ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Není Wi-Fi jako Wi-Fi

AP, Cluster, Controller, Cloud, co pro FELK ?

Ing. Martin Samek
samekma1@fel.cvut.cz

FEL-SVTI

4. říjen 2014

Wi-Fi...

...to je jako Hi-Fi :)

1985	FCC uvolnila ISM pásmo
1997	schválen IEEE 802.11 (pouze 2 Mbps)
1999	vzniká Wi-Fi Alliance

IEEE standardy

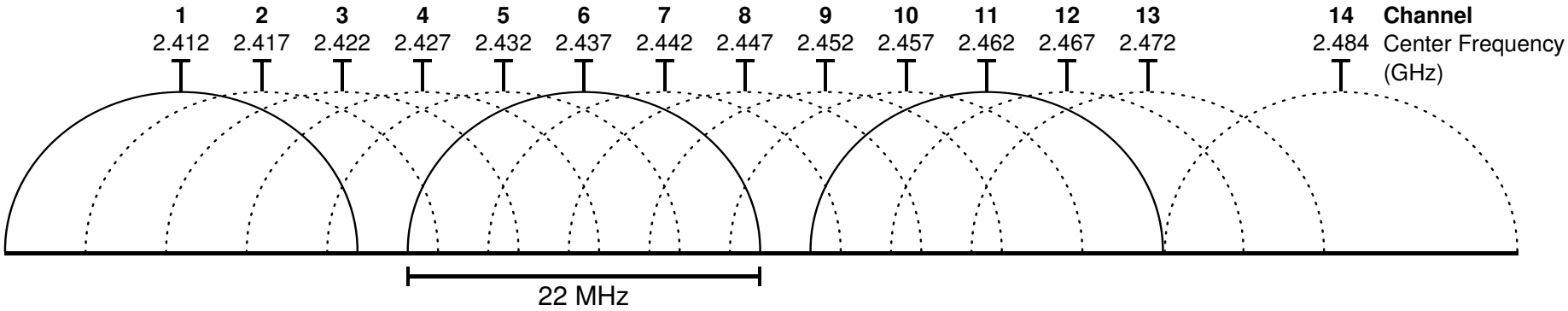
802.11b-1999	11 Mbps, DSSS
802.11a-1999	54 Mbps, OFDM
802.11g-2003	54 Mbps, OFDM
802.11n-2009	150 Mbps, 40 MHz, 4x4 MIMO
802.11ac-2014	až 160 MHz kanál, 4x4 MIMO

pre 802.11 technologie BreezeNet, později Alvarion.

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ISM pásmo 2,4-2,5 GHz

a taky Bluetooth, DECT, kamery, sluchátka, μw trouby...



EU kánaly 1-13

US kánaly 1-11

JPN kánaly 1-14, pouze DSSS

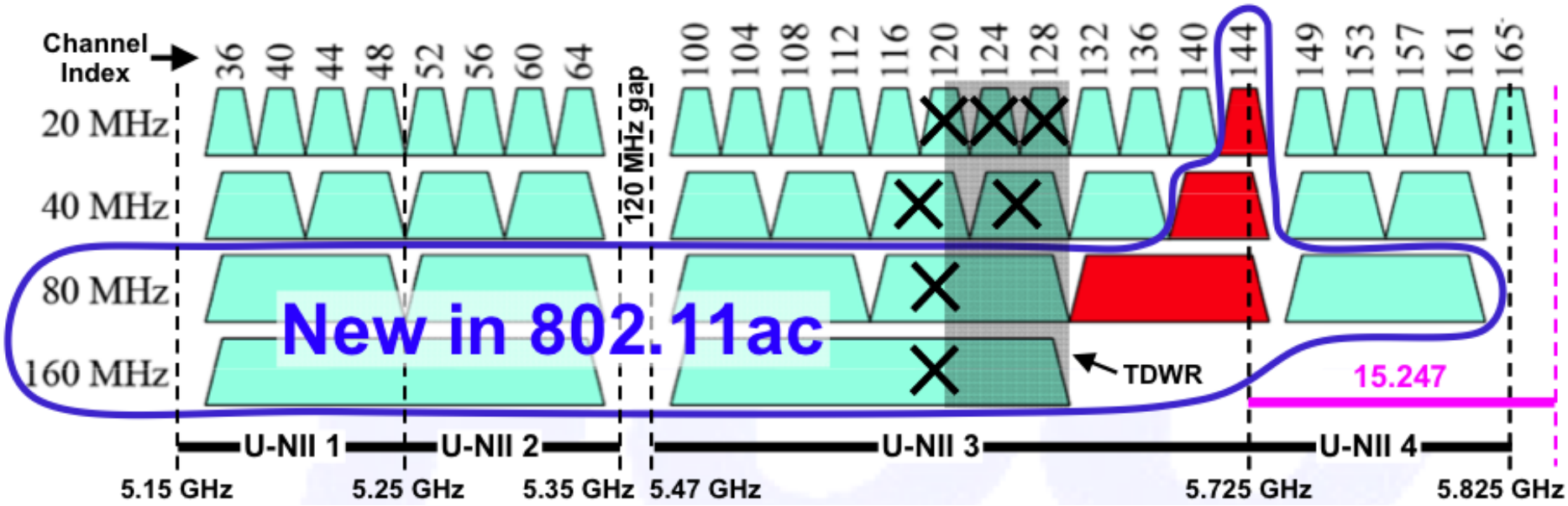
- šířka kanálu 22 MHz
- odstup kanálů 5 MHz
- 3 nepřekrývající se kanály

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ISM pásmo 5 GHz

vlastně přibližně od 4,9 GHz do 5,8 GHz

Problémem 5 GHz pásma je jeho roztříštěnost napříč celým světem vlivem různých omezení.



- Dynamic Frequency Selection
- Transmit Power Control
- globálně kanály 36-64
- meteoradary, vojenská zařízení

Další ISM pásma

Třeba. . . 900 MHz, 3,6 GHz, 5,9 GHz, 60 GHz

Mimo obecně používané pásma existují i další ISM rozsahy, které bohužel také podléhají různým omezením.

802.11ah ve volném pásmu 900 MHz, k dispozici omezený počet kanálu o šířce 1-2 MHz. Dobrá prostupnost, pro senzoriku, domácí automatizaci,. . .

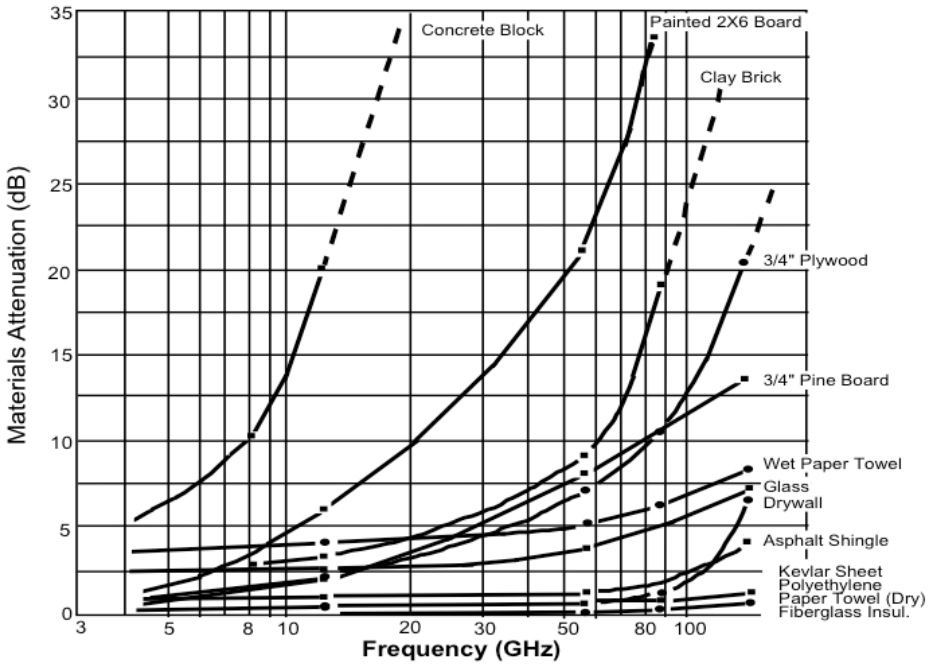
802.11y pouze v US, licencované pásmo 3,6 GHz o šířce 40 MHz.

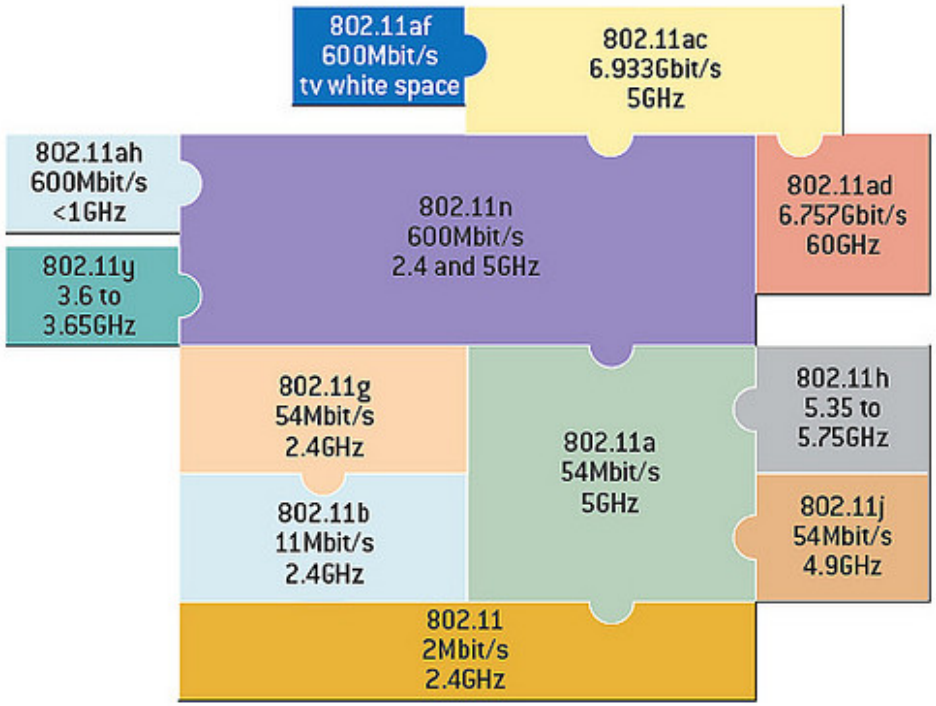
802.11p 5,9 GHz, určeno pro Wireless Access in Vehicular Environments (WAVE) a Intelligent Transportation Systems (ITS).

802.11ad v budoucnu komunikace v pásmu 60 GHz. Molekula O_2 tlumí šíření vlny o takové frekvenci.

Propustnost vs. prostupnost

Vlnová délka určuje propagaci elmag. vlny v daném prostředí.





Wi-Fi používá mechanismus CSMA-CA (Ethernet CSMA-CD, Can CSMA-DCR), snižuje reálnou propustnost. S rostoucím množstvím obsluhovaných klientů se snižuje airtime na klienta.

802.11ac-wave1 a 802.11ac-wave2

Co může očekávat v blízké budoucnosti

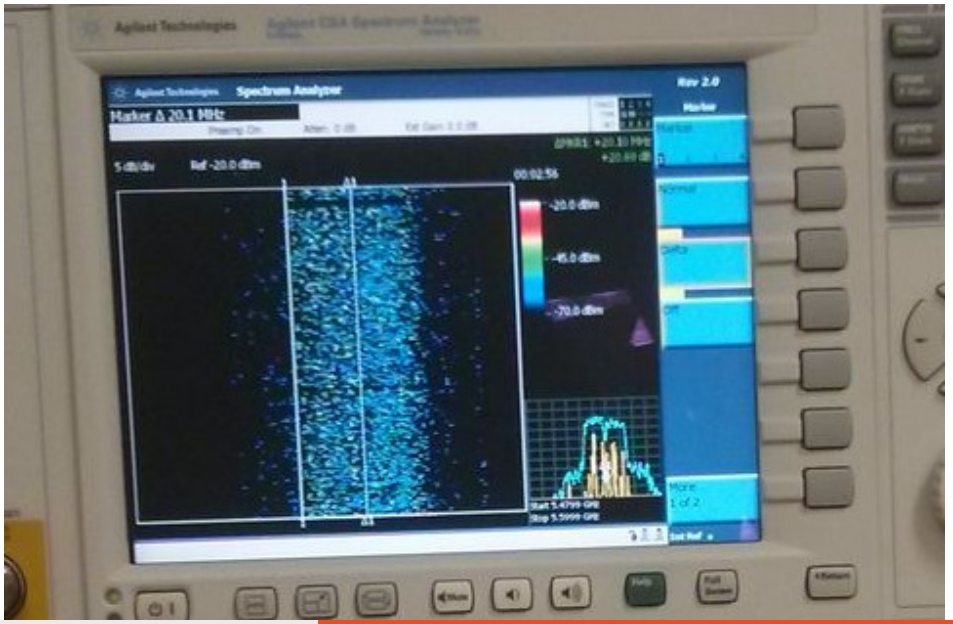
- Standard 802.11ac (někdy označován jako GigabitWiFi) je definován pouze pro pásmo 5 GHz, ve 2,4 GHz nemáme moc co slučovat, proto se zde používá klasické 802.11n.
- Oproti 802.11n umožňuje slučovat více než 2 kanály, získáme 80 MHz kanál, ve wave2 až dokonce 160 MHz široký „super kanál“. V 5 GHz začne být těsno.

Max. teoretické přenosové limity:

- 3,47 Gbps pro wave1
- 6,93 Gbps pro wave2

Prakticky kolem 1,3 Gbps, resp 2,7 Gbps (450 Mbps na 1x1 stream)

ac-paradox



Jaké provozujeme bezdrátové sítě ?

Prostředí s nízkou hustotou klientů - páteřní a distribuční spoje

Prostředí s vysokou hustotou klientů - access, zasedací místnosti, posluchárny,. . .

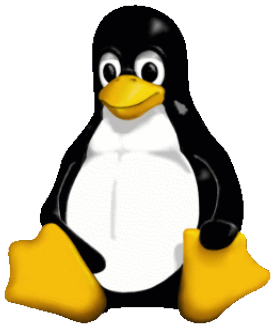
Odlišné a často protichůdné požadavky na parametry sítě.

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Výrobci hardware

Na konkrétné určení sítě se jednotliví výrobci různě orientují

- Ubiquity AirMax
- MikroTik RouterBoard
- Motorola Canopy
- řešení OpenWRT, dd-wrt,...
- ...



- Ubiquity uniFi
- Aruba Networks[a]
- Ruckus
- Extreme Networks
- Extricom
- Cisco
- ...

[a] DELL, Alcatel-Lucent, Juniper

Není to úplně zřejmé, ale mnoho řešení využívá linuxový kernel nebo GNU software.

Rozdílené přístupy k návrhu bezdrátových sítí

Od pokrytí ke kapacitě sítě

Jak se postupně uživatelé vybavovali větším množstvím zařízení, bylo potřeba změnit přístup k návrhu wifi sítí:

- v dobách 802.11b/g se sítě budovaly tzv. "na pokrytí".
- s příchodem 802.11n/ac a MIMO se přešlo k budování sítí tzv. "na kapacitu".

Rostoucí množství klientů vyžadujících bezdrátovou konektivitu nutně vede k potřebě aktivně řídit, jak je nakládáno se sdíleným komunikačním kanálem, jak jsou eliminovány vlivy zdrojů rušení a jak je zátěž distribuována na jednotlivá AP. K tomu síť musí mít „inteligenci“ schopnou problémy identifikovat a zasáhnout proti nim.

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Rozdílené přístupy k návrhu bezdrátových sítí 2

Chaoticky vs. koncepčně

Struktury a správa bezdrátových sítí

Od sady konfiguračních skriptů ke cloudu

1. více samostatných nezávisle konfigurovaných AP, pro více než 2 AP téměř nepoužitelné, autentizace může být centralizována.
2. předchozí + sada konfiguračních skriptů (pSSH, Ansible) a monitoring přes SNMP (Cacti, Nagios, Observium).
3. cluster spolupracujících AP, kdy jedno vystupuje jako master (Aruba Instant).

A kudy teče servisní komunikace (konfigurace, monitoring, AAA) ?

Struktury a správa bezdrátových sítí 2

Od sady konfiguračních skriptů ke cloudu

1. systémová AP řízená skrze SW nebo HW appliance (ubnt uniFi, Ruckus). Uživatelská data bridgována přímo do VLAN.
2. systémová AP řízená kontrolérem (Aruba, Cisco). Uživatelská data protékají kontrolérem (GRE/IPSec tunel, FW, analýza) nebo přímo do VLAN. Možnost remote AP.
3. AP konfigurovaná a monitorovaná aplikací v cloudu (Azure, EC2). Správa uživatelů a autentizace rovněž v cloudu.

A kudy teče servisní komunikace (konfigurace, monitoring, AAA) ?

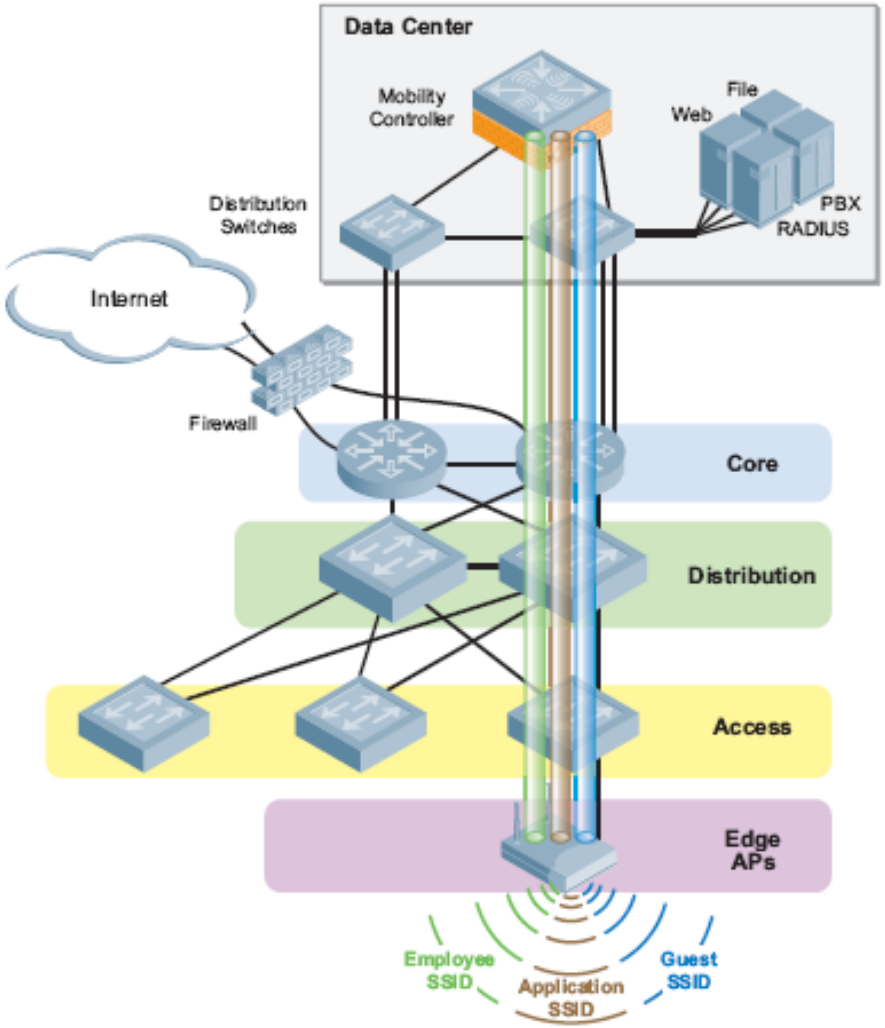
RF návrh a řízení spektra

Jak správně rozmístit AP a jak hospodařit se „vzduchem“

- můžeme dělat tzv. Site-Survey, rozmisťovat AP, měřit, analyzovat,. . . iterovat
- nebo rozmístíme AP podle vhodného vzoru, třeba „W“. O zbytek se postará síť (vhodné kanály, přesahy, identifikace rušení, přesouvání klientů (sticky-clients).
- nedopustit se zásadních chyb

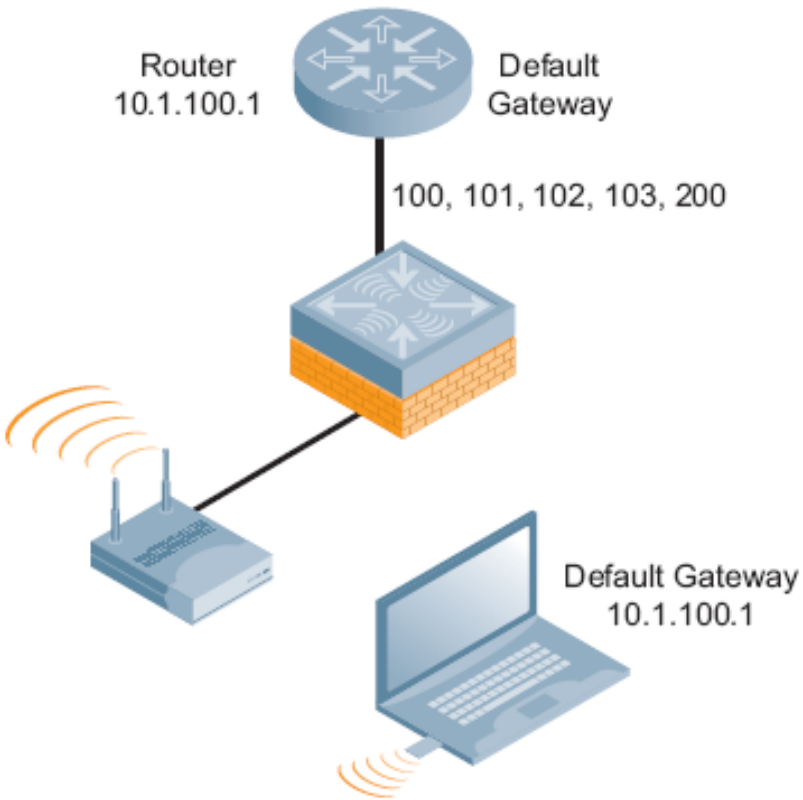
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

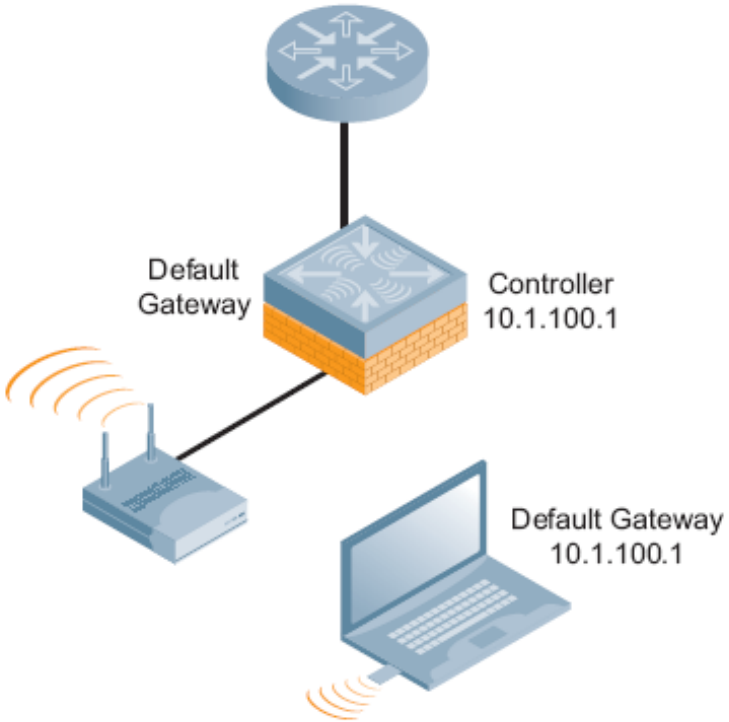
Architektura kontrolérem řízené wifi



ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

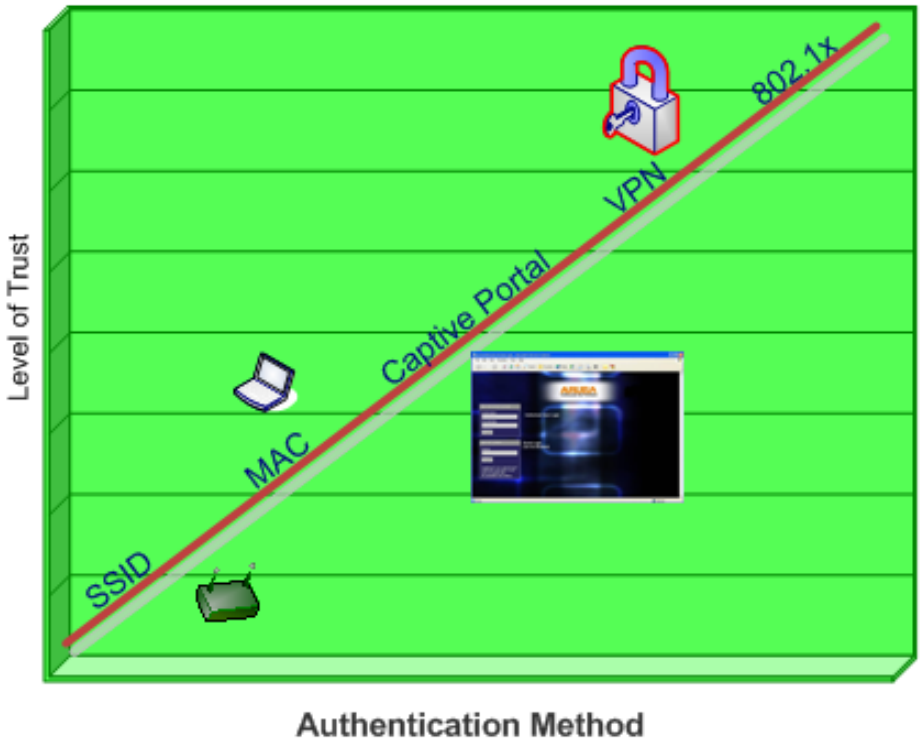
L2 vs. L3





ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Autentizace

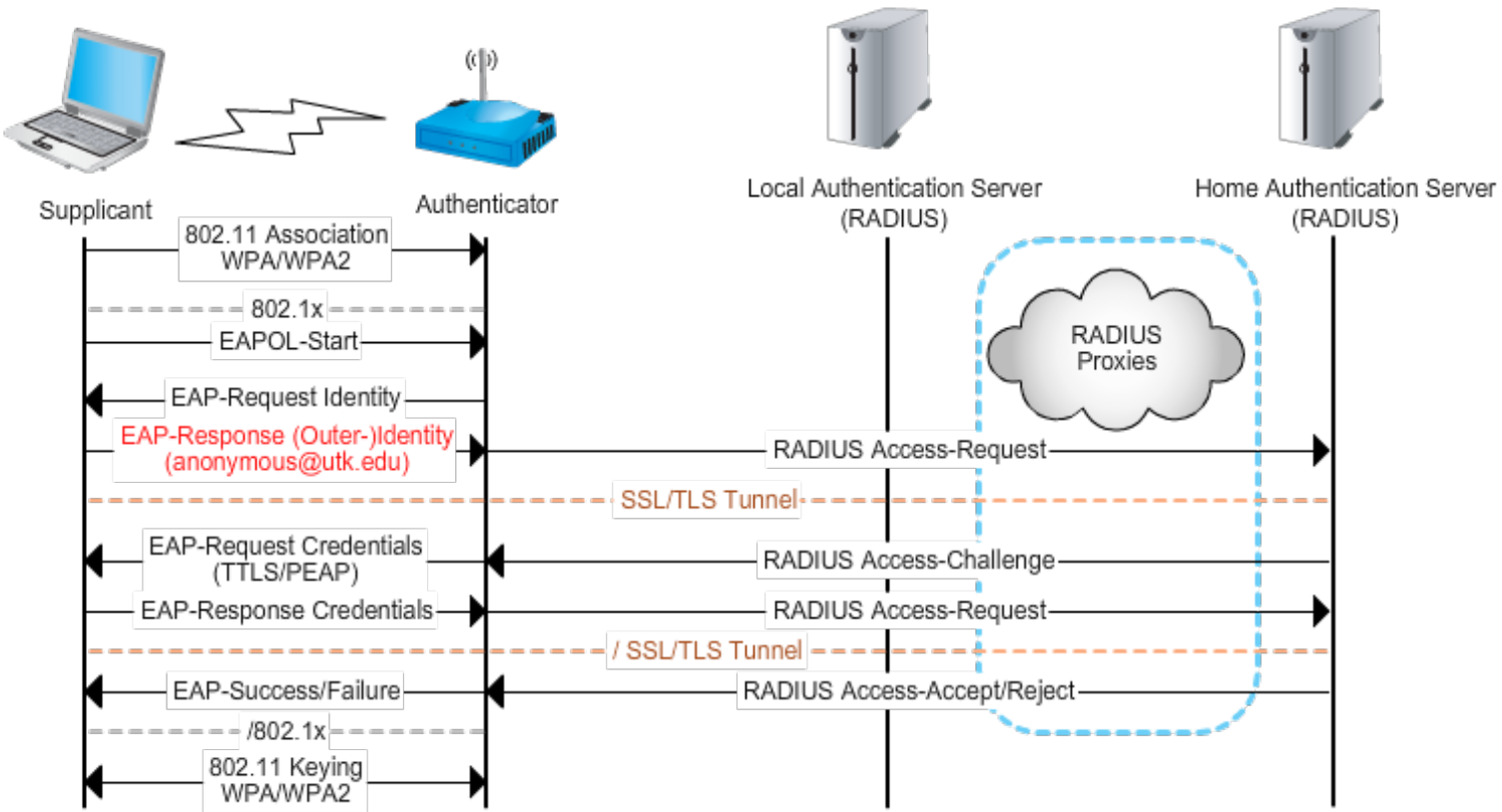


- legacy zařízení !?
- PSK je prolomené
- WPS (tlačítko + PIN) díra, WPA klíč za pár vteřin
- 802.1x (dynamické klíče) neprolomené

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

802.1x

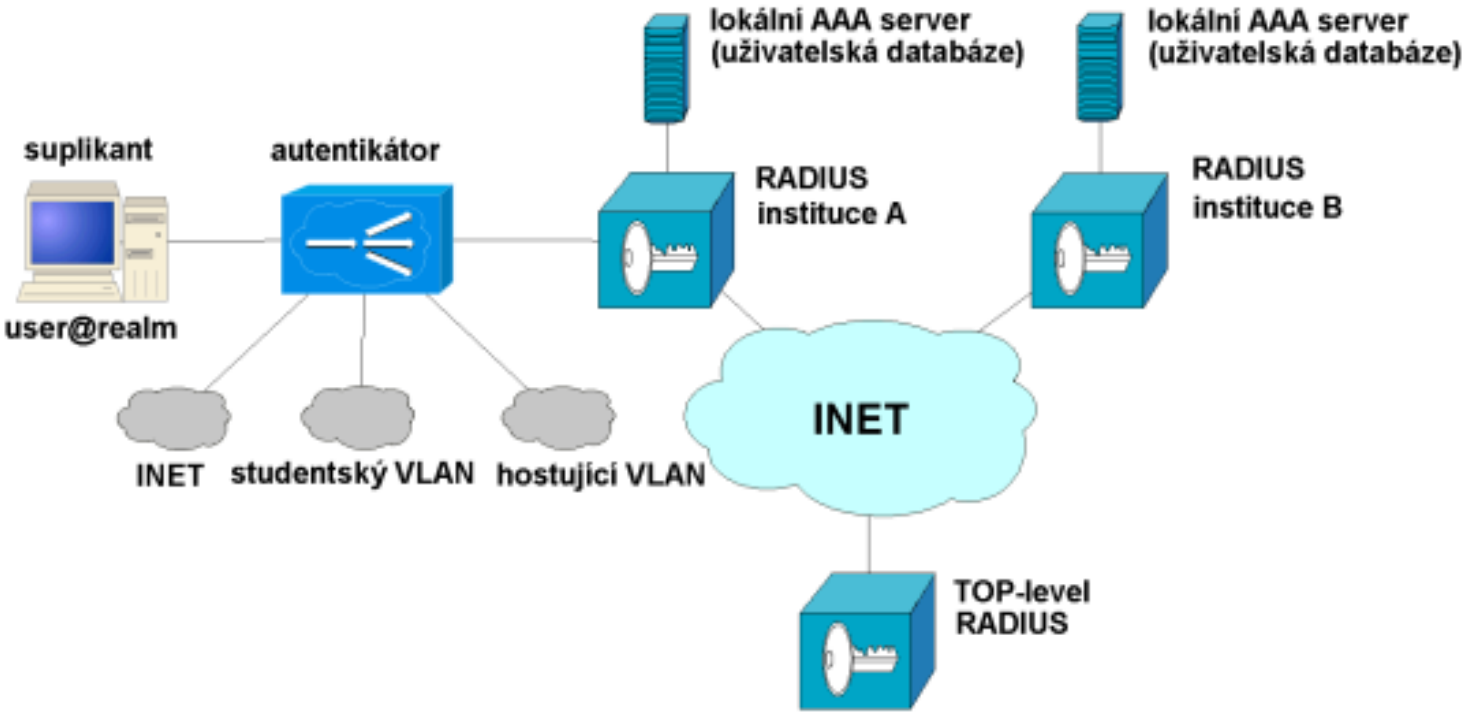
Autentizace, Autorizace, Accounting = RADIUS



ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

802.1x infrastruktura

na příkladu sítě Eduroam



http://www.eduroam.cz

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Stav na FELK v roce 2011

Nekoordinovaný decentralizovaný chaos

Do konce roku 2011 neexistovala jednoznačná koncepce rozvoje bezdrátové sítě.

- AP instalovány ad-hoc dle potřeb zaměstnanců jednotlivých pracovišť
- špatné zabezpečení (WEP/WPA, preshared-key na tabuli)
- množství vzájemně se rušících ESSID
- mezitím přežívají AP pro eduroam (Cisco AP1120, AP1245, RouterBOARD)
- nutnost každé AP konfigurovat a dohlížet jednotlivě
- s narůstajícím množstvím mobilních zařízení se začíná projevovat nedostatek IPv4 adres

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Stav na FELK v roce 2014

Jeden centrálně spravovaný systém bezdrátové sítě

Aktuálně nasazeno 31 CAP typu Aruba AP104, AP105 a AP205 v budově E a dvoji kontrolérů MC7210 v HA režimu. Konečný stav včetně druhé fáze v budově G bude zahrnovat $\approx$ 40 CAP. Aktuálně zbývají tři původní Cisco AP.

- máme dohled nad okamžitým stavem sítě i její historií.
- počet problémů hlášených uživateli klesl na minimum.
- kvalitní podpora IPv6 a hand-over klientů mezi AP.
- jsme schopni operativně reagovat na nárazové požadavky uživatelů a pracovišť (konference, hosté, DoD,...)
- práce se zjednodušila, systém „se o sebe stará sám“.
- snadno dokážeme odhalit a eliminovat pirátská AP.

Kdo jsou naši uživatelé…

studenti, zaměstnanci, návštěvníci

#GenMobile

Obsluhujeme velké množství uživatelů s různorodými požadavky na službu, kteří jsou vybaveni různými typy koncových zařízení. Na FELK se připojuje 300÷400 klientů každý den.

- v roce 2004 mělo méně než 10% studentů notebook
- v roce 2014 má 70% studentů více než jedno zařízení využívající WiFi (notebook, tablet, smartphone, ebook čtečku, wearable devices)

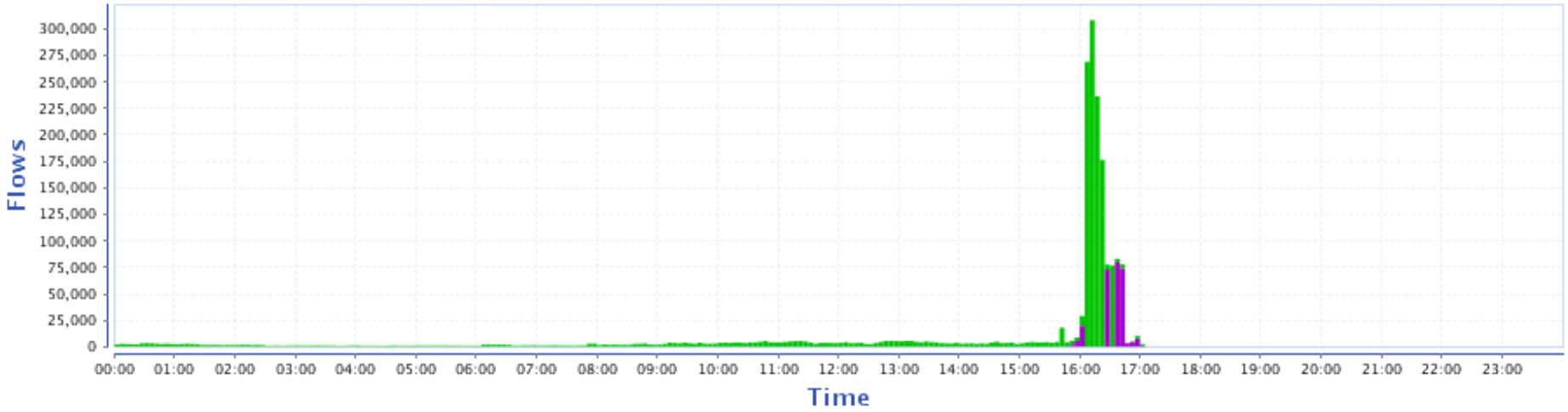
Samostatnou kategorií je experimentální elektronika jako jsou roboti, různé bezdrátové moduly, měřící přístroje ⇒ rozdílné často protichůdné požadavky na zabezpečení, propustnost, odezvu, pokrytí

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Bonus: včerejší DDoS

Nějaké pako dostalo nápad vyzkoušet si botnet

Včerejší (16:20-17:00) útok na náš SMTP relay server



- velikost útoku $\approx$ 200 *kpps*
- UDP pakety o velikosti 128 $\div$ 255 *B*
- různé IPv4 a porty na náhodné porty konkrétního stroje
- bypass pomocí blackhole routingu, hlavní provoz po IPv6

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Dotazy

?[1]

[1] Pokud není uvedeno jinak, tak uvedené ilustrace pochází z Wikipedie nebo FCC.