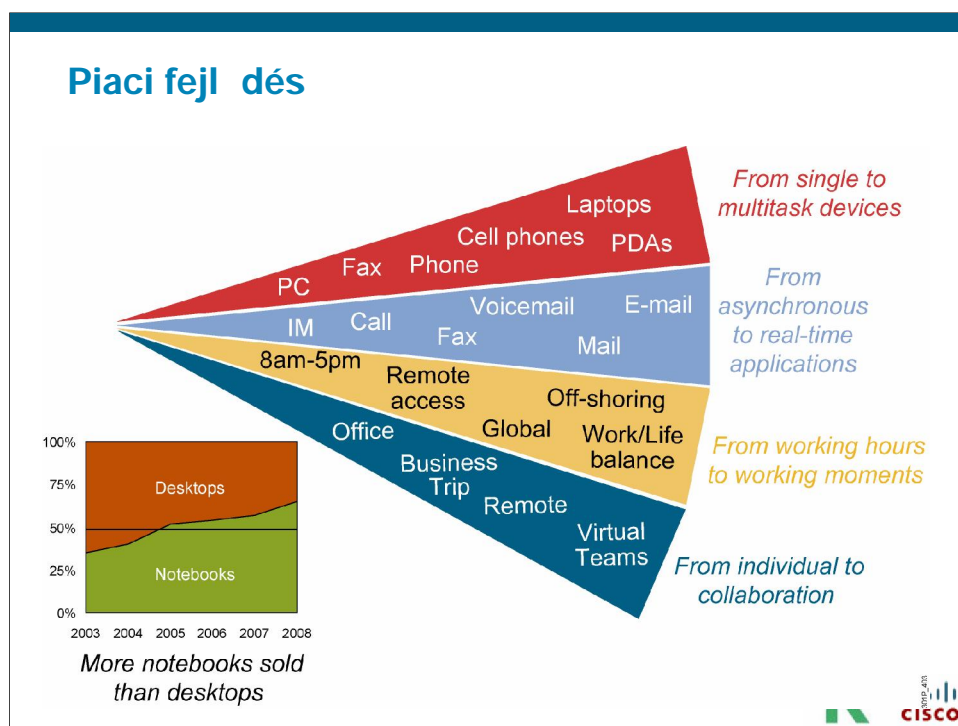


Alapvet technológiai áttekintés

WLAN – Wireless LAN





A felhasználók elvárásai alapján az internetes hálózat elérése nem elégséges fix helyeken, hanem annak elérését bárhol lehet végre kell tenni. Ezt az igényt mutatja az is, hogy sokkal jobban terjednek a mobil eszközök, mint az asztali számítógépek. A felhasználók nagy százaléka szeretné a leveleit a különböző helyszíneken megnézni, nem csak az irodában.

A WLAN terjedésének másik oka, hogy olcsóbb a telepítése mint a vezetékes hálózatoknak és kényelmesebbek is lehetnek, mert nincs benne helyhez kötöttség az irodában sem.

WLAN hálózatok előnyei:

- bárhol elérhető, ahol van elérési pont (Access Point (AP))
- nincs fix helyhez kötve épületen belül sem a felhasználó
- ha nincs vezetékes hálózat az épületben, nem kell kiépíteni azt
- olcsóbb a telepítése, mint egy vezetékes hálózatnak

WLAN hálózatok hátrányai:

- az átviteli közeg „védtelen, bárki számára hozzáférhető”, az információkhoz könnyebben hozzá lehet jutni
- nem áll meg a jelek terjedése az iroda falainál
- a környezeti tényezők zavarhatják a működését
- nem nyújt azonos sávszélességet a hozzáférési ponttól különböző távolságban (közelebb gyorsabb – távolabb lassabb)

Különbségek a WLAN és LAN között

- WLANs use radio waves as the physical layer.
- Radio waves have problems that are not found on wires.
 - Connectivity issues:
 - Coverage problems
 - Interference, noise
 - Privacy issues
- Access points are shared devices similar to an Ethernet hub for shared bandwidth.
- WLANs must meet country-specific RF regulations.



WLAN-ok és LAN-ok közti különbségek

- A WLAN rádió hullámokat használ fizikai réteggént, ellentétben a LAN által használt kábelekkel.
- Rádió hullámok problémákat okozhatnak, amely a vezetékes hálózatokon nem fordul el .
 - Ilyenek lehetnek a kapcsolódási problémák, jelek torzulása, interferencia; valamint a titkosítási problémák, mivel a jelek azon számára is érzékelhet ek, akik számára nem szólnak
- Az Ethernet hálózatokhoz hasonlóan a hozzáférési pontokat itt is megosztják az eszközök között, mint ahogy egy Hub megosztja a sávszélességet.
- WLAN-ok esetében minden országban speciális frekvencia tartományokat jelölnek ki, ahol használhatóak.

Rádió Frekvenciás Átvitel

- Radio frequencies are radiated into the air via an antenna, creating radio waves.
- Objects can affect radio wave propagation resulting in:
 - Reflection
 - Scattering
 - Absorption
- Higher frequencies allow higher data rates; however, they have a shorter range.



A rádió frekvenciás átvitel

A rádió hullámokat a levegőbe sugározzák antennák segítségével, amelyek elállítják és terjesztik a jeleket. A jelek terjedése közben problémák léphetnek fel, pl. elmerülhet, visszaverődhet, vagy szétszóródhat.




Reflection: Visszaverődés: amikor a RF hullám visszapattan valamilyen objektumról (pl. fém vagy üveg felület)

Scattering: Szétszóródás: amikor a RF egyenetlen felülettel ütközik (pl. durva felület) és szétszóródik több irányba

Absorption: Elnyelés: amikor a RF elnyelődik valamilyen objektum által (pl. fal)

Általánosságban elmondható, hogy nagyobb frekvencia tartomány nagyobb sebességet engedélyez, de a hatótávolság kisebb lesz.

Wireless LAN biztonsági kérdései

"WAR DRIVERS"	HACKERS	EMPLOYEES
Find "Open" Networks; Use Them to Gain Free Internet Access	Exploit Weak Privacy Measures to View Sensitive WLAN Info and Even Break into WLANs	Plug Consumer-Grade APs/Gateways into Company Ethernet Ports to Create Own WLANs
		

ALEF X CISCO

A WLAN biztonsági kérdései

A vezeték nélküli hálózatok hátránya, hogy a fizikai kapcsolatok hiánya és a rádiós csatorna jellege miatt több potenciális támadásnak vannak kitéve, mint a vezetékes társaik. Fontos tehát, hogy a vezeték nélküli hálózatok megfelelő védelmi mechanizmusokkal legyenek ellátva, melyek minden körülmények között biztosítják a biztonságos működést.

Biztonság szempontjából támadók lehetnek:


War driver: megfelelő hardverrel (WLAN kártyás eszköz) rendelkezve WLAN hálózat szkennelése, azaz keresése, és ha lehetséges annak ingyenes használata.

Hacker-ek: kihasználják a hálózat gyenge titkosításait és hozzáférnek a WLAN hálózatokhoz.

Alkalmazottak: akik önhatalmúlag a vállalati hálózatban access pointot telepítenek, de nem látják el a megfelelő védelemmel.

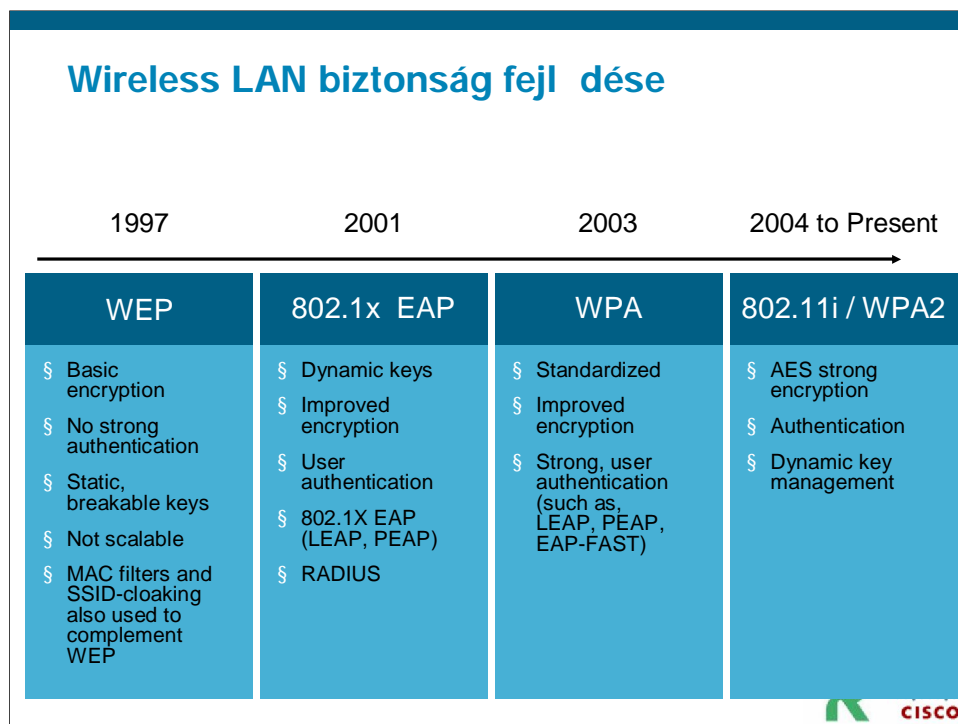
Biztonsági fenyegetések enyhítése

Control and Integrity	Privacy and Confidentiality	Protection and Availability
Authentication	Encryption	Intrusion Prevention System (IPS)
Ensure that legitimate clients associate with trusted access points.	Protect data as it is transmitted and received.	Track and mitigate unauthorized access and network attacks.



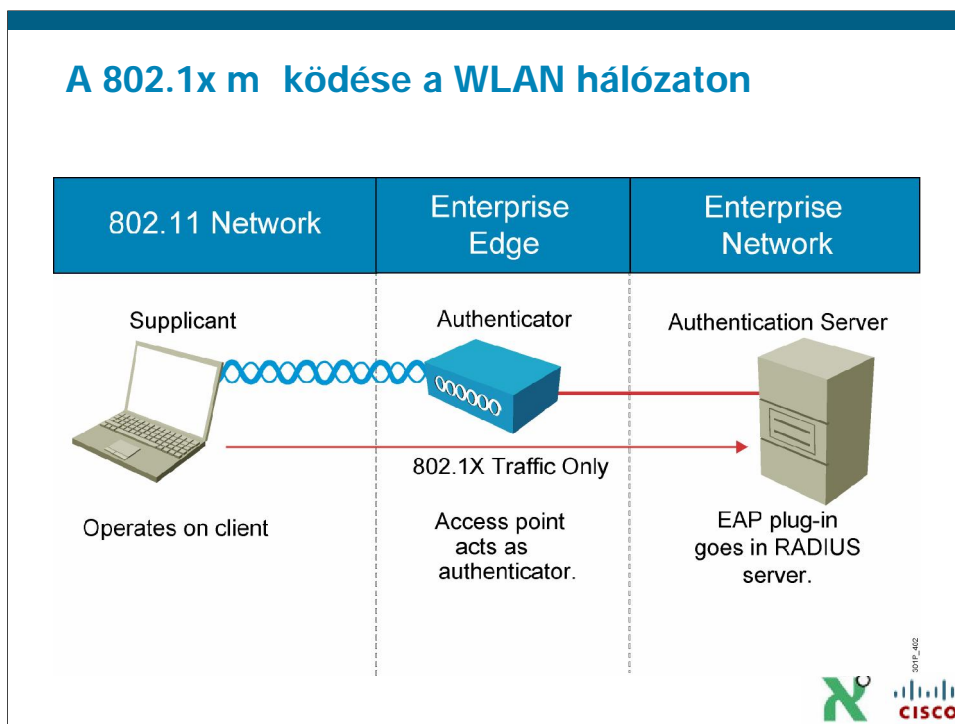
Egy biztonságos WLAN-ban az alábbi dolgokra kell figyelni:

- authentikáció: ellenőrizni, hogy csak a jogosult felhasználók férjenek hozzá a hálózathoz
- Titkosítás: az adatok titkosítás után továbbítódjanak a hálózaton, mert a csatorna bárki számára hozzáférhető
- Behatolás érzékelő rendszer, behatolás megelőző rendszer: illetéktelen hozzáférések követése és mérséklése.



A fenti ábrán a wireless LAN-okon használt különböző titkosítási módszerek láthatóak, amelyek mind a hálózathoz való hozzáférésre, mind az adatok átvitelére vonatkoznak. A használatuk azért szükséges, hogy a vezeték nélküli hálózatokat is legalább olyan biztonságossá tegyünk, mint a vezetékeseket.

A 802.1x m kódése a WLAN hálózaton



A fenti ábrán a 802.1x által nyújtott autentikáció m kódése látható.

Ennek az autentikációnak az a lényege, hogy egy WLAN hálózathoz való kapcsolódási igény felmerülésekor az autentikáció egy szerverrel való kommunikáció során történik meg és a sikeres autentikálás után a szerver utasítja az access point-ot a kapcsolat felvételére.

Összefoglalás

Összefoglalás

- WLAN fogalma
- WLAN biztonság fontossága



