissivun ja käyttäjähallintaa (keskihintainen)
Henkilökohtainen jaettu avain	Mahdollistaa hyvän tietoturvan olemalla myös helppokäyttöinen ja helposti toteutettavissa	Ei tuettuna kaikissa tukiasemissa	Riippuu valmistajien hinnoittelupolitiikasta. Vaatii käyttäjähallintaa (luultavasti keskihintainen)
802.1x autentikointi ja WPA2/AES-salaus (eduroam)	Erittäin tietoturvallinen Automaattinen liittyminen verkkoon ensimmäisen liittymisen jälkeen.	Konfigurointiongelmia esiintyy Rajattu käyttäjäkunta (eduroam-vierailijaverkkopalvelu on vain yliopistoille, ammattikorkeakouluille ja tutkimuslaitoksille)	Vaatii RADIUS-palvelimen ja käyttäjien opastusta (keskihintainen)

IT-hallinnon näkökulmasta täysin avoimeen verkkoon liittyy se riski, että väärinkäytötapauksissa vain laite voidaan selvittää MAC-osoitteen perusteella – ei käyttäjää. Web-autentikointiin perustuva verkko on IT-hallinnon kannalta hieman suojatumpi koska kuka tahansa ei päästetä verkkoon. Käyttäjän kannalta riski on kuitenkin suurempi käytettäessä kyseisiä menetelmiä. Käyttäjän tekemisiä avoimessa tai web-autentikointiin perustuvassa verkossa voidaan helposti salakuunnella tai manipuloida, eikä käyttäjä välttämättä tiedä, miten suojautuminen erilaisilta verkkouhilta pitäisi tapahtua. Eli käyttäjän kannalta olisi hyvin tärkeätä tarjota tietoturvallista eduroam-vierailijaverkkoa, joka perustuu 802.1x autentikointiin ja WPA2/AES-salaukseen. Henkilökohtainen jaettu salaisuus tarjoaa myös hyviä mahdollisuuksia vierailijaverkoksi, mutta tällä hetkellä vain muutama laitevalmistaja tukee menetelmää.

Halvin ratkaisu lienee avoin verkko, muut ratkaisut edellyttävät investointeja kuten esim. RADIUS-palvelimen hankinnan. Myös opertointikustannuksia verrattaessa avoin verkko on halvin, muut ratkaisuehdotukset vaativat jonkin verran käyttäjähallintaa ja käyttötukea.